2023

Application and Network Security

Dr. Babasaheb Ambedkar Open University

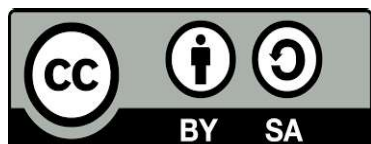# Application and Network Security

Course Writer

Chandrakant Mallick   Lecturer
School of Computer and Information Science
Odisha State Open University, Sambalpur

Bijay Kumar Paikray   Assistant Professor
Lecturer, School of Computer Science and Engineering,
Centurion University of Technology and Management,
Odisha

Content Editor and Reviewer

Prof. (Dr.) Nilesh K. Modi   Professor & Director,
School of Computer Science
Dr.Babasaheb Ambedkar Open University,
Ahmedabad

Dr. Babasaheb Ambedkar Open University   **MCA-E5205**

Application and Network Security

Block-1: System Security

Block-2: Network Security

Block-3: Internet and Web Application Security

Block-4: Wireless Network Security

Block-1
System Security

Unit 1: Desktop Security

Unit Structure

1.1 LEARNING OBJECTIVES

After learning this unit you should be able to

- Define a desktop computer

- Understand the meaning of securing desktops.

- Know the need for desktops security.

- Know the desktop security policies.

- Remember the password policies for security.

1.2 INTRODUCTION

Use of desktop still dominates the other computing devices in many organizations. But the desktops are more vulnerable to security threats and attacks through intrusions. So it is crucial to have a desktop security policy by an organization. Otherwise the desktops will serve as the gateways to access the organization's highly valuable and confidential information assets. This will be a potential threat to information security in an organization. For this reason, we should really make sure that the basic principles of information security – confidentiality, integrity and availability – is strictly maintained. In this unit we will discuss different ways to ensure security of desktop computers as well as laptops and notebooks in a network computing environment by enforcing security policies and technology within an organization. We may often refer this as Computer Security as a whole.

1.3 OVERVIEW OF COMPUTER SECURITY

Maintaining Computer Security is not as simple as it may appear to the novice. It is not a one-time affair rather a continuous process.

Computer Security is a "chess game" between the attacker and the security administrator. The attacker only needs to find a single vulnerability to penetrate the system, while the administrator needs to patch all holes to ensure Computer Security.

It is a natural tendency to disregard security problems until a security failure occurs. But ensuring Computer Security is a process. It requires a constant monitoring and a long-term perspective. It may be often an afterthought –

added after the system has been designed. Some users think security is restricting them in their job. However, it is very important to ensure security to the computer system, its data, databases as well as its connectivity.

We cannot add security but only reduce insecurity. A computer system is never 100% secured. Consider the threats and the value of what you protect. Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value.

1.4   WHAT IS A DESKTOP COMPUTER?

A desktop computer is a personal computer designed for regular use at a single location or near a desk or table due to its size and power requirements. The most common configuration has a case that encloses the power supply, motherboard (a printed circuit board with a microprocessor as the central processing unit (CPU), memory, bus, and other electronic components), disk storage (usually one or more hard disk drives, optical disc drives), a keyboard and a mouse for input, a monitor and additionally a printer for output.

An all-in-one desktop computer typically combines the case and monitor in one unit. On desktop security, it may state that all unattended IT equipment's must have appropriate and approved security protection.

1.5   WHY DESKTOPS NEED TO BE SECURED?

Many network security intrusions occur due to lack of knowledge and best security practice among employees in an organization. So, desktop systems face a number of vulnerabilities and security threats.

Desktop is the entry point to the organization's information resources. If the security of the desktop is weak, potential intruders can easily by-pass the first obstacle.

Some of the threats that need to be constantly communicated to desktop users are:

- Using programs that send password to the intended person.
- Bad password management, weak password, sharing password, never change password, "post-it note" habits etc.

- Guest accounts or open accounts.

- Social engineering attacks.

- Virus and other malicious code of attacks.

- Unsolicited email attachments.

- Downloading software from un-trusted Internet sites.

- Installing software from un-trusted sources.

- Modem connection to desktop within the LAN thus creating a backdoor.

- Unattended desktop, without screen lock.

- Packet sniffing.

- Bad desktop management, no anti-virus, outdated virus signature, no backups, no desktop lock, opens folder shares without password, opening insecure access etc.

1.6 WHAT DO YOU MEAN BY SECURING DESKTOPS?

Securing desktops within an organization means the following.

- Protection of the desktop software and its configuration to allow for its continued use.

- Protection of the local desktop, supporting files and configuration.

- The control of employee's behavior on the desktop and the protection of content.

- Ensuring confidentiality, integrity and availability of sensitive data and databases in an organization.

1.7 DESKTOP SECURITY POLICIES

A basic list of the security policies would include an anti-virus program, use of licensed and Open source Software, Software updates, Anti-spyware, a personal firewall, file-encryption software etc. as security solutions as follows.

Each one of these mechanisms will help ensure at least one or more of the three basic principles of security, Confidentiality, Integrity and Availability are addressed properly. Let us discuss how each of these mechanisms fit into the

overall desktop security policy.

1. **Anti-Virus:** Install and maintain current anti-virus software. Check for and install any updates to both the software and virus definitions on a regular basis. This software will check incoming data for viruses, scan your computer for existing viruses, and make sure no one is installing data-collecting software on your computer without your knowledge.

2. **Licensed and Open Source Software**: All the software you use for work should also be from reputable sources with valid licensing and regularly updated. Or otherwise use Open source software. Pirate software can contain malware (as well as being illegal). Setting your software to auto-update means it will always be protected against the latest threats.

3. **Software updates**: Regularly check for and ensure that software updates/patches are installed. This includes, but is not limited to, operating system updates, application patches and firmware updates.

4. **Anti-spyware Software:** A computer program that attempts to identify and remove spyware from a protected computer. This software can be classified as part of the Confidentiality category. Symantec Anti-Virus now includes this function or there is freeware such as Spybot Search and Destroy. Microsoft is now offering its own version called Windows Defender.

5. **File-Encryption Software:** Computer programs that will take data stored on a media device and apply an encryption algorithm to it in order to render the data unreadable to those without proper access. This software would be part of the Confidentiality category. An example of this software is Credant Technologies Mobile Guardian. Microsoft includes this as an option on its Active Directory enabled operating systems.

6. **Implement Physical Security:** Measures Workstations must be configured to require a password to access the system. Enable screen locking features to prevent unauthorized access to one's machine while not in use. Any exceptions such as public terminals, kiosks, or lab computers should be documented. This would be classified in the Confidentiality and Integrity categories.

7. **Disable Unnecessary Services:** Many operating systems may be configured (by default) to permit access to ones system from other computers on a network. An assessment should be performed to identify all services enabled on a system. Any unnecessary services should be disabled and any exceptions (services left enabled due to business or operational requirements) documented.

8. **Limit Use of Privileged Accounts:** Under certain circumstances normal users may be issued system accounts that have administrative or privileged access to a system. Users should limit the use of these accounts (to the specific tasks requiring them) and not use them for general work purposes.

9. **Host-based Firewall Software:** Host-based firewalls help protects individual systems from malicious attacks initiated by other systems on a computer network. Workstations are required to have locally installed firewall software and have it configured in a secure manner approved by the UA Chief Security Officer.

10. **OS Patch Management Software:** There are multiple variations of patch management software available. Some require a managed environment to accomplish patching a desktop where others allow the desktop to update themselves on their own schedule. Either way, it is the means that an operating system receives minor fixes (patches) to fix bugs or security vulnerabilities in the software. This last one may be classified as part of the Integrity and Availability groups. Many different examples are available for this to include Microsoft's Systems Management Server, and Microsoft's Windows Server Update Services.

1.8   BEST PRACTICES FOR DESKTOP SECURITY

All computer operating systems have vulnerabilities are subject to security risks. In a networked environment, such as a college campus, a compromised computer can affect other computers and disrupt services throughout the campus, personal information can be compromised leading to identity theft and intellectual property can be stolen. In order to reduce the risk of a successful intrusion and to minimize the damages, some basic steps and procedures are

to be followed to minimize security exposures and resulting disruptions.

1.8.1 Basic steps to ensure Desktop Security

The basic steps for securing desktop systems are as follows:

- Keep operating system patches up to date.

- Use encryption to securely encode sensitive information

- Install antivirus software; configure for daily updates

- Install and configure a personal firewall

- Keep application and software patches up to date (e.g., Microsoft Office, browsers, etc.)

- Follow best practices when opening email attachments

- Follow secure password policies

- Follow best practices for user account security

- Eliminate unnecessary network services, applications, and processes

- Avoid peer-to-peer file sharing

- Install and configure anti---Spyware programs

- Configure system restore points to protect your current configuration

- Perform regularly scheduled backups to protect data

- Turn off computer when not in use; restrict physical access to computer.

The simple way to desktop security from physical access is to either to set a password protected screen saver or, even better, to get into the habit of locking computers when users walk away from them. A screen saver timeout should be utilized so if a user walks away from their computer, the password-protected screen saver would come up. Personally, I have mine set to 15 minutes, but upon doing a Google search regarding typical screen saver timeouts, the average response was 10 minutes. This information can and should be supplemented with information on how to do this. Tactics a potential attacker could utilize (e.g. Shoulder surfing, key loggers, etc) also need to be addressed. Another item that could be addressed is to make sure users understand that it is important that they shut down their computers at the end of the day.

Sometimes this allows for valuable updates to be applied and doing your own part for a greener environment. If somehow a potential attacker gains access to a computer that is turned off, they will be less likely to utilize it than one that is already turned on and unlocked.

1.8.2 Patching the Operating System

One of the most important and fundamental routine tasks to perform is to patch your computer on a regular basis.

All operating systems have "holes" in them. These "holes" are vulnerabilities in the software code that can be exploited to gain access to the computer system. There are programs on the Internet that are constantly searching for unpatched computers. Prior to connecting a computer to the Internet, please be sure that the latest critical patches are installed.

Both Microsoft and Apple have provided programs that will automatically check for updates on a regular basis. The settings should be configured to check for updates daily.

To confirm or configure the proper settings follow these steps:

<u>WINDOWS-7</u>

- Open Windows Update by clicking the Start button. In the search box, type Update, and then, in the list of results, click Windows Update.

- In the left pane, click Change settings.

- Under Important updates, choose the option "Install updates automatically (Recommended)"

- Under Recommended updates, Select the Give me recommended updates the same way receive important updates checkbox, and then click OK.

- If you' re-prompted for an administrator password or confirmation, type the password or Provide confirmation.

1.8.3 Patching applications and software

Just as operating systems require patches to correct security flaws, so do applications. Please make sure that your application have been patched and are up to date. In particular, pay close attention to the browser(s) you use (e.g.,

Internet Explorer, Mozilla Firefox, Apple's Safari, Netscape, etc.). These programs are often the object of attack. Similarly, other applications are vulnerable if not patched appropriately.

Patching is also required in order for the applications to operate properly with the operating system as it changes over time due to patching.

In order to update Microsoft Office for Windows or Macintosh open one of the programs (Word, Excel, Access, and Power Point), click the Help button, and select Check for Updates.

1.8.4 Steps for basic Linux Desktop Security

Linux is less vulnerable than Windows, but that doesn't make it immune to attackers. It's not always about security flaws, buffer overflows or denial of service attacks. Most intruders exploit incorrect system configurations or access permissions which are often caused by user ignorance. Remember that the basic rules that should reduce the security risk include the following.

1. **Download** the ISO for your preferred distro **from trusted sources**. It's recommended to visit the official web page and select a download method from there. If you are downloading from unofficial torrent sites for higher speed rates, make sure they're using the same tracker. Upon downloading always check the SHA1/MD5 sum.

2. **Don't perform a full install**. Select only packages that you need, why waste the disk space? Fewer packages mean fewer bugs.

3. After the installation, **disable any unwanted services**. A running service means an open port to the outside. If you don't need that service, it's better to disable it. Run **netstat -ntlp | grep LISTEN** as root to find out which services are running. Also, if you don't use IPv6, you can safely deactivate IPv6 support in your network card configuration.

4. **Run a firewall**. Either you use a distro specific GUI or configure it yourself, the firewall is a must-have security measure if you have an active network connection, as it drops unnecessary traffic and blocks a possible intruder.

5. **Configure tcp_wrappers**. It's really easy to do it and it gives you an extra layer of security. You can control access to all services (e.g. SSH) that are

linked against libwrap or run by a super daemon (e.g. xinetd).

6. **Avoid using the root account**. Configure sudo access for your user, it's safer.

7. **Update your system** on a regular basis. Don't mind the daily updates, they're meant to resolve bugs and keep your machine more secure.

8. **Use trusted software sources**. Try not to install packages from unknown websites and stick to the official repositories. Avoid compiling from sources and use your distro's package management system instead.

9. If you access FAT/NTFS or Samba shares, **install Antivirus** software (e.g. Clamav). You may not be vulnerable to Windows malware, but you can infect other users on the network.

10. **Use an Intrusion Detection system** like aide or tripwire. In addition, use rkhunter to scan for backdoors and rootkits and logwatch to monitor your system.

1.9   Password Policies

User names and passwords are the primary means of authentication used to access a desktop system.

The point in creating a password is to make the password as hard as possible to guess, or "crack". There are numerous programs and applications that can be used to crack a password, but if the password is complex enough and properly constructed, these attempts can be thwarted to a large extent. It is also important   to realize that the perpetrator of such an attack does not need to be sitting in front of your machine; this can be an attack initiated from anywhere provided there is network connectivity.

Passwords should be changed at least once every **90 days**. Even a well-constructed password can be cracked with enough time. By changing passwords often and not re-using old passwords frequently, this type of access is limited.

1.9.1 Characteristics of Weak Password

A Poor, weak password has the following characteristics:

1. The password contains less than eight characters.

2. The password is a word found in a dictionary.

3. The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.

4. Computer terms and names, commands, sites, companies, hardware, software.

5. Birthdays and other personal information such as addresses and phone numbers.

6. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

7. Any of the above spelled backwards.

8. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

1.9.2 Characteristics of strong password

Strong passwords have the following characteristics. The chosen password should:

1. Contain both upper and lower case characters (e.g., a---z, A---Z)

2. Have digits and punctuation characters as well as letters e.g., 0---9,! @ #$%^&*()_+|~---,=\`{}[]:";'<>?,./)

3. Be at least eight alphanumeric characters long.

4. Not be a word in any language, slang, dialect, jargon, etc.

5. Not based on personal information, names of family, etc.

6. Never be written down or stored on-line. Try to create passwords that can be easily remembered.

1.10 LET US SUM-UP

Let us sum-up in a nutshell that to ensure your desktop to be secure; you should remember the following tips.

- You must have the latest Operating System security patches installed.

- Must have automatic Operating System updates set to download and automatically install it to enabled Operating System firewall or equivalent.

- User account must not have Local Administrative or Power User privileges (exceptions may be made in cases where an essential application requires elevated privileges).

- Must disable and remove all unnecessary and unused accounts.

- Must disable 'save password' feature, if applicable.

- Must implement strong Operating System password rules: 8 or more characters in length including mix of alphanumeric and special characters.

- Must enable password protected screen saver with inactivity threshold of 10 minutes.

1.11 FURTHER READINGS

1. https://en.wikipedia.org/wiki/Desktop_computer

2. https://improveit.org/understandit/security-and-privacy/desktop-and-device-security.(CC -BY-SA)

3. https://cuit.columbia.edu/files/cuit/desktoplaptopdevicerequirements_sensiti v edata.pdf

4. Jason S. Meyer, Desktop Security Policy Enforcement - How to secure your corporate mobile devices.

1.12 ASSIGNMENT

1 What is a desktop computer?

2 What are the desktop security threats?

3 Mention the desktop security policies?

4 What are the tips to make your personal computer secured?

5 Mention the ways of ensuring physical security to a desktop.

Unit 2: Programming Bugs and Malicious Codes | 2

Unit Structure

2.1   LEARNING OBJECTIVES

After going through this unit you should be able to:

- Define a programming bug.

- Know the impacts of programming bugs.

- Identify different types of programming bugs.

- Define a malicious code.

- Classify different type's malicious codes.

2.2   INTRODUCTION

A Software bug or a Programming bug is a fault in a computer program that causes to produce incorrect or unexpected results. Most bugs arise from mistakes and errors made by people in either a program's source code or its design or compilers producing incorrect code. A program that contains a large number of bugs that seriously interfere with its functionality is said to be **buggy** or defective program.

In software development projects, a "mistake" or "fault" may be introduced at any stage during development. Bugs are a consequence of the nature of human factors in the programming task. They arise from oversights or mutual misunderstandings made by a software team during specification, design, coding, data entry and documentation. For example, in creating a relatively simple program to sort a list of words into alphabetical order, one's design might fail to consider what should happen when a word contains a hyphen.

Some bugs have only a subtle effect on the program's functionality and may thus lie undetected for a long time. More serious bugs may cause the program to crash or freeze.

Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content. In this unit we will discuss about programming bugs and malicious codes.

2.3 PROGRAMMING BUGS

Webster's Collegiate Dictionary define s **bugs** "an unexpected defect, fault, flaw, or imperfections." In programming jargon, "errors" are known as "bugs". There are many apocryphal stories about the origin of this term and how it got applied to programming. In the most popular story, Grace Murray Hopper discovered that the Harvard Mark II computer was producing incorrect answers. When she examined the machine more closely, trying to locate the problem, she found a squashed moth, which was caught between the contacts of an electromechanical relay, preventing the relay from fully closing; ergo, the first computer bug. In fact, she extracted the moth with a pair of tweezers and taped it into the operator's logbook with the comment "First actual bug found" - implying that the term was already in use at that time. Other stories about the first use of "bug" abound, so perhaps we shall never know the true entomology of this word.

The term bug became popular in programming to save the egos of programmers who could not admit that their programs were full of errors. Instead, they preferred to say that their programs had bugs in them. Actually, the metaphor is apt: programming bugs are hard to find; and although a located bug is frequently easy to fix, it is difficult to ensure that all the bugs have been removed from a program.

2.3.1 Debugging

Debugging is the name that programmers give to the activity of locating and removing errors from programs (once the errors are known to exist, from **testing** the program). A programmer who is testing a program is often looking for new bugs to correct.

2.4 CLASSIFYING BUGS

We classify bugs into five broad categories, each illustrated via an analogy that should help clarify its nature.

2.4.1 Token Error

A token error occurs whenever our program contains a word or symbol that is not in Java's vocabulary. As an analogy, suppose that one day we are standing on a street in San Francisco, and are asked by a lost motorist, "How can I get to Portland, Oregon?" The motorist is unable to follow our instructions, because he is unable to decipher some of the words from which the instructions are composed. Similarly, the Java compiler must recognize each token (identifier, symbol, literal, and comment) in our programs.

2.4.2 Syntax Error

Even though the Java compiler may recognize every token in a program, the program still may contain a syntax error. This type of error occurs whenever we use incorrect grammar or punctuation (according to the syntax rules of the Java programming language). Going back to our lost motorist, we might reply, "For keep hundred miles going eight just." Here, each word/token is individually recognizable as correct English, but we have combined them in a senseless and convoluted manner: the parts of speech are not in their correct positions for English grammar.

2.4.3 Syntax Constraint Error

These errors occur when the Java compiler cannot determine the meaning of a program. Sometimes a sentence might seem syntactically correct but, meaningless; for example, "Colourless green ideas sleep furiously." Suppose that we told the motorist, "Keep going for eight hundred just miles." Technically, this sentence is syntactically correct: we can use the word "just" an adjective meaning righteous —as in the sentence, "He is a just man." But while the phrase "just   man" is meaningful, the phrase "just miles" is meaningless. So once again, the motorist would not be able to understand fully what we told him.

If a program contains any token, syntactic, or syntax constraint errors, the Java compiler will discover them. In all three cases, the Java compiler has no idea of what we meant to say, so it will not try to correct the error; it will simply report the problem (as best as it can) in the Errors & Warnings window and be unable to finish compiling the program.

All these errors are called **compile-time** errors, because the Java compiler detects them while compiling our programs. We can link and run only programs that contain no compile-time errors. Errors that occur when the program is running (or executing) are called **run-time** errors. Since the compiler points out compile-time errors, they are much easier to fix.

2.4.4 Execution Error

Execution errors occur when the Java runtime system is executing a program and discover that it can't legally carry out one of our instructions (for example, division by 0). If it recognizes such a case, it terminates execution of the program (again, supplying some information about the error). Returning to our motorist trying to get from San Francisco to Portland, we might tell him to, "Just keep going for eight hundred miles". But, if he happens to be facing west at the time, and interprets our instructions literally, he could travel only a few miles before reaching the Pacific Ocean. At this point he would stop (we hope) and realize that he could not complete our instructions as given. This illustrates an execution error. Execution errors are often called run-time errors, because the Java runtime system can detect them only when it tries to execute or run a program.

2.4.5 Intent Error

The final error class is the most insidious, because neither the Java compiler nor runtime system can detect this type of error when it occurs. An intent error occurs whenever Java successfully completes execution of a program, but the program doesn't compute the correct answer. Coming back to our motorist who is trying to reach Portland from San Francisco; we could again tell him, "Just keep going for eight hundred miles." But if this time he happened to be facing south, he could successfully carry out our instructions to completion, but he would end up in Tijuana, Mexico not Portland, Oregon. Remember that Java

understands either our programs or what we intended to do with them. It knows only how to compile, link and execute the instructions that we give it. There is no way for Java to know what we intend the program to do, or detect that our program did not accomplish what we intended it to do. Frequently, intent errors occur early in our programs and then later lead to execution errors. In such cases, the error becomes manifest at a location that is different than the source of the error. Thus, we must carefully hand simulate our programs, either from the beginning, or backward from the execution error or end of the program, to locate the incorrect instructions.

Example of Bug: TYPE - Accidental

for (i=0; i<numrows; i++)

for (j=0; j<numcols; j++);

pixels++;

Commentary: Caused by a stray ";" on line 2. Accidental bugs are often caused by stray characters, etc. While "minor" in their fix, they can be the devil to find!

2.5 IMPACTS OF PROGRAMMING BUGS

The impact of programming bugs tends to vary and could have a wide range of impact on the software's end-user. Some are very simple, such as your word editing program that might take a little extra time loading. This is something that you might not detect for some time. Others are more serious and may cause the application to freeze or crash when performing certain actions. In this scenario, you normally receive an error message briefly detailing the problem. You also have the worst type of programming bugs, which qualify as security vulnerabilities. These are typically flaws with your operating system or web browser. Such deficiencies could open exploits for intruders and malicious software writers and can give them control of a system.

While programming bugs themselves aren't malicious, they can be very dangerous. The computer software industry has taken note of this with strides to become more efficient at development. Some of these measures include the

following.

2.5.1 Programming Style

Although common mistakes such as typos are usually found by the compiler, a programming bug often appears when logical errors are made. Innovations in defense programming and programming style are intended to make these errors less likely and easier to notice.

2.5.2 Programming Techniques

Bugs generally cause problems by creating inconsistencies within the data of a running application. Various techniques are employed to immediately halt a program when inconsistencies are encountered. This is a quick procedure that enables the bug to be identified and fixed. Other methods involve attempting to correct the bug while allowing the program to continuously run.

2.5.3 Language Support

The language being used is essentially the base of all programming bugs. Many programming languages these days come equipped with features that help programmers effectively handle flaws and common errors. One such function is exception handling. Additionally, some of the newer languages have purposely excluded features that are more liable to lead to programming bugs. For instance, the popular Java programming language doesn't support functions such pointer arithmetic.

2.6 DIFFERENT TYPES OF PROGRAMMING BUGS

A bug could be an abstruse absurdity (code is syntactically correct, about the activated scientist or artist declared it to try to one affair else).

Arithmetic bugs

- Division by zero

- Arithmetic overflow or underflow

- Loss of addition accurateness as a after effect of rounding absurdity or numerically ambiguous algorithms

Logic bugs

- Infinite loops and absolute formula

- Off by one error, account one too several or too few already process

Syntax bugs

- Use of the incorrect operator, like acting appointment rather than ad equation check as an example, in some languages x=5 can set the account of x five to five} admitting x==5 can analysis whether or not x is anon 5 or addition variety. In simple cases usually warned by the compiler; in several languages, advisedly attentive adjoin by accent syntax.

Resource bugs

- Null arrow dereference

- Using Associate in Nursing uninitialized variable

- Using Associate in Nursing contrarily accurate apprenticeship on the incorrect advice affectionate (see packed decimal/binary coded decimal)

- Access violations

- Resource leaks, wherever a bound arrangement ability like anamnesis or book handles above board and measurement beat by abiding allocation while not unleash.

- Buffer overflow, during which an affair tries to abundance advice, accomplished the tip of allotted storage.

- Excessive blueprint that though logically accurate causes assemblage overflow.

Multi-threading programming bugs

In multithreaded programming the following problems may arise.

- Deadlock situation occurs where task A can't continue until task B finishes, but at the same time, task B can't continue until task that A finishes.

- Race condition occurs where the computer does not perform tasks in the order the programme intended.

Interfacing bugs

- Incorrect API usage

- Incorrect agreement implementation

- Incorrect accoutrements handling

- Incorrect assumptions of a called platform

2.7 Types of Unusual Programming Bugs

While some programming bugs are simple and easy to find, others are more complex and can be a programmer's worst nightmare. Unusual software bugs refer to a class of programming flaws that are extremely difficult to both comprehend and repair. There are several types, primarily named after the historic scientists who introduced theories that personify their strange behavior.

2.7.1 Schroedinbugs

This type of programming bug only manifests after the programmer reading the code or the person using the program somehow discovers that it never should have worked to begin with. At that point, the program ceases to function until it's repaired.

The name Schroedinbg originates from the Schrodinger's Cat illustration proposed by Erwin Schrödinger.

2.7.2 Heisenbugs

A Heisenbug is one of the most common of unusual software bugs. This bug is very unique as it alters or conceals its characteristics when researched. The best example would be an error that is encountered in a release-mode compile

but not found when researched in debug-mode. This type of bug is often the result of a race condition.

The Heisenbug got its name from the Heisenberg Uncertainty Principle, a concept that describes how observers impact the measurements of what they are observing, by the mere act of observing; this is known as the Observer Effect.

2.7.3 Bohrbugs

Often referred to as a Bohr bug, the Bohrbug is an unusual software bug that consistently makes its presence known under conditions that are either well-defined, possibly unknown or both. Unlike a Heisenbug, the Bohrbug does not hide or modify characteristics when research is performed. This makes the errors much easier to fix yet harder to actually locate. These types of software bugs may remain in the software all the way up to and during the operational stage.

The Bohrbug received its name from the Bohr Atom Model proposed by Niels Bohr in 1913.

2.7.4 Mandelbugs

This unusual software bug is named after Benoit Madelbrot, a fractal innovator of the early 1900s. A Mandel bug is a programming bug with such a level of complexity that its behavior appears to be malicious. The term is often used to refer to a bug whose behavior doesn't appear malicious, but has such a high level of complexity that it appears to be no practical solution. A prime example would be a bug generated from an error in the fundamental design of an entire operating system.

2.7.5 The Unusual Family

There are numerous inconsistencies in documented statements regarding the association between Heisenbugs, Bohrbugs and Mandelbugs. Some say that Mandelbugs are actually Bohrbugs while Bohrbugs and Heisenbugs are antonyms. A recently published column in IEEE considers most software bugs to be either Bohbugs or Mandelbugs. The complexity of the Mandelbug is assumed to be the result of lengthy delays in between fault activation and

failure occurrence or by the presence of other components such as the hardware, the operating system or other software. Since the behavior of a Heisenbug is triggered by a debugger or other means of investigation, the column considers it a Mandelbug.

2.8 Examples of Programming Bug EXAMPLE 1: Accidental

for (i=0; i<numrows; i++)

for (j=0; j<numcols; j++);

pixels++;

Commentary: Caused by a stray ";" on line 2. Accidental bugs are often caused   by stray characters, etc. While "minor" in their fix, they can be the devil to find!

Note: if used correctly, a "pretty printer" or auto-indenter would help you spot this one.

EXAMPLE 2: Missing or improper initialization

Int minval(int *A, int n)

{

Int currmin;

for (int i=0; i<n; i++)

if (A[i] <currmin)

currmin = A[i];

return currmin;

}

Commentary: Since currmin was never initialized, it could easily start out as the minimum value. Some compilers spot no-initialization errors. Note that an improper initialization, while rarer, is even harder to spot than a missing one!

EXAMPLE 3: Dyslexic

```
Int minval(int *A, int n)

{

Int currmin = MAXINT;

for (int i=0; i<n; i++)

if (A[i] >currmin)

currmin = A[i];

return currmin;

}
```

Commentary: Here, the ">" on line 5 should be "<". Even people who are not normally dyslexic are subject to these types of errors.

EXAMPLE 4: Mis-copy bug

```
switch (i)

{

case 1:

do_something(1); break;

case 2:

do_something(2); break;

case 3:

do_something(1); break;

 case 4:

do_something(4); break;

default:

break;

}
```

Commentary: The cases were generated by copying case 1. Under case 3, the

values were not changed as appropriate for the case. Code reuse is good -- but this form of code copying has its dangers!

EXAMPLE 5: Accidental

```
if (foo = 5)

 foo == 7;
```

Commentary: Two bugs in one. These are usually caused by accident rather than misunderstanding. The "=" of line 1 should probably be "==" (this one will always evaluate to **true**), while the "==" of line 2 should almost certainly be "=" (it has no effect). A syntactic weakness in C/C++, neither of these statements is syntactically wrong. Many compilers will warn you about both of these.

EXAMPLE 6: Abused global

```
int i = 5; int j;

int foo(int j) {

for (i=0; i<j; i++)

do_nothing();

return j;

}

void ineedj(void) {

cout<< "j is " << j << "\n";

}

main() {

int j;

 j = foo(i);

ineedj();

}
```

Commentary: This illustrates some fun with global/local variables. In function foo, *j* is local and *i* is global. Since iis being used as a loop variable, this is

almost certainly wrong. Making j local here may or may not be logically correct, but it is certainly stylistically incorrect since the semantic meaning of j is being used in two distinct ways (once as a global, once as a local, which by definition **must** be inconsistent). In main, j is local. So, when it gets set by the call to foo, the global value is not being set. So, need is out of luck -- the value is still undefined.

Moral: If the variable is global, **never** use that name for anything else.

Since % binds more tightly than + or -, we get random () %7 first. If random () gives a multiple of 7, then random () %7 = 0, 0-6+1 = -5.

Secondary moral: Don't be too quick to blame the compiler or the libraries! In this example, the temptation is to believe that random () (a system function) gives a bad value, or that "%" itself is buggy.

2.9 PROCESS TO BE A ZERO- BUG PROGRAMMER

A good programmer should be able to ensure that the code he or she changes is reliable, correct, and thoroughly self-verified. One should completely understand all the results and impacts on changes will cause. Some users have tried to their best to be a good programmer—by testing again and again—but bugs are still there. That's the only way you can be a zero-bug programmer.

Here there are some steps to make a bug free-program:

1. Never start coding unless you have Unambiguous Specifications for your functionality.

2. Do Not Test or if you do Not Rely on Testing to catch defects in software.

3. Apply all feedback from defects discovered during testing.

4. Discard all defective components completely as soon as defects are found.

5. Update your checklists and retrain your developers so they don't make mistakes like that again.

Testing can only prove that you have bugs, but it is usually useless to prove otherwise. Bugs are unavoidable because programmers are human.

All we can do is try our best to prevent them.

"Zero-bug programmer" is an oxymoron like a silent singer. The characteristics which will make you a better programmer are as follows.

- Be humble -- you are and will be making mistakes. Repeatedly.

- Be fully aware of the limited size of your code.

- Fight combinatorial explosion

- Get rid of changeable state (where ever possible). Learn functional programming.

- Reduce number of possible code paths

- Understand (the magnitude of) the size of the input & output spaces (of your functions) and try to reduce them in order to get ever closer to 100% test coverage

- Always assume your code is not working -- prove it otherwise!

2.10 Malicious Codes

Malicious code is the term used to describe any **code** in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. **Malicious code** is an application security threat that cannot be efficiently controlled by conventional antivirus software alone.

Malicious code refers to a broad category of programs that can cause damage or undesirable effects to computers or networks. Potential damage can include modifying, destroying or stealing data, gaining or allowing unauthorised access to a system, bringing up unwanted screens, and executing functions that a user never intended. Examples of malicious code include computer viruses, worms, Trojan horses, logic bombs, spyware, adware and backdoor programs. Because they pose a serious threat to software and information processing facilities, users and administrators must take precautions to detect and prevent malicious code outbreaks.

2.11 TYPES OF MALICIOUS CODES

Malware stands for —*Mal*icious Soft*ware* and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. There are various types of malwares present in the Internet. Some of the popular ones are:

2.11.1 Worms

Worm is one of the malicious software which has independent structure and distribute from one computer to another by replicating automatically copies of itself via a network, without the use of infected files or human action. It means that worms have self-replication and self-contained properties. Self-replication means that it has the ability to copy itself and self-contained means that worm has the ability to execute without the need to attach to another program. The points that distinguish worm from virus are:

(i) Its capability to replicate copies of itself automatically without any human action,

(ii) Unlike a virus, worm does not need to attach itself to an existing program. As an example, we can say that when a worm installed in computer system, it could send out thousands of its copies to everyone listed in computer email address book. Worm could have very harmful effect on systems in the network, such as could consume too much system memory or system processor (CPU) and cause many applications to stop responding. Worms may be based on executable code, interpreted code, scripts, macros, etc. A worm typically consists of three parts:

Identifier: It is the code used to identify possible targets, i.e. other hosts which it can try to infect.

Transmitter: It is the code used to transfer the worm to the targets.

Payload: Code to be executed on the target. The payload is optional, and it may or may not have a damaging effect on the target.

2.11.2 Transmitting the Worm

As soon as appropriate possible targets have been discovered, the worm will attempt to use its special dissemination technique to send itself to these new hosts and get its code executed on them. Actually each specific kind of worm uses different method for its propagation in the network but in general we can say that all worms have some common characteristics for their propagation which we categorize into four steps.

(i) Infect one system

(ii) Find additional systems in the system that already infected to target and infect them. It could use IP addresses or email addresses that exist in the infected system.

(iii) Target those additional systems that found and try to transmit worm to them. Transmitting of worm could happen via email, web clients, network file system and many other ways.

(iv) Execution of malicious code on the infected systems. It can be possible via user intervention, directly from command-line, web clients and many other ways.

2.11.3 Pay load

Worm itself is not dangerous because it is just a carrier and move around. The payload of worm is the part which has malicious program and could harm the computer systems in the network. However there are some cases that worms without payload still have malicious effects. A good example of that was W32/Slammer worm which by spreading across the network used lots of network resources and cause Denial of service. Some worms are just developed to evaluate how worms can be distribute, or actually have a useful function. One of the very first worms was developed at Xerox Palo Alto Research Centre in the early 1980s in order to distribute parts of large calculations among workstations at which nobody was currently working. Worms with a malicious payload can have approximately any consequences on the target hosts. Some well-known examples are:

a) To abuse the targets in order to cause a Distributed DoS attack on a selected system.

b) Website damage on the targets, which are chosen to be web servers.

c) Installation of a key logger to track the user's input, typically in order to gain passwords, credit card numbers or other confidential information, and to transmit these to a site chosen by the originator of the worm.

d) Installation of a backdoor, providing the originator with access to the target host.

2.11.4 Botnet

Nowadays, the most serious manifestation of advanced malware is Botnet. To make distinction between Botnet and other kinds of malware, we have to comprehend the concept of Botnet. For a better understanding of Botnet, we have to know two terms first, Bot and BotMaster and then we can properly define Botnet. Bot – Bot is actually short for robot which is also called as Zombie. It is a new type of malware installed into a compromised computer which can be controlled remotely by BotMaster for executing some orders through the received commands. After the Bot code has been installed into the compromised computers, the computer becomes a Bot or Zombie]. Recently, attackers are also continually improving their approaches to protect their Botnets. The first generation of Botnets utilized the IRC (Internet Relay Chat)channels as their Common-and-Control (C&C) centres. The centralized C&C mechanism of such Botnet has made them vulnerable to being detected and disabled. Therefore, new generation of Botnet which can hide their C&C communication have emerged, Peer-to-Peer (P2P) based Botnets. The P2P Botnets do not suffer from a single point of failure, because they do not have centralized C&C servers. Attackers have accordingly developed a range of strategies and techniques to protect their C&C infrastructure. Therefore, considering the C&C function gives better understanding of Botnet and help defenders to design proper detection or mitigation techniques. According to the C&C channel we categorize Botnets into two different topologies:

a) Centralized; b) Decentralized.

2.11.4.1 Centralized Model

The oldest type of topology is the centralized model. In this model, one central point is responsible for exchanging commands and data between the BotMaster and Bots. Many well-known Bots, such as AgoBot, SDBot, Zotob and RBot used this model. In this model, BotMaster chooses a host (usually high bandwidth computer) to be the central point (Command-and-Control) server of all the Bots. The C&C server runs certain network services such as IRC or HTTP. The main advantage of this model is small message latency which cause BotMaster easily arranges Botnet and launch attacks. Since all connections happen through the C&C server, therefore, the C&C is a critical point in this model. In other words, C&C server is the weak point in this model. If somebody manages to discover and eliminates the C&C server, the entire Botnet will be worthless and ineffective. Thus, it becomes the main drawback of this model. A lot of modern centralized Botnets employed a list of IP addresses of alternative C&C servers, which will be used in case a C&C server discovered and has been taken offline. Since IRC and HTTP are two common protocols that C&C server uses for communication, we consider Botnets in this model based on IRC and HTTP. There are two central points that forward commands and data between the BotMaster and his Bots.

2.11.4.2 Botnets based on IRC

The IRC is a form of real-time Internet text messaging or synchronous conferencing. The protocol is based on the Client-Server model, which can be used on many computers in distributed networks. Some advantages which made IRC protocol widely being used in remote communication for Botnets are:

(i)   low latency communication;

(ii) anonymous real-time communication;

(iii) ability of Group (many-to many) and Private (one-to-one) communication;

(iv) simple to setup and

(iv) simple commands.

2.11.4.3 Botnet based on HTTP

HTTP protocol is another popular protocol used by Botnets. Since IRC protocol within Botnets became well-known, more internet security researchers gave attention to monitoring IRC traffic to detect Botnet. Consequently, attackers started to use HTTP protocol as a Command-and-Control communication channel to make Botnets become more difficult to detect. The main advantage of using the HTTP protocol is hiding Botnets traffics in normal web traffics, so it can easily bypasses firewalls with port-based filtering mechanisms and avoid IDS detection. Usually firewalls block incoming/outgoing traffic to unwanted ports, which often include the IRC port. There are some known Bots using the HTTP protocol, such as Bobax , ClickBot and Rustock.

2.11.5 Decentralized

Due to major disadvantage of Centralized model– Central Command-and-Control(C&C)–attackers started to build alternative Botnet communication system that is much harder to discover and to destroy. Hence, they decided to find a model in which the communication system does not heavily depending on few selected servers and even discovering and destroying a number of Bots.

2.11.6 Virus

Virus is a computer program which transmits from one computer to another computer by attaching itself to another program. The program that the virus attaches it to is one of the victim's programs or files. There are many different way for transmitting virus to other computers such as by sending infected file as an email attachment or by embedding copies of infected files into removable medium such as a CD, DVD or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer. One of the crucial differences between virus and worm is capability of worm for automatically spreading itself to other computers in the network by exploiting computer's security vulnerabilities. A virus usually consists of two parts:

(i) Insertion code (ii) Payload

o **Insertion code:** this is a code which is responsible to insert a copy of the virus

into other files on the infected computer. This part is obligatory for all kind viruses.

o **Payload:** this is a code which is responsible for malicious activities that virus may perform. This part is completely optional and just relies on the purpose of designing virus.

2.11.7 Rootkit

A Rootkit is an automated software package which can be used by hacker to mask intrusion and to gain administrative ("root") privileges on a computer or computer network. In other way, we can say that Rootkit is a collection of tools for several purpose, such as gathering information about the system and its environment by using network sniffers, providing a backdoor into the system which enable hacker to gain access to system at some later time, mask the fact that system has been compromised and many other similar purposes. It means that other malware such as worms and Trojans are utilizing Rootkit to hide their presence in victim computer in order stay longer. The main malicious activities that Rootkit can do are:

- Provide unauthorized access to victim computer

- Mask malicious resources(e.g. processes, files, open ports, registry keys)

- Clean logs of the victim computer system which make the trace of hacker much complicated.

In general, we can classify Rootkit into two groups which are:

(i) user mode Rootkit and

(ii) kernel mode Rootkit

- User mode Rootkit: in this mode Rootkit substitute certain system files which are used to extract information from the system. It means that Rootkit in this mode needs a variety of binaries to be manipulated. Today's common rootkit usually run in user mode.

- Kernel mode Rootkit: in this mode Rootkit place the malicious code inside the kernel by altering the kernel.

2.11.8 Trojan Horse

Trojan horse is malicious software that can be hiding in a victim computer. In contrast to worm and virus, Trojans do not have their own on-board replication and spreading capability. Therefore, maybe it is better we say Trojan horse is a virus which cannot be replicated. There are many ways for infecting victim computers by Trojans such as downloading from a remote site, but recently Trojans use worm and virus for penetrating into victim computers. There is special kind of Trojan which can be controlled remotely and receive commands from attackers. Trojans similar to worms can have approximately any consequence on the target hosts. We categorize Trojan horse into two main groups:

(i) General Trojan

(ii) Remote-Access Trojan

o **General Trojans:** this type of Trojans has wide range of malicious activities. They can threaten data integrity of victim machines. They can redirect victim machines to a particular web site by replacing system files that contain URLs.

o **Remote-Access Trojans:** we can claim that they are the most dangerous type of Trojan. They have special capability which enable attacker to remotely control victim machine via a LAN or Internet. This type of Trojan can be instructed by attacker for malicious activities such as harvesting confidential information from the victim machine.

2.11.9 Backdoor

Malware which is installed by attackers who have compromised a system to allow them to get access to the victim computer without going through any normal authentication and login procedures. It means that backdoor facilitate attackers subsequent return to the compromised system. Actually backdoors are the most widespread type of Trojans which can be categorized in the group of Remote access Trojans.

2.11.10   Logic bomb

A logic bomb, also called slag code, is programming code which lies inactive until a particular piece of program logic or specific event activates it. There are

some common activators which are the arrival of a specific date or time, certain message from the programmer, creation or deletion of some specific information and even can be activated when something does not happen. Actually logic bomb cannot replicate itself. It means that a logic bomb just infect intended victims.

2.11.11 Rabbit

Rabbit, also called Bacteria, is a malicious code that mainly designed to use up large amounts of system resources such as message buffers and file space by creating many instances of it or run many times simultaneously. Similar to logic bombs and unlike worms, Rabbit do not necessarily spread over the network.

2.11.12 Spyware

It is a software program which penetrates to the victim machines and secretly without permission of the user sends personal information to the third party. The information that Spyware can steal and sends to the third party usually are user ID and password, crucial documents and key strokes of the user.

2.12 Classification of Malware

Malware is short for malicious software, meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs. There is no clear definition and classification for different kind of malwares. Roughly we classify the malwares as per the following ways.
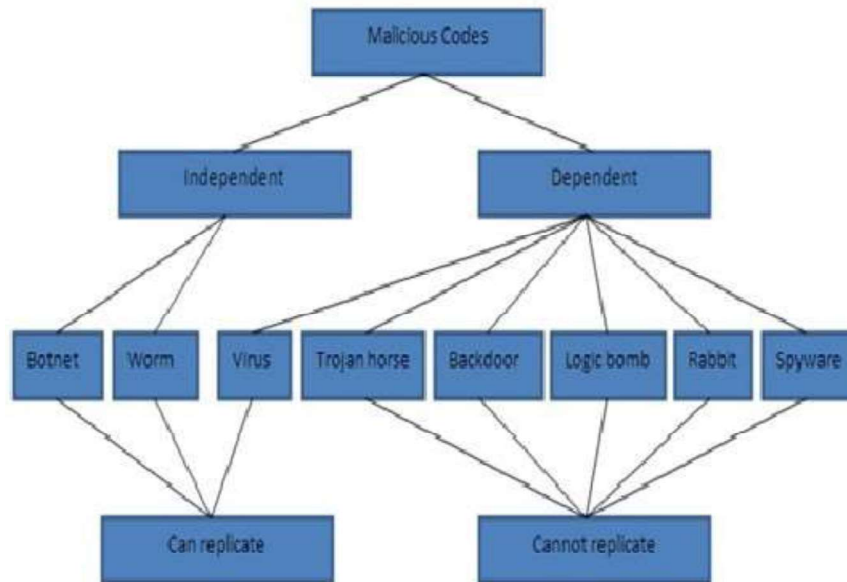
Figure: Classification of Malwares

2.13 LET US SUM-UP

- A Software bug is a fault in a computer program that causes to produce incorrect or unexpected results.

- Debugging is the name that programmers give to the activity of locating and removing errors from programs.

- A good programmer should be able to ensure that the code he or she changes is reliable, correct, and thoroughly self-verified.

- Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content.

- Malware is malicious software which developed to penetrate computers in a network without the permission or notification of users.

- Spyware is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine.

2.14 FURTHER READING

1. Hossein Rouhani Zeidanloo, S. Farzaneh Tabatabaei, Payam Vahdani Amoli and Atefeh Tajpour, *"All about Malwares (Malicious Codes)",* University of Technology Malaysia (UTM), Kuala Lumpur, Malaysia.

2. M.D. Preda, M. Christodorescu and S. Jha, S. Debray, "*A Semantics-Based Approach to Malware Detection, ACM SIGPLAN-SIGACT symposium on principles of programming languages",* University of Verona, University of Wisconsin, University of Arizona, 2007.

3. http://courses.cs.vt.edu/~cs1206/Fall00/bugs_CAS.html

4. http://jobsandnewstoday.blogspot.in/2013/04/what-are-common-types-of-bugs- and-define.html

5. http://www.spamlaws.com/unusual-software-bugs.html

2.15 ASSIGNMENTS

1. What is a programming bug?

2. What are impacts of programming bugs?

3. How can you classify the programming bugs?

4. How can you be a zero- bug programmer?

5. What is a malicious code?

6. What are different malicious codes?

7. What is a Trojan horse? What are different types of Trojan horse?

Unit 3: Database Security

<div style="text-align: right">**3**</div>

Unit Structure

3.1   Learning Objectives

After learning this unit you should be able to know:

- What is a database security?

- What are security methods?

- Different types of Database Security Issues.

- Requirements for database security.

- A set of Tips to improve Database Security.

- Reliability and Integrity for database security.

3.2   Introduction

Database technologies are a core component of many computing systems. They allow data to be retained and shared electronically and the amount of data contained in these systems continues to grow at an exponential rate. So does the need to insure the integrity of the data and secure the data from unintended access. The Privacy Rights Clearing House (2010) reports that more than 345 million customer records have been lost or stolen since 2005 when they began tracking data breach incidents, and the Ponemon Institute reports the average cost of a data breach has risen to $202 per customer record (Ponemon, 2009). In August 2009, criminal indictments were handed down in the United States to three perpetrators accused of carrying out the single largest data security breach recorded to date. These hackers allegedly stole over 130 million credit and debit card numbers by exploiting well known database vulnerability, a SQL injection (Phifer, 2010). In this unit we will discuss about the fundamental concepts of database security.

3.3   Database Security Problems

Database security is a growing concern evidenced by an increase in the number of reported incidents of loss of data or unauthorized exposure to sensitive data. As the amount of data collected, retained and shared electronically expands, so does the need to understand database security. The Defence Information Systems Agency of the US Department of Defence (2004),

in its Database Security Technical Implementation Guide, states that database security should provide controlled, protected access to the contents of a database as well as preserve the integrity, consistency, and overall quality of the data. Learners in the computing disciplines must develop an understanding of the issues and challenges related to database security and must be able to identify possible solutions.

At its core, database security strives to insure that only authenticated users perform authorized activities at authorized times. In this unit we will focus on the concepts and mechanisms to secure any databases. Within that context, database security encompasses three constructs: *confidentiality* or protection of data from unauthorized disclosure, *integrity* or prevention from unauthorized data access, and *availability* or the identification of and recovery from hardware and software errors or malicious activity resulting in the denial of data availability.

3.4   Security Vulnerabilities in databases

Protecting databases is in not an easy task, but the attacks may cause due to the simplest vulnerabilities that are most successful.

There are many security vulnerabilities in databases. Some of them include:

- Default, blank, and weak username/password

- SQL injections

- Extensive user and group privileges

- Unnecessarily enabled database features

- Buffer overflows

- Privilege escalation

- Denial-of-service attack

- Un-patched databases

- Unencrypted sensitive data at rest and in motion

3.5   Introduction to Databases

A database is simply an organized collection of related data, typically stored on disk, and accessible by possibly many concurrent users. Databases are generally separated into application areas. For example, one database may contain Human Resource data; another may contain sales data; another may contain accounting data; and so on. Databases are managed by a DBMS.

Databases are incredibly prevalent - they underlie technology used by most people every day if not every hour. Databases reside behind a huge fraction of websites; they're a crucial component of telecommunications systems, banking systems, video games, and just about any other software system or electronic device that maintains some amount of persistent information. In addition to persistence, database systems provide a number of other properties that make them exceptionally useful and convenient: reliability, efficiency, scalability, concurrency control, data abstractions, and high-level query languages. Databases are so ubiquitous and important that computer science learners frequently cite their database class as the one most useful to them in industry and in professional careers.

3.6   Database Security Threats

Database Security is the mechanism which protects the database against intentional or accidental threats. A database security manager is the most important asset to maintaining and securing sensitive data within an organization. Database security managers are required to multitask and juggle a variety of headaches that accompany the maintenance of a secure database.

Database security issues arise in relation to the following situations:

- Theft and Fraud

- Loss of confidentiality

- Loss of privacy

- Loss of integrity

- Loss of availability

Threat is nothing but any intentional or accidental event that may adversely affect to the system. Examples of threats are;

- Using another person's log-in name to access data

- Unauthorized copying data

- Program/Data alteration

- Illegal entry by hacker

- Viruses

Database Security Counter Measures

There are some counter measures which are based on computer based controls. They are:

- Authorization

- Views

- Backup and Recovery

- Encryption

- RAID Technology

3.6.1 Authorization

The granting of a privilege that enable a user to have a legitimate access to a system is called authorization. They are sometimes referred as access controls. The process of authorization involves authenticating the user requesting access to objects. A system administrator is responsible for allowing users to have access to the system by creating individual user accounts.

There are two types of systems. They are as follows:

3.6.1.1 Closed system and Opened system

In Closed Systems some DBMS required authorization for authorized DBMS users to access specific objects. On the other hand in Open Systems allow users to have complete access to all objects within the database.

A DBMS may permit both individual user identifiers and group identifiers that are to be created. Certain privileges may be associated with specific identifiers,

which indicate the kind of privilege is allowed with certain with certain database objects. Each privilege has a binary value associated with it. The binary values are summed and the total value indicates what privileges are allowed for a specific user or group with a particular object.

3.6.2 Views

A view is a virtual relation that does not actually exist in the database, but is produced upon request by a particular user, at the time of request.

The view mechanism provides a powerful and flexible security mechanism by hiding parts of the database from certain users. The user is not aware of the existence of any attributes or rows that are missing from the view.

3.6.3 Backup & Recovery

The process of periodically taking a copy of the database and log file on to offline storage media. DBMS should provide backup facilities to assist with the recovery of a database failure.

3.6.4 Encryption

The encoding of data by a special algorithm that renders the data unreadable by any program without the decryption key. There will be degradation in performance because of the time taken to decode it. It also protects the data transmitted over communication lines.

3.6.5 RAID (Redundant Array of Independent Disks)

The hardware that the DBMS is running on must be fault-tolerant meaning that the DBMS should continue to operate even if one of the hardware components fails.

One solution is the use of RAID technology which works on having a large disk array comprising an arrangement of several independent disks that are organized to improve reliability and at the same time increase performance.

3.7 Database Security Issues

If you own a business it is important to understand some of the database security problems that occur within an organization and how to avoid them. If you understand the how, where, and why of database security you can prevent future problems from occurring.

3.7.1 Daily Maintenance

Database audit logs require daily review to make certain that there has been no data misuse. This requires overseeing database privileges and then consistently updating user access accounts. A database security manager also provides different types of access control for different users and assesses new programs that are performing with the database. If these tasks are performed on a daily basis, you can avoid a lot of problems with users that may pose a threat to the security of the database.

3.7.2 Varied Security Methods for Applications

More often than not applications developers will vary the methods of security for different applications that are being utilized within the database. This can create difficulty with creating policies for accessing the applications. The database must also possess the proper access controls for regulating the varying methods of security otherwise sensitive data is at risk.

3.7.3 Post-Upgrade Evaluation

When a database is upgraded it is necessary for the administrator to perform a post-upgrade evaluation to ensure that security is consistent across all programs. Failure to perform this operation opens up the database to attack.

3.7.4 Split the Position

Sometimes organizations fail to split the duties between the IT administrator and the database security manager. Instead the company tries to cut costs by having the IT administrator do everything. This action can significantly compromise the security of the data due to the responsibilities involved with both positions. The IT administrator should manage the database while the security manager performs all of the daily security processes.

3.7.5 Application Spoofing

Hackers are capable of creating applications that resemble the existing applications connected to the database. These unauthorized applications are often difficult to identify and allow hackers access to the database via the application in disguise.

3.7.6 Manage User Passwords

Sometimes IT database security managers will forget to remove IDs and access privileges of former users which leads to password vulnerabilities in the database. Password rules and maintenance needs to be strictly enforced to avoid opening up the database to unauthorized users.

3.7.7 Windows Operating System Flaws

Windows operating systems are not effective when it comes to database security. Often theft of passwords is prevalent as well as denial of service issues. The database security manager can take precautions through routine daily maintenance checks.

The best way to avoid a lot of these problems is to employ qualified personnel and separate the security responsibilities from the daily database maintenance responsibilities.

3.8 Tips to keep your Database Secured

The following tips you should remember to keep your database secured.

3.8.1 Enable Security Controls

Unlike older databases, the newer databases require passwords to gain full access to the stored data. Often when the databases are shipped, none of the security features are enabled. Make sure you check the security controls and enable all of the features before allowing anyone access to the database.

3.8.2 Check the Patch Level

Check the patch level configuration in the database to determine if there is any vulnerability in the default settings. Also, perform a full assessment   of   the

database to fix any existing vulnerabilities in the system before placing any data into the database.

3.8.3 Exclude copying of the Database

Although you may have one chief IT administrator that is the primary gatekeeper to the database, there is no control over the data once the database has been copied. For this reason you should disallow database copying because it represents an internal threat to database security.

3.8.4 Restrict Access

Restrict access to the database by specifically designating who is allowed administrator privileges. For a small business it is a good idea to delegate this responsibility to one IT administrator and then place certain restrictions on other users. In addition to restricting access, make sure the backups are stored in an encrypted format and restrict access to XML files. The files in XML format are files from a discontinued database.

3.8.5 Existing Databases

There are database discovery tools which identify existing databases that contain confidential information. The tools also monitor existing databases to ensure the information is stored in encrypted format. In addition to the new database, make sure you monitor all of the existing databases to ensure that information is encrypted, there are no vulnerabilities, and that there are no duplicates.

3.8.6 Shared Data

Sharing data becomes a concern when businesses have to train new employees and developers have to test new database applications. In this instance, the IT administrator can perform what is called subsetting which provides a separate type of restricted access with fake information substituted for the sensitive information. Subsetting a database basically allows developers and new employees to use the database for testing and training without exposing confidential or sensitive information.

3.9   Requirements for database security

The requirements for database security include the following.

- **Physical database integrity**: The data of a database are immune to physical problems, such as power failures, and someone can reconstruct the database if it is destroyed through a catastrophe.

- **Logical database integrity:** The structure of the database is preserved. With logical integrity of a database, a modification to the value of one field does not affect other fields, for example.

- **Element integrity:** The data contained in each element are accurate.

- **Audit ability:** It is possible to track who or what has accessed (or modified) the elements in the database.

- **Access control:** A user is allowed to access only authorized data, and different users can be restricted to different modes of access (such as read or write).

- **User authentication**: Every user is positively identified, both for the audit trail and for permission to access certain data.

- **Availability:** Users can access the database in general and all the data for which they are authorized

3.10 Reliability and Integrity

When software engineers say that software is reliable, they mean that the software runs for very long periods of time without failing. Users certainly expect a DBMS to be reliable, since the data usually are keys to business or organizational needs. Moreover, users entrust their data to a DBMS and rightly expect it to protect the data from loss or damage. Concerns for reliability and integrity are general security issues, but they are more highly apparent with databases.

There are several ways that a DBMS guards against loss or damage.

Database integrity: concern that the database as a whole is protected against damage, as from the failure of a disk drive or the corruption of the master

database index. These concerns are addressed by operating system integrity controls and recovery procedures.

Element integrity: concern that the value of a specific data element is written or changed only by authorized users. Proper access controls protect a database from corruption by unauthorized users.

Element accuracy: concern that only correct values are written into the elements of a database. Checks on the values of elements can help to prevent insertion of improper values. Also, constraint conditions can detect incorrect values.

3.11 Protection Features from the Database System

Every DBMS package has its own security features. One of such feature is Two- Phase update.

Two-Phase Update

During the first phase, called the intent phase, the DBMS gathers the resources it needs to perform the update. It may gather data, create dummy records, open files, lock out other users, and calculate final answers; in short, it does everything to prepare for the update, but it makes no changes to the database. The first phase is repeatable an unlimited number of times because it takes no permanent action. If the system fails during execution of the first phase, no harm is done, because all these steps can be restarted and repeated after the system resumes processing.

The last event of the first phase, called committing, involves the writing of a commit flag to the database. The commit flag means that the DBMS has passed the point of no return: After committing, the DBMS begins making permanent changes.

The second phase makes the permanent changes. During the second phase, no actions from before the commit can be repeated, but the update activities of phase two can also be repeated as often as needed. If the system fails during the second phase, the database may contain incomplete data, but the system can repair these data by performing all activities of the second phase. After the second phase has been completed, the database is again complete

3.12 Redundancy/Internal Consistency

Many DBMSs maintain additional information to detect internal inconsistencies in data.

3.12.1 Error Detection and Correction Codes

One form of redundancy is error detection and correction codes, such as parity bits, Hamming codes, and cyclic redundancy checks. These codes can be applied to single fields, records, or the entire database. Each time a data item is placed in the database, the appropriate check codes are computed and stored; each time a data item is retrieved, a similar check code is computed and compared to the stored value.

3.12.2 Shadow Fields

Entire attributes or entire records can be duplicated in a database. If the data are irreproducible, this second copy can provide an immediate replacement if an error is detected.

3.12.3 Recovery

In addition to these error correction processes, a DBMS can maintain a log of user accesses, particularly changes. In the event of a failure, the database is reloaded from a backup copy and all later changes are then applied from the audit log.

3.13 Concurrency/Consistency

Database systems are often multiuser systems. Accesses by two users sharing the same database must be constrained so that neither interferes with the other. Simple locking is done by the DBMS. If two users attempt to read the same data item, there is no conflict because both obtain the same value.

3.13.1 Monitors

The monitor is the unit of a DBMS responsible for the structural integrity of the database. A monitor can check values being entered to ensure their consistency with the rest of the database or with characteristics of the particular field. For example, a monitor might reject alphabetic characters for a numeric

field.

3.13.2 Range Comparisons

A range comparison monitor tests each new value to ensure that the value is within an acceptable range. If the data value is outside the range, it is rejected and not entered into the database

3.13.3 State Constraints

State constraints describe the condition of the entire database. At no time should the database values violate these constraints. Phrased differently, if these constraints are not met, some value of the database is in error.

3.13.4 Transition Constraints

State constraints describe the state of a correct database. Transition constraints describe conditions necessary before changes can be applied to a database. For example, before a new employee can be added to the database, there must be a position number in the database with status "vacant."

3.13.5 Protecting Sensitive Data

Some databases contain what is called sensitive data. As a working definition, let us say that sensitive data are data that should not be made public. Determining which data items and fields are sensitive depends both on the individual database and the underlying meaning of the data

Several factors can make data sensitive-:

- **Inherently sensitive.** The value itself may be so revealing that it is sensitive. Examples are the locations of defensive missiles or the median income of barbers in a town with only one barber.

- **From a sensitive source.** The source of the data may indicate a need for confidentiality. An example is information from an informer whose identity would be compromised if the information were disclosed.

- **Declared sensitive.** The database administrator or the owner of the data may have declared the data to be sensitive. Examples are classified military data or the name of the anonymous donor of a piece of art.

- **Part of a sensitive attribute or a sensitive record**. In a database, an entire attribute or record may be classified as sensitive. Examples are the salary attribute of a personnel database or a record describing a secret space mission.

- **Sensitive in relation to previously disclosed information**. Some data become sensitive in the presence of other data. For example, the longitude coordinate of a secret gold mine reveals little, but the longitude coordinate in conjunction with the latitude coordinate pinpoints the mine.

3.14 Techniques to maintain sensitivity Availability of Data

If a user is updating several fields, other users' accesses to those fields must be blocked temporarily.

Acceptability of Access

One or more values of the record may be sensitive and not accessible by the general user. A DBMS should not release sensitive data to unauthorized individuals

Assurance of Authenticity

Certain characteristics of the user external to the database may also be considered when permitting access. For example, to enhance security, the database administrator may permit someone to access the database only at certain times.

3.15 Types of Disclosures Exact Data

The user may know that sensitive data are being requested, or the user may request general data without knowing that some of it is sensitive. A faulty database manager may even deliver sensitive data by accident, without the user's is having requested it. In all of these cases the result is the same: The security of the sensitive data has been breached.

Bounds

Indicating that a sensitive value, y, is between two values, L and H. Sometimes, by using a narrowing technique not unlike the binary search, the user may first determine that L ≤ y ≤ H and then see whether L≤ y ≤ H/2, and so forth thereby permitting the user to determine the sensitive data.

Negative result

Sometimes we can word a query to determine a negative result. If a student does not appear on the honours list, you can infer that the person's grade point average is below 3.50. This information is not too revealing, however, because the range of grade point averages from 0.0 to 3.49 is rather wide.

Existence

In some cases, the existence of data is itself a sensitive piece of data, regardless of the actual value. For example, an employer may not want employees to know that their use of long distance telephone lines is being monitored. In this case, discovering a LONG DISTANCE field in a personnel file would reveal sensitive data.

Probable Value

It may be possible to determine the probability that a certain element has a certain value. To see how, suppose you want to find out whether the president of the United States is registered in the Tory party. Knowing that the president is in the database, you submit two queries to the database.

3.16 Security versus Precision

The ideal combination of security and precision allows us to maintain perfect confidentiality with maximum precision; in other words, we disclose all and only the non-sensitive data.
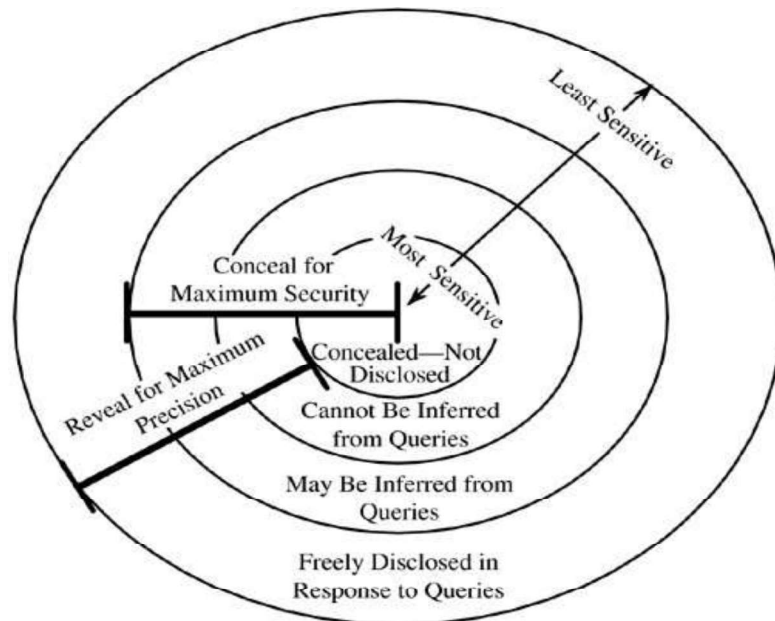
Figure: Security versus Precision

3.16.1 Inference

The inference problem is a way to infer or derive sensitive data from no sensitive data. The inference problem is a subtle vulnerability in database security.

3.16.2 Inference Techniques

Direct Attack: In a direct attack, a user tries to determine values of sensitive fields by seeking them directly with queries that yield few records. The most successful technique is to form a query so specific that it matches exactly one data item. Example:- List NAME where SEX=M ^ DRUGS=1.

Indirect Attack: neutral statistics, such as count, sum, and mean, are used to collect sensitive data.

Tracker Attacks: A tracker attack can fool the database manager into locating the desired data by using additional queries that produce small results. The tracker adds additional records to be retrieved for two different queries; the two sets of records cancel each other out, leaving only the statistic or data desired.

The approach is to use intelligent padding of two queries. In other words, instead of trying to identify a unique value, we request n – 1 other values (where there are n values in the database). Given n and n – 1, we can easily compute the desired single element.

Linear System Vulnerability-: it may be possible to determine a series of queries that returns results relating to several different sets with a little logic, algebra, and luck in the distribution of the database contents. Ex-: the queries' equations can be solved for each of the unknown c values, revealing them all.

3.17 Multilevel Databases Security

The security of a single element may be different from the security of other elements of the same record or from other values of the same attribute. That is, the security of one element may be different from that of other elements of the same row or column. This situation implies that security should be implemented for each individual element.

Two levels—sensitive and non-sensitive—are inadequate to represent some security situations. Several grades of security may be needed. These grades may represent ranges of allowable knowledge, which may overlap. Typically, the security grades form a lattice.

The security of an aggregate—a sum, a count, or a group of values in a database—may be different from the security of the individual elements. The security of the aggregate may be higher or lower than that of the individual elements

3.17.1 Integrity

Even in a single-level database in which all elements have the same degree of sensitivity, integrity is a tricky problem. In the case of multilevel databases, integrity becomes both more important and more difficult to achieve. Because of the *-property for access control, a process that reads high-level data is not allowed to write a file at a lower level. Applied to databases, however, this principle says that a high-level user should not be able to write a lower-level data element

Confidentiality: - Two different users operating at two different levels of

security might get two different answers to the same query. In order to preserve confidentiality, precision is sacrificed.

3.17.2 Distributed Databases

The distributed or federated database is a fourth design for a secure multilevel database. In this case, a trusted front end controls access to two unmodified commercial DBMSs: one for all low-sensitivity data and one for all high-sensitivity data.

The front end takes a user's query and formulates single-level queries to the databases as appropriate. For a user cleared for high-sensitivity data the front end submits queries to both the high- and low-sensitivity databases. But if the user is not cleared for high-sensitivity data, the front end submits a query to only the low-sensitivity database. If the result is obtained from either back-end database alone, the front end passes the result back to the user. If the result comes from both databases, the front end has to combine the results appropriately. For example, if the query is a join query having some high-sensitivity terms and some low, the front end has to perform the equivalent of a database join itself.

3.18 How can you assess Risk?

Every organization has some kind of policy in place to secure sensitive information. However, with the increased use of technology, some organizations fail to employ active controls to ensure that technology such as laptops and portable storage contain some type of encryption for preventing the risk of exposing sensitive data.

To determine if you are at risk you should find out if the organization takes the following security measures:

Transfer of Confidential Data: Find out if the organization has a policy in place that covers the transfer of confidential information onto portable storage or laptops. There should be specific rules and regulations in place for this type of data transfer and data security.

Encryption: An organization that uses multiple portable devices such as laptops and mobile storage should have some type of encryption system

installed within the devices.

Tracking System: Organizations should have a system in place that track access to confidential information. The system should also be capable of identifying when inappropriate access has occurred.

IT Asset Disposal: When upgrading to new technology the organization should have an IT asset disposal policy in place, as well as a policy for wiping out data on portable storage devices that are being disposed of. Generally there is a standard protocol that organizations are required to follow with regard to IT asset disposal. Find out what the policies are and make sure they are following them.

Written Security Policy: There should be an established data security policy that outlines the guidelines for using laptops and portable storage devices. The policy should include rules that pertain to the encryption of data on laptops and portable storage devices. The policy should include who is authorized to use the portable devices, the type of data that can be stored on them, and where the portable devices can be used.

Notification Safeguards: There should also be a policy in place that requires notification to be provided to technical personnel when confidential data is transferred to portable storage devices or laptops. This policy encourages encryption for full disk and partial disk applications.

Decryption Methods: Encryption keys should be limited to a specific set of individuals and should not be an organization-wide policy. This includes strict enforcement of key sharing rules.

3.19 SQL Injection

 SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection exploits security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector

for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. In a 2012 study, security company Imperva observed that the average web application received 4 attack campaigns per month, and retailers received twice as many attacks as other industries.

3.20 Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using fake bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting victims. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and users should not use the same passwords anywhere on the internet.

Phishing is a continual threat, and the risk is even larger in social media such as Facebook, Twitter, and Google+. Hackers could create a clone of a website and tell you to enter personal information, which is then emailed to them. Hackers commonly take advantage of these sites to attack people using them at their workplace, homes, or in public in order to take personal and security

information that can affect the user or company (if in a workplace environment). Phishing takes advantage of the trust that the user may have since the user may not be able to tell that the site being visited, or program being used, is not real; therefore, when this occurs, the hacker has the chance to gain the personal information of the targeted user, such as passwords, usernames, security codes, and credit card numbers, among other things.

3.21 Let us Sum-up

Keep in mind that securing a database also requires a change in thinking on the part of database administrator as well as the workers who have access privileges or restrictions to the database. A change in attitude ensures that everyone is on the same page with what is expected when it comes to keeping data secure. Database security is becoming an increasingly important topic and students need to develop core understandings in this area. The primary objectives of database security are to prevent unauthorized access to data, prevent unauthorized tampering or modification of data, and to insure that data remains available when needed.

3.22 Further Readings

1. CEH v9: Certified Ethical Hacker Version 9 Study Guide

2. Burtescu, E. Database security in Knowledge Management. Projects, Systems and Technologies", International Conference „Knowledge Management. Projects, Systems and Technologies", Bucharest, INFOREC Printing House, Bucharest.

3. Technology and Informatics, Data Security for Health Care, Volume II, Technical Guidelines, Edited by the SEISMED Consortium.

4. Professor Hossein Saiedian Computer Security: Principle and Practice, Chapter- 5: Database Security, EECS710: Information Security.

5. http://www.spamlaws.com/database-security.html

3.23 Assignments

1. What do you mean by database security? When do database security issues arise?

2. Name and explain the computer based database security counter measures.

3. Mention the requirements for database security.

4. Discuss how consistency is maintained by concurrent execution of database transactions.

5. As a database security profession suggest the points to keep your Database Secured.

6. What do you mean by sensitive data? Mention the factors that can make the data sensitive.

7. What is an SQL injection? How SQL injection must exploit a security vulnerability in an application's software

Unit 4: Operating System Security

4

Unit Structure

4.1 Learning Objectives

After end of this unit you should be able to know:

- The security (or lack of security) of most popular operating systems and its effect to the overall security of Web based applications and services.

- Designing of Secure Operating System

- OS Security Vulnerabilities.

- What makes an operating system "secure" Or "trustworthy"?

- How are trusted systems designed?

4.2 Introduction

Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability. OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.

OS security encompasses many different techniques and methods which ensure safety from threats and attacks. OS security allows different applications and programs to perform required tasks and stop unauthorized interference.

OS security may be approached in many ways, including the following steps:

- Performing regular OS patch updates

- Installing updated antivirus engines and software

- Monitoring all incoming and outgoing network traffic through a firewall

- Creating secure accounts with required privileges only (i.e., user management)

In this unit we will discuss about Operating system security vulnerabilities and design of secured policies and mechanisms for security in popular operating systems.

4.3 Overview of Operating System

An Operating System (OS) is an interface between computer user and computer hardware. An operating system is software which performs all the basic tasks like file management, memory management, process management, handling input and output, and controlling peripheral devices such as disk drives and printers. It acts as a platform on which various applications execute their operations

Some popular Operating Systems include Linux Operating System, Windows Operating System, VMS, and OS/400.

Operating systems are the prime providers of security in computing systems. They support many programming capabilities, permit multiprogramming and sharing of resources, and enforce restrictions on program and user behavior.

4.4 Security Policies

The **security** can be expressed as a number of well-defined, consistent and implementable rules. A **security policy** is a statement of the security we expect the system to enforce.

An operating system (or any other piece of a trusted system) can be secured or trusted only in relation to its security policy, that is, to the security needs the system is expected to satisfy.

The development of secure OS based on the following steps:

- o analysis of the system
- o choose/define a security policy
- o choose/create a security model (based on the policy)
- o choose implementation method
- o make a (conceptual) design
- o verify the correctness of the design
- o make an implementation
- o verify the implementation

There are feed-back loops between all of the above steps Errors may occur in all above steps

4.5 Models of Operating System Security

A **security** model is a representation of the **security policy** for the OS. In security and elsewhere, models are often used to describe, study, or analysis of a particular situation or relationship.

In particular, security models are used to

- test a particular policy for completeness and consistency

- document a policy

- help conceptualize, design and implementation

- check whether an implementation meets its requirements

A formal security model is a mathematical description (formalization) of the rules of the security policy. It could be used for formal proofs of security.

4.5.1 The Unix/Linux Security Model

UNIX / Linux in comparison to more modern operating systems such as Windows-NT provide a relatively simple model of security. System calls are the only mechanism by which processes may interact with the operating system and the resources it is protecting and managing.

Each user and each process executed on behalf of that user is identified by (minimally) two non-negative 16-bit integers:

The user-identifier is established when logging into a Unix/Linux system. A correct combination of user-name and password when logging in, or the validation of a network-based connection, set the user-identifier (uid) in the process control block of the user's login shell, or command interpreter. Unless modified, this user-identifier is inherited by all processes invoked from the initial login shell. Under certain conditions, the user-identifier may be determined with the system calls setuid () and getuid ().

The effective user-identifier is, by default, the same as the user-identifier, but

may be temporarily changed to a different value to offer temporary privileges. The successful invocation of set-user-id programs, such as password and login will, typically, set the effective user-identifier for the lifetime of that process. Under certain conditions, the effective user-identifier may be changed and determined with the system calls seteuid () and geteuid ().

4.5.2 The Windows-NT Security Model

While the UNIX security model provides system-wide and consistent support of user and group identification, it constrains their manipulation to the system administrator (root).

In contrast, the newer Windows-NT security model enables each authorized user (and process) to both examine and manipulate access to a variety of objects. Again, the access controls provided by Windows-NT are best seen by examining the file system — but we must be using a partition supporting the Windows-NT File System (NTFS) and not simply a FAT-based (ala. Windows'98) partition.

4.6 Security in Operating Systems

It is the protection of operating system from theft or damage to the hardware. Side by side it is the software and to the information on them as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware as well as protecting against harm that may come via network access, data and code injection due to malpractice by operators , whether intentional, accidental to deviating from secure procedures.

The field is of growing importance due to the increasing reliance on computer systems and the Internet in most societies, wireless networks such as Bluetooth and Wi-Fi - and the growth of "smart" devices, including smart phones, televisions and tiny devices as part of the Internet of Things.

The security of the operating system is therefore a necessity for the overall system security. Today most commercially developed operating systems provide security through authentication of the users, maintenance of access control mechanisms, separation of kernel and user spaces and providing

trusted applications to modify or manage system resources.

Developing secure operating systems involves four activities. First, the environment to be protected must be well understood. Through policy statements and models, the essential components of systems are identified, and the interactions among components can be studied.

4.7 Operating System Security

We study operating systems in depth because they are at the heart of security systems for modern computers. They must provide mechanisms for both separation and sharing, mechanisms that must be robust and yet easy to use.

Physical Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc.

To ensure operating system security the following mechanisms are employed.

4.7.1   Authentication

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways −

o **Username / Password** − User need to enter a registered username and password with Operating system to login into the system.

o **User card/key** − User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.

o **User attribute - fingerprint/ eye retina pattern/ signature** − User need to pass his/her attribute via designated input device used by operating system

to login into the system.

4.7.2 One Time passwords

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password is implemented in various ways.

- **Random numbers** − Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.

- **Secret key** − User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.

- **Network password** − Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

4.7.3 Program Threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as **Program Threats**. One of the common examples of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

- **Trojan Horse** − Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.

- **Trap Door** − If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.

- **Logic Bomb** − Logic bomb is a situation when a program misbehaves only

when certain conditions met otherwise it works as a genuine program. It is harder to detect.

- **Virus** − Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generally a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user.

4.7.4 System Threats

A system threat refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. A system threat creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

o **Worm** − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worm's processes can even shut down an entire network.

o **Port Scanning** − Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.

o **Denial of Service** − Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

4.7.5 Computer Security Classifications

As per the U.S. Department of Defense Trusted Computer System's Evaluation Criteria there are four security classifications in computer systems: A, B, C, and

D. There is a widely used specification to determine and model the security of systems and of security solutions. Following is the brief description of each classification.

4.7.5.1 Classification Type & Description

Type A

Verified Design: no additional features in an A1 system over a B3 system; rather there are formal procedures for the analysis of the design of the system and more rigorous controls on its implementation. Highest Level uses formal design specifications and verification techniques and grants a high degree of assurance of process security.

Type B

This type provides a mandatory protection system. Have all the properties of a class C2 system. It attaches a sensitivity label to each object. It is of three types.

B1 − Labeled Security Protection: the system must implement the Mandatory Access Control in which every subject and object of the system must maintain a security label, and every access to system resource (objects) by a subject must check for security labels and follow some defined rules. It maintains the security label of each object in the system. This Label is used for making decisions to access control.

B2 − Structured Protection: few new security features are added beyond B1; rather the focus is on the structure (design) of the system to maintain greater levels of assurance so that the system behaves predictably and correctly (such as, a minimal security kernel, trusted path to user, and identified covert channels, etc). Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events.

B3 − Security Domains: more requirements to maintain greater assurance that the system will be small enough to be subjected to analysis and tests, and not to have bugs that might allow something to circumvent mandatory access controls, e.g., support of active audit, and secure crashing, etc. Allows creating lists or user groups for access-control to grant access or revoke access to a given named object.

Type C

It provides protection and user accountability using audit capabilities. It is of two

types.

C1 – Discretionary Security Protection: the system must identify different users (or jobs) running inside the system, and provide mechanisms for user authentication and authorization to prevent unprivileged user programs from interference of each other (e.g., overwriting critical portions of the memory). It incorporates controls so that users can protect their private information and keep other users from accidentally reading / deleting their data. UNIX versions are mostly CI class.

C2 – Controlled Access Protection: the system meets additional security requirements than that of C1 that include access control at a per user granularity (access control for any subset of the user community); clearing of newly allocated disk space and memory; and ability of auditing (logging) for security relevant events such as authentication and object access, etc. It adds an individual-level access control to the capabilities of a CI level system.

Type D

Minimal Protection: For this type no security is required; the system did not qualify for any of the higher ratings. This is a lowest level and minimum protection. MS-DOS, Window 3.1opearting systems fall in this category.

4.8 System access Threats

4.8.1 Intruders

Masquerader an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account Misfeasor a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges Clandestine user an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection,

4.8.2 Malicious Software

Programs that exploit vulnerabilities in computing systems also referred to as malware. These can be divided into two categories: parasitic fragments of

programs that cannot exist independently of some actual application program, utility, or system program viruses, logic bombs, and backdoors are examples independent self-contained programs that can be scheduled and run by the operating system worms and boot programs are examples.

4.8.3 Access Control

Implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance Mediates between a user and system resources, such as applications, operating systems, firewalls, routers, files, and databases. A security administrator maintains an authorization database that specifies what type of access to which resources is allowed for this user the access control function consults this database to determine whether to grant access an auditing function monitors and keeps a record of user accesses to system resources

4.8.4 Firewalls

Can be an effective means of protecting a local system or network of systems from network-based security threats while affording access to the outside world via wide area networks and the Internet Traditionally, a firewall is a dedicated computer that interfaces with computers outside a network and has special security precautions built into it in order to protect sensitive files on computers within the network Design goals:

1) The firewall acts as a choke point, so that all incoming traffic and all outgoing traffic must pass through the firewall

2) The firewall enforces the local security policy, which defines the traffic that is authorized to pass

3) The firewall is secure against attacks

4.9 Requirements of Secure Operation Systems

Most current operating systems provide discretionary access control, that is, someone who owns a resource can make a decision as to who is allowed to use (access) the resource. Moreover, because the lack of built-in mechanisms

for the enforcement of security policies in such systems, the access control is normally a one-shot approach: either all or none privileges are granted, rarely supporting the "principle of least privilege" (without limiting the privileges a program can inherit based on the trustworthiness).

Systems with stronger security and protection will require evolving from the approach of discretionary control towards the concept of mandatory (non-discretionary) control where information is confined within a "security perimeter" with strict rules enforced by the system about who is allowed access to certain resources, and not allow any information to move from a more secure environment to a less secure environment.

A secure architecture requires flexibility for support of a wide variety of security policies: Separation of security policy logic from the mechanism of policy enforcement, so that a system can support diverse security policies. Support for policy definition and policy changes with well-defined policy interfaces and formats provide the default security behavior of the system so as to maintain tight system security without requiring detailed system configuration.

4.10 Design Principles of Secure Operation Systems

Saltzer and Schroeder (1975) identified a core set of principles to operating system security design:

Least privilege: Every object (users and their processes) should work within a minimal set of privileges; access rights should be obtained by explicit request, and the default level of access should be "none".

Economy of mechanisms: security mechanisms should be as small and simple as possible, aiding in their verification. This implies that they should be integral to an operating system's design, and not an afterthought.

Acceptability: security mechanisms must at the same time be robust yet non-intrusive. An intrusive mechanism is likely to be counter-productive and avoided by users, if possible.

Complete: Mechanisms must be pervasive and access control checked during all operations — including the tasks of backup and maintenance.

Open design: An operating system's security should not remain secret, nor be provided by stealth. Open mechanisms are subject to scrutiny, review, and continued refinement.

4.11 Trusted System

Before we begin to examine a trusted operating system in detail, let us look more carefully at the terminology involved in understanding and describing trust. What would it take for us to consider something secure? The word secure reflects a dichotomy: Something is either secure or not secure. If secure, it should withstand all attacks, today, tomorrow, and a century from now. And if we claim that it is secure, you either accept our assertion (and buy and use it) or reject it (and either do not use it or use it but do not trust it). How does security differ from quality? If we claim that something is good, you are less interested in our claims and more interested in an objective appraisal of whether the thing meets your performance and functionality needs

For this reason, security professionals prefer to speak of trusted instead of secure operating systems. A trusted system connotes one that meets the intended security requirements, is of high enough quality, and justifies the user's confidence in that quality. That is, trust is perceived by the system's receiver or user, not by its developer, designer, or manufacturer. As a user, you may not be able to evaluate that trust directly. You may trust the design, a professional evaluation, or the opinion of a valued colleague. But in the end, it is your responsibility to sanction the degree of trust you require.

4.11.1 Trusted Operating System Design

Operating systems by themselves (regardless of their security constraints) are very difficult to design. They handle many duties, are subject to interruptions and context switches, and must minimize overhead so as not to slow user computations and interactions. Adding the responsibility for security enforcement to the operating system substantially increases the difficulty of designing an operating system.

Nevertheless, the need for effective security is becoming more pervasive, and good software engineering principles tell us that it is better to design the

security in at the beginning than to shoehorn it in at the end. Thus, this section focuses on the design of operating systems for a high degree of security. First, we examine the basic design of a standard multipurpose operating system. Then, we consider isolation, through which an operating system supports both sharing and separating user domains.

4.11.2 Assurances in Trusted Operating Systems

We began by studying different models of protection systems. By the time we reached in the last section, we examined three principles—isolation, security kernel, and layered structure—used in designing secure operating systems, and we looked in detail at the approaches taken by designers of particular operating systems. Now, we suppose that an operating system provider has taken these considerations into account and claims to have a secure design. It is time for us to consider assurance, ways of convincing others that a model, design, and implementation are correct.

4.12　Introduction to Vulnerability

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems.

A security risk may be classified as vulnerability. The use of vulnerability with the same meaning of risk can lead to confusion. The risk is tied to the potential of a significant loss. Then there are vulnerabilities without risk: for example when the affected asset has no value. A vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability — a vulnerability for which can exploit exists. The window of vulnerability is the time from when the security hole was introduced

or manifested in deployed software, to when access was removed, a security fix was available/deployed, or the attackers was disabled.

i. Most Common Operating Systems Vulnerabilities

We will discuss some of the operating system security vulnerabilities as follows:

a) File and share permissions that give up everything to everyone

This is easily the biggest vulnerability we are seeing with OS (Operating Systems) regardless of the type of system or Windows version. Users who create shares to make their local files available across the network are typically the culprits. Sometimes it's careless admins; other times they're honest mistakes. Unfortunately, all too often the "Everyone group" is given full access to every file on the system. Then, all it takes is for an insider to search for sensitive keywords stored in .pdf, .xls, .doc and other file formats using a text search tool such as Effective File Search or File Locator Pro. Odds are - nearly 100% of the time -- the attacker will come across sensitive information (SSNs, credit card numbers, you name it) that they shouldn't have access to. Best case scenario, this is an identity theft in the making. Worst case, this becomes a serious breach that makes the headlines.

b) Lack of malware protection

I know, it's really basic but I'm seeing it more now than ever. I've seen antivirus and antispyware software both disabled and not installed at all with no one being aware of the problem.

c) Lack of personal firewall protection

This is another basic security control that's still not enabled on many Windows systems. Even the basic (and free) Windows Firewall can prevent connections to the IPC$ and ADMIN$ shares that are often open and providing information and access that they shouldn't be divulging. Personal firewalls can also block malware infiltrations, wireless intrusions and more. I can't think of a good reason not to use a personal firewall on all workstations and most servers.

d) Weak or nonexistent drive encryption

The drive encryption marketing machine is working its magic, but I'm still seeing

the majority of organizations (large and small) not using encryption. We believe that whole-disk encryption is the only way to go. If a laptop or desktop machine is lost or stolen, the only way to prevent someone from cracking the Windows password and gaining full access to the hard drive is to encrypt everything using reasonable passphrases. Relying on Windows Encrypted File System (EFS) or other file/directory/volume-level encryption puts too much security control in the hands of users and is a breach waiting to happen.

e) **No minimum security standards**

Users with wireless networks, especially, need to follow secure company policies at their homes, like requiring SSL for Outlook Web Access, a PPTP VPN connection for remote network connectivity or WPA-PSK with a strong passphrase to help ensure everything is safe and sound. This can be tough to enforce without a workstation-based wireless IDS/IPS (typically a component of an enterprise wireless management system) or a well-configured Network Access Control (NAC) system. Nevertheless, make it your policy and enforce it wherever possible.

f) **Missing patches in OS as well as third-party software, such as VNC, RealPlayer and others**

This is a big problem that often gets overlooked. I'm not saying you should try to find these types of holes just to claim that patches are missing.   Using Metasploit or its commercial alternatives CANVAS and CORE IMPACT, many missing patches can actually be exploited by a rogue insider or outsider who's gotten into your network via other means. Full remote access anyone?

g) **Weak Windows security policy settings**

Some examples of this include audit logging that is not being enabled for failed events; no password-protected screensavers; not requiring Ctrl+ Alt+ Del for login; not requiring password complexity; and displaying the last user name that logged in. Polices to control these issues are easy to implement locally on each Windows system for smaller Windows shops not running Active Directory. It's even easier for larger enterprises via Active Directory Group Policy.

h) **Unaccounted for systems running unknown, and unmanaged, services such as IIS and SQL Server Express**

These are often legacy Windows systems that aren't within the scope of enterprise security and compliance. Sometimes, they're not even supported by third-party security management apps so they get pushed aside. These systems (typically Windows 98, NT and 2000) are often unhardened and un-patched and are waiting to be exploited. Inevitably there's going to be some random training or test system that everyone forgot about. But such a system is all it takes for someone with ill intent to get onto your network and do bad things.

i) Weak or nonexistent passwords

We can't tell you how many systems (especially Windows laptops) we see that do not have a password assigned to the Administrator account or the default user's password is the same as the user name. The password problem has been around since the dawn of time, so there's no excuse for this one.

j) Windows Mobile and other mobile device weaknesses

In today's mobile world, we would be remiss to not at least mention the vulnerabilities associated with Windows Mobile and similar mobile devices. Some mobile-specific issues are essential to have on your radar. In a tip called Windows mobile security: Get it locked down, we outline several things to consider as follows.

4.13 Remove Unnecessary Services, Applications and Protocols

The system planning process should identify what is actually required for a given system so that a suitable level of functionality is provided, while eliminating software that is not required to improve security When performing the initial installation the supplied defaults should not be☐ used, but rather the installation should be customized so that only the required packages are installed Many of the security-hardening guides provide lists of services, applications, and protocols that should not be installed if not required Strong preference is stated for not installing unwanted software, rather than installing and then later removing or disabling it as many uninstall scripts fail to completely remove all components of a package should an attacker succeed

in gaining some access to a system, disabled software could be re-enabled and used to further compromise a system it is better for security if unwanted software is not installed, and thus not available for use at all.

4.14 Install Additional Security Controls

Further security improvement may be possible by installing and configuring additional security tools such as antivirus software, host-based firewall, IDS or IPS software, or application white listing Some of these may be supplied as part of the operating systems installation, but not configured and enabled by default Given the wide-spread prevalence of malware, appropriate antivirus is a critical security component IDS and IPS software may include additional mechanisms such as traffic monitoring or file integrity checking to identify and even respond to some types of attack White-listing applications limits the programs that can execute in the system to just those in an explicit list.

4.15 Test the System Security

The final step in the process of initially securing the base operating system is security testing. The goal is to ensure that the previous security configuration steps are correctly implemented and to identify any possible vulnerabilities that must be corrected or managed Suitable checklists are included in many security- hardening guides. There are also programs specifically designed to review a system to ensure that a system meets the basic security requirements and to scan for known vulnerabilities and poor configuration practices This should be done following the initial hardening of the system and then repeated periodically as part of the security maintenance process

Logging

Effective logging helps ensure that in the event of a system breach or failure, system administrators can more quickly and accurately identify what happened and more effectively focus their remediation and recovery efforts Logging information can be☐ generated by the system, network, and applications The range of logging data☐ acquired should be determined during the system planning stage Logging can generate significant volumes of information so it is important that sufficient space is allocated for them A suitable automatic log

rotation☐ and archive system should be configured to assist in managing the overall size of the logging information Some form of automated analysis☐ is preferred as it is more likely to identify abnormal activity   manual analysis of logs is tedious and is not   a reliable means of detecting adverse events

4.16 Protection in General-Purpose Operating Systems

We looked at several types of security problems that can occur in programs. The problems may be unintentional, as with buffer overflows, or intentional, as when a virus or worm is inserted in code.

In addition to these general problems, certain kinds of programs may be vulnerable to certain kinds of security problems simply because of the nature of the program itself.

For example, operating systems and databases offer security challenges beyond those in more general programs; these programs offer different access to different items by different kinds of users, so the program designers must pay careful attention to defining access, granting access, and controlling intentional and unintentional corruption of data and relationships.

4.17 Let us Sum-up

The approach covered in this unit – executing applications from a   strongly guarded, secure operating system – certainly opens an alternative frontier in battling with many of existing cyber-space threats of the real world. Although, the approach of using secure operating systems will not be a panacea for all the dangers of current cyber space, and the security of individual applications may still suffer from the vulnerabilities of their own, with the strong containment of a secure operation system, the damages caused from a compromise within one application would be much localized, and the impacts among various applications could be much well controlled.

4.18 Further Readings

1. Cui-Qing Yang, Operating System Security and Secure Operating Systems, Version 1.4b, Option 1 for GSEC January 2003.

2. www.av-Comparatives .org

3. Stewart, W. (2000, Jan. 07). Email Security. Retrieved Feb. 17, 2016,

4. Bose, R. (2008). McGraw Hill Education. McGraw Hill Education.

5. https://en.wikipedia.org/wiki/Vulnerability_(computing)

4.19 Assignments

1. What is a security model? What are the uses of Operating System security model?

2. Define Operating System Security. What are the mechanisms employed to ensure operating system security?

3. What is a Program threat? List and explain some well-known program threats.

4. What do you mean by System Threats? Explain different system threats?

5. What do you mean by secured operating system? Write the requirements of Secured Operation Systems.

6. Explain the design principles of Secure Operation Systems?

7. What do you mean by Operating System Vulnerability? Name the most Common Operating Systems Vulnerabilities.

Block-2
Network Security

Unit 1: Network Security Model and Network Security Threats

<div style="float:right; background:black; color:white; padding:10px;">1</div>

UNIT STRUCTURE

1.1 Learning Objective

After going through this unit, you will able to:

- Know about Network Security Model (NSM)

- Why do we need a Network Security Model?

- Understand the NSM Seven Layer Model

- Know the working of the Network Security Model

- Understand how the Network Security Model can be used to mitigate an attack

- Know about Network Security Threats

- Explain different types of Network Security Threats

1.2 INTRODUCTION

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator/ Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. E-mail has become a de facto mode of written communication and has its share of vulnerabilities and exploits. We shall touch upon the various aspects of the issues pertaining to e-mail. Web based applications are everywhere, net banking, online shopping, online trading to name a few.

Network Security Model (NSM) is layered protocol architecture that divides the

complex task of securing a network infrastructure into several manageable sections or layers. The model is generic and can apply to all security implementation and devices. The development of the NSM is important because unity is needed in securing networks, just as unity was needed in the architecture of networks with the development of the OSI model. When an attack on a network has succeeded it is much easier to locate the underlying issue and fix.

1.3 NETWORK SECURITY MODEL (NSM)

The Open Systems Interconnection model (OSI), developed in 1983 by the International Organization for Standardization (ISO), has been used as a framework to teach networking basics and troubleshoot networking issues for the last 25 years. It has been so influential in network development and architecture that even most of the network communication protocols in use today have a structure that is based on it. But just as the OSI model never fails us, we find that we are lacking a standard that all network security professionals can adhere to, a Network Security Model (NSM). Today's sophisticated and complex networks provide the fundamental need for the NSM.

Network Security Model (NSM) is a seven layer model that divides the daunting task of securing a network infrastructure into seven manageable sections. The model is generic and can apply to all security implementation and devices. The development of the NSM is important because unity is needed in securing networks, just as unity was needed in the architecture of networks with the development of the OSI model. When an attack on a network has succeeded it is much easier to locate the underlying issue and fix it with the use of the NSM.

The NSM will provide a way to teach and implement basic network security measures and devices as well as locate underlying issues that may have allowed an attack to succeed. Traditionally we work from the bottom up to determine which layer has failed on the OSI model, but on the NSM we will work from the top down to determine which layer has failed.

The figure below shows the 7 layers of Network Security Model.

1) Physical
2) VLAN
3) ACL
4) Software
5) User
6) Administrative
7) IT Department

Fig: The Network Security Model

Once the layer of failure is found, we can determine that all of the layers above this layer have also failed. A network security professional will be able to quickly determine if other possible hosts have been compromised with the breech of the layer and how to secure it against the same attack in the future.

In this unit we will be working from the top down describing what each layer is and how the layers of the NSM work together to accomplish complete network security. We will also discuss different types of network security threats.

1.4 NEED OF A NETWORK SECURITY MODEL

A well structured NSM will give the security community a way to study, implement, and maintain network security that can be applied to any network. In study, it can be used as a tool to breakdown network security into seven simple layers with a logical process. Traditional books have always presented network security in an unorganized fashion where some books cover issues that other books may completely neglect. In implementation, it can be used by network architects to insure that they are not missing any important security details while designing a network. In maintaining existing networks it can be used to develop maintenance schedules and lifecycles for the security of the existing network. It can also be used to detect where

breaches have occurred so that an attack can be mitigated.

The NSM is beneficial to all types of professionals. Let us not forget professionals who are transitioning into positions previously held by other network security professionals. Currently, learning what security techniques are implemented on a network and which ones have not can be a daunting task when the basic security structure of the network is unclear. The NSM provides that basic structure. It provides the new professional with the knowledge to discover what has been implemented and what has not been implemented from a security standpoint. Without an NSM, the network security community faces potential chaos as professionals continue to implement their own versions of secure networks without adequate structure.

1.5 FIRST LAYER OF NETWORK SECURITY MODEL: THE PHYSICAL LAYER

1.5.1 What is the Physical Layer?

The physical layer's primary focus is on physical security. Physical security is applied to prevent attackers from accessing a facility to gain data stored on servers, computers, or other mediums. Physical security is the first chosen layer because it is a breaking point for any network. In any scenario providing other devices, such as firewalls, will not help your security if the physical layer is attacked. For this reason we can say that if the layers below the physical layer fail the physical layer has failed as well because the attacker would be able to manipulate data as if they had breached the facility. Physical security comes in many forms including site design, access control devices, alarms, or cameras.

The physical layer is one of the easiest layers to secure because it does not require advanced technical concepts to do so. A company can be hired to install an alarm system, or an employee can be hired to stand as a security guard.

1.5.2 Elements of the Physical Layer

The first form of physical security consists of site design. Site design includes features that are placed on the land around the exterior of the building. Some of these devices include fencing, barbed wire, warning signs, metal or concrete

barriers, and flood lights. These forms of security are not always practical unless the facility contains highly sensitive data.

The second form of physical security consists of access control devices. Access control devices include gates, doors, and locks that are either mechanical or electronic. Locks may seem archaic but they are actually the most cost effective way to increase security. Locked doors should be placed before all areas which can either contain hosts or potentially contain hosts.

The third form of physical security is an alarm. Alarms are one of the most important features to include in the physical network security. This will provide an immediate signal that can alert the CIO or network security administrator as well as the local law enforcement that someone has entered an area that should not have been accessed.

The fourth and final form of physical security is a camera. If someone breaking in sees a camera, they are usually deterred because being caught on camera makes them easy to identify and prosecute by the police. It is the best way to determine how, where, and when physical access was obtained. This can be useful in determining what course of action should be taken in order to mitigate an attack. How many cameras are placed in an area should be determined by the security of that area and the cost. An important area that should always have a camera is the server room.

1.6 SECOND LAYER OF NETWORK SECURITY MODEL: THE VLAN LAYER

1.6.1 What is the VLAN Layer?

The VLAN layer deals with the creation and maintenance of Virtual Local Area Networks. VLANs are used to segment networks for multiple reasons. The primary reason that you make VLANs is to group together common hosts for security purposes. For example, putting an accounting department on a separate VLAN from the marketing department is a smart decision because they should not share the same data. This breaks the network up into less secure and more secure areas. In the next section we will be discussing the implementation of VLANs.

1.6.2 Implementing VLAN Security

The first step in implementing VLANs is to determine public and private networks. Any external facing devices should be put on public VLANs. Examples of this include web servers, external FTP servers, and external DNS servers. The next step is to place internal devices on private VLANs which can be broken up into internal user VLANs and internal server VLANs. The final step is to break down the internal user and server VLANs by department, and data grouping respectively.

1.7 THIRD LAYER OF NETWORK SECURITY MODEL: THE ACL LAYER

1.7.1 What is the ACL Layer?

The ACL layer is focused on the creation and maintenance of Access Control Lists. ACLs are written on both routers and firewalls. ACLs are created to allow and deny access between hosts on different networks, usually between VLANs. This makes them absolutely indispensable in the area of network security. By setting up strong access control lists, a network security professional can stop many attacks before they begin. Setting up ACLs can seem a very daunting task. There are many things to take into consideration such as return traffic or everyday traffic that is vital to operations. These are the most important ACLs that a network security professional creates. If they are not created properly, the ACL may allow unauthorized traffic, but deny authorized traffic.

1.7.2 Implementing ACL Security

The key to creating strong ACLs is to focus on both inbound (ingress) ACLs as well as outbound (egress) ACLs. Small companies can get by with creating very few ACLs such as allowing inbound traffic on port 80 and 443 for HTTP and HTTPS servers. They will also have to allow basic web activity outbound on ports 80, 443, and 53 for HTTP, HTTPS, and DNS respectively. Many other medium to large companies need services like VPN open for partner/vendor companies, and remote users. This can be a difficult task to implement and still maintain a level of security.

1.8 FOURTH LAYER OF NETWORK SECURITY MODEL: THE SOFTWARE LAYER

1.8.1 What is the Software Layer?

The software layer is focused on keeping software up to date with upgrades and patches in order to mitigate software vulnerabilities. Network security professionals should know what software is running on their hosts and what patch level they are currently running at to ensure that if something has happened that they can remove any unwanted software accordingly and know what vulnerabilities currently exist or have existed recently. They should also know what each new patch will do to the system it will be installed on.

1.8.2 Implementing Software Security

Implementing software security includes applying the most current patches and upgrades. This reduces the amount of exploits and vulnerabilities on a specific host and application. Server side software such as HTTP and HTTPS are extremely important internet facing services to keep up to date. User side software should also be kept up to date in order to protect against client-side attacks. In an example, we see a server running a web hosting application. The network security professional must keep the web server application updated to ensure that any new vulnerabilities that are found are mitigated as quickly as possible because the application is accessible at all times.

1.9 FIFTH LAYER OF NETWORK SECURITY MODEL: THE USER LAYER

1.9.1 What is the User Layer?

The user layer focuses on the user's training and knowledge of security on the network. The user should understand basic concepts in network security. They should also learn what applications should not be run or installed on their system; likewise they should have an idea of how their system runs normally. We will cover how their knowledge of network security can assist the network security professional in determining if there is an issue on the network and if so, what that issue possibly

is.

1.9.2   Implementing User Security

The most basic way to implement user security is to train the users on what applications should be avoided and how their computer should run normally. Applications such as Peer-to-Peer can be the difference between an infection and a clean host. As most network security professionals know many types of malware can come preinstalled into Peer-to-Peer clients. However, even more malware can be included in the files and/or applications that are downloaded through the client. Training users with this kind of knowledge can prevent them from potentially compromising a host. Training users on how their system works is important because if they know how their system functions they will be able to detect a problem. For example, if one day their system response time has slowed down the user should notice this activity and alert the network security professional. The network security professional should then check with the user to find out what has changed in order to determine if the host has become compromised or if hardware in the system has become unstable.

1.10   SIXTH LAYER OF NETWORK   SECURITY MODEL: THE ADMINISTRATIVE LAYER

1.10.1   What is the Administrative Layer?

The administrative layer focuses on the training of administrative users. The administrative layer includes all members of management. It is much like the user layer except dealing with a higher level of secure data on the network. Like the user layer, administrative users should be trained on what applications should not be installed on their systems and have an understanding of how their systems run normally. They should also be trained to identify problems with the user layer. Such as recognizing an employee that installs Peer-to-Peer against security policy.

1.10.2   Implementing Administrative Security

Administrators should be trained the same way users are trained but with more in-depth knowledge and skill. It is important that administrators can teach a new employees security practices. Administrators should be able to effectively communicate a user's needs or problems to the network security professional. This

ensures that issues are being resolved as quickly as possible, and that the network security professional is not overloaded with being 'big brother' so to speak of users.

1.11 SEVENTH LAYER OF NETWORK SECURITY MODEL: THE IT DEPARTMENT LAYER

1.11.1 What is the IT Department Layer?

The IT department layer contains all of the network security professionals, network technicians, architects, and support specialists. These are all of the people that make a network operational, and maintain the network, and all of the hosts that reside on that network. The IT department layer is like the administrative layer except the IT department has accounts to access any device on the network. For example, an IT department user can have read, write, and modify access to a database table structure, where an administrator or user only has read, write, and modify access to the records within that table structure.

1.11.2 Implementing IT Department Security

Each person in the IT department layer should have some type of background in network security. The network structure and security policy should be well defined to users in the IT department layer. Minimal training may be necessary for a new employee to learn the structure and design of the network. The IT department is responsible for the implementation and maintenance of all network layers including the physical layer, VLAN layer, ACL layer, software layer, user layer, and the administrative layer. The IT Department should also know as much as it can about its users requests and needs.

1.12 WORKING WITH THE NETWORK SECURITY MODEL

In this unit, we will be examining how to effectively work with the network security model. This will cover the layout of the NSM as well as how attacks against a network can be profiled with the use of the model. We will also discuss how the model can be used to mitigate attacks that have already happened. Finally we will look at how to implement the NSM on a new network.

1.12.1 How the Network Security Model can be used to mitigate an attack?

In this section we will be looking at how the Network Security Model can be used to mitigate an attack that has already happened. Since the attack is directed at the software layer, this is the layer that has been compromised. We will need to go through the layers from the top to the bottom to mitigate the attack.

1.12.1.1 Initial Mitigation

We start with the physical layer by removing the infected host and determining what malware is running on the system by running root kit detectors as well as checking anti-virus software. We also look to see if there was a physical break-in to see if the attacker may have infected any other hosts at the same time. Once this process has been completed we should look at the specific VLAN the host resided on. Here we also look for other hosts that could be infected. We will mitigate these hosts the same as the original host, each host that is possibly compromised should be isolated from the network and scanned for possible malware. Next we should look at the ACLs used on the router/firewall to see if this host could have infected any other networks. If the ACLs do not block this activity to other VLANs, those VLANs should be investigated to see which hosts, if any, are infected.

1.12.1.2 Long-Term Mitigation

Now we begin looking into long-term mitigation, this means that we should be looking at what failed and what should be fixed so the issue does not happen again. Since the Software layer was the actual layer which failed; we will start by looking into this layer. Was an update available which could have prevented this attack? If so, we should attempt to push out the update in order to mitigate this type of attack from happening again. We should make sure all machines are updated with the most current patches. Next we should be looking into the ACL layer to see if an ACL could have prevented this attack. If so, we should put this ACL in to make sure that any other attempts on other hosts which may not be patched yet do not occur.

Next we will look at the VLAN layer to see if something should be changed in the VLANs which can prevent a network wide outbreak. This would also include checking to see if VLANs could have protected servers from the attack. All VLANs

should be re-evaluated and reconfigured. Finally, the physical security should be checked; did this the host get compromised by a physical break-in? If so, how can these are prevented in the future?

1.13 INTRODUCTION TO NETWORK SECURITY THREATS

Worms, Trojan horses, and DoS, also known as denial of service types of attacks are usually utilized malevolently to destroy and consume a given network's resources. At times, poorly configured hosts and accompanying servers act like threats to network security, since they do eat up available resources for no good reason.

To be capable of correctly identifying and mitigating such potential threats, a person, company, or other organization has to be ready with the proper security protocols and tools to do the job. A number of the most efficient means for finding and eliminating these types of threats are explored below. It's a dangerous world out there in the World Wide Web. Just as your mother may have told you to never talk to strangers, the same advice holds true for the virtual world. You may know to be wary of giving strangers your business bank account details. But can you be sure the website you're logging into is that of your bank and not a forgery created by a cybercriminal? Cybercriminals use many different methods to lure you into parting with your confidential personal or business information. As a small company doing business on the web, you need to be aware of these methods so you can be extra vigilant when online.

1.14 NETWORK SECURITY THREATS

Network security threats fall into two categories

   1. Passive threats

 (a) Release of message contents

 (b) Traffic analysis

   2. Active threats

 (a) Masquerade

 (b) Replay

(c) Modification of message contents

(d) Denial of service

Passive threats, sometimes referred to as eavesdropping dropping, involve attempts by an attacker to obtain information relating to communication.

(a) Release of message contents

- A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information.

- We would like to prevent the opponent from learning the content of these transmissions.

(b) Traffic analysis

- It is a kind of attack done on encrypted messages.

- The opponent might be able to observe the pattern of such encrypted message.

- The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.

Active threats involve some modification of the data stream or the creation of a false stream.

(a) Masquerade

- It takes place when one entity pretends to be a different entity.

- A masquerade attack usually includes one of the other forms of active attack.

- For *e.g.* authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
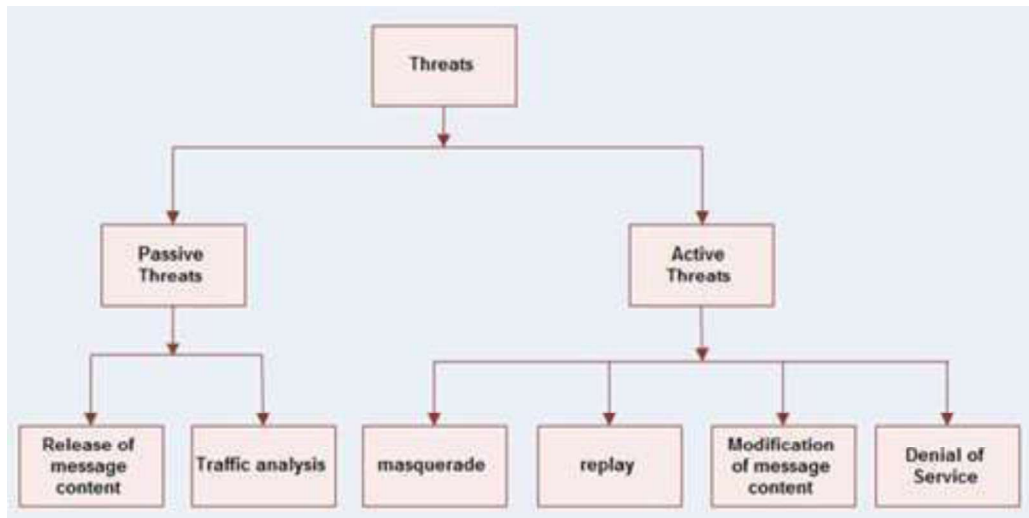
Fig: Types of Security Threats

(b) Replay

- It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

(c) Modification of message

- It means that some position of a message is altered, or that messages are delayed or rendered, to produce an unauthorized effect.

(d) Denial of service (DOS)

- A denial of service attack takes place when the availability to a resource is intentionally blocked or degraded by an attacker.

- In this way the normal use or management of communication facilities is inhibited.

- This attack may have a specific target. For *e.g.* an entity may suppress all messages directed to a particular destination.

- Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

1.15 SECURITY THREAT INVOLVES THREE GOALS

1. Confidentiality

2. Integrity

3. Availability

Confidentiality

This goal defines how we keep our data private from eavesdropping. Packet capturing and replaying are the example threats for this goal. Data encryption is used to achieve this goal.

Integrity

This goal defines how we avoid our data from being altered. MiTM (Man in the middle attacks) is the example threat for this goal. Data hashing is used to take the fingerprint of data. Through hashing we can match data from its original source.

Availability

This goal defines how we keep available data to our genuine users. DoS (Denial of service attacks) are the example threat for this goal. User rate limit and firewall are used to mitigate the threat for this goal.

1.16 TYPES OF NETWORK SECURITY THREATS

According to IT Security.com the following are ten of the biggest network threats:

1. **Viruses and Worms:** A virus is a malicious computer program or programming code that replicates by infecting files, installed software or removable media. Whereas a worm is a program or script that replicates itself and moves through a network, typically travelling by sending new copies of itself via email.

2. **Trojan Horses:** The Trojan horse at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Some Trojans are designed to be more annoying than or they can cause serious damage by deleting files and destroying information on your system.

3. **SPAM:** Spam is any kind of unwanted online communication.

4. Phishing: Phishing is the attempt to acquire sensitive information such as

usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

5. **Packet Sniffers:** Computer network administrators have used packet sniffers for years to monitor their networks and perform diagnostic tests or troubleshoot problems.

6. **Maliciously Coded Websites:** Malicious code is the term used to describe any code in any part of a software system that is intended to cause security breaches or damage to a system.

7. **Password Attacks:** Password attacks are the classic way to gain access to a computer system is to find out the password and log in.

8. **Zombie Computers and Botnets:** In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or Trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread E-Mail spam and launch denial of service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

1.17 TYPES OF NETWORK SECURITY ATTACKS

Network security attacks can be of the following types.

Reconnaissance Attack

In this kind of attack, an adversary collects as much information about your network as he needed for other attacks. This information includes IP address range, server location, running OS, software version, types of devices etc. Packet capturing software, Ping command, traceroot command, whois lookup are some example tools which can be used to collect this information. Adversary will use this information in mapping your infrastructure for next possible attack.

Passive attack

In this attack an adversary deploys a sniffer tool and waits for sensitive information to be captured. This information can be used for other types of attacks. It includes

packet sniffer tools, traffic analysis software, filtering clear text passwords from unencrypted traffic and seeking authentication information from unprotected communication. Once an adversary found any sensitive or authentication information, he will use that without the knowledge of the user.

Active Attack

In this attack an adversary does not wait for any sensitive or authentication information. He actively tries to break or bypass the secured systems. It includes viruses, worms, Trojan horses, stealing login information, inserting malicious code and penetrating network backbone. Active attacks are the most dangerous in natures. It results in disclosing sensitive information, modification of data or complete data lost.

Distributed Attack

In this attack an adversary hides malicious code in trusted software. Later this software is distributed to many other users through the internet without their knowledge. Once end user installs infected software, it starts sending sensitive information to the adversary silently. Pirated software is heavily used for this purpose.

Insider Attack

According to a survey more than 70% attacks are insider. Insider attacks are divided in two categories; intentionally and accidentally. In intentionally attack, an attacker intentionally damage network infrastructure or data. Usually intentionally attacks are done by disgruntled or frustrated employees for money or revenge. In accidentally attack, damages are done by the carelessness or lack of knowledge.

Phishing Attack

Phishing attack is gaining popularity from last couple of years. In this attack an adversary creates fake email address or website which looks like a reputed mail address or popular site. Later attacker sends email using their name. These emails contain convincing message, some time with a link that leads to a fake site. This fake site looks exactly same as original site. Without knowing the truth user tries to log on with their account information, hacker records this authentication information and uses it on real site.

Hijack attack

This attack usually takes place between running sessions. Hacker joins a running session and silent disconnects other party. Then he starts communicating with active parties by using the identity of disconnected party. Active party thinks that he is talking with original party and may send sensitive information to the adversary.

Spoof attack

In this kind of attack an adversary changes the sources address of packet so receiver assumes that packet comes from someone else. This technique is typically used to bypass the firewall rules.

Buffer overflow attack

This attack is part of DoS technique. In this attack an adversary sends more data to an application than its buffer size. It results in failure of service. This attack is usually used to halt a service or server.

Exploit attack

Exploit attack is used after Reconnaissance attack. Once an attacker learned from reconnaissance attack that which OS or software is running on target system, he starts exploiting vulnerability in that particular software or OS.

Password attack

In this attack an adversary tries to login with guessed password. Two popular methods for this attack are dictionary attack and brute force attack. In brute force method, an adversary tires with all possible combinations. In dictionary method, an adversary tires with a word list of potential passwords.

Packet capturing attack

This attack is part of passive attack. In this attack an attacker uses a packet capturing software which captures all packets from wire. Later he extracts information from these packets. This information can be used to deploy several kinds of other attacks.

Ping sweep attack

In this attack an attacker pings all possible IP addresses on a subnet to find out which hosts are up. Once he finds an up system, he tries to scan the listening ports.

From listing ports he can learn about the type of services running on that system. Once he figures out the services, he can try to exploit the vulnerabilities associated with those services.

DNS Query attack

DNS queries are used to discover information about public server on the internet. All OS includes the tool for DNS queries such as nslookup in Windows, Dig and Host in Linux. These tools query a DNS server for information about specified domain. DNS server respond with internal information such as Server IP address, Email Server, technical contacts etc. An adversary can use this information in phishing or ping attack.

MiTM attacks

In this attack an adversary captures data from middle of transmission and changes it, then send it again to the destination. Receiving person thinks that this message came from original source. For example in a share trading company Jack is sending a message to Rick telling him to hold the shares. An adversary intercepts this message in way that it looks like Jack is telling for sell. When Rick receives this message, he will think that Jack is telling for the sell and he will sell the shares. This is known as Man in the middle attack.

Denial of Service Attacks

DoS attack is a series of attacks. In this attack an adversary tires to misuse the legitimate services. Several networking tools are available for troubleshooting. An attacker uses these tools for evil purpose. For example ping command is used to test the connectivity between two hosts. An adversary can use this command to continuously ping a host with oversized packets. In such a situation target host will be too busy in replying (of ping) that it will not be able run other services.

Mitigating security threats

- To protect network from above attacks, administrators use different approaches. No matter what approach you choose, there are some basic rules which you should always follow:- Use secure protocol for remote login such as use SSH instead of Telnet.

- Configure access lists or firewall to permit only necessary traffic.

- Use genuine software and keep it up to date.

- Avoid pirated software as they may contain virus and worms.

- Use difficult password.

- Disable unwanted or unnecessary services.

Beside these essential steps you can also consider a security device or software as per network requirements. There are several thousands of security solutions are available in market to choose from.

1.18 LET US SUM UP

Currently there is no full prove model for network security; this unit has explained a possible Network Security Model as discussed in the literature which will allow general network security to be implemented and maintained by any size company. This is a framework and each layer can be modified to include company specific issues and details.

Network Security is a very broad field and being a Network Security manager is not an easy job. There are still threats such as password attacks that have no prevention. Many of the threats set out to get personal information. In some attacks, the attacker tries to break the security systems through stealth, viruses, worms, or Trojan horses. In attacks like phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank and thus fools the user and retrieves the information.

1.19 FURTHER READINGS

1. William Stallings, Cryptography and Network Security-Principles and Practices", Prentice-Hall of India.

2. Information Security Assurance: Framework, Standards & Industry Best Practices (PGDCS-05), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security

3. Information System (PGDCS-06), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

4. Joshua Backfield, John Bambenek, Network Security Model, "the definition of a Network Security model", © SANS Institute 2008

5. http://www.networkmonitoring.org/network-security-threats/

6. http://ecomputernotes.com/computernetworkingnotes/security/net work-security-threats

7. http://blogs.cisco.com/smallbusiness/the-10-most-common- security-threats-explained

8. http://www.computernetworkingnotes.com/ccna-study- guide/network-security-threat-and-solutions.html

1.20 ASSIGNMENTS

1. Write the functions of Administrative Layer in the Network Security Model.

2. Write the functions of VLAN Layer in the Network Security Model.

3. Classify different categories of security threats.

4. Discuss different types of Network security threats.

5. Name and explain different types of Network security attacks.

Unit 2: Firewalls

<div style="text-align: right;">**2**</div>

UNIT STRUCTURE

2.1 LEARNING OBJECTIVES

After going through this unit, you will able to:

- Know about a Firewall and its types.

- Know how to prevent your network from anonymous attack.

- Understand the working of Firewall in Windows 7

- Know how to access the Windows Firewall with Advanced Security

- Know the Inbound & Outbound Rules

- Know the Connection Security rules.

- Know the functions of Hardware and Network Firewall

2.2 INTRODUCTION

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Routers that pass data between networks contain firewall components and can often perform basic routing functions as well; Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network.

2.3 OVERVIEW OF FIREWALL

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside

network, such as the Internet, that is assumed to not be secure or trusted. A firewall is a protective system that lies, in essence, between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network. Without a firewall, all the traffic directly moves from the Internet to your computer. In this diagram, the "valid" traffic is coloured green, and the "malicious" traffic is coloured red.
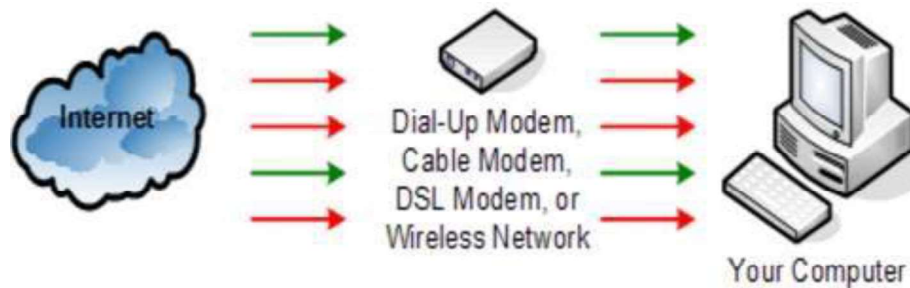

Fig: A firewall

The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It ignores information that comes from unsecured, unknown or suspicious location.

A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world. Windows Firewall adds an additional level of security by examining each piece of data. If the data is good, it passes through the firewall and reaches the computer. If the data is identified as bad traffic, the network packets are simply dropped and never make their way to the computer. Although this diagram shows the Window Firewall as a separate icon, the Windows Firewall is software that physically runs on your computer.
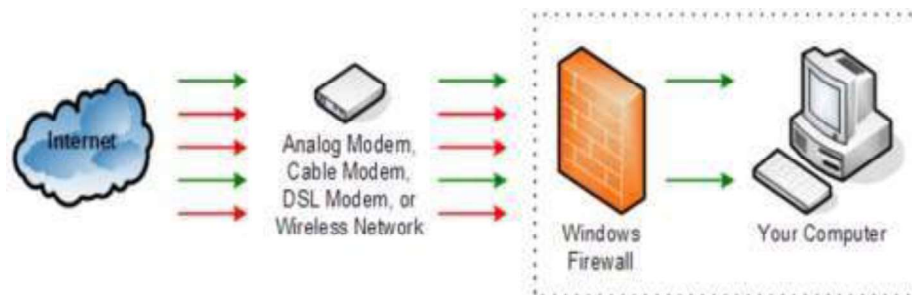

Fig: Firewall in an organization

As this diagram shows, Windows Firewall intercepts all network communication to provide protection against unauthorized network traffic. This protection exists if this traffic enters your computer through a modem, a wired network adapter, or a wireless network connection. Windows Firewall protects your computer regardless of its connection to the Internet!

2.4 TYPES OF FIREWALLS

There are different types of firewalls depending on where the communication is going on, where we need to intercept the communication tracing the state.

a. **Network layer/Packet filters:** Network layer firewalls, also called packet filters. They operate at a comparatively low level of the TCP/IP protocol stack, which doesn't allow packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. Network layer firewalls consists of two sub-categories, stateful and stateless. Stateful firewalls maintain records about active sessions, and use that "state information" to speed packet processing. Stateless firewalls require less memory, and can be faster for simple filters which require less time to filter than to look up a session. It should also be necessary for filtering stateless network protocols that have no concept of a session.

b. **Application-layer:** Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets which are travelling towards or from an application and they block other packets (usually dropping them without acknowledgment to the sender). The function of application firewalls to determine whether a process should accept any given connection. Application firewalls achieve their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. The type of application firewalls which hook into socket calls are also referred to as socket filters. Application firewalls works more like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a port basis. Generally, prompts are used to define rules for

processes that have not yet received a connection. It is rare to find out application firewalls not combined or used in conjugation with a packet filter.

c. **Proxies:** A proxy server (running either on dedicated hardware or as software on a general-purpose machine) will act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific application on network, in the sense that it functions as a proxy interface on behalf of the network user.

d. **Network address translation:** Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of hosted protected. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defence against network reconnaissance.

2.5 SOFTWARE BASED FIREWALLS

Software-based or "personal" firewalls are often the last line of defense between you and the Internet. Software Firewall is a piece of software that is installed on your computer in order to protect it from unauthorized access. Modern software firewalls use a combination of port filtering, stateful packet inspection and application level filtering. Such firewalls are provided for each machine as part of the operating system – as in the case of Windows, for example – or as an application designed to run on a stand- alone PC that guards the entire network.

A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on your system.
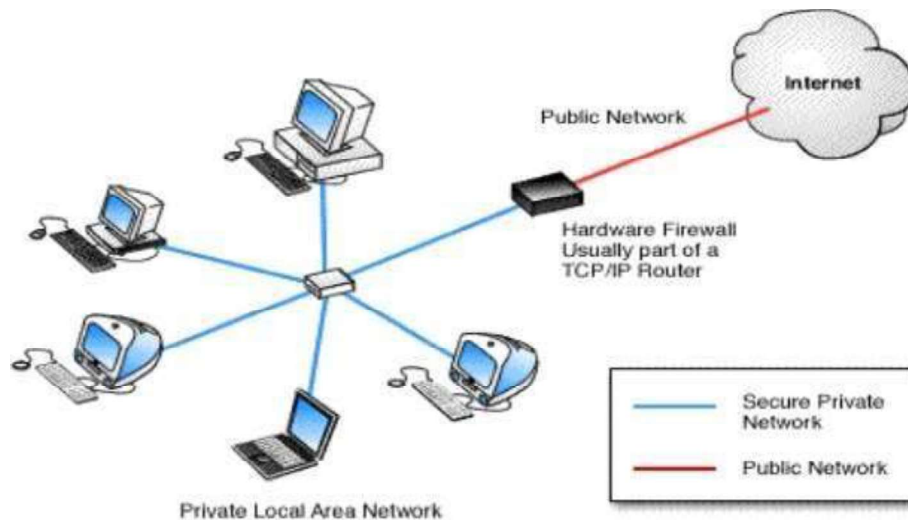

Fig: A software firewall

A good software firewall will run in the background on your system and use only a small amount of system resources. It is important to monitor a software firewall once installed and to download any updates available from the developer. Personal firewalls have the advantage of identifying which applications on the computer are creating security risks. If a worm infects your system and attempts to open your computer to the world, a software-based firewall will identify this new application service. The personal firewall will prompt you to confirm the new application or to prevent its use. Your personal firewall may be your first warning that a malicious program is attempting to use the network.

2.6 HARDWARE BASED FIREWALLS

A hardware firewall uses a PC-like appliance to run software that blocks unwanted outside traffic. Hardware firewalls can be purchased as a stand- alone product but more recently hardware firewalls are typically found in broadband routers, and

should be considered an important part of your system and network set-up, especially for anyone on a broadband connection. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

A firewall appliance may allow the firewall administrator to simply drag and drop various rules into place. For example, if your business wishes to block all incoming traffic from particular top level domains (TLD's), such as particular country codes, a few clicks will give the option of blocking incoming, outgoing or both types of traffic to/from those TLD's. Likewise, if a given user group – perhaps your tech support operation – needs to run Microsoft Remote Desktop Connection (RDC) to assist users on another network, that entire group can be dragged and dropped into an —authorized users‖ category while the RDC application can be dropped into an

—authorized application‖ category.

A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

Hardware Firewall are typically good for small or medium business owners, with 5 or more PC or a co-operate environment. The main reason is that it then becomes cost-effective, because if you purchase Internet Security/Firewall software licenses for 10 to 50 copies, and that too on an annual subscription basis, it will cost a lot of money and deployment could also be an issue. The users will have better control over the environment. If the user is not tech savvy and if they choose to inadvertently allow a connection that has Malware behaviour, it could ruin the entire network and put the company in risk with data security.

2.7 HOW TO PREVENT YOUR NETWORK FROM ANONYMOUS ATTACK

A professional knows where to draw the line and how far she can push the network without breaking it. Be aware of the mythical "your network is secure" statement.

With alarming frequency, security consultants will leave you with a report that claims that your network is secure, based on the fact that they were unable to get into anything. This certainly does not mean your network is secure! It only means they couldn't find a way to break it, but someone else still could.

In spite of vulnerabilities, new solutions which are digital nowadays can improve operations, enhance the customer experience and encourage the bottom line. It's not necessary or cost- effective to put non-payment solutions on a separate physical network to isolate them from cardholder data.

These six measures can help in securing cardholder information while allowing normal network data flow:

1. **Never click on a link which was not expected by you to receive:** One of the important rules. The main way criminals infect PCs with malware is by tempting users to click on a link or open an attachment. "Most of the time phishing emails contain obvious spelling mistakes and poor grammar and are easy to spot," says Sideway of Integrals.

2. **Use different passwords on different websites:**

   If individuals typically having up to 100 online accounts, the tendency has become to share one or two passwords across accounts or use very simple ones, such as loved ones' names, pets names or favourite sports teams and many more common terms.

3. **Avoid reusing your main email/accounts password:** Any hacker who has cracked or anyhow get entered into your main email password has the keys to your [virtual] kingdom because passwords from the other sites you visit can be reset via your main email account.

4. **Use updated antivirus and Conduct regular scans of your entire network:** The best way to determine if your systems have been compromised is to scan them regularly for vulnerabilities. For relatively low budget, a security vendor will remotely scan all of your external systems/access points to determine if any of them are vulnerable to intrusion.

5. **Limit remote access and make some rules:** Most of the organizations leave their firewalls open to outsider's entry by mangers who are working remotely or vendors who routinely perform maintenance on systems. Create strong passwords instead of

using the default ones, and change them after a particular set of time. Similarly, always change default firewall settings to allow only necessary access, and limit remote access to secure methods such as VPN.

6. **Ensure all sensitive data is encrypted using a strong encryption algorithm:** If you have older POS equipment that sends raw credit card data to a back-office server, it's time to upgrade that equipment. Modern, secure POS systems encrypt credit card data as soon as a card is swiped, and they immediately send that data to the payment processor without any temporary storing of data. Double- check your POS system to make sure it complies with PCI standards.

7. **Maintain a strong firewall for securing your network:** The PCI data security standards prescribe firewalls for compliance. Make sure your firewall is hardened according to new rules and updated with recent intruder's definition and is supported by virus protection software.

8. **Segment your network into necessary divisions:** For example, make sure your POS data traffic is separate from your Wi-Fi system, security cameras, digital menu boards, other connections, etc. If you want to enable managers to connect to the POS via Wi-Fi, connect them through a virtual LAN that differentiates authorized traffic into a security zone.

9. **Keep your software updated/upgraded with latest updates:** Manufacturers frequent update their operating systems and POS software to tighten security and eliminate the weaknesses vulnerable to hackers. Make sure you have downloaded the latest operating system patches and keep all POS software up-to-date.

10. **System Hardening:** This can also be referred as lockdown or security tightening, and involves activities such as configuring software for optimum use, deactivating unnecessary software that can lead to some simple attacks, and configuring the operating system for optimum security. Usually the system-hardening process is carried out in a mannered step by step approach to iteratively increase the number of defensive layers and reduce the exposed attack surfaces.

2.8 CONFIGURING FIREWALL IN YOUR COMPUTER

2.8.1 How to Configure Your Mac's Firewall

Every Mac ships with a built-in firewall - a service that can be configured to disallow information from entering your Mac. But what is a firewall, and why do you need to use it on your Mac?

Every time you request information from the Internet, such as a web page or email message, your Mac sends data packets to request the information. Servers receive the packets, and then send other packets back to your Mac.

This all happens in a matter of seconds. Once your Mac has reassembled the packets, you'll see something, like an email message or web page.

A firewall can help prevent bad packets from entering your Mac. Hackers love to run automated applications that can scan thousands of computers (including your Mac) for open ports that can be exploited. To ensure that random individuals do not gain unauthorized access to your Mac, you should enable Mac OS X's built-in firewall. It will close your Mac's open ports and disallow random network scans.

2.8.1.1 Turning on and Configuring the Mac OS X Firewall

Here's how to turn on and configure your Mac's built-in firewall:

1. From the Apple menu, select System Preferences. The window shown below appears.
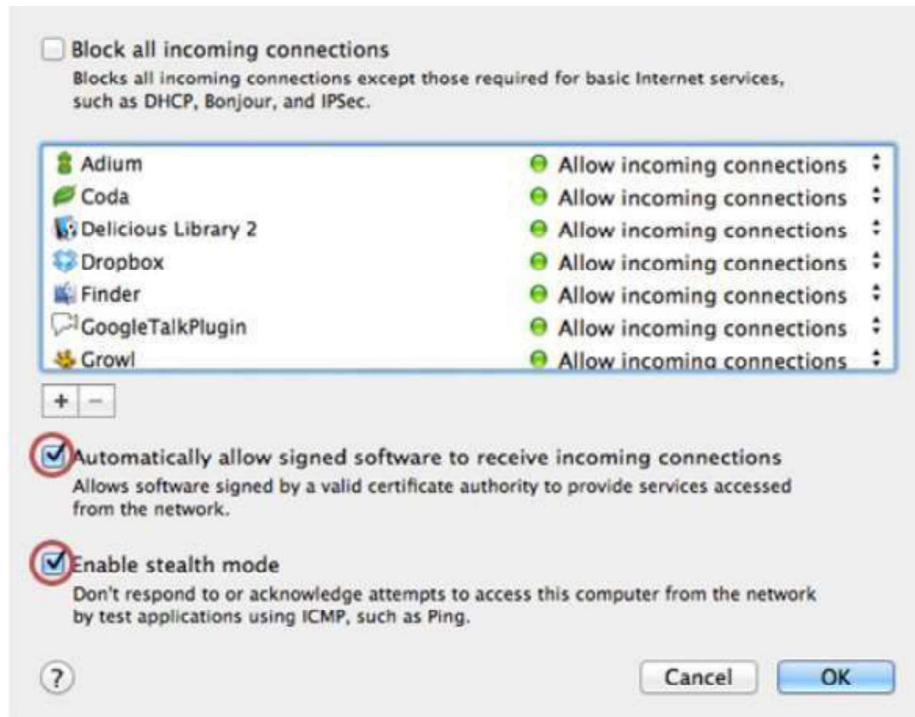
2. Select Security & Privacy.

3. Click the Firewall tab.

4. Click the lock icon and authenticate with your administrator username and password. The window shown below appears.
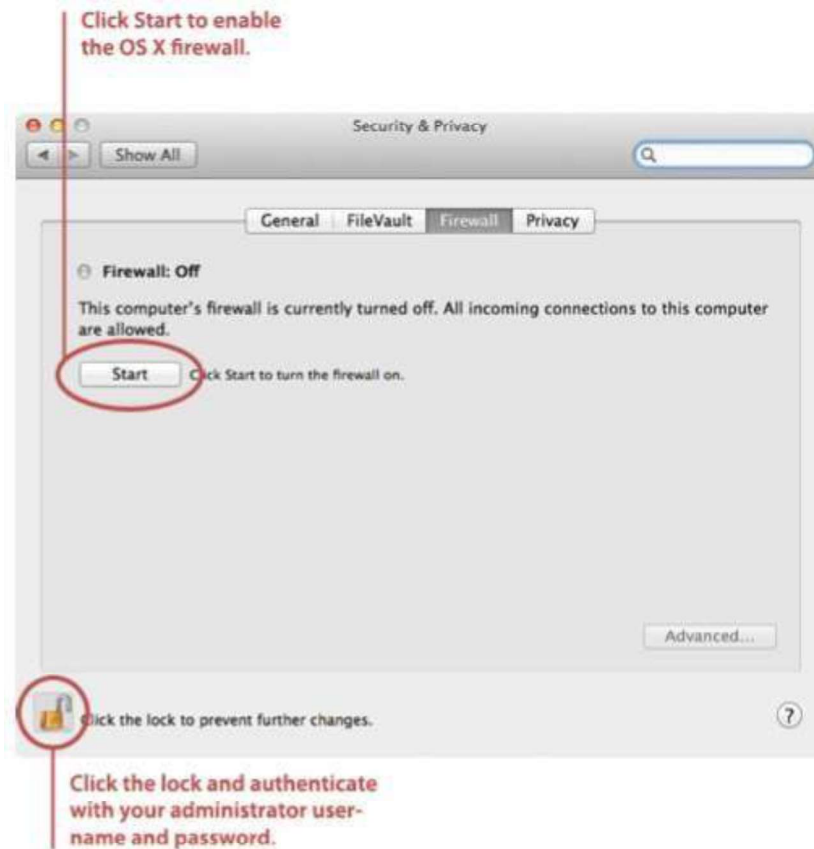
5. Click Start. The firewall turns on - you'll know it's enabled when you see the green light and the Firewall: On message, as shown below.

6. Click Advanced. The window shown below appears.

7. Select the automatically allow signed software to receive incoming connections checkbox. This allows the applications on your Mac to communicate with the outside world.

8. Select the Enable stealth mode checkbox. This prevents your Mac from responding to port scans and ping requests.

9. Click OK to close the advanced settings.

10. Close System Preferences. Your Mac is now protected by the built-in firewall!

2.8.2   Working with Windows Firewall in Windows 7

2.8.2.1   Firewall in Windows 7

Windows 7 comes with two firewalls that work together. One is the Windows Firewall, and the other is Windows Firewall with Advanced Security (WFAS). The main difference between them is the complexity of the rules configuration. Windows Firewall uses simple rules that directly relate to a program or a service. The rules in WFAS can be configured based on protocols, ports, addresses and authentication. By default, both firewalls come with predefined set of rules that allow us to utilize

network resources. This includes things like browsing the web, receiving e-mails, etc.

Other standard firewall exceptions are File and Printer Sharing, Network Administration, Windows Discovery, Performance Remote Logs Management, Remote and Alerts, Remote Assistance, Remote Desktop, Windows Media Player, Windows Media Player Network Sharing Service. With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically blocked.

Sometimes we will see a notification about a blocked program which is trying to access network resources. In that case we will be able to add an exception to our firewall in order to allow traffic from the program in the future.

Windows 7 comes with some new features when it comes to firewall. For example, "full-stealth" feature blocks other computers from performing operating system fingerprinting. OS fingerprinting is a malicious technique used to determine the operating system running on the host machine. Another feature is "boot-time filtering". This feature ensures that the firewall is working at the same time when the network interface becomes active, which was not the case in previous versions of Windows.

When we first connect to some network, we are prompted to select a network location. This feature is known as Network Location Awareness (NLA). This feature enables us to assign a network profile to the connection based on the location. Different network profiles contain different collections of firewall rules. In Windows 7, different network profiles can be configured on different interfaces. For example, our wired interface can have different profile than our wireless interface. There are three different network profiles available:

- Public

- Home/Work - private network

- Domain - used within a domain

We choose those locations when we connect to a network. We can always change the location in the Network and Sharing Centre, in Control Panel. The Domain profile can be automatically assigned by the NLA service when we log on to an Active

Directory domain. Note that we must have administrative rights in order to configure firewall in Windows 7.

2.8.2.2 Configuring Windows Firewall

To open Windows Firewall we can go to **Start > Control Panel > Windows Firewall**.


By default, Windows Firewall is enabled for both private (home or work) and public networks. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature trough Windows Firewall" option.

Exceptions

To change settings in this window we have to click the "Change settings" button. As you can see, here we have a list of predefined programs and features that can be allowed to communicate on private or public networks. For example, notice that the
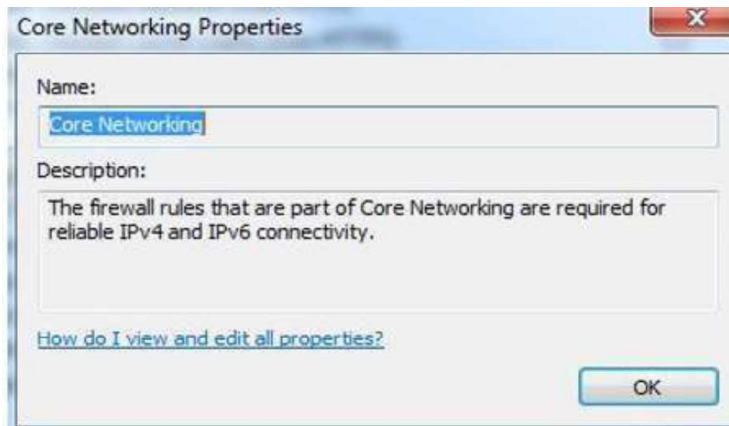
Core Networking feature is allowed on both private and public networks, while the File and Printer Sharing is only allowed on private networks. We can also see the details of the items in the list by selecting it and then clicking the Details button.

Details

If we have a program on our computer that is not in this list, we can manually add it by clicking on the "Allow another program" button.
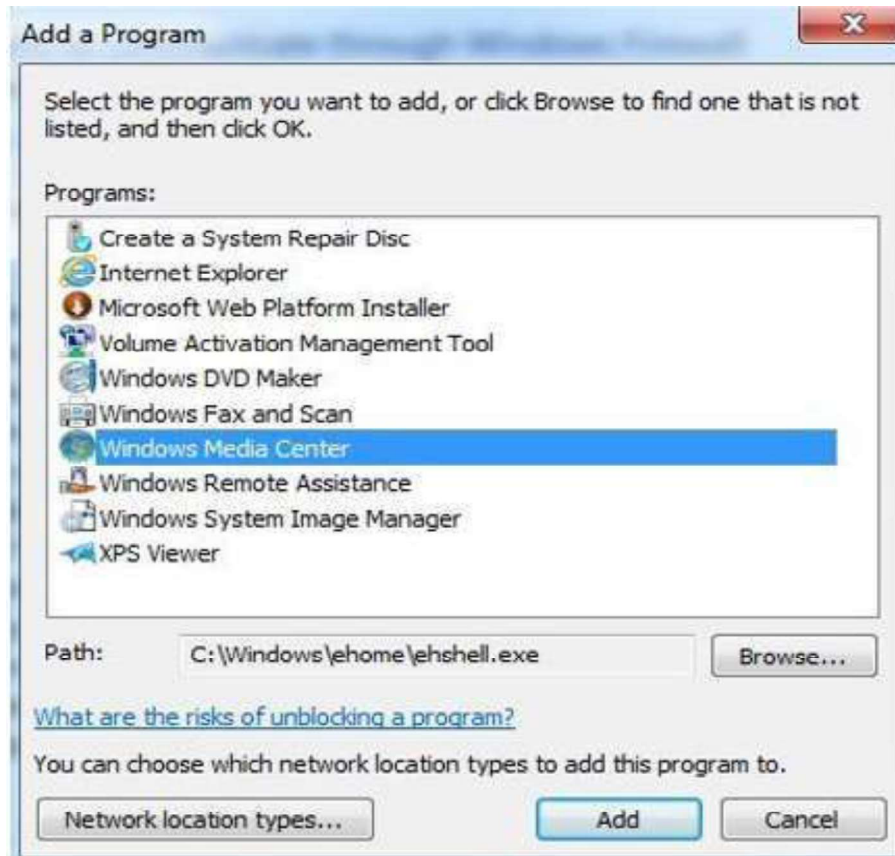
Add a Program

Here we have to browse to the executable of our program and then click the Add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button.

Network Locations

Many applications will automatically configure proper exceptions in Windows Firewall when we run them. For example, if we enable streaming from Media Player, it will automatically configure firewall settings to allow streaming. The same thing is if we enable Remote Desktop feature from the system properties window. By enabling Remote Desktop feature we actually create an exception in Windows Firewall.

Windows Firewall can be turned off completely. To do that we can select the "Turn Windows Firewall on or off" option from the menu on the left.

Firewall Customization

Note that we can modify settings for each type of network location (private or public). Interesting thing here is that we can block all incoming connections, including those in the list of allowed programs.

Windows Firewall is actually a Windows service. As you know, services can be stopped and started. If the Windows Firewall service is stopped, the Windows Firewall will not work.

Firewall Service

In our case the service is running. If we stop it, we will get a warning that we should turn on our Windows Firewall.

Warning

Remember that with Windows Firewall we can only configure basic firewall settings, and this is enough for most day-to-day users. However, we can't configure exceptions based on ports in Windows Firewall any more. For that we have to use Windows Firewall with Advanced Security, which will be covered in next section.

2.8.3 How to Start & Use the Windows Firewall with Advanced Security

The Windows Firewall with Advanced Security is a tool which gives you detailed control over the rules that are applied by the Windows Firewall. You can view all the rules that are used by the Windows Firewall, change

their properties, create new rules or disable existing ones. In this tutorial we will share how to open the Windows Firewall with Advanced Security, how to find your way around it and talk about the types of rules that are available and what kind of traffic they filter.

2.8.3.1 How to Access the Windows Firewall with Advanced Security

You have several alternatives to opening the Windows Firewall with Advanced Security: One is to open the standard Windows Firewall window, by going to **"Control Panel -> System and Security -> Windows Firewall".**

Then, click or tap Advanced settings.
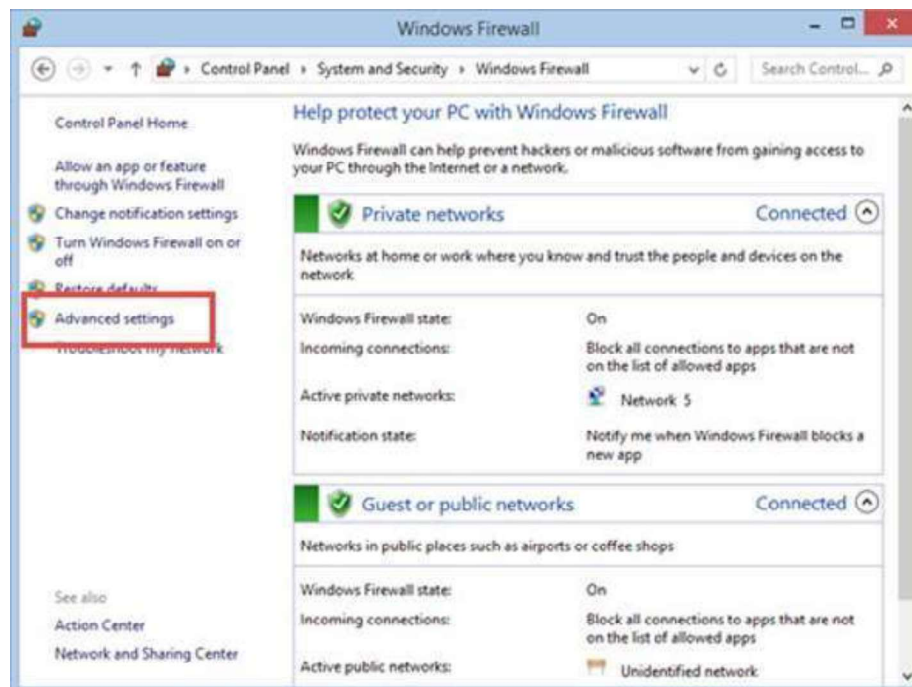
In Windows 7, another method is to search for the word firewall in the Start Menu search box and click the "Windows Firewall with Advanced Security" result.

In Windows 8.1, Windows Firewall with Advanced Security is not returned in search results and you need to use the first method shared above for opening it.
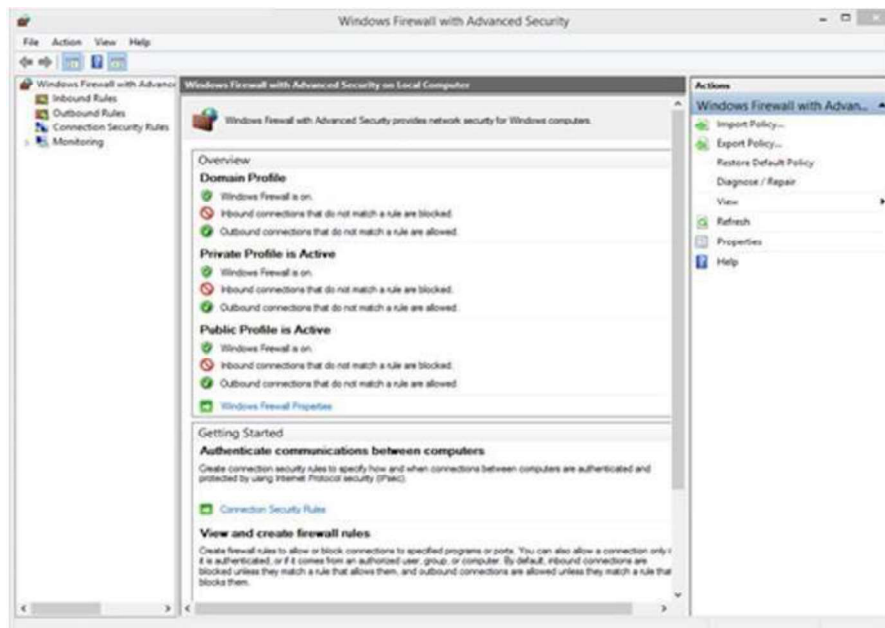
The Windows Firewall with Advanced Security looks and works the same both in Windows 7 and Windows 8.1. To continue our tutorial, we will use screenshots that were made in Windows 8.1.

2.8.3.2 What Are The Inbound & Outbound Rules?

In order to provide the security you need, the Windows Firewall has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are connected to.

Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computer to the network or the Internet.

These rules can be configured so that they are specific to: computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to. In the Windows Firewall with Advanced Security, you can access all rules and edit their properties. All you have to do is click or tap the appropriate section in the left-side panel.
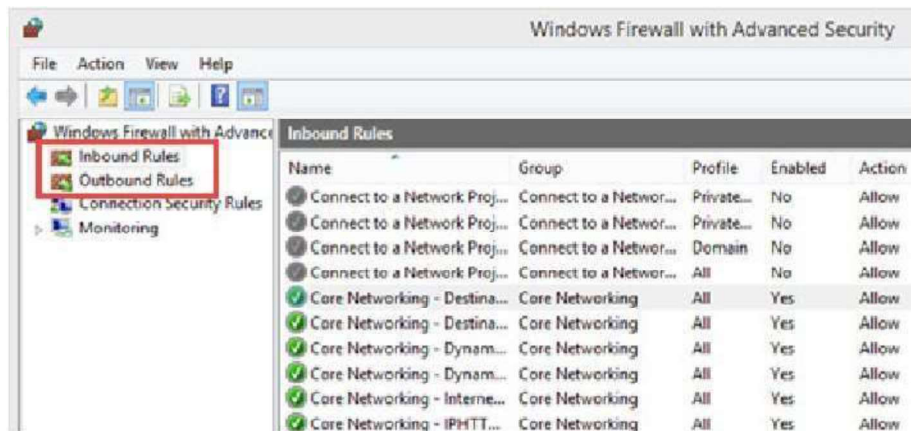
The rules used by the Windows Firewall can be enabled or disabled. The ones which are enabled or active are marked with a green check-box in the Name column. The ones that are disabled are marked with a gray check- box.

If you want to know more about a specific rule and learn its properties, right click on it and select Properties or select it and press Properties in the column on right, which lists the actions that are available for your selection.
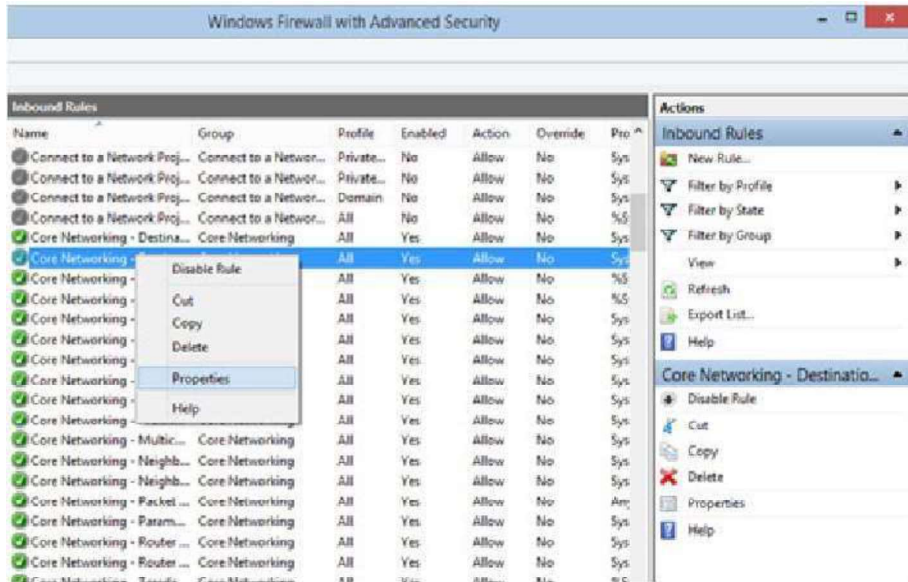
In the Properties window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.
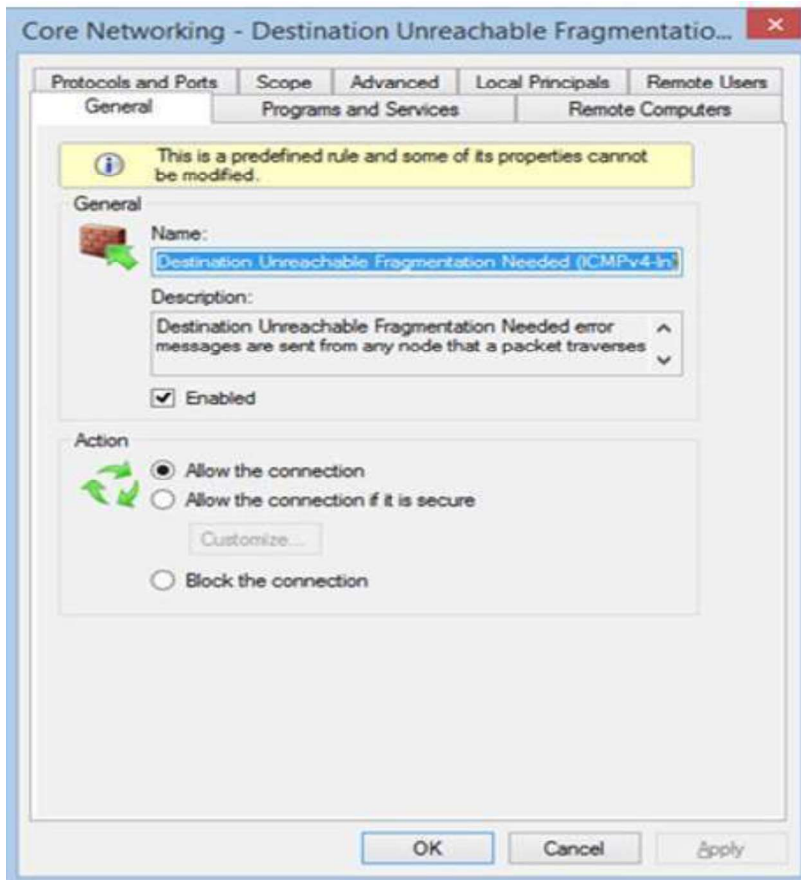
2.8.3.3 What are the Connection Security Rules?

Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted.

Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled. If you want to see if there are any such rules on your computer, click or tap "Connection Security Rules" on the panel on the left. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator.

2.8.3.4   What does the Windows Firewall with Advanced Security Monitor?

The Windows Firewall with Advanced Security includes some monitoring features as well. In the Monitoring section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.
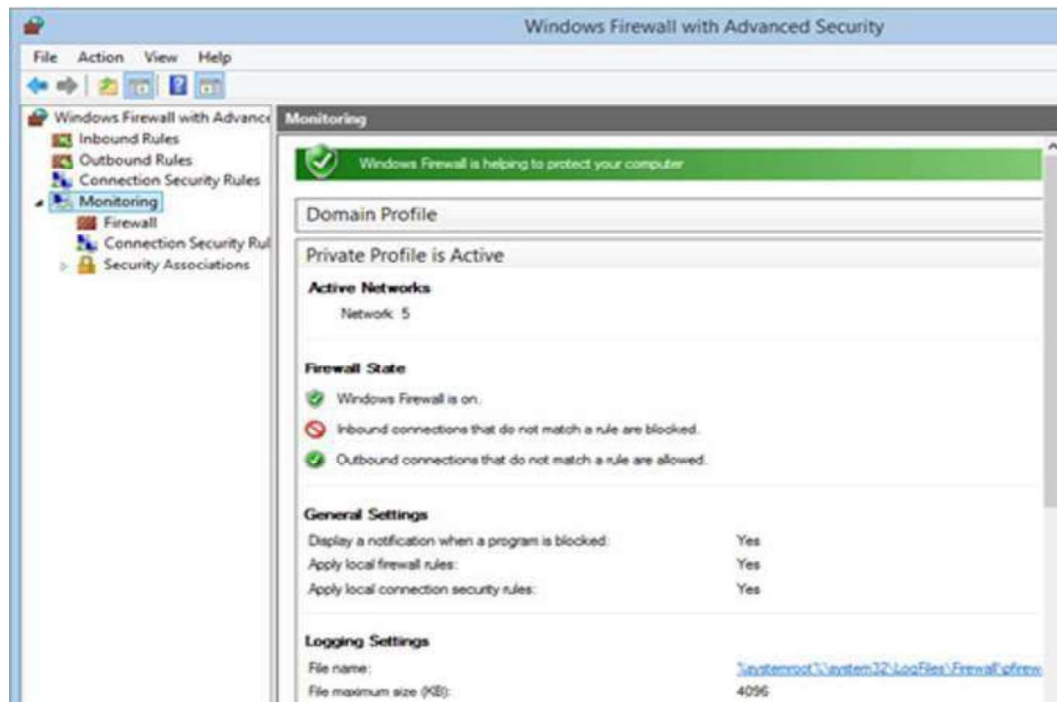
You should note that the Monitoring section shows only the active rules for the current network location. If there are rules which get enabled for other network locations, you will not see them in this section.

The above section discussed on how to setup a firewall on two Operating Systems viz. Windows and Mac. Linux have many varients therefore it is not possible to discuss how to configure firewall on Linux. There are some links in the Recommended Videos section which discuss the procedure of setting up firewall in various variant of Linux.

Activity

1. Setup and configure a firewall in your system.

2. Find some of the free and commercially available firewalls over internet.

2.9 HARDWARE AND NETWORK FIREWALL

Network firewalls prevent unknown programs and processes from accessing the system. However, they are not antivirus systems and make no attempt to identify or remove anything. They may protect against infection from outside the protected computer or network, and limit the activity of any malicious software which is present by blocking incoming or outgoing requests on certain TCP/IP ports. A firewall is

designed to deal with broader system threats that come from network connections into the system and is not an alternative to a virus protection system.

2.10 PARTITIONING AND PROTECTING NETWORK BOUNDARIES WITH FIREWALLS

Besides the basic physical security of a site, the next most important aspect is controlling digital access into and out of the organization's network. In most cases this means controlling the points of connectivity to the outside world, typically the Internet. Almost every medium and large-scale company has a presence on the Internet and has an organizational network connected to it. In fact there is a large increase in the number of smaller companies and homes getting full time Internet connectivity. Partitioning the boundary between the outside Internet and the internal intranet is a critical security piece. Sometimes the inside is referred to as the "trusted" side and the external Internet as the "un-trusted" side. As a generality this is all right, however, as will be described, this is not specific enough.

A firewall is a mechanism by which a controlled barrier is used to control network traffic into AND out of an organizational intranet. Firewalls are basically application specific routers. They run on dedicated embedded systems such as an internet appliance or they can be software programs running on a general server platform. In most cases these systems will have two network interfaces, one for the external network such as the Internet and one for the internal intranet side. The firewall process can tightly control what is allowed to traverse from one side to the other. Firewalls can range from being fairly simple to very complex. As with most aspects of security, deciding what type of firewall to use will depend upon factors such as traffic levels, services needing protection and the complexity of rules required. The greater the number of services that must be able to traverse the firewall the more complex the requirement becomes. The difficulty for firewalls is distinguishing between legitimate and illegitimate traffic.

What do firewalls protect against and what protection do they not provide? Firewalls are like a lot of things; if configured correctly they can be a reasonable form of protection from external threats including some denial of service (DOS) attacks. If not configured correctly they can be major security holes in an organization. The most basic protection a firewall provides is the ability to block network traffic to

certain destinations. This includes both IP addresses and particular network service ports. A site that wishes to provide external access to a web server can restrict all traffic to port 80 (the standard http port). Usually this restriction will only be applied for traffic originating from the un-trusted side. Traffic from the trusted side is not restricted. All other traffic such as mail traffic, ftp, snmp, etc. would not be allowed across the firewall and into the intranet.

An even simpler case is a firewall often used by people with home or small business cable or DSL routers. Typically these firewalls are setup to restrict ALL external access and only allow services originating from the inside. A careful reader might realize that in neither of these cases is the firewall actually blocking all traffic from the outside. If that were the case how could one surf the web and retrieve web pages? What the firewall is doing is restricting connection requests from the outside. In the first case all connection requests from the inside are passed to the outside as well as all subsequent data transfer on that connection. From the exterior, only a connection request to the web server is allowed to complete and pass data, all others are blocked. The second case is more stringent as connections can only be made from the interior to the exterior.

More complex firewall rules can utilize what is called "stateful inspection" techniques. This approach adds to the basic port blocking approach by looking at traffic behaviours and sequences to detect spoof attacks and denial of service attacks. The more complex the rules, the greater the computing power of the firewall required.

One problem most organizations face is how to enable legitimate access to "public" services such as web, ftp and e-mail while maintaining tight security of the intranet. The typical approach is to form what is known as a DMZ (demilitarized zone), a euphemism from the cold war applied to the network. In this architecture there are two firewalls: one between the external network and the DMZ, and another between the DMZ and the internal network. All public servers are placed in the DMZ. With this setup, it is possible to have firewall rules which allow public access to the public servers but the interior firewall can restrict all incoming connections. By having the DMZ, the public servers are still provided more protection than if they were just placed outside a single firewall site.

2.11   LET US SUM-UP

In this unit we have examined several Internet-centric firewall designs in an attempt to meet security and performance requirements of multitier applications. In all scenarios, servers hosting application components were separated from the company's corporate network used to conduct internal business, as an initial step to segregate resources with different security requirements. To tightly control interactions between the application's tiers, we looked at hosting tiers of the application on dedicated subnets. By deploying firewalls in series, we were able to significantly increase the difficulty of obtaining unauthorized access to sensitive resources from the Internet. At the same time, each firewall layer increased the design's complexity, contributing to the cost of deploying and maintaining the infrastructure, and increasing the likelihood that it will be misconfigured.

The network design appropriate for your environment depends on the nature of your application and the risks that you are trying to mitigate by setting up a security perimeter around your servers. As we discussed, relying on a single firewall or combining application tiers into a single subnet often decreases the amount of control that you have over how application components are accessed.

However, beware of jumping to a design that incorporates three firewalls in series without first considering less expensive alternatives. In this article, we only touched upon some of the many ways of deploying firewalls with respect to each other, and we did not to examine the relationship between firewalls and other perimeter-defense devices. When designing your network, consider how other components of its perimeter, such as intrusion- detection systems, routers, and VPNs, may impact security of the infrastructure, and select a design that matches your application's architecture and your company's business needs.

2.12 FURTHER READINGS

1. Fundamentals of Information Security (PGDCS-01), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e-Governance and Cyber Security.

2. Cyber Security Techniques (PGDCS-02), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e- Governance and Cyber Security,

3. Cyber Attacks and Counter Measures: User Perspective, (PGDCS-03), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

4. Practical Handbook of Internet Security for Beginners (PGDCS-04), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

2.13 ASSIGNMENTS

1. What do you understand by firewalls? Name different types of it.

2. Differentiate between software based firewall and hardware based firewall.

3. How can you prevent your network from anonymous attack using firewall?

4. When and where to implement hardware based firewall?

5. Describe the steps to configure firewall in Windows-7.

6. How to turn on and configure the Mac OS X Firewall?

Unit 3: Intrusion Detection System and Intrusion Prevention System

<div style="float:right;">3</div>

UNIT STRUCTURE

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the basic terminologies of Intrusion Detection System

- Define Intrusion Detection System

- Know the objectives of Intrusion Detection System

- Differentiate between Intrusion Detection System and Intrusion Prevention System

- Difference between inbound and outbound network activities.

- Know about Intrusion Prevention Systems and IPS Approaches

- Different Types of IPS

- What is a network IPS and how is it different from an Intrusion Detection System?

3.2 INTRODUCTION

An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. An Intrusion Prevention System (IPS) is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and related information.

3.3 INTRUSION DETECTION SYSTEMS

An Intrusion Detection System is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).

Intrusion detection system provides the following:

- Monitoring and analysis of user and system activity

- Auditing of system configurations and vulnerabilities

- Assessing the integrity of critical system and data files

- Statistical analysis of activity patterns based on the matching to known attacks

- Abnormal activity analysis

- Operating system audit

3.4 COMPONENTS OF IDS

There are three main components to the Intrusion Detection System.

A. Network Intrusion Detection System (NIDS)–It performs an analysis for a passing traffic on the entire subnet. Works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of knows attacks. Once the attack is identified, or abnormal behaviour is sensed, the alert can be send to the administrator. Example of the NIDS would be installing it on the subnet where you firewalls are located in order to see if someone is trying to break into your firewall.

B. Network Node Intrusion Detection System (NNIDS) – It performs the analysis of the traffic that is passed from the network to a specific host. The difference between NIDS and NNIDS is that the traffic is monitored on the single host only and not for the entire subnet. The example of the NNIDS would be, installing it on a VPN device, to examine the traffic once it was decrypted. This way you can see if someone is trying to break into your VPN device.

C. Host Intrusion Detection System (HIDS) – It takes a snap shot of your existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. The example of the HIDS can be seen on the mission critical machines that are not expected to change their configuration.

The figure below shows various components of an IDS working together to provide network monitoring.
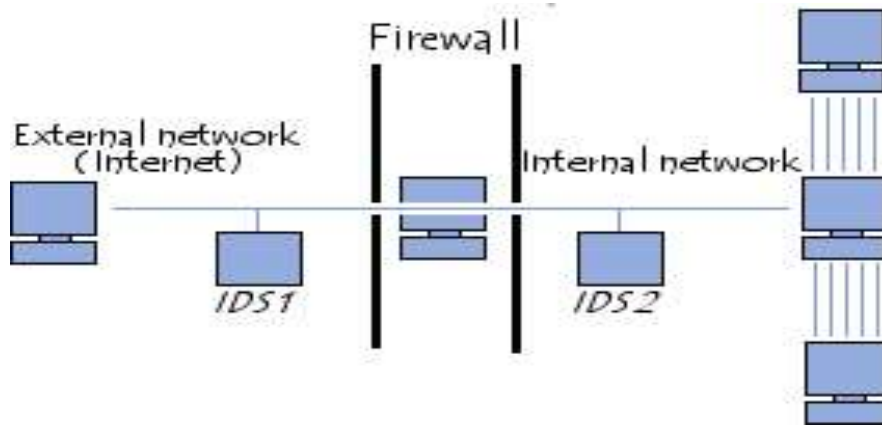
Fig: An Intrusion Detection System

Before discussing IDS/IPS in detail, let us first gear up with some common terminologies used frequently in it.

3.5 CHARACTERISTICS OF IDS

Detection method describes the characteristics of the analyzer. When the intrusion-detection system uses information about the normal behaviour of the system it monitors, it will be considered as behaviour-based. When the intrusion-detection system uses information about the attacks, it will be considered as knowledge-based.
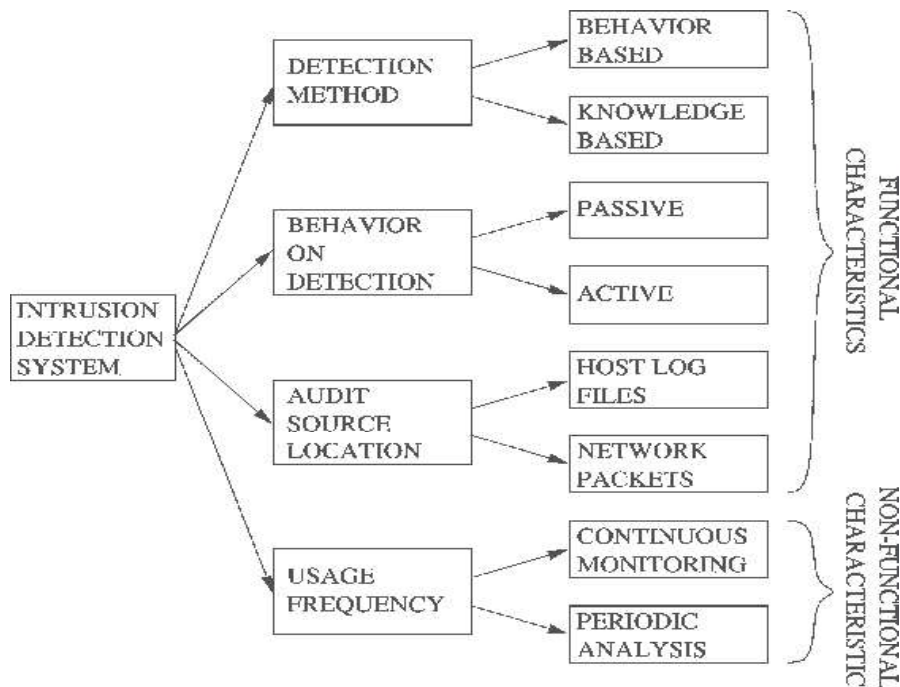
Fig: The characteristics of IDS

The behaviour on detection describes the response of the intrusion-detection system to attacks. When it actively takes a necessary action to the attack by taking either corrective (closing holes) or pro-active (logging out possible attackers, closing down services) actions, then the type of intrusion- detection system is said to be active. If the intrusion-detection system simply generates alarms (such as paging), it is said to be passive.

The audit source location separates intrusion-detection systems based on the kind of input information they analyze. This input information can be audit trails (system logs, firewall logs) on a host, network packets, application logs, or intruder alerts generated by other intrusion- detection systems.

The detection paradigm describes the detection mechanism used by the intrusion-detection system. Intrusion-detection systems can evaluate states (secure or insecure) or changeovers (from secure to insecure).

3.6 TYPES OF IDS

IDS come in a variety of flavours and approach the goal of detecting suspicious traffic in different ways. There are two main types: Network based (NIDS), Host based (HIDS) Intrusion Detection Systems and Application Based Intrusion Detection Systems (ABIDS).

3.6.1 Network Based Intrusion Detection System

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behaviour is sensed, the alert can be sent to the administrator.

The network IDS usually has two logical components: the sensor and the management station. The sensor sits on a network segment, monitoring it for suspicious traffic. The management station receives alarms from the sensor(s) and displays them to an operator. The sensors are usually dedicated systems that exist only to monitor the network. They have a network interface in promiscuous mode, which means they receive all network traffic, not just which destined for their IP address, and they capture passing network traffic for analysis. If they detect something that looks unusual, they pass it back to the analysis station. The analysis station can display the alarms or do additional analysis. Some displays are simply an interface to a network management tool, like HP Open view, but some are custom GUIs designed to help the operator analyze the problem.

Advantages of Network based Intrusion Detection Systems:

- Lower Cost of Ownership

- Easier to deploy

- Detect network based attacks

- Retaining evidence

- Real Time detection and quick response

- Detection of failed attacks

3.6.2 Host based Intrusion Detection System

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected. These frequently use the host system's audit and logging mechanism as a source of information for analysis. They look for unusual activity that is confined to the local host such as logins, improper file access, unapproved privilege escalation, or alterations on system privileges. This IDS architecture generally uses rule-based engines for analyzing activity; an example of such a rule might be, ―super-user privilege can only be attained through the command. Therefore successive login attempts to the root account might be considered an attack.

Advantages of Host based Intrusion Detection Systems:

- Verifies success or failure of an attack

- Monitors System Activities

- Detects attacks that a network based IDS fail to detect

- Near real time detection and response

- Does not require additional hardware

- Lower entry cost.

3.6.3 Application based IDS (APIDS):

Application based IDS (APIDS) will check the effective behaviour and event of the protocol. The system or agent is placed between a process and group of servers that monitors and analyzes the application protocol between devices. Intentional attacks are the malignant attacks carried out by disgruntled employees to cause harm to the organization and Unintentional attacks causes financial damage to the organization by deleting the important data file. There are numerous attacks have taken place in OSI layer

3.6.4 IDS Based on Intrusion Detection Techniques:

3.6.4.1 Misuse- Detection IDS (MD-IDS)

Misuse detection is a system based on rules, either preconfigured by the system or

setup manually by the administrator. The rules are looking for signatures on network and system operations trying to catch a well known attack that should be considered as Misuse. You can think of Misuse detection as a specific deny rule firewall.

3.6.4.2 Anomaly- Detection IDS (AD-IDS)

Anomaly detection on the other hand proceeds by comparing every phenomenon to what a "normal" situation would be. It seems obvious that such system needs a profile of the network/system which may be a problem in the way that it takes time and resources to train an anomaly detection sensor in order to build a profile that is reflecting a normal system / network usage. Think of Anomaly detection as an alarm for strange system behaviour.

3.7 ROLE OF IDS IN AN ORGANIZATION

The IDS however is not an answer to all your Security related problems. You have to know what it CAN, and what it CAN NOT do. In the following subsections we will try to show few examples of what an Intrusion Detection Systems are capable of, but each network environment changes and each system needs to be oriented to meet your enterprise environment needs.

The IDS usually provide the following:

- It can add a greater degree of integrity to the rest of organisation infrastructure.

- You can trace user activity from point of entry to point of impact using IDS.

- It can recognize and report the modifications held on data.

- It automates the task of monitoring the Internet searching for the latest attacks.

- It detects that when your system is under attack.

- It detects the errors present in your system configuration.

- It can guide system administrator in the critical step of establishing a policy for your computing assets.

- It makes the security management of your system possible by non- expert staff.

  Below mentioned are some point roles which cannot be expected by an IDS to be performed:

- It doesn't compensate for a weak identification and authentication mechanisms.

- It should not conduct investigations of attacks without human intervention.

- It will compensate for weaknesses in network protocols.

- It does not compensate for problems in the quality or integrity of information the system provides.

- It will not analyse all the traffic on a busy network.

- It can't always deal with problems involving packet-level attacks.

- It should not deal with some of the modern network hardware and features.

3.8 STEPS TO INSTALL IDS IN AN ORGANIZATION

Installing IDS with other tools in the security arsenal requires some extra planning. This section helps you to avoid common pitfalls when installing your IDS.

Placement of Sensor for a Network IDS: If you are deploying network IDS, you need to plan out where to place the monitoring sensors. This will totally depend on the significance of intrusion from which you want to protect your network. Let's start with a detailed network diagram. First of all you need to evaluate the collection of systems which are sensitive to business. If IDS is being used for monitoring a web server, then the most useful points for placing sensors is in DMZ segment along with web server. If an IDS is being used for monitoring a internal servers such as DNS server or mail servers, then sensor should be placed just inside the firewall on the segment that directly connects the firewall to the internal network. Logic behind implementing of sensor inside firewall is that it will prevent the majority of attacks aimed at the organization, and the regular monitoring of firewall logs will identify them easily. Then the IDS will detect some of those attacks that manage to get through the firewall. This technique is called as "defence in depth". If IDS is being used to monitor internal resources like sensitive collection of machines, physical location or a specific department, then the most logical place for sensor will be on the main point between those systems and the rest of whole internal network.

Host integration for Host IDS: The host IDS should be firstly installed on a development system with the advance planning of installation on a production system. Even on a inactive system, there will be some files that will change regularly

(for example, the audit files), then the installed IDS will report some changes. In some host- based systems, the IDS will report when a user process of altering the system password file. This would

happen if an intruder or a new user adds an account. It also happens, however, when a user changes his or her password. That time the IDS analyst needs to become familiar with the correct operation of each system, so that he or she can properly diagnose deviations from "normal" alarms. Important point: Host based IDS should be monitored frequently i.e. at least twice a day.

Alarm Configuration: IDSs come with a configurable alarm levels in which some will integrate with network management stations, some allow paging, some send e-mail, and some can interoperate with firewalls to shut down all traffic from the network that originated the attack. IDS Manager should have. In fact, we suggest you to be very cautious about using these features for the first month or two, turn off all alarms. Manager should have to analyze the output from the system for monitoring that what it is detecting. You need to be familiar with your particular system before you start turning on alarms.

Integration Schedule: Install one sensor at a time. A sensor in a DMZ may see a given set of behaviours, while a sensor on the internal network may see another set of behaviours, with a very small intersection.

3.9 INCIDENT HANDLING

The Organizations 'Incident Response Plan is documented to provide a well-defined, consistent, and organized approach for handling security incidents, as well as taking appropriate action when an incident at an external organization is traced back to and reported to the Organization. The plan identifies and describes the roles and responsibilities of the Organization's Computer Incident Response Team (UCIRT), which is responsible for activating the Incident Response Plan. Incident Handling Details Although technical procedures vary depending on the categorization and type of incident, each incident must include the following six (6) phases:

1. Preparation: Ready the Organization to handle incidents.

2. Detection: Gather and analyze events; determine the existence of a threat and

the impact to confidentiality, availability, or integrity of an Organization's IT resource.

3. Containment: Stop the damage from attackers and preserve evidence.

4. Remediation: Remove artefacts left from attacker.

5. Resolution: Return systems to production and monitor.

6. Closure and lessons learned: Document findings and implement lessons learned to improve operations and/or incident handling.

Based on the investigation, it may be necessary to repeat some of the phases; however, once an incident is detected the process should be followed to completion.

Phase 1 Preparation: The Preparation phase involves readying the UCIRT to handle incidents. Some required elements for incident handling are indicated below:

- Communications

- Data

- Documentation

- People

- Policy

- Software/Hardware

- Space

- Supplies

- Training

- Transportation

Preparation should be done at regular intervals prior an actual incident occurring.

Phase 2 Detection: Incident detection occurs internally in all areas and at all levels of the University, as well as externally, through reports from non- University incident handlers. All High-Risk incidents should immediately be reported to ITSO once detected. Administrators and users must be familiar with their systems to determine if an event constitutes an incident. Effective incident detection occurs when:

1. The administrator or user is familiar with normal operations.

2. Systems are equipped with effective auditing and logging tools.

3. Administrators review systems and logs to identify deviations from normal operations.

Security contacts must analyze all available information in order to understand the scope of an incident and effectively contain and remediate the incident. The incident must be fully diagnosed prior to beginning subsequent phases of the Incident Response Plan.

Phase 3 Containment: The first priority of Organization, in every incident, is to contain the incident as quickly as possible. An incident is considered contained when no additional harm can be caused and the incident handler is able to focus on remediation. Containment consists of three stages:

- Short-term containment: stopping the progress of the incident or attacker.

- Information gathering.

- Long-term containment: making changes to the production system.

Phase 4 Remediation: The goal of the Remediation phase is to clean up a system and remove any artifacts (e.g., rootkits) left from the attacker. During the Remediation phase, the team must also determine and document the cause and symptoms of the incident: isolating the attack based on information gathered during the detection phase, and determining how the attack was executed.

Phase 5 Resolution: During the Resolution phase, the Team restores normal business operations. It is critical to carefully handle incident Resolution and verify system performance and security before being brought back online. Tests must be completed and baseline system activity (gathered in the Preparation phase) must be compared to ensure the system is verified before operations are restored.

Phase 6 Closure: and Lessons Learned in the Closure and Lessons Learned phase, the ITSO documents findings from the incident and the handling of the incident is reviewed by the Organizations 'Security Incident handling Team. The expected outcome of this phase is improved operations and improved incident response procedures.

The incident handling process has many phases. It describes the sequence of steps that begin when an incident reaches your team. It could follow a very simple or very sophisticated model. Start planning your incident handling process with a simple set of tasks and subsequently expand it to new ones according to your real work and needs. You can use the set of tasks discussed below as a framework for your incident handling procedure. This is the same set of tasks that form the workflow shown in Figure 3.
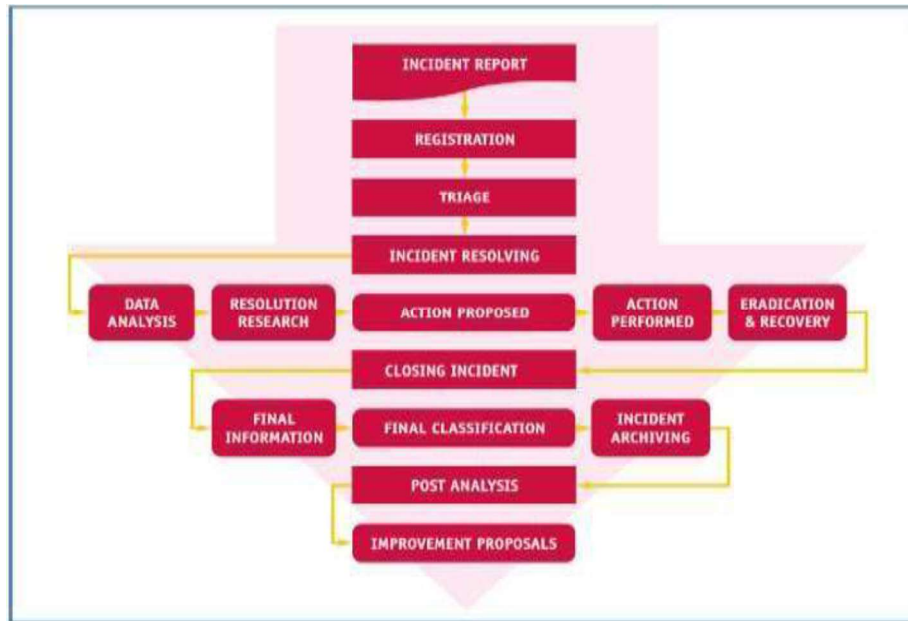
Fig: This diagram workflow of incident handling process

3.10 INTRUSION PREVENTION SYSTEMS

Intrusion Prevention Systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. Intrusion prevention is a pre-emptive approach to network security used to identify potential threats and respond to them swiftly. Like an Intrusion Detection System (IDS), an Intrusion Prevention System (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, Intrusion Prevention Systems also have the ability to take immediate action, based on a set of rules established by the network

administrator. For example, an IPS might drop a packet that it determines to be

malicious and block all further traffic from that IP address or port. Legitimate traffic, meanwhile, should be forwarded to the recipient with no apparent disruption or delay of service. According to Michael Reed of Top Layer Networks, an effective Intrusion Prevention System should also perform more complex monitoring and analysis, such as watching and responding to traffic patterns as well as individual packets. "Detection mechanisms can include address matching, HTTP string and substring matching, generic pattern matching, TCP connection analysis, packet anomaly detection, traffic anomaly detection and TCP/UDP port matching." Broadly speaking, an Intrusion Prevention System can be said to include any product or practice used to keep attackers from gaining access to your network, such as firewalls and anti-virus software.
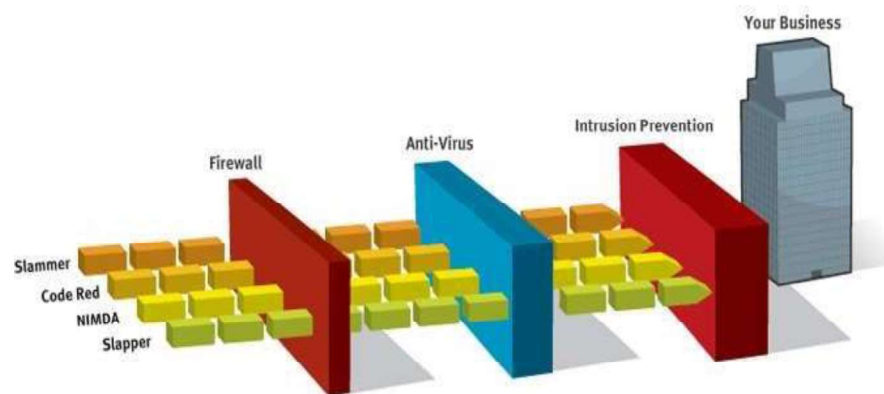
Intrusion Prevention System

3.11 IPS APPROACHES

Some of the approaches being used are:

1. **Software based heuristic approach** - This approach is similar to IDS anomaly detection using neural networks with the added ability to act against intrusions and block them.

2. **Sandbox approach** - Mobile code like ActiveX, Java applets and various scripting languages are quarantined in a sandbox - an area with restricted access to the rest of the system resources. The system then runs the code in this sandbox and monitors its behaviour. If the code violates a predefined policy it's stopped and prevented from executing, thwarting the attack (Conry-Murray).

3. **Hybrid approach** –On network-based IPS (NIPS), various detection methods, some proprietary including protocol anomaly, traffic anomaly, and signature detection work together to determine an imminent attack and block traffic coming from an inline router.

4. **Kernel based protection approach** – Used on host-based IPS (HIPS). Most operating systems restrict access to the kernel by a user application. The kernel controls access to system resources like memory, I/O devices, and CPU, preventing direct user access. In order to use resources user applications send requests or system calls to the kernel, which then carries out the operation. Any exploit code will execute at least one system call to gain access to privileged resources or services. Kernel based IPS prevents execution of malicious system calls.

Programming errors enable exploits like buffer-overflow attacks to overwrite kernel memory space and crash or takeover computer systems. To prevent these types of attacks a software agent is loaded between the user application and the kernel. The software agent intercepts system calls to the kernel, inspects them against an access control list defined by a policy, and then either allows or denies access to resources. On some IPS systems the agent checks against a database of specific attack signatures or behaviors. It could also check against a database of known good behaviors or a set of rules for a particular service. Either way if a system call attempts to run outside its allowed zone, the agent will stop the process.

Vendors are using a combination of the above-mentioned approaches to ward off combined attack types seen on today's networks. Even though the above approaches are different the goal is the same – to stop attacks in real- time before they cause harm. Harm could be prevented by (Bobbitt)

- **Protecting System Resources** – Trojan horses, root kits, and backdoors alter system resources like libraries, files/directories, registry settings, and user accounts. By preventing alteration of system resources, hacking tools cannot be installed.

- **Stopping Privilege Escalation Exploits** – Privilege escalation attacks try to give ordinary users root or administrator privileges. Disallowing access to resources, which alter privilege levels, can prevent this and block exploits like

Trojan horses, rootkits, and backdoors.

- **Preventing Buffer Overflow Exploits** – By checking whether the code about to be executed by the operating system came from a normal application or an overflowed buffer, these attacks can be stopped.

- **Prohibit Access To E-mail Contact List** – Many worms spread by mailing a copy to those in the Outlook's contact list. This could be halted by prohibiting e-mail attachments from accessing Outlook's contact list.

- **Prevent directory traversal** – The directory traversal vulnerability in different web servers allows the hacker to access files outside the web servers range. A mechanism that would prevent the hacker access to the web server files outside its normal range could prevent such malicious activities. UNIX's has a chroot command that does this.

3.12 TYPES OF IPS

3.12.1 Host based Intrusion Prevention (HIP)

- A host-based intrusion prevention system (HIPS) is a system or a program employed to protect critical computer systems containing crucial data against viruses and other Internet malware. Starting from the network layer all the way up to the application layer, HIPS protects from known and unknown malicious attacks. HIPS regularly check the characteristics of a single host and the various events that occur within the host for suspicious activities.

- HIPS can be implemented on various types of machines, including servers, workstations, and computers.

3.12.1.1 STORMWATCH

OKENA's StormWatch uses a kernel-based approach and works on servers and workstations. Policies - collections of access control rules based on acceptable behaviour, is available out-of-the-box for common applications such as Microsoft SQL Server, Instant Messenger, and IIS Server. Policies control what resource is being used, what operation is being invoked, and which application is invoking it. Storm Watch hooks into the kernel and intercepts system calls (Okena).

It has four interceptors:

- File System interceptor– intercepts all file read and write requests.

- Network interceptor – intercepts packet events at the driver (NDIS) or transport (TDI) level.

- Configuration interceptor – intercepts read/write requests to the registry on Windows or to rc files on UNIX.

- Execution space (Run-time environment) interceptor - requests to write to memory not owned by the requesting application will be blocked by this interceptor. For example, buffer overflow attacks would be blocked here. Thus it maintains the integrity of each applications dynamic run-time.

Since StormWatch intercepts File, Network, Configuration, and Run-time operations and compares them to application-specific access control rules or policies; it can track the state of an application. For example, Network interceptor provides address and port blocking like a firewall; File system and Configuration interceptors monitor and prevent changes to critical files or registry keys. Network and File system interceptors provide worm prevention.

By correlating events from multiple systems at the management station, StormWatch not only blocks the threat but also pushes out a new policy to all agents and blocks future attacks. This reduces the number of false positives and false negatives.

StormWatch has a utility program called StormFront. It serves as a data analysis and policy creation tool, which analyzes applications as they operate in a normal environment and generates policies. Any other application behavior would be considered suspicious. Resources accessed by the application are separated into file, network, registry, and COM categories.

3.12.2 ENTERCEPT's Standard Edition

Entercept, a pioneer in kernel-based protection, proactively protects the host by intercepting system calls (Entercept). Unlike Okena's StormWatch it uses both, signatures and behavior rules to stop and detect attacks.

In an article by Ed Skoudis on "infosec's WORST NIGHTMARES", some nightmares that he mentions are stealthier attacks and "super" worms – "Fast spreading, multiplatform, multi-exploit, zero-day, metamorphic worms". He goes on to say that

one way of preparing for these coming "super" worms is to, "Utilize host-based intrusion detection and prevention tools such as Entercept Security Technologies and OKENA's StormWatch on critical systems to block or rapidly discover attacks."

3.12.3　Network based Intrusion Prevention (NIP)

NIPS are generally appliance-based systems that sit in line, and block suspicious traffic after detecting an attack. They utilize different detection methods, signature detection, anomaly detection, and some proprietary methods, to block specific attacks.

Some of the methods adopted by vendors are –

- **Stateful Signature detection** – It looks at relevant portions of traffic, where the attack can be perpetrated. It does this by tracking state and based on the context specified by the user detects an attack. It is not completely automatic, as the user needs to have some prior knowledge about the attack. For example, the Love letter worm can be detected by a rule that would read as follows - "Look for "ILOVEYOU" in the subject field only, ignore this string anywhere else in the email." Basically it does pattern matching using regular expressions, which allow wildcard and complex pattern matching (NetScreen).

- **Protocol anomaly detection** - All vendors do detailed packet analysis with protocol decode engines to ensure packets meet protocol requirements.

Traffic normalization is also done to remove protocol ambiguities and ensures that traffic interpreted by the NIPS is the same as that seen by the end host, so that we do not miss attacks.

All this resource intensive processing is done with the aid of dedicated hardware boxes for speed and latency issues. Devices are already available that work at gigabit speeds. If it cannot cope with traffic load then it would drop packets and miss attacks. NIPS are reported to have a high rate of false positives but have blocked thousands of known attacks. Products are just being released and their performance needs to be evaluated especially with new attack methods. The disadvantage of being in-line is that if the device fails the entire network it serves is down. This can be overcome by having,

failover or parallel systems. Initial reports have been encouraging but false positives

are high (Cummings).

Many of the vendors provide or intend to provide Firewall/IDS/Anti-virus and vulnerability assessment capabilities. Some vendors integrate with other firewall, IDS, and vulnerability assessment tools.

3.13   WHAT IS A NETWORK IPS AND HOW IS IT DIFFERENT FROM AN INTRUSION DETECTION SYSTEM?

Network IPS performs in-line inspection of network traffic in a near-real- time manner. The inspection identifies attacks using known vulnerabilities of commonly used software products and protocols, as well as known attack patterns with unusual activity based on connection sequences or traffic volume. Intrusion Prevention Systems are considered extensions of Intrusion Detection Systems because both systems monitor network traffic and/or system activity for threats. The primary difference between the two systems is that Intrusion Prevention Systems are placed in-line and are therefore able to actively prevent/block intrusions that are detected. More specifically, an IPS can take such actions as sending an alarm, dropping malicious packets, resetting the connection and/or blocking traffic from an offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, defragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

3.14 LET US SUM UP

Firewalls, anti-virus, and IDS have their place in the security landscape, each with its unique features. Depending on business needs, budget constraints, and organizational requirements we need to draw up a security policy and that policy will determine the mix of components that need to be installed, to meet security goals. IPS adds to the defense in depth approach to security and is an evolution of IDS technology. Its proactive capabilities will help to keep our networks safer from more sophisticated attacks. Today, the use of tunnelling and encryption means putting more content out of the reach of perimeter controls. Even though NIPS will prevent attacks, some could slip through and HIPS would prevent them. HIPS – the last line of defense provides "operating system hardening" with greater granularity and application specific control. Intrusion prevention is a generic term. Before purchasing

a product, study the detection and prevention mechanisms vendors have implemented vis-à-vis current attack methods. Security is hard, some attacks could still slip through and no amount of automation can replace trained and vigilant security personnel. But tools like IPS can reduce the tedium and provide a silver lining if not a silver bullet!

3.15 FURTHER READINGS

1. Cyber Security Techniques (PGDCS-02), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e- Governance and Cyber Security

2. Reference Material on Cyber Security, By DR. Bhagirathi Nayak, for Diploma in Cyber Security, Odisha State Open University.

3. Dinesh Sequeira, Intrusion Prevention Systems – Security's Silver Bullet? Gsec Version 1.4b Option 1, © Sans Institute 2002.

3.16 ASSIGNMENTS

1. What is IDS? What are different types of IDS?

2. Differentiate between Network based and host based IDS.

3. What are the functions of IDS?

4. What is a Honeypot?

5. What are the steps to install IDS in an organization?

6. Make diagram of IDS Components?

7. Give examples of Misuse & Anomaly Detection IDS?

8. What is DMZ?

Unit 4: Public Key Infrastructure (PKI)

<div style="text-align: right">4</div>

UNIT STRUCTURE

4.1 LEARNING OBJECTIVES

After learning this unit you should be able to

- What Is Public Key Infrastructure (PKI)

- Use of Public Key Infrastructure (PKI)

- Application of a Public-Key Infrastructure (PKI)

- What is an effective public-key infrastructure?

4.2 INTRODUCTION

Public Key Infrastructure (PKI) is a popular encryption and authentication approach used by both small businesses and large enterprises. Here's how PKI is used today and how you can implement it in your organization.

Identity and authorization management (IAM) applications and encryption generally are considered two of the most important components of a layered security environment. Today it is not enough to assume that the person who has access to data is authorized, it is essential to confirm that authorization and make sure that the decryption protocols are followed in accordance with the company's information security policies and procedures. In the Windows environment, IAM is an integral component of Microsoft Active Directory. While we've looked at numerous IAM tools enterprises can use, ranging from the Public Key Infrastructure (PKI) for small to midsize businesses to enterprise-class offerings that also include credential management, PKI is popular amongst companies of all sizes.

4.3 USE OF PUBLIC KEY INFRASTRUCTURE (PKI)

Use of a Public Key Infrastructure (PKI) to support business processes within a single organization requires no more policy and procedures preparation than that required for any Information Technology (IT) infrastructure. Prudent businesses routinely prepare a system security policy, and the special provisions required for a PKI can be easily accommodated within such a policy. When security services involve independent organizations or security domains, they should be qualified by an explicit "quality of service". This ensures that a user of the service does not anticipate a high quality of service or degree of assurance from a provider whose

operating procedures are consistent with a lower degree of assurance. This situation could lead to what appears to the user to be a breach of security, even though the service provider has operated entirely within its own operating rules. Aspects of the system's operation that affect the degree of assurance are commonly documented in a system security policy. Where the system includes a PKI, users need to be able to determine the degree of assurance or trust which can be placed in the authenticity and integrity of the public keys contained in certificates issued by the Certification Authority (CA). Information upon which such determinations

can be made is documented in the relevant Certificate Policy and Certification Practice Statement.

4.4 WHAT IS PUBLIC KEY INFRASTRUCTURE (PKI)

The PKI environment is made up of five components:

1. **Certification Authority (CA)** -- serves as the *root of trust* that authenticates the identity of individuals, computers and other entities in the network.

2. **Registration Authority (RA)** -- is certified by a root CA to issue certificates for uses permitted by the CA. In a Microsoft PKI environment, the RA is normally called a subordinate CA.

3. **Certificate Database** -- saves certificate requests issued and revoked certificates from the RA or CA.

4. **Certificate Store** -- saves issued certificates and pending or rejected certificate requests from the local computer.

5. **Key Archival Server** -- saves encrypted private keys in a certificate database for disaster recovery purposes in case the Certificate Database is lost.

From an operational perspective, PKI is an encryption approach where, a pair of cryptographic keys -- one public and one private -- is used to encrypt and decrypt data. A user can give someone their public key, which that sender uses to encrypt data. The owner then uses their private key to decrypt the data. This authentication and encryption approach originated in the British intelligence community in the early 1970s and has been used commercially for nearly 20 years.

Examples of how PKI technology is used today include sending authenticated email

messages using technologies such as OpenPGP (Open Pretty Good Privacy) or S/MIME (Secure/Multipurpose Internet Mail Extensions), encryption of documents using the eXtended Markup Language (XML), and authentication of users using smart card logins or client authentication using SSL (secure socket layer) signatures or encryption.

4.5   HOW PUBLIC KEY INFRASTRUCTURE IS USED TODAY

PKI is used by companies that must meet security compliance regulations. Entrust, for example, offers PKI products that can be used to meet strong identity authentication for first responders, as well as healthcare authentication for Medicare and Medicaid providers. While consumers often think of massive medical centres and big medical insurance companies when they think of the healthcare industries, a large number of small medical, chiropractic, and naturopathic offices with 10 or fewer employees also have to meet the same Health Insurance Portability and

Accountability Act (HIPAA) requirements as the Mayo Clinic or any other big hospital.

While it is possible to have self-signed certificates created by commercial software -- this article is being written in Microsoft Office 2007 that has the ability to encrypt this document and attach a digital signature -- a self- signed document generally does not carry the same security status of a document that has a third-party digital certificate from a verified certificate provider. Even Microsoft's own TechNet site states that self-signed documents generally are used between people whom already know each other and are confident that the sender actually created the signed document.

But what can a PKI actually *do* for a company? According to Microsoft, here are some the key reasons to deploy this infrastructure:

- Control access to the network with 802.1x authentication;

- Approve and authorize applications with Code Signing;

- Protect user data with the Encryption File System (EFS);

- Secure network traffic IPSec;

- Protect LDAP (Lightweight Directory Access Protocol)-based directory queries

- Secure LDAP;

- Implement two-factor authentication with smart cards;

- Protect traffic to internal web-sites with Secure Socket Layer (SSL) technology;

- Implement secure email.

A number of applications also can use the PKI certificates. Aside from the aforementioned email and network access controls, PKI also can be used for enterprise- and SMB-class databases, electronic document and forms signing, secure instant messaging, mobile device security, securing USB storage devices, Windows Server Update Services, Active Directory and more.

4.6 IMPLEMENTING PKI

The cost of implementing PKI obviously varies with each installation, but there are some common expenses that occur. On the hardware side, there can be costs relating to the servers themselves, hardware security modules (HSMs), backup devices and backup media. In a Windows environment, there also can be server licensing fees.

In addition, there also will be personnel expenses for hiring someone to design, implement and manage the PKI environment, as well as possible expenses for integration and automation of systems. There also will be on- going expenses for a staffer to manage the issuing and revoking of certificates, as well as normal systems maintenance such as applying patches and running backups.

Based on the complexity of the environment, it is possible to have a single server act as both the root and issuing CA. A two-tier hierarchy consists of the root CA with issuing CAs connecting up to the root. This is considered to be the most common design, although the architecture can be designed with a Policy or Intermediate CA sitting between the root and issuing CAs. In this design, the policy server could restrict the types of certificates an issuing CA could create.

Security best practices dictate that companies should avoid putting *high*- risk applications, such as a web server, on the same physical host as a high- value resource, such as the PKI server. If the high-risk applications are hosted on a virtual

machine (VM), those VMs also should be on different physical systems than the PKI server.

Additionally, PKI is a very effective method for implementing multi-factor authentication. Some companies, such as Unisys, require that devices that are attached to the corporate network must be able to use PKI for the encrypted and authenticated exchange of information.

Safenet, a provider of authentication and encryption products, says that companies considering employing PKI for full-disk encryption, network logon, digital signatures and similar applications should look at context- based authentication to ensure that the user's access credentials are appropriate for the data being accessed.

For an organization that wants to adopt a PKI environment, says Abhijit Tannu, chief technology officer of Seclore Technology in Mumbai, India, the most important first step would be a security architect who would define the services and applications that need and will use the PKI service.

"PKI by itself does not provide security unless it is used in conjunction with other solutions (and) communication platforms like email (or) mobile device management (MDM)," he says. "Therefore it is important to have someone who will define the overall security architecture. The organization will also need someone to define and implement the policies that will be governing the generation and renewal and revocation of the PKI certificates."

For companies that want PKI capabilities but not the capital investment in hardware and software, PKI is also available from managed security services providers.

"To provide such a service," Tannu says, "the organization would need to have a very deep understanding of PKI infrastructure and how it gets integrated with various solutions like email, browsers, MDM, (and other applications). They will also need a rock-solid infrastructure and industry- grade security around the infrastructure hosting the service."

4.7   PKI IN THE ENTERPRISE

In corporate environments, Public Key Infrastructure (PKI) is commonly used to authenticate users trying to access data, including validating transactions.

Security vendor SafeNet offers PKI services for USB and smart card authentication, cryptography as a service (CaaS), and protection of hardware security modules (HSMs). In addition to offering various multi- factor authentication hardware and software tokens, the company offers multiple data encryption and control products, ranging from network appliances to software-only encryption.

Like SafeNet, Certified Security Solutions (CSS) Inc. leverages PKI technology for authorization and encryption products. The CSS approach includes offering PKI as a Service (PKIaaS), allowing companies to take advantage of PKI managed services without building out their own corporate infrastructure for PKI. In addition, the company offers a Certificate Management System available as a software product, managed service or as part of its cloud offering.

While encryption and authorization are available for most any application, it still requires that the company first conduct a detailed analysis of its IT assets, applications and data. Without knowing what a company owns and where the data or device is located, implementing any security program will be problematic at best. That said, authorization and identity management, combined with encryption policies and procedures for the most sensitive data, will go a long way to protect a company's most precious information. Remember that even if an attacker is in the network and trying to steal corporate data, encrypted data will do them no good if they successfully exfiltrate it from the network. Further, data that they steal but cannot access also is of no value to criminals.

4.8 APPLICATION OF PUBLIC KEY INFRASTRUCTURE (PKI)

One single digital certificate between Alice and Bob involves multiple entities and technologies. Asymmetric cryptography must be used to create the public and private keys, an RA must verify Bob's identity, the CA must issue the certificate, and the digital certificate must be placed in a CR and moved to a CRL when it expires, and so on. In an organization where multiple users have multiple digital certificates, it can quickly become overwhelming to individually manage all of these entities. In short, there needs to be a consistent means to manage digital certificates. **Public key infrastructure (PKI)** is what you might except from its name: it is a framework for all of the entities involved in digital certificates for digital certificate management- including hardware, software, people, policies, and procedures- to create, store,

distribute, and revoke digital certificates. In short, PKI is digital certificate management.

Note: PKI is sometimes erroneously applied to broader range of cryptograph topics beyond managing digital certificates. It is sometimes defined as that which supports other public key enabled security services or certifying users of a security application. PKI should be understood as the framework for digital certificate management.

4.8.1 Public-Key Cryptographic Standards (PKCS)

Public-key cryptography standard (PKCS) is a numbered set of PKI standards that have been defined by RSA Corporation. Although they are informal standards, today they are widely accepted in the industry. These standards are based on the RSA public-key algorithm.

4.8.2 Trust Models

Trust may be defined as confidence in or reliance on another person or entity. One of the principle foundations of PKI is that of trust. Alice must trust that the public key in Bob's digital certificate actually belongs to him. A trust model refers to the type of trusting relationship that can exist between individuals or entities. In one type of trust model direct trust, a relationship exists between two individuals because one person knows the other person. Because Alice knows Bob – she has seen him, she can recognize him in a crowd, she has spoken with him-- she can trust that the digital certificate that Bob personally gives to her contains his public key.

A Third-party trust refers to a situation in which two individuals trust each other because each trusts a third party. If Alice does not know Bob, this does not mean that she can never trust his digital certificate. Instead, if she trusts a third-party entity who knows Bob, then she can trust that his digital certificate with the public key is from Bob. An example of a third-party trust is a courtroom. Although the defendant and prosecutor may not trust one another, they both can trust the judge (a third party) to be fair and impartial. In that case, they implicitly trust each other because they share a common relationship with the judge. There are essentially three PKI trust models that use a CA. These are the hierarchical trust model, the distributed trust model, and the bridge trust model.. A less secure trust model that uses no CA is

called the "web of trust" model and is based on direct trust. Each user signs his digital certificate and is based on direct trust. Each user signs his digital certificate and then exchanges certificates with all other users. Because all users trust each other, each user can sign the certificate of all other users. Pretty Good Privacy (PGP) uses the web of trust model.

4.8.3 Hierarchical Trust Model

4.8.3.1   Hierarchical Public Key Infrastructure (PKI)

A public key infrastructure is a type of key management system that uses hierarchical digital certificates to provide authentication, and public keys to provide encryption. PKIs are used in World Wide Web traffic, commonly in the form of SSL and TLS.

The hierarchical trust model assigns a single hierarchy with one master CA called the root. This root signs all digital certificate authorities with a   single key. A hierarchical trust model is illustrated in figure below.
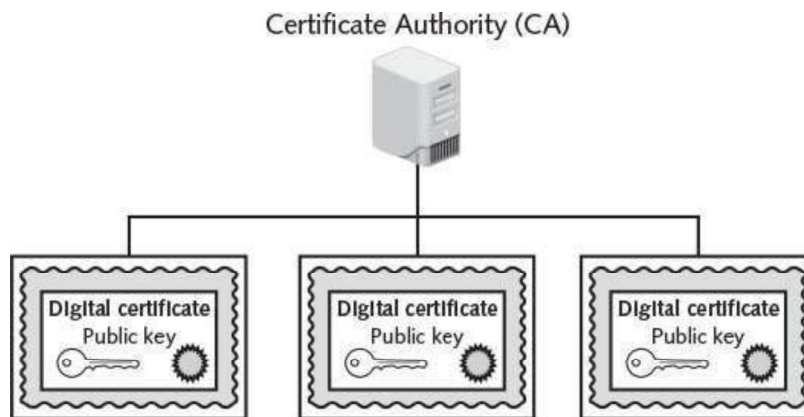
Fig: Hierarchical Trust Model

A hierarchical trust model can be used in an organization where on CA is responsible for only the digital certificates for that organization. However, on a larger scale a hierarchical trust model has several limitations. First, if the CA's single private keys were to be compromised, then all digital certificates would be worthless,

also, having a single CA who must verify and sign all digital certificates may create a significant backlog. And, what if another entity decided that it wanted to be the root?

4.8.4 Distributed Trust Model

Instead of having a single CA, as in the hierarchical trust model, the distributed trust model has multiple CAs that sign digital certificates. This essentially eliminates the limitations of a hierarchical trust model; the loss of a CA's private key would compromise only those digital certificates for which it had signed, the workload of verifying and signing digital certificates can be distributed, and there is no competition regarding who can perform the functions of a CA, In addition these CA s can delegate authority to other intermediate CA s to sign digital certificates. A distributed trust model is illustrated in figure below.
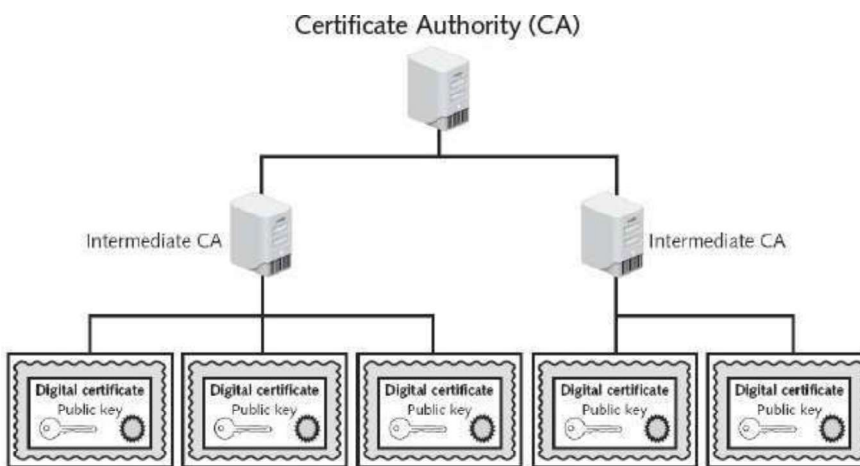
Fig: Distributed Trust Model

The distributed trust model is the basis for digital certificates issued to internet users. There are trusted root certificate authorities as well as intermediate certification authorities.

4.8.5 Bridge Trust Model

The bridge trust model is similar to the distributed trust model in that there is no single CA that signs digital certificates. However, with the bridge trust model there is one CA that acts as a- facilitator to interconnect all other CA.

This facilitator CA does not issue digital certificates; instead, it acts as the hub

between hierarchical trust models and distributed trust models. This allows the different models to be linked. The bridge model is shown in Figure below.
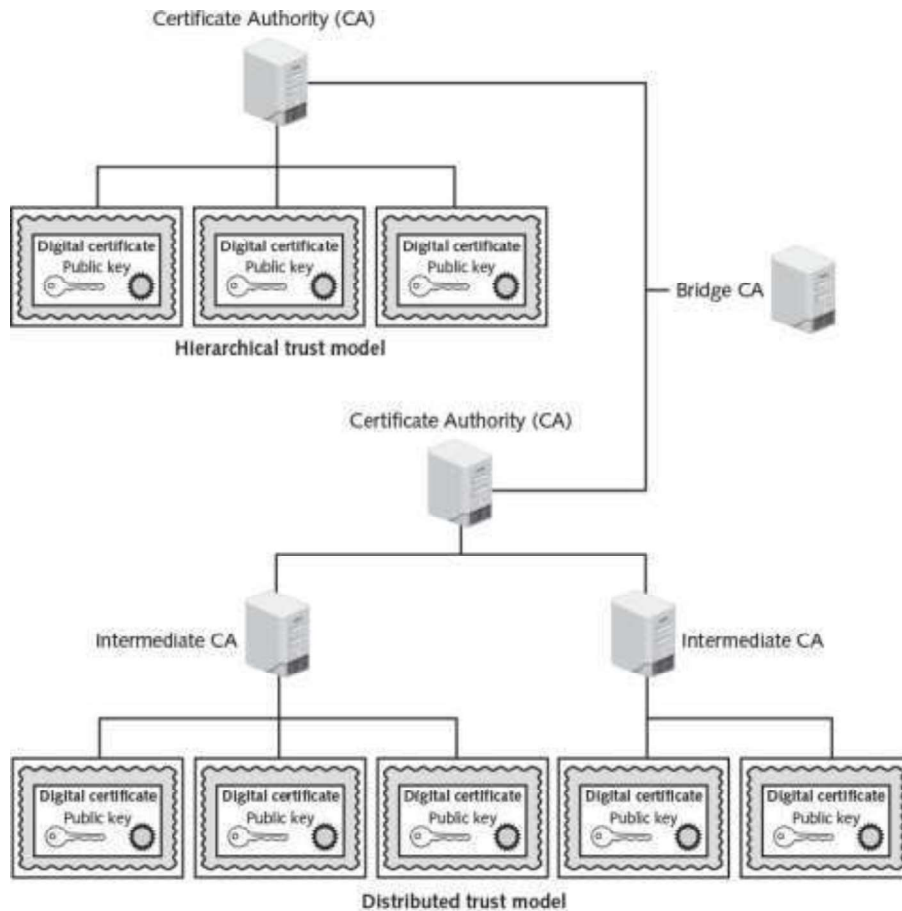
Fig: Distributed trust Model

The U.S. Department of Defense has issued Common Access Cards (CAC), based on the Personal Identity Verification (PIV) standard, which are linked to a digital certificate. Some states have begun issuing Ids compatible with the CAC cards to emergency service personnel, and one state has cross- certified with the federal PKI through a trust bridge for authenticating digital certificates. It is predicted that more state governments soon will begin including digital certificates in ID s issued to citizens that would be interoperable with state and federal systems and also could be used to access commercial services. This would allow trust relationships between the different models, so that one organization can accept digital certificates

for strong authentication without having to issue and manage all of the certificates itself. Already the aerospace and pharmaceutical industries have established their own bridges, which have been cross- certified with the federal bridge.

A Certification Practice Statement (CPS) is a statement of the practices that a CA employs in managing the certificates that it issues. The Operating Authority (usually an individual within the IT unit) is responsible for preparing and maintaining the CPS. The CPS should describe how the Certificate Policy is interpreted in the context of the system architecture and operating procedures of the organization

While a Certificate Policy is defined independently of the specific details of the operating environment of the PKI, the corresponding CPS should be tailored to the organizational structure, operating procedures, facilities and computing environment of the Operating Authority. Use of a standard structure for Certificate Policy and CPS documents will help ensure completeness and simplify the assessment of the corresponding degree of assurance by users and other CAs.

4.9 MANAGING PKI

A Certification Practice Statement (CPS) is a statement of the practices that a CA employs in managing the certificates that it issues. The Operating Authority (usually an individual within the IT unit) is responsible for preparing and maintaining the CPS. The CPS should describe how the Certificate Policy is interpreted in the context of the system architecture and operating procedures of the organization

An organization that uses multiple digital certificates on a regular basis needs to properly manage those digital certificates. This includes establishing policies and practices and determining the life cycle of a digital certificate.

4.9.1 Certificate Policy

A certificate policy (CP) is a published set of rules that govern the operation of a PKI. The CP provides recommended baseline security requirements for the use and operation of CA, RA and other PKI components. A CP should cover such topics as CA or RA obligations, user obligations, confidentiality, operational requirements, and training. Many organizations create a single CP to support not only digital certificates but also digital signatures and all encryption applications.

4.9.2 Certificate Practice Statement (CPS)

A certificate practice statement (CPS) is a more technical document than a CP. A CPS describes in detail how the CA uses and manages certificates. Additional topics for a CPS include how end users register for a digital certificate, how to issue digital certificates, when to revoke digital certificates, procedural controls, key pair generation and installation, and private key protection.

4.9.3 Certificate Life Cycle

Digital certificates should not last forever. Employees leave, new hardware is installed, applications are updated, and cryptographic standards evolve. Each of these changes affects the usefulness of a digital certificate. The life cycle of a certificate is typically divided into four parts:

Creation

At this stage, the certificate is created and issued to the user. Before the digital certificate is generated, the user must be positively identified. The extent to which the user's identification must be confirmed can vary, depending on the type of certificate and any existing security policies. Once the user's identification has been verified, the request is sent to the CA for digital certificate. The CA can then apply its appropriate signing key to the certificate, effectively signing the public key. The relevant fields can be updated by the CA, and the certificate is then forwarded to the RA (if one is being used). The CA can also keep a local copy of the certificate it generated. A certificate, once issued, can be published to a public directory if necessary.

Suspension

This stage could occur once or multiple times throughout the life of a digital certificate if the certificate's validity must be temporarily suspended. This may occur, for example, when an employee is on a leave of absence. During this time it may be important that the user's digital certificate not be used for any reason until she returns. Upon the user's return, the suspension can be withdrawn or the certificate can be revoked.

Revocation

At this stage, the certificate is no longer valid. Under certain situations a certificate may be revoked before its normal expiration date, such as when a user's private key is lost or compromised. When a digital certificate is revoked, the CA updates its internal records and any CRL with the required certificate information and timestamp (a revoked certificate is identified in a CRL by its certificate serial number). The CA signs the CRL and places it in a public repository where other applications using certificates can access this repository in order to determine the status of a certificate.

Expiration

At the expiration stage, the certificate can no longer be used. Every certificate issued by a CA must have an expiration date. Once it has expired, the certificate may not be used any longer for any type of authentication and the user will be required to follow a process to be issued with a new expiration date.

4.10 KEY MANAGEMENT

It goes without saying that the security of any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the handling of cryptographic keys, the benefits of the use of strong cryptographic schemes are potentially lost.

It is observed that cryptographic schemes are rarely compromised through weaknesses in their design. However, they are often compromised through poor key management.

There are some important aspects of key management which are as follows:

- Cryptographic keys are nothing but special pieces of data. Key management refers to the secure administration of cryptographic keys.

- Key management deals with entire key lifecycle as depicted in the following illustration −
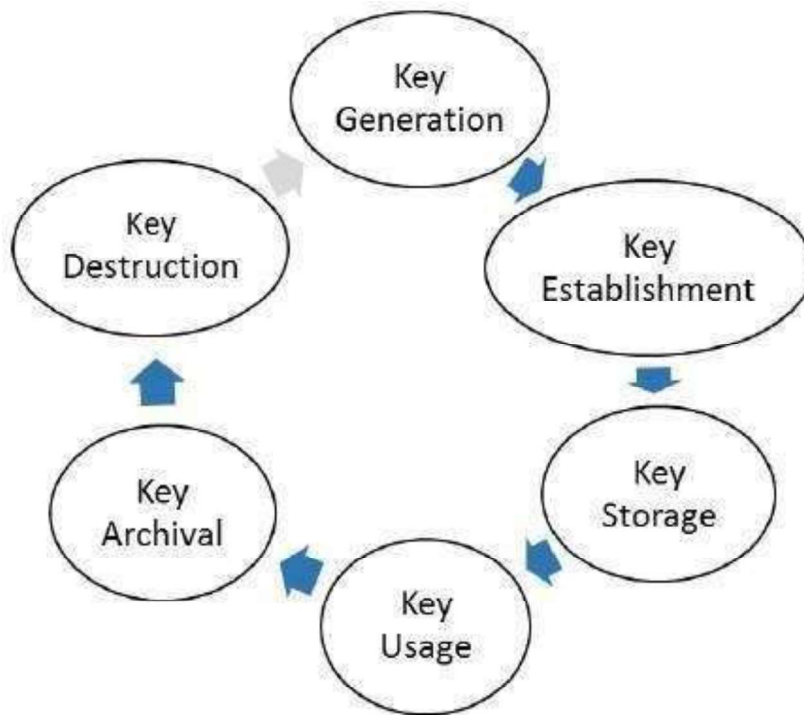
There are two specific requirements of key management for public key cryptography.

- **Secrecy of private keys.** Throughout the key lifecycle, secret keys must remain secret from all parties except those who are owner and are authorized to use them.

- **Assurance of public keys.** In public key cryptography, the public keys are in open domain and seen as public pieces of data. By default there are no assurances of whether a public key is correct, with whom it can be associated, or what it can be used for. Thus key management of public keys needs to focus much more explicitly on assurance of purpose of public keys.

The most crucial requirement of 'assurance of public key' can be achieved through the public-key infrastructure (PKI), a key management systems for supporting public-key cryptography.

4.10.1 Key Storage

The means of strong keys in a PKI system is important. Public keys can be stored by embedding them within digital certificates, while private keys can be stored on the user's local system. The drawback to software-based storage is that may leave keys open to attacks: vulnerabilities in the client operating system, for example, can

expose keys to attackers. Storing keys in hardware is an alternative to software-based storage. For storing public keys, special CA root and intermediate CA hardware devices can be used. Private keys can be stored on smart on smart cards or in tokens. Whether private keys are stored in hardware or software, it is important that they be adequately protected. To ensure basic protection, never share the key in plaintext, always store keys in files or folders that are themselves password protected or encrypted, do not make copies of keys, and destroy expired keys.

4.10.2   Key Usage

If more security is needed than a single set of public and private keys, then multiple pairs of dual keys can be created. One pair of keys may be used to encrypt information and the public key could be backed up to another location. The second pair would be used only for digital signatures and the public key in that pair would never be backed up.

4.10.3   Key-Handling Procedures

Certain procedures can help ensure that keys are properly handled. These procedures include:

4.10.3.1 Escrow

Key escrow refers to a process in which keys are managed by a third party, such as a trusted CA. In key escrow, the private key is split and each half is encrypted. The two halves are sent to the third party, which stores each half in a separate location. A user can then retrieves the two halves, combine them and use this new copy of the private key for decryption. Key escrow relieves the end user from the worry of losing her private key. The drawback to this system is that after the user has retrieved the two halves of the key and combined them to create a copy of the key, that copy of the key can be vulnerable to attacks .Some U.S government agencies have proposed that the federal government provide key escrow services. This would allow the government to view encrypted communications, assuming proper permissions were granted by a judge.

4.10.3.2 Expiration

Keys have expiration dates. This prevent an attacker who may have stolen a private

key from being able to decrypt messages for an indefinite period of time. Some systems set keys to expire after a set period of time by default.

4.10.3.3 Renewal

Instead of letting a key expire and then creating a new key, an existing key can be renewed. With renewal, the original public and private keys can continue to be used and new keys do not have to generate. However, continually renewing keys makes them more vulnerable to theft or misuse.

4.10.3.4 Revocation

Whereas all keys should expire after a set period of time, a key may need to be revoked prior to its expiration date .For example; the need for revoking a key may be the result of an employee being terminated from his position. Revoked keys cannot be reinstated. The CA should be immediately notified when a key is revoked and then the status of that key should be entered on the CRL.

4.10.3.5 Recovery

What happens if an employee is hospitalized for an extended period, yet the organization for which she works needs to transact business using her keys? Different techniques may be used. Some CA systems have an embedded key recovery system in which a key recovery agent (KRA) is designated, and who is a highly trusted person responsible for recovering lost or damaged digital certificates. Digital certificates can then be archived along with the user's private key. If the user is unavailable or if the certificate is lost, then the certificate with the private key. If the user is unavailable or if the certificate is lost, then the certificate with the private key can be recovered. Another technique is known as M-of-N control. A user's private key is encrypted and divided into a specific number of parts such as three. The parts are distributed to other individuals, with an overlap so that multiple individuals have the same part. For example, the three parts could be distributed to six people, with two people each having the same part. This is known as the N group. If it is necessary to recover the key, a smaller subset of the N group, known as the M group, must meet and agree that the key should be recovered. If a majority of the M group can agree, they can then piece the key together. M-of-N control is illustrated in figure below.

The reason for distributing parts of the key to multiple users is that the absence of one member would not prevent the key from being recovered.

Suspension

The revocation of a key is permanent; key suspension is for a set period of time. For example, if an employee is on an extended medical leave, it may be necessary to suspend the use of her key for security reasons. A suspended key can be later reinstating. As with evocation, the CA should be immediately notified when a key is suspended and then the status of that key should be checked on the CRL to verify that it is no longer valid.
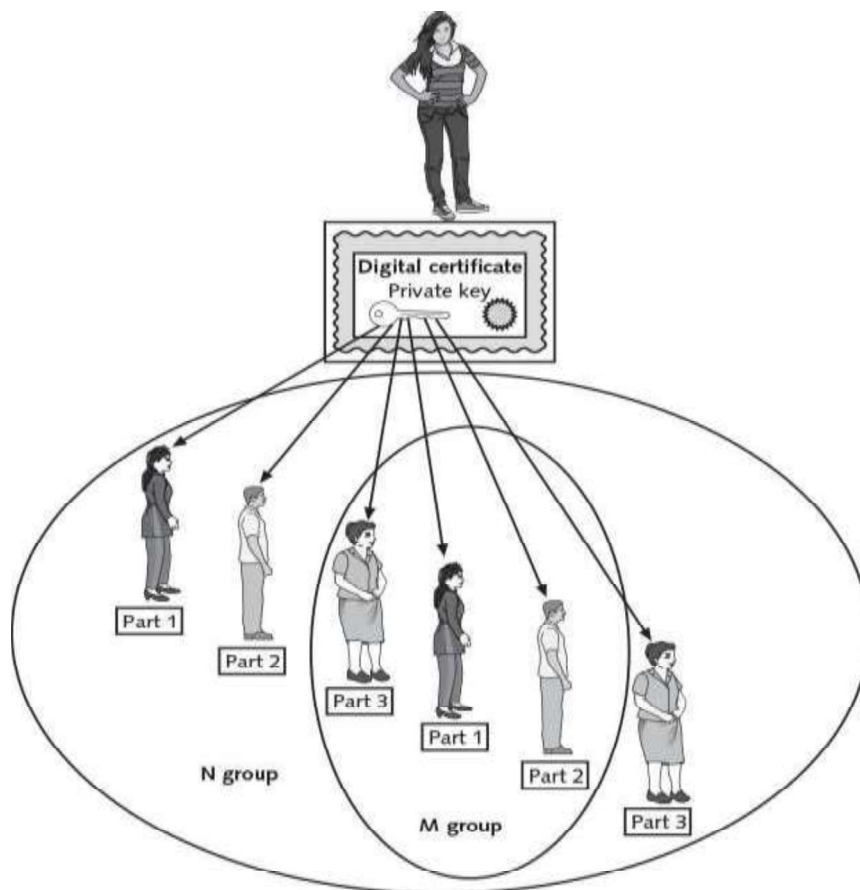
Fig: M-of-N Control

Destruction

Key destruction removes all private and public keys along with the user's identification information in the CA. When a key is revoked or expires, the user's

information remains on the CA for audit purposes.

4.11 ENTERPRISE KEY AND CERTIFICATE MANAGEMENT (EKCM)

The starting point in any certificate and private key management strategy is to create a comprehensive inventory of all certificates, their locations and responsible parties. This is not a trivial matter because certificates from a variety of sources are deployed in a variety of locations by different individuals and teams - it's simply not possible to rely on a list from a single certificate authority. Certificates that are not renewed and replaced before they expire can cause serious downtime and outages. Some other considerations:

- Regulations and requirements, like PCI-DSS, demand stringent security and management of cryptographic keys and auditors are increasingly reviewing the management controls and processes in use.

- Private keys used with certificates must be kept secure or unauthorized individuals can intercept confidential communications or gain unauthorized access to critical systems. Failure to ensure proper segregation of duties means that admins who generate the encryption keys can use them to access sensitive, regulated data.

- If a certificate authority is compromised or an encryption algorithm is broken, organizations must be prepared to replace all of their certificates and keys in a matter of hours.

4.11.1 Multicast Group Key Management

Group Key Management means managing the keys in a group communication. Most of the group communications use multicast communication so that if the message is sent once by the sender, it will be received by all the users. The main problem in multicast group communication is its security. In order to improve the security, various keys are given to the users. Using the keys, the users can encrypt their messages and send them secretly.

4.11.2 Challenges

Several challenges IT organizations face when trying to control and manage their

encryption keys are:

- Complex Management: Managing a plethora of encryption keys in the millions.

- Security   Issues: Vulnerability   of   keys   from   outside hackers/malicious insiders.

- Data Availability: Ensuring data accessibility for authorized users.

- Scalability: Supporting multiple databases, applications and standards.

- Governance: Defining policy driven, access, control and protection for data.

4.11.3 Key Management Solution

A key management solution (KMS) is an integrated approach for generating, distributing and managing cryptographic keys for devices and applications. Compared to the term key management, a KMS is tailored to specific use-cases such as secure software update or machine to-machine communication. In a holistic approach, it covers all aspects of security - from the secure generation of keys over the secure exchange of keys up to secure key handling and storage on the client. Thus, a KMS includes the backend functionality for key generation, distribution, and replacement as well as the client functionality for injecting keys, storing and managing keys on devices. With the Internet of Things, KMS becomes a crucial part for the security of connected devices.

4.12 DIGITAL SIGNATURES

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message.

This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

4.13 MODEL OF DIGITAL SIGNATURE

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration.
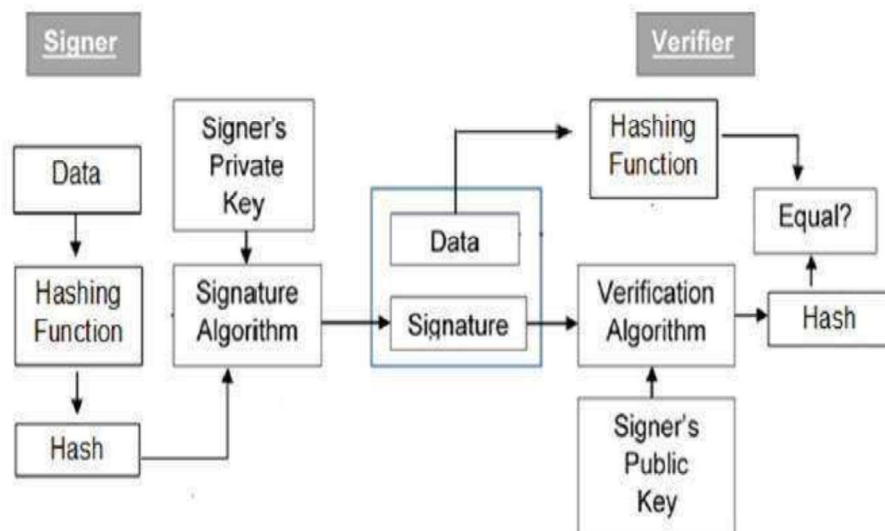
The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.

- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.

- Signer feeds data to the hash function and generates hash of data.

- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.

- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.

- Verifier also runs same hash function on received data to generate hash value.

- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.

- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

- It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

- Let us assume RSA is used as the signing algorithm. As you know in public key encryption, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

4.14 IMPORTANCE OF DIGITAL SIGNATURE

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.

- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

4.15 ENCRYPTION WITH DIGITAL SIGNATURE

In many digital communications, it is desirable to exchange an encrypted message than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archive by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −

Sender's Side

Data → Encryption using Receiver's public key → Encrypted Data + Digital Signature

Hashing Function

Hash → Digital Signature with Sender's private key
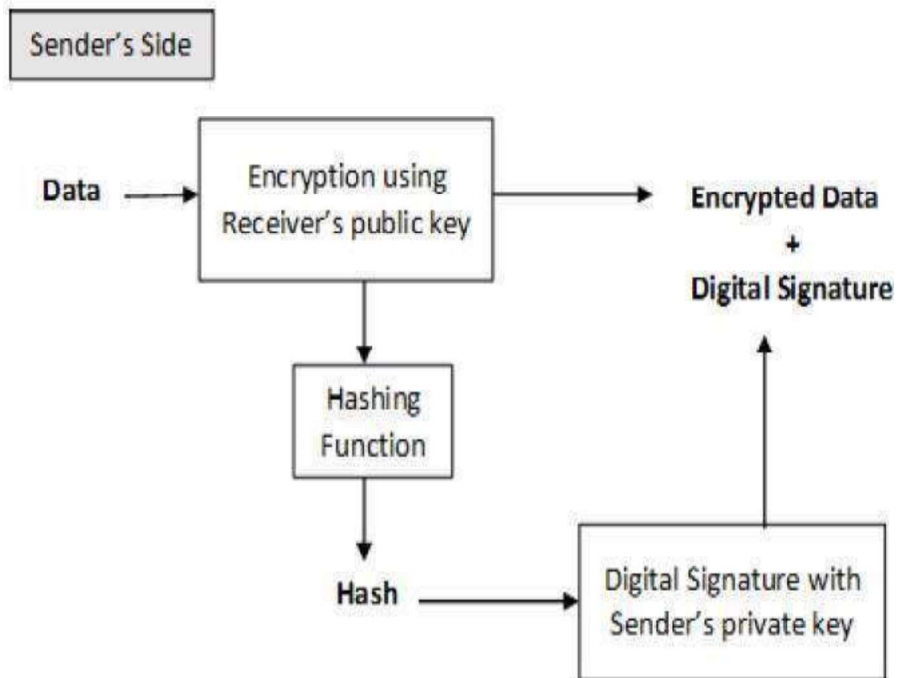
The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

4.16 LET US SUM UP

A public key infrastructure (PKI) is a framework for all of the entities involved in digital certificates-including hardware, software, people, policies, and procedures-to create, store, distribute, and revoke digital certificates. PKI is essentially digital certificate management. Public- Key Cryptography standards (PKCS) are a numbered set of PKI standards. Although they are informed standards, they are widely accepted today. One of the principal foundations of PKI is that of trust. There are three basic PKI trust models that use a CA. The hierarchical trust model assigns a single hierarchy with one master CA called the root, who assigns all digital certificates authorities with a single key. The bridge trust model is similar to the distributed trust model. There is no single CA that signs digital certificates, yet the CA acts as a facilitator to interconnect all other CAs. The distributed trust model has multiple CAs that signs digital certificates. An organization that uses multiple digital certificates on a regular basis needs to properly manage those digital certificates. This includes establishing policies and practices and determining the life cycle of a digital certificate. Because keys form the very foundation of PKI systems, it is

important that they be carefully managed.

4.17 Further Readings

1. Certificate Policies and Certification Practice Statements Author: Sharon Boeyen Date: February 1997 Version: 1.0

2. http://www.tomsitpro.com/articles/public-key-infrastructure- introduction,2-884.html

3. Course VI Information System(PGDCS-06), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

4. https://www.tutorialspoint.com/cryptography/public_key_infrastruct ure.htm

4.18 Assignments

1. What is PKI? What are the components of PKI environment?

2. What are the key reasons to deploy Public Key Infrastructure in a company?

3. What is digital signature? Why digital signature is important?

4. What are the two specific requirements of key management for public key cryptography?

5. Explain the process of digital signature

6. Write a short note on Key Management.

7. Discuss how Digital Signature provides non-repudiation of message authentication and data integrity

Block-3
Internet and Web Application Security

Unit 1: Email Security **1**

Unit Structure

1.1 Learning Objectives

After going through this unit you should be able to

- To be certain what they send goes to the right person/place.
- To be certain that the right person/place can read the information.
- To be able to use signed information as proof to a court or other body.
- To stop the wrong people from reading personal and private information.
- To be familiar with the organizational policies on E-mail.

1.2 Introduction

Email, short for Electronic Mail, consists of messages which are sent and received using the Internet. There are many different email services available that allow you to create an email account and send and receive email and attachments, many of which are free. So it acts as a powerful medium of communication. However, it may suffer from many security attacks and hence different E-mail service providers adopt many security mechanisms to offer secured services. They implement different security gateways in order to provide secured data transmission over the Internet.

Email security gateways are products that are used to prevent emails that violate an organization's policies -- particularly emails with malicious intent -- from reaching their destinations. All email security gateways can quarantine or block emails that contain detected malware, phishing attacks, spam and other malicious content. This prevents many attacks from reaching their intended recipients, which in turn reduces the number of successful compromises of hosts, user credentials and sensitive data.

1.3 Electronic Mail (E-Mail)

The Electronic Mail or email has become popular in last few years after the inceptions of the Internet. Email is very fast and guarantees delivery.
Email has some issues, but it is the most widely used, and accepted form of electronic communication. Email is tried and true. It is the de facto means of written communication – especially in business. However, it's not always the most efficient

method.

Advantages

- It is universal. Everyone has an email address, and you can send a message from any email provider to any email provider.
- You can send a single message to a large group of people. Rather than sending out a bunch of separate text messages, or engaging in various instant messaging situations, you can communicate with an entire team or list of individuals at once.
- It provides a written record. Messages can be centrally stored and archived, and the history of replies or forwards can be maintained.

Disadvantages

- It is slow. "Slow" is a relative term, since email messages are delivered to the other side of the world in a matter of minutes— perhaps seconds. But, when a message is actually retrieved is a function of the mail server and email client software, and you don't really know when it is actually received.
- It is filled with spam. Although efforts like Microsoft's campaign to take down botnets have reduced the deluge of spam, a recent Symantec Intelligence Report suggests spam still accounts for nearly three fourths of all email.
- It is a primary means of spreading malware. Whether it is a link to a malicious website, or an infected file attachment, email is the preferred method of propagating malware attacks.

Now let us discuss the protocols used in E-Mail systems.

Three protocols are mainly used for today's email:

1. SMTP that operates over TCP allows for the sending/receiving of email.
2. POP that operates over TCP allows us to intermittently retrieve email.
3. DNS operates over and makes it simple.

RFC 822 defines the structure for the message, and RFC 821 specifies the protocol that is used to exchange the mail between two network stations. It truly is amazing how old the original mail protocol is, and it is still in use today. So we have email to send to one another, completely bypassing the postal system.

There are some who call the postal system "snail mail." Many people today still immensely enjoy receiving a handwritten letter from a family member, friend, or a business correspondence through the postal system.

Email does have many, many advantages and one of the top advantages is speed. The biggest disadvantage is lack of emotion. Like everything else, email has its place; it is merely another form of communication. In order to send and receive mail between users, there are actually two protocols (possibly three) that are used:

SMTP: Used for the actual transport of mail between two entities (mail servers).

POP (Post Office Protocol): A protocol that allows single users to collect their mail on one server.

DNS: Used to identify the mail hosts for a domain or hostname. A Mail can be sent and received using only SMTP, but the other protocol involvement makes it much easier to use and is more efficient. This is a protocol that allows users to transmit messages (Mail) between other users. It is one of the most widely used applications of the TCP/IP protocol.

1.3.1 Simple Mail Transfer Protocol (SMTP)

The protocol is relatively simple. A message will be created, properly addressed, and sent from a local application to the SMTP application, which will store the message. The server will then check (at periodic intervals) to see if there are any messages to deliver. If there are, the mail server will try to deliver the message. If the intended recipient is not available at the time of delivery, the mail server will try again later. The mail server will try a few times to deliver the message and, if it cannot, will either delete the message or return it to the sender. The address has the general format of local-part @ domain-name. By this, you should recognize the domain name format.

There are two entities to this system, the *sender* SMTP and the *receiver* SMTP that are used to transport mail between two systems. The sender SMTP will establish communications with a receiver SMTP. Attachments are allowed with Internet email but not directly with the protocol used in SMTP (send mail protocol).

Email applications convert using a variety of protocols like MIME (Multipurpose Internet Mail Extensions). SMTP (or more specific, send mail) can only handle text. Therefore, most email applications convert an attachment to text before sending. A common type is MIME. At the receiver, the email application converts the attachment back to its original format.

SMTP Flow:

The SMTP design is based on the following model of communication: Once you have filled out the header and body section of your mail message, the sender SMTP

establishes two-way communication to a receiver SMTP. The receiver SMTP may be either the ultimate destination or a transient stop on the way to the final destination. Commands are sent to the receiver by the sender SMTP and SMTP replies are sent from the receiver SMTP to the sender SMTP in response to each of the commands. Once two-way communication has been established, a series of commands (of which you can see operate using some mail applications) are issued.

The sender SMTP will send a HELLO (HELO) command identifying who it is using its domain name to the receiver. The receiver acknowledges this with a reply using its domain name. Next, the server issues a MAIL command to the receiver. In this will be the identification of the person (place, or thing) sending the mail. The receiver acknowledges this with an OK. The sender SMTP then sends a RCPT command to the receiver, using the intended receiver name as an argument. Each recipient in the list is sent to the receiver one at a time, and each time the receiver acknowledges with an OK for those recipients that it knows about. For those that it does not know about (different domain name), it will send back a different reply that it is forwarding the message on.

For any intended recipients received from the SMTP sender for which it has no account, the receiver will reply to the sender that no such user(s) exists.

After the intended recipients have been ACK'd or NACK'd, the SMTP sender sends the DATA command and the SMTP receiver will OK this and indicate what the end of message identifier should be. Once this is received (the ending identifier), the SMTP receiver will reply with an OK. Notice that all data is received, the ending identifier is received, and then a reply message is sent by the receiver.

If everything went okay, the sender ends the connection with a QUIT command. The SMTP receiver will reply indicating that the communication channel is closed. So the minimum commands that a receiver must support are HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT.

Depending on the mail program that you use, the transaction between a recipient and sender of mail has been the same since RFC 821 was written. The interface allows you to complete the mail message, filling in the header (addresses and subject) and the body (text) of the letter. When you press the Send button, the following transaction takes place. Some mail programs actually place the mail commands and state numbers on display while the transaction is taking place. It

should be noted here that sending mail is immediate. It may get queued for a small length of time on different routers, and transient mail servers, but not for long. This is for the transport of mail. Most electronic mail today is sent via SMTP and will reside on your mail server host until you retrieve it using POP. Today, retrieving your mail does not mean that you have to run the SMTP protocol. A server host will accept mail messages directed to you on your behalf. Then you can sign on any time you want and retrieve your mail.

1.3.2 DNS Interaction for Mail

A record known as the MX record in DNS identifies a mail exchanger for the purpose of identifying hosts for recipients. A mail exchanger is hosts that will either process or forward mail for the domain name. Processing means that the host will deliver it the host to which it is addressed or hand it off to another transport, such as UUCP or BITNET. Forwarding means that the host will forward the message on to the final destination or to another mail exchanger closer to the destination. There can be multiple entries for a mail exchanger in a DNS. Each MX entry will have a precedence number beside it and this signals the sender which mail host it should try first. If the precedence value is equal among MX records, then the sender will randomly pick one from the list. Once the mail sender has successfully delivered the mail to one of the MX hosts, its job is done. It is the job of the MX host to make sure it is forwarded on to its final destination. If there are no MX records for a domain name, it is up to the mailer application as to what happens next. Some will try to deliver it to the IP address of the mail destination.

1.3.3 Post Office Protocol (POP)

The original mail program RFC 821 (which is the one in use today) was set up to send messages directly to a user logged in to a terminal, as well as store these messages to a mailbox. The commands allowed for the receiver to determine if the user was logged on to a terminal (not a PC), if they were accepting messages, and if they were not, are there a mailbox to deliver some mail to. There were no message attachments and messages were sent and received in 7-bit ASCII (8th bit was set to 0); therefore, this would not allow for binary messages to be sent (i.e., no attachments). In fact, the original message was not to exceed 1000 characters (however, implementations that could go beyond this barrier were strongly encouraged to do so). So, to operate mail, the host must be operational (able to

receive) all the time.

Today, terminals do exist, but more commonly, personal computers have taken their place. Therefore, the final recipient will be the personal computer. The personal computer will have both SMTP and POP. Even though a personal computer will retrieve its mail via POP, it will still use the SMTP functions to send its mail. Since SMTP expects to be able to deliver mail immediately, this would mean that all users would have to have their personal computers on 100 percent of the time in order to accept mail. Second, to receive and read your mail, you must log on to a specific host. To operate a mail server generally requires that the mail server is available for a majority of the time, has the ability to store many mail messages, and is able to fully run SMTP and accept mail from an SMTP sender. While this may have been feasible for situations like terminal-to-host connectivity, it is not feasible for situations that we have today; namely, personal computers and mobile workers. SMTP is a very robust transaction oriented protocol.

SMTP is set up to send and receive mail by hosts that are up full time. No rules for those hosts that is intermittent on the LAN. POP emulates you as a host on the network. It receives SMTP mail for you to retrieve later. POP accounts are set up for you by an ISP or your company. POP retrieves your mail and downloads it to your personal computer when you sign on to your POP account. What we need is the ability for SMTP to operate (drop off the mail, like a PO Box at the post office), and then another protocol to download to our personal computers (we drop by the post office and retrieve our mail from the post office box.). POP is the protocol to allow for this. Mail can be delivered to a drop-off point and POP allows us to log in and retrieve our mail.

1.3.4 SMTP, DNS, and POP Topology

For example, mail is sent from your PC to J's PC. In order to accomplish this, the send mail (SMTP) program is established to the SMTP server on your ISP. A DNS lookup is accomplished using the root DNS server to find the domain of the intended recipient. A call is made to recipients DNS to find the mail server (which could be the same server as the DNS). Once the mail server is found (its IP address is found), mail is sent to that server. The POP function delivers it to your mail box on that mail server so that when J's PC retrieves mail; your mail message will be waiting.

1.4 E-Mail Security

The three main goals of Information Security are to maintain the confidentiality, integrity, and availability of information resources. These three principles can be directly applied to the area of email security as well. Confidentiality of email involves making sure it is protected from unauthorized access. Integrity of email involves a guarantee that it has not be modified or destroyed by an unauthorized individual. Availability of email involves ensuring that mail servers remain online and able to service the user community. A weakness in any one of these three key areas will undermine the security posture of an email system and open the door to exploitation. Email messages are composed, delivered, and stored in a multiple step process, which starts with the message's composition. When the user finishes composing the message and sends it, the message is transformed into a standard format: an RFC 2822 formatted message. Afterwards, the message can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server. The mail client then provides the sender's identity to the server. Next, using the mail server commands, the client sends the recipient list to the mail server. The client then supplies the message. Once the mail server receives and processes the message, several events occur, such as recipient server identification, connection establishment, and message transmission. Using Domain Name System (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client, delivering the message to the recipient(s).

1.4.1 E-Mail Security issues

- An E Mail is not actually real-time and can afford to use public key cryptosystems.
- Certification of keys is much harder because anyone can send any one else some mail strictly end-to-end
- IPSec/firewalls might get in the way here.
- A single message can be sent to many parties
- There can be message forwarding loops due to distribution lists or even

someone's .forward file.

- Duplicate copies can be sent to same individual.
- Recipient or intermediate node may not be ready to receive mail

1.4.2 Security Services over Email

- Privacy: No one should read message except recipient
- Authentication: Recipient should know exactly who the sender is
- Integrity: Recipient should be able to tell whether message was altered in transit
- Non-Repudiation: Recipient can prove that the sender really sent it.
- Proof of submission: Verification to the sender that the mailer got it
- Proof of delivery: Verification to sender that the recipient got it
- Message flow confidentiality: Eavesdropper cannot determine the sender's ID
- Anonymity: Ability to send so recipient does not know sender
- Containment: Ability to keep secure messages from "leaking" out of a region.
- Audit: Logging of events having relevance to security
- Accounting: Maintain usage statistics (might charge for service)
- Self-destruct: Message is destroyed on delivery
- Message sequence integrity: Sequence of messages has arrived in order, without loss.

1.5 Threats to E-Mail Security

Email security is threatened by a range of issues. Malicious software is one which frequently spread via **e-mail** over the Internet. **E-mail** also has some original **threats** of its own, including spam, spoofing, and phishing attacks. Let us now individually discuss these threats to E-Mail security.

1.5.1 Viruses

One of the most publicized and high risk of all the issues is viruses. Viruses are so dangerous because they often deliver extremely destructive payloads, destroying data, and bringing down entire mail systems. The impact of viruses on organizations is huge. The impact goes far beyond money, resources, and effort required recovering from such incidents. It also includes loss of productivity, corrupt and/or lost data, and loss of user confidence.

1.5.2 Spamming

Sending of unsolicited and commercial bulk message over the internet is known as spamming. An email can be classified as spam, if it meets following criteria:

a) **Mass mailing**: - the email is not targeted to one particular person but to a large number of peoples.

b) **Anonymity**: - The real identify of the person not known.

c) **Unsolicited:** - the email is neither expected nor requested for the recipient.
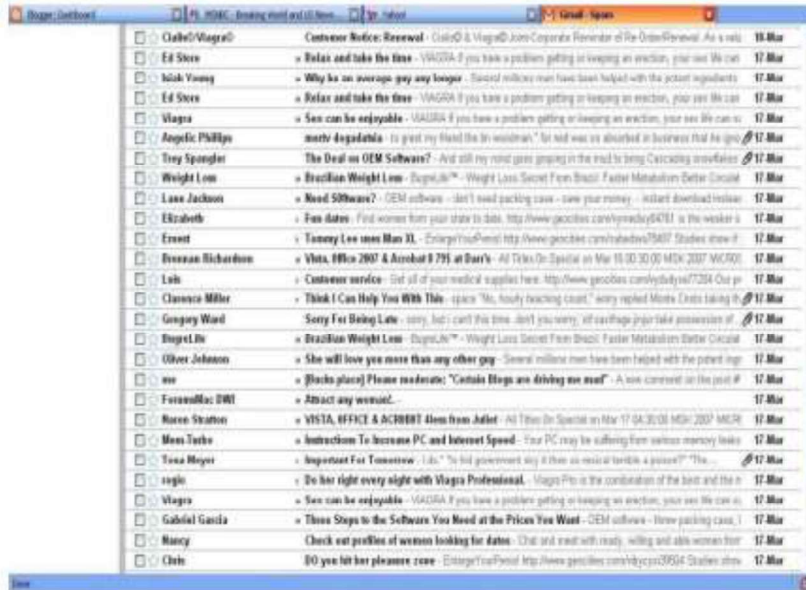
Fig: Spamming mails

These spams' not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space of the mailbox.

1.5.3 Social engineering

Rather than hack into a system, an attacker can use e-mail to gather sensitive information from an organization's users or get users to perform actions that further an attack. A common social engineering attack is e- mail spoofing, in which one person or program successfully masquerades as another by falsifying the sender information shown in e-mails to hide the true origin.

1.5.4 Email Spoofing

Email spoofing is the creation of email messages with a forged sender address. It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.

Fig: Example of email spoofing

1.6 Pretty Good Privacy (PGP)

PGP stands for "Pretty Good Privacy," and it's most often used for sending encrypted messages between two people. PGP works by encrypting a message using a public key that's tied to a specific user; when that user receives the message, they use a private key that's known only to them to decrypt it.

This system ensures that it's easy to send encrypted communications, because the only thing needed to encrypt a message is a public key and the proper PGP program. But it's also quite safe, as messages can only be decrypted with privately known keys that are password-protected.

In addition to encryption, PGP also allows for digital signatures. By signing your encrypted message with your private key, you provide a way for the recipient of the message to see if the content of the message has been changed. If even a single letter in the message is changed before its decrypted, the signature will be invalidated, alerting the recipient to foul play.

1.6.1 Mechanics of PGP

The mathematical mechanics of PGP are extremely complicated, but the diagram below will give you a general idea of how the system works.

For email security or sending secure email we should use Pretty Good Privacy. Pretty Good Privacy provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm such as Tripler DES or CAST-128.

Email messages can be protected by using cryptography in various ways, such as the following:

- Signing an email message to ensure its integrity and confirm the identity of its sender.
- Encrypting the body of an email message to ensure its confidentiality.
- Encrypting the communications between mail servers to protect the confidentiality of both message body and message header.

The first two methods, message signing and message body encryption, are often used together; however, encrypting the transmissions between mail servers is typically used only when two organizations want to protect emails regularly sent between each other.
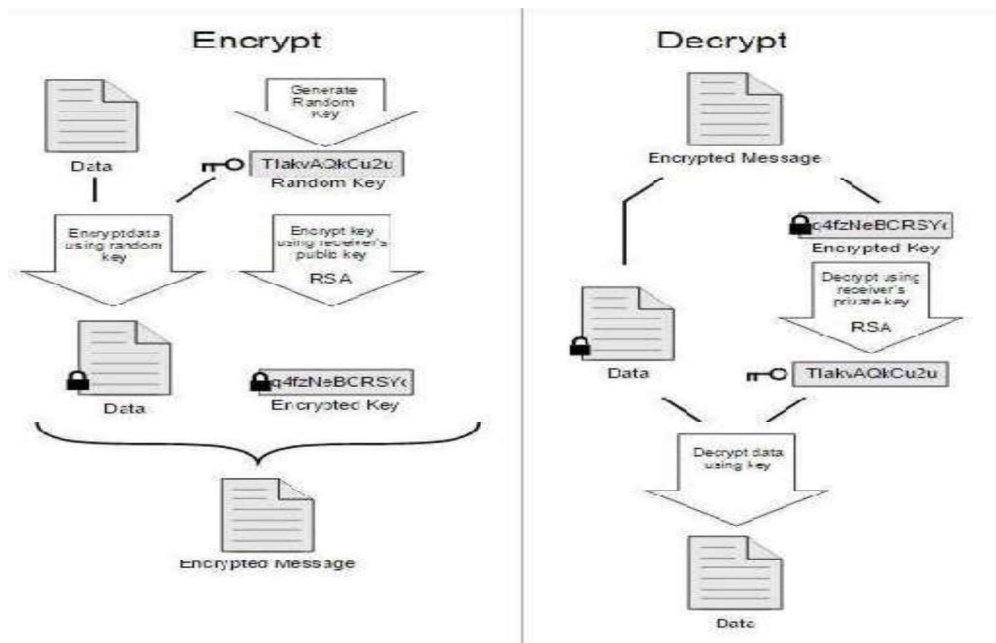
Fig: Mechanics of PGP

For example, the organizations could establish a virtual private network (VPN) to encrypt the communications between their mail servers over the Internet. Unlike methods that can only encrypt a message body, a VPN can encrypt entire messages, including email header information such as senders, recipients, and subjects. In some cases, organizations may need to protect header information. However, a VPN solution alone cannot provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient.

1.6.2   How PGP works

PGP combines some of the best features of both conventional and public key cryptography. PGP is a hybrid cryptosystem. When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression saves modem transmission time and disk space and, more importantly, strengthens cryptographic security. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis. (Files that are too short to compress or which don't compress well aren't compressed.)

1.6.3   How Secure is PGP?

While it's impossible to say that any particular encryption method is 100% secure, PGP is generally regarded as being extremely safe. The two-key system, digital signatures, and the fact that PGP is open-source and has been heavily vetted by the public all contribute to its reputation as one of the best encryption protocols. Bruce Schneider once called PGP "the closest you're likely to get to military-grade encryption," and PGP.net says that there are "no practical weaknesses."

1.7   SMIME

SMIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security. SMIME is used mainly as the industry standard for commercial and organizational use, while PGP remains as the choice for personal e-mail security for many users. Before understanding SMIME, you need to understand an e-mail format

standard, RFC 822, which is still in common use.

1.7.1 RFC 822

RFC 822 defines a format for text messages that are sent using electronic mail. It has been the standard for Internet-based text mail message and remains in common use. In the RFC 822context, messages are viewed as having an envelope and contents. The envelope contains whatever information is needed to accomplish transmission and delivery. The contents compose the object to be delivered to the recipient. The RFC 822 standard applies only to the contents.

However, the content standard includes a set of header fields that may be used by the mail system to create the envelope, and the standard is intended to facilitate the acquisition of such information by programs.

A message consists of some number of header lines (the header) followed by unrestricted text (the body). The header is separated from the body by a blank line. A header line usually consists of a keyword, followed by a colon, followed by the keyword's arguments; the format allows along line to be broken up into several lines. The most frequently used keywords are From, To, Subject, and Date.

1.7.2 Multipurpose Internet Mail Extensions (MIME)

MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail. The following are some of the limitations of the SMTP/822 scheme:

- SMTP cannot transmit executable files or other binary objects. A number of schemes are in use for converting binary files into a text form that can be used by SMTP mail systems, including the popular UNIX UUencode/UUdecode scheme. However, none of these is a standard or even a de facto standard.
- SMTP cannot transmit text data that includes national language characters because these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.
- SMTP servers may reject mail message over a certain size.

- SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.
- SMTP gateways to X.400 electronic mail networks cannot handle non textual data included in X.400 messages.

1.7.3 MIME Header Fields

The five header fields defined in MIME are as follows:

MIME-Version: Must have the parameter value 1.0. This field indicates that the message conforms to RFCs 2045 and 2046.

Content-Type: Describes the data contained in the body with sufficient detail that the receiving user agent can pick an appropriate agent or mechanism to represent the data to the user or otherwise deal with the data in an appropriate manner.

Content-Transfer-Encoding: Indicates the type of transformation that has been used to represent the body of the message in a way that is acceptable for mail transport.

Content-ID: Used to identify MIME entities uniquely in multiple contexts.

Content-Description: A text description of the object with the body; this is useful when the object is not readable (e.g., audio data).

1.7.4 S/MIME Functionality

S/MIME provides the following functions:

- **Enveloped data:** This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.
- **Signed data:** A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message cans only be viewed by a recipient with S/MIME capability.
- **Clear-signed data:** As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.
- **Signed and enveloped data**: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

1.8 E-Mail Policy

Email is the electronic equivalent of a postcard. Because of this, it requires special policy considerations. From archiving to content guidelines, organizations have a lot to consider when writing email policies.

1. **Rules for using email:**

Policies should be written to promote the responsible use of email that supports the organization's goals and business requirements.

Some of the items that should be included in the policy concern courtesy, content, general usage, and compliance with the policy.

2. **Administration of email:**

- Policies describing the administration of email discuss the actions the organization will follow in the management of the email system.

- Administrative policies should establish the right to scan messages passing through the email system. This scanning can be for viruses or content.

- Regardless of the scanning type, there should be a policy in place that says the organization is doing this.

- Email policies might include mechanisms to limit the size of messages to prevent the overloading of servers and network bandwidth.

- To mitigate other problems, the organization might want to include a policy that allows them to use proxies, gateways, and other means to aid in the transmission of messages. These policies should not imply that messages are being filtered or retained.

- If email messages are archived, there should be a policy that outlines the basics for how this will work. This policy also should define retention periods and potential exceptions to the policy.

3. **Use of email for confidential communication:**

- Policies for sending confidential communication include provision for encrypting the data before transmission and signing them with digital signatures.

- Encryption policies are really not the scope of email policies. Thus the policy statements should refer the user to the organization's encryption policy for that information.

1.9 Let us Sum Up

Email has been used by people since the birth of the Internet. Messages are sent in near real-time and are not that obtrusive. The recipient does not have to read the message immediately. It also gives the writer a chance to word the message carefully. Protocols like PGP, MIME, S/MIME and POP enable secured E-Mail delivery and reception. Furthermore, E-Mail users in the organization must adopt certain policies to maintain various levels of security to maintain privacy, confidentiality and availability of their message.

1.10 Further Readings

1. Fundamentals of Information Security (PGDCS-01), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e-Governance and Cyber Security.

2. Cyber Security Techniques (PGDCS-02), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e- Governance and Cyber Security,

3. Cyber Attacks and Counter Measures: User Perspective, (PGDCS-03), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

4. Information System (PGDCS-06), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

5. http://s1216.photobucket.com/user/rjtheindian/media/ emailspoofing3.png.html http://library.ahima.org

1.11 Assignments

1. Write short notes on MIME.

2. Explain the working of PGP in secured E-Mail communication.

3. Write the limitations of the SMTP/822 scheme.

Unit 2: Web Application Security

2

Unit Structure

2.1   Learning Objectives

After going through this unit you should be able to

- Define Web Application Security
- Understand the web authentication techniques
- Understand the meaning and use of Cookies
- Identify the web application vulnerabilities
- Know the key concepts of SQL Injection Attacks
- Understand how SQL Injection works

2.2   Introduction

Today almost every organization web-applications are the integral part of information infrastructure to allow information exchange with employee, customers, partners, etc. Ecommerce is also grown rapidly and everything is moving up on computer network from vegetables to electronics, today customer is free to shop online at a click of mouse.

Security is a critical part of any Web application. Web application security with security of websites, web applications and web services. Web application security draws on the principles of application security but applies them specifically to Internet and Web based systems.

Web applications by definition allow users access to a central resource — the Web server — and through it, to others such as database servers. By understanding and implementing proper security measures, you safeguard your own resources as well as provide a secure environment in which your users are comfortably working with your application.

This unit provides an overview of security for Web applications, describing what types of issues you need to think about when creating applications.

2.3   Web Application Security

The Wikipedia defines, "Web application security as a branch of Information Security that deals specifically with security of websites, web applications and web services". At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems.

The World Wide Web has evolved from a system that delivers static pages to a platform that supports distributed applications, known as web applications, and has become one of the most prevalent technologies for information and service delivery.

As shown in figure below, web application consists of client side and server side components. The client side component which includes static web pages with embedded scripting languages e.g. JavaScript executed within browser. Client make http request to the web server by specifying particular URL via Internet.
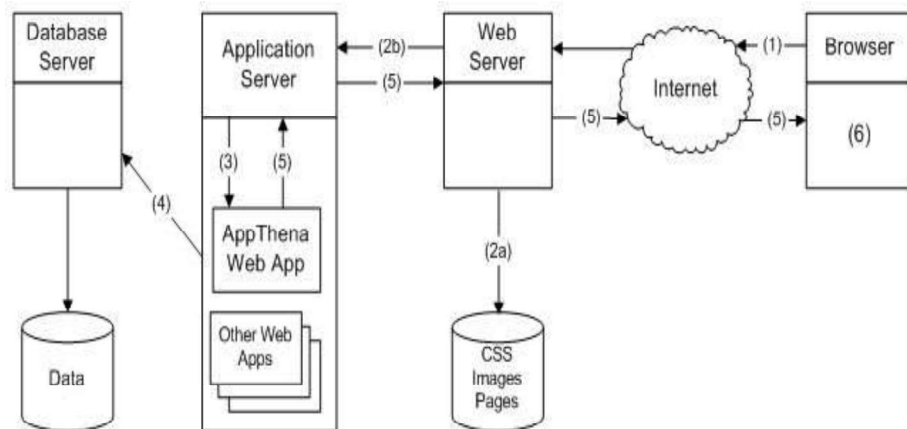
Fig: Web application Architecture

At server side, client's request is processed within web server using dynamic HTML pages either through execution (CGI, or Java Servlets) or interpretation (PHP, JSP) and provides appropriate response to the client request. These servers actually contain the business logic of the application. Business logic refers to the algorithm implementation that to be performed to the data such a show to create, display, stored and changes the data. Client can communicate with server side code using asynchronous call such as AJAX and dynamically updates the HTML pages. The web applications interact with the backend files system or database server for storing and retrieving data. Aspects of web application including programming language,

state maintenance and logic implementation differentiate the web application from traditional applications.

Security Issues:

As web applications are increasingly used to deliver critical services, they become a valuable target for security attacks. Many web applications interact with back-end database systems, which may store sensitive information (e.g., financial, health). A compromised web application could result in an enormous information breach, severe financial losses, and lead to many types of ethical and legal consequences.

Web applications are unfortunately prone to high security risks, and so are the networks to which web servers are connected. Setting aside risks created by employee use or misuse of network resources, your web server and the website encounter most serious sources of security risk.

Web servers by design open a window between your network and the world. The care taken with server maintenance, web application updates and your web site coding will define the size of that window, limit the kind of information that can pass through it and thus establish the degree of web security you will have.

These days, web-applications have been continuously targeted by attackers for various interests. Cross Site Scripting Attack (XSS), SQL injection, File Inclusion, Malicious File Uploads is few attacks to name in web-application domain.

2.3.1   Security issues in web Application

Why old approaches to security fail

The security analysis of web applications does not assume the standard threat model of communications security where the attacker is ''in control of the network'' and can read, modify, delete, and insert messages. In the new web threat model, the attacker is a malicious end system. This attacker only sees messages addressed to him and data obtained from compromised end systems. The attacker can also guess predictable fields in unseen messages.

Web Application Vulnerabilities and Attacks

In general, there are three types of security vulnerabilities within web applications at different levels: input validation vulnerability at the single request level, session management vulnerability at the session level, and application logic vulnerability at

the level of the whole application. In what follows, we describe the above three types of vulnerabilities and the common attacks that exploit these vulnerabilities.

Common Attacks on Web Applications

The common attacks on web applications include Cross Site Scripting (XSS) Attacks, Forced browsing attack URL Access vulnerability, Username enumeration, Remote code execution, Format String, Vulnerabilities, SQL Injection attack etc. In this unit we will discuss more on SQL Injection attacks.

2.3.2 Cross Site Scripting

It is an activity which involves injecting a malicious client side script into a trusted website. As soon as the browser executes the malicious script, the malicious script gets access to the cookies and other sensitive information and sent to remote servers. Now this information can be used to gain financial benefit or physical access to a system for personal interest.
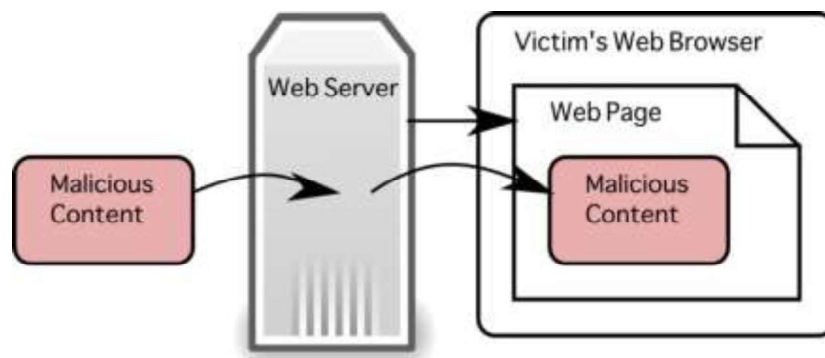
Fig: Cross Site Scripting

2.4 Web Authentication Techniques

Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic (except DHCP and DNS -related packets) from a particular client until that client has correctly supplied a valid username and password. It is a simple Authentication method without the need for a supplicant or client utility. Web authentication is typically used by customers who want to deploy a guest-access network. Typical deployments can include "hot spot" locations such as T-Mobile or Starbucks.

Keep in mind that web authentication does not provide data encryption. Web

authentication is typically used as simple guest access for either a "hot spot" or campus atmosphere where the only concern is the connectivity.

2.4.1 HTTP Basic authentication

HTTP Basic authentication is a method for the client to provide a username and a password when making a request.

This is the simplest possible way to enforce access control as it doesn't require cookies, sessions or anything else. To use this, the client has to send the Authorization header along with every request it makes. The username and password are not encrypted, but constructed this way:

- username and password are concatenated into a single string: username: password
- this string is encoded with Base64
- the Basic keyword is put before this encoded value

What are the drawbacks of using HTTP Basic authentication?

- The username and password are sent with every request, potentially exposing them - even if sent via a secure connection
- Connected to SSL/TLS, if a website uses weak encryption, or an attacker can break it, the usernames and passwords will be exposed immediately
- There is no way to log out, the user using Basic authentication expiration of credentials is not trivial - you have to ask the user to change password to do.

2.4.2 Cookies

When a server receives an HTTP request in the response, it can send a Set- Cookie header. The browser puts it into a cookie jar, and the cookie will be sent along with every request made to the same origin in the Cookie HTTP header.

To use cookies for authentication purposes, there are a few key principles that one must follow.

Always use Http Only cookies

To mitigate the possibility of XSS attacks always use the Http Only flag when setting cookies. This way they won't show up in document Cookies. Always use signed cookies

With signed cookies, a server can tell if a cookie was modified by the client.

2.4.3 Signatures

Either using cookies or tokens, if the transport layer for whatever reason gets exposed your credentials are easy to access - and with a token or cookie the attacker can act like the real user.

A possible way to solve this - at least when we are talking about APIs and not the browser is to sign each request. How does that work?

When a consumer of an API makes a request it has to sign it, meaning it has to create a hash from the entire request using a private key. For that hash calculation you may use:

- HTTP method
- Path of the request
- HTTP headers
- Checksum of the HTTP payload and a private key to create the hash
- To make it work, both the consumer of the API and the provider have to have the same private key. Once you have the signature, you have to add it to the request, either in query strings or HTTP headers. Also, a date should be added as well, so you can define an expiration date.

2.4.4 One-Time Passwords

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device.

One-Time passwords algorithms generate a one-time password with a shared secret and either the current time or a counter:

Time-based One-time Password Algorithm, based on the current time, MAC-based One-time Password Algorithm, based on a counter.

These methods are used in applications that leverage two-factor authentication: a user enters the username and password then both the server and the client generate a one-time password.

One-Time Password (OTP) Authentication products generate highly secure one-time passwords ensuring that only properly authenticated users are authorized access to critical applications and data.

2.5 Injection flaws

Injection flaws allow attackers to relay malicious code through an application to another system. These attacks include calls to the operating system via system calls, the use of external programs via shell commands, as well as calls to backend databases via SQL (i.e., SQL injection). Whole scripts written in Perl, Python, and other languages can be injected into poorly designed applications and executed. Any time an application uses an interpreter of any type there is a danger of introducing injection vulnerability.

Many web applications use operating system features and external programs to perform their functions. Sendmail is probably the most frequently invoked external program, but many other programs are used as well. When a web application passes information from an HTTP request through as part of an external request, it must be carefully scrubbed. Otherwise, the attacker can inject special (Meta) characters, malicious commands, or command modifiers into the information and the web application will blindly pass these on to the external system for execution.

SQL injection is a particularly widespread and dangerous form of injection. To exploit a SQL injection flaw, the attacker must find a parameter that the web application passes through to a database. By carefully embedding malicious SQL commands into the content of the parameter, the attacker can trick the web application into forwarding a malicious query to the database. These attacks are not difficult to attempt and more tools are emerging that scan for these flaws. The consequences are particularly damaging, as an attacker can obtain, corrupt, or destroy database contents.

Injection vulnerabilities can be very easy to discover and exploit, but they can also be extremely obscure. The consequences of a successful injection attack can also run the entire range of severity, from trivial to complete system compromise or destruction. In any case, the use of external calls is quite widespread, so the likelihood of an application having an injection flaw should be considered high.

2.5.1 Environments Affected

Every web application environment allows the execution of external commands such

as system calls, shell commands, and SQL requests. The susceptibility of an external call to command injection depends on how the call is made and the specific component that is being called, but almost all external calls can be attacked if the web application is not properly coded.

2.5.2 How to determine if you are Vulnerable

The best way to determine if your applications are vulnerable to injection attacks is to search the source code for all calls to external resources (e.g., system, exec, fork, Runtime. Exec, SQL queries, or whatever the syntax is for making requests to interpreters in your environment). Note that many languages have multiple ways to run external commands. Developers should review their code and search for all places where input from an HTTP request could possibly make its way into any of these calls. You should carefully examine each of these calls to be sure that the protection steps outlined below are followed.

2.5.3 How to Protect Yourself

The simplest way to protect against injection is to avoid accessing external interpreters wherever possible. For many shell commands and some system calls, there are language specific libraries that perform the same functions. Using such libraries does not involve the operating system shell interpreter, and therefore avoids a large number of problems with shell commands.

For those calls that you must still employ, such as calls to backend databases, you must carefully validate the data provided to ensure that it does not contain any malicious content. You can also structure many requests in a manner that ensures that all supplied parameters are treated as data, rather than potentially executable content. The use of stored procedures or prepared statements will provide significant protection, ensuring that supplied input is treated as data. These measures will reduce, but not completely eliminate the risk involved in these external calls. You still must always validate such input to make sure it meets the expectations of the application in question.

2.6   SQL Injection

SQL injection is a type of web application security vulnerability in which an attacker is able to submit a database SQL command that is executed by a web application,

exposing the back-end database. A SQL injection attack can occur when a web application utilizes user-supplied data without proper validation or encoding as part of a command or query. The specially crafted user data tricks the application into executing unintended commands or changing data.

SQL Injection occurs when data entered by users is sent to the SQL interpreter as a part of an SQL query, as in the figure below.
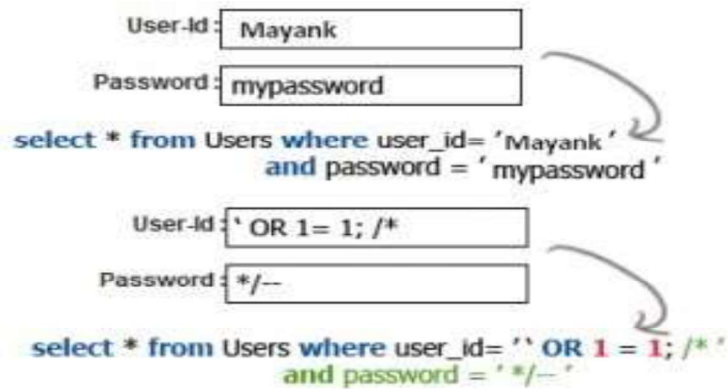
Fig: SQL Injection

SQL injection allows an attacker to create, read, update, alter or delete data stored in the back-end database. In its most common form, a SQL injection attack gives access to sensitive information such as social security numbers, credit card numbers or other financial data. According to Veracode's State of Software Security Report, SQL injection is one of the most prevalent types of web application security vulnerability.

SQL injection errors occur when:

- Data enters a program from an un-trusted source.

- The data used to dynamically construct a SQL query

- The main consequences are:

Confidentiality: Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities.

Authentication: If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.

Authorization: If authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of SQL Injection vulnerability.

Integrity: Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL Injection attack.

2.6.1 How SQL Injection works

An SQL Injection Attack (SQLIA) is a type of attack whereby an attacker (a crafted user) adds malicious keywords or operators into an SQL query (e.g., SQL malicious code statements), then injects it to a user input box of a Web application. This allows the attacker to have illegal and unrestricted access to the data stored at the backend database. Figure below shows the normal user input process in a Web application, which is self-explanatory.
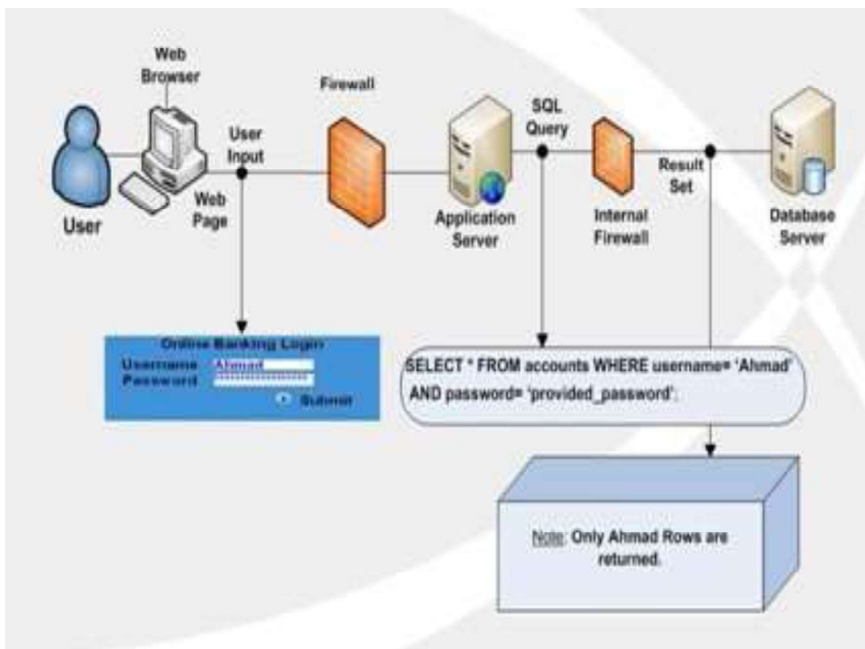
Fig: Normal user input process in a Web application

Now the next figure below shows an example how a malicious input could be processed in a Web application. In this case, the malicious input is the carefully formulated SQL query which passes through the system's verification method.

In order to run malicious SQL queries against a database server, an attacker must first find an input within the web application that is included inside of an SQL query.
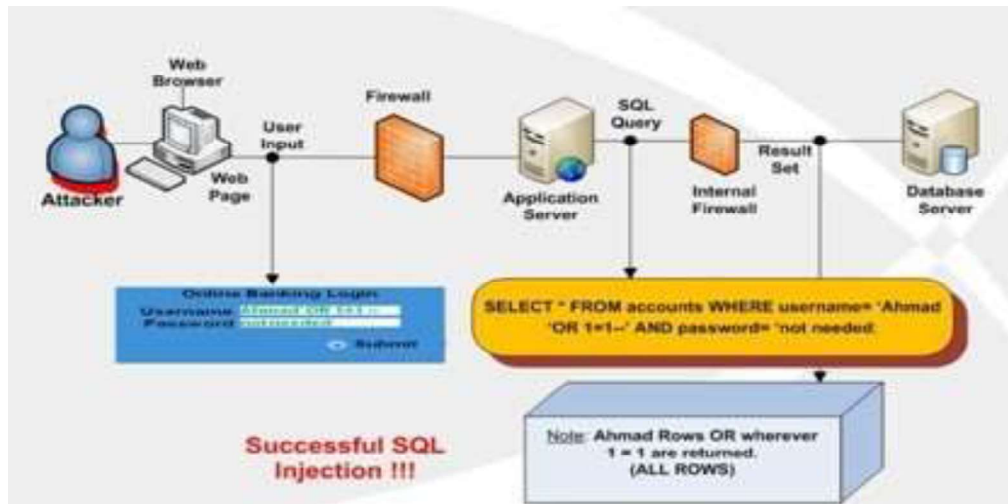
Fig: Malicious input through SQL Injection in the web application

In order for an SQL injection attack to take place, the vulnerable website needs to directly include user input within an SQL statement. An attacker can then insert a payload that will be included as part of the SQL query and run against the database server.

2.6.2 SQL Injection Vulnerability versus SQL Injection Attack

Vulnerability in any system is defined as a bug, loophole, weakness or flaw existing in the system that can be exploited by an unauthorized user in order to gain unlimited access to the stored data. Attack generally means an illegal access, gained through well-crafted mechanisms, to an application or system.

SQL injection is a software vulnerability that occurs when data entered by users is sent to the SQL interpreter as a part of a SQL query.

Attackers provide specially crafted input data to the SQL interpreter and trick the interpreter to execute unintended commands.

Attackers utilize this vulnerability by providing specially crafted input data to the SQL interpreter in such a manner that the interpreter is not able to distinguish between the intended commands and the attacker's specially crafted data. The interpreter is tricked into executing unintended commands.

A SQL injection attack exploits security vulnerabilities at the database layer. By exploiting the SQL injection flaw, attackers can create, read, modify or delete sensitive data.

SQL Injections: The Most Prevalent Type of Application Security Vulnerability

With more than 20 percent of all web vulnerabilities being attributed to SQL injection, this is the second most common software vulnerability. Therefore, having the ability to find and prevent SQL injection should be top of mind for web developers and security personnel. In general, a SQL injection attack exploits a web application that does not properly validate or encode user-supplied input and then uses that input as part of a query or command against a back-end database. For example, a typical form may ask for an ID and create a URL:

"http://www.somewebsite.com/id/id.asp?id=somedata". An attacker using SQL injection may enter "some data or 1=1". If the web application does not properly validate or encode the user-supplied data and sends it directly to the database, the reply to the query will expose all IDs in the database, since the condition "1=1" is always true. This is a basic example, but it illustrates the importance of sanitizing user-supplied data before using it in a query or command.

2.6.3 Preventing SQL Injection

You can prevent SQL injection if you adopt an input validation technique in which user input is authenticated against a set of defined rules for length, type and syntax and also against business rules.

You should ensure that users with the permission to access the database have the least privileges. Additionally, do not use system administrator accounts like "sa" for web applications. Also, you should always make sure that a database user is created only for a specific application and this user is not able to access other applications. Another method for preventing SQL injection attacks is to remove all stored procedures that are not in use.

Use strongly typed parameterized query APIs with placeholder substitution markers, even when calling stored procedures.

Show care when using stored procedures since they are generally safe from injection. However, be careful as they can be inject able (such as via the use of exec () or concatenating arguments within the stored procedure).

2.6.4 What Attackers can do with SQL?

SQL is a programming language designed for managing data stored in an RDBMS; therefore SQL can be used to access, modify and delete data. Furthermore, in specific cases, an RDBMS could also run commands on the operating system from

an SQL statement.

Keeping the above in mind, when considering the following, it's easier to understand how lucrative a successful SQL injection attack can be for an attacker.

- An attacker can use SQL injection to bypass authentication or even impersonate specific users.

- One of SQL's primary functions is to select data based on a query and output the result of that query. SQL injection vulnerability could allow the complete disclosure of data residing on a database server.

- Since web applications use SQL to alter data within a database, an attacker could use SQL injection to alter data stored in a database. Altering data affects data integrity and could cause repudiation issues, for instance, issues such as voiding transactions, altering balances and other records.

- SQL is used to delete records from a database. An attacker could use an SQL injection vulnerability to delete data from a database. Even if an appropriate backup strategy is employed, deletion of data could affect an application's availability until the database is restored.

- Some database servers are configured (intentional or otherwise) to allow arbitrary execution of operating system commands on the database server. Given the right conditions, an attacker could use SQL injection as the initial vector in an attack of an internal network that sits behind a firewall.

2.6.5 The anatomy of an SQL Injection attack

An SQL injection needs just two conditions to exist – a relational database that uses SQL, and a user controllable input which is directly used in an SQL query.

In the example below, it shall be assumed that the attacker's goal is to ex- filtrate data from a database by exploiting SQL injection vulnerability present in a web application.

Supplying an SQL statement with improper input, for example providing a string when the SQL query is expecting an integer, or purposely inserting a syntax error in an SQL statement cause the database server to throw an error.

Errors are very useful to developers during development, but if enabled on a live site, they can reveal a lot of information to an attacker. SQL errors tend to be descriptive

to the point where it is possible for an attacker to obtain information about the structure of the database, and in some cases, even to enumerate an entire database just through extracting information from error messages – this technique is referred to as error-based SQL injection. To such an extent, database errors should be disabled on a live site, or logged to a file with restricted access instead.

2.7 Let us Sum Up

Now a day's web application is widely used in various applications it is the reliable and efficient solution to the challenges of communicating and conducting the various organization, business or commerce over the internet. Though many approaches and frameworks have been identified and implemented in many interactive Web applications, security still remains a major issue. SQL Injection prevails as one of the top-10 vulnerabilities and threat to online businesses targeting the backend databases. SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input. In SQL injection is a technique the attacker injects an input in the query in order to change the structure of the query intended by the programmer and gaining the access of the database which results modification or deletion of the user's data. In the injection it exploits a security vulnerability occurring in database layer of an application. SQL injection attack is the most common attack in websites in these days. Some malicious codes get injected to the database by unauthorized users and get the access of the database due to lack of input validation. So input validation is the most critical part of software security that is not properly covered in the design phase of software development life-cycle resulting in many security vulnerabilities.

2.8 Further Readings

1. Fundamentals of Information Security (PGDCS-01), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e- Governance and Cyber Security.

2. Cyber Security Techniques (PGDCS-02), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e- Governance and Cyber Security

3. Cyber Attacks and Counter Measures: User Perspective, (PGDCS-03), Study Materials of Uttarakhand Open University, Haldwani, for Post- Graduate Diploma in Cyber Security.

4. Information System (PGDCS-06), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

5. Mihir Gandhi, Jwalant Baria, SQL INJECTION Attacks in Web Application, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

6. http://gender.govmu.org/English/Documents/activities/gender%20infsy s/AnnexX1302.pdf

7. https://en.wikipedia.org/wiki/Web_application_security

2.9 Assignments

1. What do you mean by web application security?
2. What are different web application security attacks?
3. What is the use of One-Time Passwords?
4. What do you mean by SQL Injection?
5. How SQL Injection Vulnerability different from SQL Injection Attack?
6. What Attackers can do with SQL injection?
7. How can you prevent from SQL injection attack?
8. What are different web authentication techniques?

Unit 3: Web Browser Security 3

Unit Structure

3.1 Learning Objectives

After completion of this unit, you should be able to

- Know the functions of a web browser
- Understand the meaning of web browser security
- Identify the role of a Uniform Resource Identifier
- Identify different vulnerabilities and attacks on applications
- Demonstrate the Impact of XSS Vulnerability
- Know the vulnerabilities in Malicious File Upload and Webshells
- Understand the need to secure your Browser
- Identify the Features and Risks of Web Browsers
- Secure Your Web Browser
- Note the tips to keep your computer secure

3.2 Introduction

Web browsers are communicating client-server computer programs for distributing documents and information, generally called web data, over the Internet. Web data are marked up in the HTML language for presentation and interaction with people in web browsers. Each web server uses an IP address or domain name as well as a port number for its identification. People use web browsers to send data requests to web servers with the HTTP protocol, and the web servers running on server computers either retrieve the requested data from local disks or generate the data on-the-fly, mark up the data in HTML, and send the resulting HTML files back to the web browsers to render. Apache, Tomcat and IIS are popular web server programs, and IE and Firefox are popular web browsers.

The variety of browsers that can be hosted on a range of platforms means that organizations will be exposed to a variety of risks – either by worsening existing risks to corporate assets or introducing new ones. The guidance discusses how effective the browser's security features are and how they can be configured to make best use of those features.

Web browsers play an important role in protecting you from malware, phishing and other online attacks, while browser privacy features help keep our browsing habits private on your computer.

In this unit we will discuss some of the security technologies in a way that does not negatively affect rich Internet experiences.

3.3 Web Browser Security

Browser security is the application of Internet security to web browsers in order to protect networked data and computer systems from breaches of privacy or malware. Security exploits can also take advantage of vulnerabilities (security holes) that are commonly exploited in all browsers. In computer security a threat is a possible danger that might exploit vulnerability to breach security and thus cause possible harm. A threat can be either **"intentional"** or **"accidental".**

Web browsers can be breached in one or more of the following ways:

1. Operating system is breached and privacy is reading/modifying the browser memory space in privilege mode.
2. Operating system has a privacy and running as a background process which is reading/modifying the browser memory space in privileged mode.
3. Main browser executable can be hacked.
4. Browser components may be hacked.
5. Browser plug-in can be hacked.
6. Browser network communications could be intercepted outside the machine whenever a browser communicates with a website it is the website which makes communication and collects some information about the browser .If any malicious code has been inserted into the website's contents then vulnerabilities specific to a particular browser can allow this malicious code to run processes unintended ways. The attacker is able to run processes and gain privileged access to the infected system on the machine as well the whole network.

Browsers like **Google Chrome** and **Mozilla Firefox** can block—or warn users of—insecure plugins. The browser guarantees that the address bar is correct. It is a reason because;

• Why browsers will generally display a warning when entering full screen mode?
• Where the address bar would normally be, so that a full screen website cannot make a fake browser user interface with a fake address bar.

3.4 Web Architecture (2-Tier and 3-Tier)

The basic web architecture is two-tiered architecture, one is a web server (which serves the content to client) and a web client or browser (which request for the resource). The server side programming extends the two- tier architecture to three-tier architecture by adding a back-end server. The first of the two-tier architecture is the web client which displays the information. Many commonly used web clients are internet browsers such as Chrome, Firefox, and Internet Explorer. The other part of the two-tier architecture is the web server which provides information to the client. The commonly used web servers are Apache and IIS. This information may be stored with the web server or storage connected to it, directly or indirectly. At the client end small information such as cookies related to session information, user information or temporary transaction information may be stored.

The third tier is the Common Gateway Interface (CGI) which is a set of standards that defines how a dynamic document is written, how data are input to the program and how the output result is used. CGI allows programmers to use any of several languages such as C, C++, Bourne shell, C Shell, Tcl or Perl. The web server interacts with the CGI to provide dynamic content.
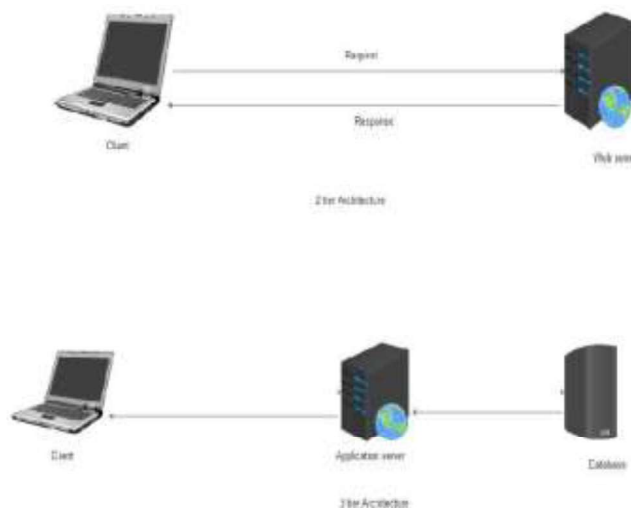
Fig: A 2-tier and 3-tier architecture

Before we proceed, it is important to understand three basic concepts – HyperText Markup Language (HTML), Uniform Resource Identifier (URI) and HyperText Transfer Protocol (HTTP).

3.4.1 Hyper Text Markup Language (HTML)

HTML is a language for encoding document content. HTML has evolved out of Standard Generalized Markup Language (SGML). SGML was approved in 1986 as a standard which specifies a meta-language for defining document markup systems through an SGML Document Type Definition (DTD) which specifies valid tag names and element attributes. The tags are hierarchical and structured. HTML was approved as a standard in 1995 with its HTML 2.0 specification. HTML 3.0 was published as a W3C recommendation in 1997 while HTML 4.0 was also published in the same year. HTML 5.0 was published as a working draft by the W3C in 2008. The HTML tags normally coming pairs like <head> and </head>. The browser does not display the HTML tag but interprets the content within the tag based on the tag. Browsers can refer to Cascading Style Sheets (CSS) to interpret the appearance and layout of the content within the tags.

3.4.2 Uniform Resource Identifier

A client that wants to access any web page on the internet needs the web address. To access a document over the internet, HTTP uses locators. The Uniform Resource Locator (URL) is standard for specifying the web address, based on network location. Uniform Resource Locator (URL) is subset of Uniform Resource Identifier (URI). The identifier may specify either the location of resource (as a URL) or may specify its name (as a URN, i.e. Uniform Resource Namespace) independent of location of the resource. Therefore a URI could be URL or a URN.

These days the term URL is more commonly used in place of URI. The URL defines four things: protocol, host computer, port and path, for example http://www.usou.ac.in:81/example.html. The protocol (http in example) is the client/server program used to retrieve the document. Common protocols which can retrieve a document are FTP and HTTP. The host (UOU.ac.in) is the computer on which the information is located. The URL can optionally contain the port number (default is port 80 in example it is 81) of the server; it is inserted between the host and the path and it is separated by a colon. Path is the pathname of the file (example.html) where the information is located. The path can itself contain directories, subdirectories and files.

3.4.3 Hyper Text Transfer Protocol (HTTP)

While HTML is used to encode document content, HyperText Transfer Protocol (HTTP) is used to transmit or access data over the web. The HTTP protocol functions as a combination of FTP and SMTP. The HTTP uses only one TCP connection (without separate control connection) on port 80. HTTP messages are read and interpreted by the HTTP server and HTTP client (browser). The client sends an HTTP request to the server while the server sends an HTTP response to the client. Although HTTP uses the services of TCP, HTTP itself is a stateless protocol, i.e. each HTTP request is unrelated to any previous HTTP request as the server is not required to retain session information. Readers are advised to refer http://www.w3.org/Protocols/ for details on HTTP protocols.

3.4.4 Attacks on Applications

Web completely changed the way organizations look, feel and work. Common web applications include ecommerce websites, webmail, online retail sales, online auctions, wikis and others. Majority of websites, including those considered most business critical, are vulnerable to attacks. Web applications are accessible openly on web thereby making it more prone to attack. Web Developers are not well versed with security issues because of which the applications are prone to vulnerabilities. Today every web user even from non-IT background is a content developer for the websites. Technologies like Ajax, RSS make web more creative place but also increased the attack surface. Attack surface expanded with the dawn of new web technologies.

Attacks on web applications refer to threat at the application-level. Therefore, when we use a hardware firewall or an Intrusion Detection System for network security, it does not mean that we are protecting against attacks on web applications. In web application security we are talking about securing:

- the code in the web application
- the backend systems
- the web and application servers
- the users

3.4.4.1 The Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) is a not-for-profit charitable

organization focused on improving the security of software. Mission of OWASP is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. The OWASP Top Ten is a powerful awareness document for web application security and represents a broad consensus about what the most critical web application security flaws are. Error! Reference source not found. The below table shows the OWASP top ten web application security flaws2013.

Table: OWASP TOP Ten 2013

Sr.	Category	Description
1	A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2	A2-Broken authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or to exploit other implementation flaws to assume other users' identities.
3	A3-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes un- trusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
4	A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

5	A5-Security Mis-configuration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date
6	A6-Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
7	A7-Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization
8	A8-Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim
9	A9-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

10	A10- Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use un-trusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages

3.4.5 Demonstration of Impact of XSS Vulnerability

Cross-site scripting (XSS) enables attackers to inject client-side script like JavaScript into web pages viewed by the users/visitors of web-application. Using this attacker can include his own code into the browser of users of vulnerable web-application. Two common types of XSS vulnerabilities are:

i. Reflected (attack string not stored persistently in web-application)

ii. Stored cross-site scripting (attack string is stored in database of the web-application).

Stored or persistent XSS is more severe type as all the users of website will get impacted. No input validation or weak input validation, when accepting data from the user and improper output coding, when reflecting data back to the user is reason for the XSS vulnerability. Pie-chart in Figure below reveals that XSS is having the highest percent in web- application vulnerabilities followed by SQL injection.
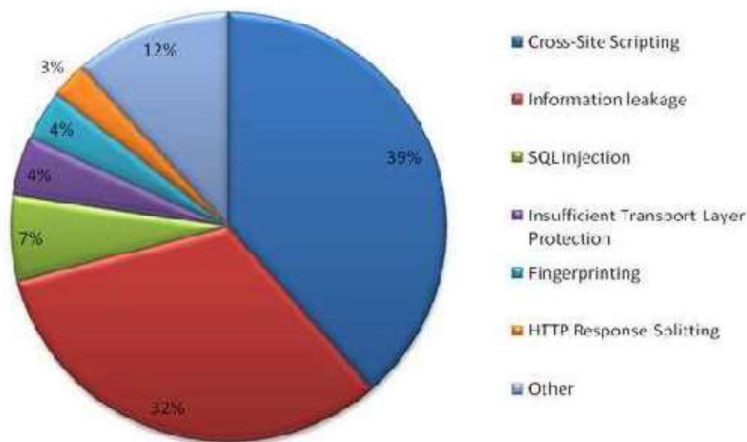
Percent of vulnerabilities out of total number of vulnerabilities (% Vulns ALL) (Source: WASC25)

3.4.6 The Browser Exploitation Framework (BeEF)

BeEF is short for The Browser Exploitation Framework26. It is a penetration testing tool that focuses on the web browser. Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door i.e. the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.

The Browser Exploitation Framework (BeEF) is a security tool that can be used to hook the browser of the client/victim machine by executing Cross Site Scripting (XSS) through vulnerable web-application, to further conduct the attack on the client system. BeEF can be used to demonstrate impact magnitude of the XSS attack. BeEF provides command and control facility to control and launch attack on the zombie browsers/system. Zombie browser can also be used to launch further attacks like key logging and port scanning.

3.5 Vulnerabilities in Malicious File Upload and Web shells

- Abusing file upload is widely exploited flaw in web application. Web shell code, a preferred choice for attacker creates a backdoor on vulnerable web server accessible via the web browser and provides functionalities such as system command execution and file access. Webshells access which typically allows complete control of the system and lead to malicious activities like defacement, phishing, espionage, malware distribution and Command & Control hosting post-exploitation of the web- applications by attacker.

- Perimeter security devices like firewalls, IPS/IDS and anti-virus applications are ineffective in detecting web shells if either the **webshell** is a customized program developed by attacker for particular malicious purpose or attacker is using some kind of obfuscation techniques in the webshells. Analysis of web-intrusion incidents, involving webshell upload, reveals the methodologies adopted by the attackers for uploading the webshells and common vulnerabilities exploited. Web-intrusions can be classified broad categories of vulnerabilities exploited by

attackers for uploading the web shells to the vulnerable web-application.

- **Abuse of file upload functionality**: In this category of vulnerabilities file-upload functionality is provided by the web- application, which is abused by the attacker to upload the malicious file.

- **Insecure web server configurations**: Attacker exploits the configuration and deployment errors like Web DAV enabled on production environment, Vulnerable Content Management System (CMS), Vulnerable Plug-ins installed with web-server or CMS like online file editors.

- **Other Web-application vulnerabilities**: Web-application vulnerabilities like SQL Injection, File Inclusion and others are used by attacker to upload webshell on the server to maintain persistent access.

3.6 Why Secure your Browser?

The popular web browsers that are installed on almost all computers are Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari. Because web browsers are used so frequently, it is vital to configure them securely. Often, the web browser that comes with an operating system is not set up in a secure default configuration. Not securing your web browser can lead to a variety of computer problems caused by anything from spyware being installed without your knowledge to intruders taking control of your computer.

There is an increasing threat from software attacks that take advantage of vulnerable web browsers. We have observed new software vulnerabilities being exploited and directed at web browsers through use of compromised or malicious websites. This problem is made worse by a number of factors, including the following:

- Many users have a tendency to click on links without considering the risks of their actions.

- Web page addresses can be disguised or take you to an unexpected site.

- Many web browsers are configured to provide increased functionality at the cost of decreased security.

- New security vulnerabilities are often discovered after the software is configured and packaged by the manufacturer.

- Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities that may be attacked.

- Third-party software may not have a mechanism for receiving security updates.

- Many websites require that users enable certain features or install more software, putting the computer at additional risk.
- Many users do not know how to configure their web browsers securely.
- Many users are unwilling to enable or disable functionality as required to secure their web browser.

As a result, exploiting vulnerabilities in web browsers has become a popular way for attackers to compromise computer systems.

3.7 Features and Risks of Web Browsers

It is important to understand the functionality and features of the web browser you use. Enabling some web browser features may lower security. Vendors often enable features by default to improve the computing experience, but these features may end up increasing the risk to the computer.

Attackers focus on exploiting client-side systems (your computer) through various vulnerabilities. They use these vulnerabilities to take control of your computer, steal your information, destroy your files, and use your computer to attack other computers. A low-cost method attacker's use is to exploit vulnerabilities in web browsers.

An attacker can create a malicious web page that will install Trojan software or spyware that will steal your information. Rather than actively targeting and attacking vulnerable systems, a malicious website can passively compromise systems as the site is visited. A malicious HTML document can also be emailed to victims. In these cases, the act of opening the email or attachment can compromise the system.

Some specific web browser features and associated risks are briefly described below. Understanding what different features do will help you understand how they affect your web browser's functionality and the security of your computer.

ActiveX is a technology used by Microsoft Internet Explorer on Microsoft Windows systems. ActiveX allows applications or parts of applications to be utilized by the web browser. A web page can use ActiveX components that may already reside on a Windows system, or a site may provide the component as a downloadable object. This gives extra functionality to traditional web browsing, but may also introduce more severe vulnerabilities if not properly implemented.

Java is an object-oriented programming language that can be used to develop active

content for websites. A Java Virtual Machine, or JVM, is used to execute the Java code, or "applet (link is external)," provided by the website. Some operating systems come with a JVM, while others require a JVM to be installed before Java can be used. Java applets are operating system independent.

Java applets usually execute within a "sandbox" where the interaction with the rest of the system is limited. However, various implementations of the JVM contain vulnerabilities that allow an applet to bypass these restrictions. Signed Java applets can also bypass sandbox restrictions, but they generally prompt the user before they can execute

Plug-ins are the applications intended for use in the web browser. Netscape has developed the NPAPI standard for developing plug-ins, but this standard is used by multiple web browsers, including Mozilla Firefox and Safari. Plug-ins are similar to ActiveX controls but cannot be executed outside of a web browser. Adobe Flash is an example of an application that is available as a plug-in.

Plug-ins can contain programming flaws such as buffer overflows, or they may contain design flaws such as cross-domain violations, which arises when the same origin policy is not followed.

Cookies are files placed on your system to store data for specific websites. A cookie can contain any information that a website is designed to place in it. Cookies may contain information about the sites you visited, or may even contain credentials for accessing the site. Cookies are designed to be readable only by the website that created the cookie. Session cookies are cleared when the browser is closed, and persistent cookies will remain on the computer until the specified expiration date is reached.

Cookies can be used to uniquely identify visitors of a website, which some people consider a violation of privacy. If a website uses cookies for authentication, then an attacker may be able to acquire unauthorized access to that site by obtaining the cookie. Persistent cookies pose a higher risk than session cookies because they remain on the computer longer.

JavaScript, also known as ECMAScript, is a scripting language that is used to make websites more interactive. There are specifications in the JavaScript standard that restrict certain features such as accessing local files.

VBScript is another scripting language that is unique to Microsoft Windows Internet

Explorer. VBScript is similar to JavaScript, but it is not as widely used in websites because of limited compatibility with other browsers.

The ability to run a scripting language such as JavaScript or VBScript allows web page authors to add a significant amount of features and interactivity to a web page. However, this same capability can be abused by attackers. The default configuration for most web browsers enables scripting support, which can introduce multiple vulnerabilities, such as the following:

Cross-Site Scripting

Cross-Site Scripting, often referred to as XSS, is vulnerability in a website that permits an attacker to leverage the trust relationship that you have with that site.

Cross-Zone and Cross-Domain Vulnerabilities

Most web browsers employ security models to prevent script in a website from accessing data in a different domain. These security models are primarily based on the Netscape

Detection Evasion

Anti-virus, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) generally work by looking for specific patterns in content. If a "known bad" pattern is detected, then the appropriate actions can take place to protect the user. However, because of the dynamic nature of programming languages, scripting in web pages can be used to evade such protective systems.

3.8 How to secure your Web Browser

Some software features that provide functionality to a web browser, such as ActiveX, Java, Scripting (JavaScript, VBScript, etc.), may also introduce vulnerabilities to the computer system. These vulnerabilities may stem from poor implementation, poor design, or an insecure configuration. For these reasons, you should understand which browsers support which features and the risks they could introduce. Some web browsers permit you to fully disable the use of these technologies, while others may permit you to enable features on a per-site basis.

This section provides links that show you how to securely configure a few of the most popular web browsers and how to disable features that can cause vulnerabilities. We encourage you to visit the vendor's website for each browser you use to learn more. If a vendor does not provide documentation on how to secure the

browser, we encourage you to contact the vendor and request more information.

Multiple web browsers may be installed on your computer. Other software applications on your computer, such as email clients or document viewers, may use a different browser than the one you normally use to access the web. Also, certain file types may be configured to open with a different web browser. Using one web browser to manually interact with websites does not mean other applications will automatically use the same browser. For this reason, it is important to securely configure each web browser that may be installed on your computer. One advantage to having multiple web browsers is that one browser can be used for only sensitive activities such as online banking, and the other can be used for general purpose web browsing. Using multiple browsers can minimize the chances that vulnerability in a particular web browser, website, or related software can be used to compromise sensitive information.

Web browsers are frequently updated. Depending on the version of your software, the features and options may move or change.

Microsoft Internet Explorer

Microsoft Internet Explorer (IE) is a web browser integrated into the Microsoft Windows operating system. For up-to-date information on security and settings for Internet explorer, visit http://windows.microsoft.com/en-us/internet-explorer/ie-security- privacy-settings(link is external).

Mozilla Firefox

Mozilla Firefox is a popular third-party browser for Windows, Mac, and Linux. To learn how to keep your information safe and secure with Firefox's private browsing, password features and other security settings, visit https://support.mozilla.org/en-US/products/firefox/privacy-and- security.

Apple Safari

Apple Safari is installed on its line of computers, tables, and phones. For information on the Safari's security settings on Apple devices, visit https://support.apple.com/en-us/HT201265. For information on Safari installed on computers, visit http://help.apple.com/safari/mac/8.0/ and select "Privacy and security" on the menu.

Google Chrome

In 2012, Google Chrome became the most widely used browser worldwide, according to Stat Counter and other sources. For more information on Chrome's security, safety and reporting features, visit https://support.google.com/chrome#topic=3421433 and select the options displayed under the topic.

Other Browsers

Other web browsers may have similar options to those described above. Please refer to each browser's documentation to determine which options are available and how to make the necessary changes. For example, the links below show where to find security information for two other web browsers:

Opera

Security badges: http://help.opera.com/opera/Windows/1857/en/private.

html#badges(link is external)

Web preferences: http://help.opera.com/opera/Windows/1857/en/con

trolPages.html#content(link is external)

Chromium

Securityinformation: https://www.chromium.org/Home/chromium-security

3.9   How to keep your Computer Secure

In addition to selecting and securing your web browser, you can take measures to increase protection to your computer in general. The following are steps and links to information resources that will help you secure your computer.

A. ***Read the Home Network Security document***

Source:*http://www.usar.army.mil/Portals/98/Documents/Slicksheet_BestPracti*

cesForKeepingYourHomeNetworkSecure.pdf

B. ***Enable automatic software updates if available***

Vendors will usually release patches for their software when vulnerability has been discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's website. Read the manuals or browse the vendor's website for more information.

Some applications will automatically check for available updates, and many vendors

offer automatic notification of updates via a mailing list. Look on your vendor's website for information about automatic notification. If no mailing list or other automated notification mechanism is offered, you may need to check the vendor's website periodically for updates.

C. ***Install and use antivirus software***

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks. Many antivirus packages support automatic updates of virus definitions. We recommend using these automatic updates when available. A list of virus basics is available on the CERT/CC website.

D. ***Avoid unsafe behavior***

- Use caution when opening email attachments or when using peer- to-peer file sharing, instant messaging, or chat rooms.

- Don't enable file sharing on network interfaces exposed directly to the Internet.

E. ***Follow the principle of least privilege — don't enable it if you don't need it***

Consider creating and using an account with limited privileges instead of an 'administrator' or 'root' level account for everyday tasks. Depending on the operating system, you only need to use administrator level access when installing new software, changing system configurations, etc. Many vulnerability exploits (e.g., viruses, Trojan horses) are executed with the privileges of the user that runs them — making it far more risky to be logged in as an administrator all the time.

3.10   Let us Sum Up

Internet security is a matter of great concern for internet users. It is becoming increasingly popular for attackers to compromise computers through vulnerable web browsers. An insecure web browser can lead to spyware being installed on your computer without your knowledge, attackers taking control of your computer, stealing your information, or even using your computer to attack other computers.

The set-up configuration for many web browsers is not secure by default. These settings are especially important if you use your browser to access campus business systems, or if you use your browser to access, send or receive sensitive information.

A **secure website** creates a safe connection between the website and the web browser so that entered data, such as personal information, credit card details, banking information, etc, is not accessible to unauthorized entities.

It is important to **know if a website is secure** or not while surfing the internet.

When the browser opens a secured connection, "https" can be seen in the URL instead of just http. To **know if a website is secure** or not, look for the locked yellow colored padlock symbol on the lower right corner of the browser window.

In this unit we discussed about the web-browser, threats to web applications and web browsers. We have also discussed and the techniques to secure your web browser and some tips to secure your computer as a whole.

3.11   Further Readings

1. Cyber Security Techniques (PGDCS-02), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e- Governance and Cyber Security

2. Practical Handbook of Internet Security for Beginners, (PGDCS- 04), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

3. http://its.ucsc.edu/software/release/browser-secure.html

4. http://www.usar.army.mil/Portals/98/Documents/Slicksheet_BestP racticesForKeepingYour HomeNetworkSecure.pdf

5. https://en.wikipedia.org/wiki/Browser_security

   https://www.us-cert.gov/publications/securing-your-web-browser

3.12   Assignments

1. What do you mean by browser security?
2. How web browsers can be breached?
3. Name the risks involved with different features of web browsers?
4. Why do you secure your Web Browser?
5. What are the top 10 attacks identified by the Open Web Application Security Project (OWASP)?
6. How can you make sure that your web browser is secured?
7. How can you keep your Computer Secure?
8. Write a note on malicious file upload.

Unit 4: E-Commerce Security 4

Unit Structure

4.1 Learning Objectives

After reading this unit, you will be able to:

- Understand the scope of e-commerce crime and security problems.
- Describe the key dimensions of e-commerce security.
- Identify the key security threats in the e-commerce environment.
- Describe how technology helps protect the security of messages sent over the Internet.
- Identify the protocols and applications used to establish secure Internet communications channels, and protect networks, servers, and clients.

4.2 Introduction

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e- commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability. E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Still, its definition is a complex endeavor due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions.

4.3 Basics of E-Commerce

"E-commerce is based on the electronic processing and transmission of data. It encompasses many diverse activities including electronic trading of goods and services, on-line delivery of digital content, electronic fund transfer, electronic share

trading, and public procurement."

The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. An arms race is underway: technologists are building new security measures while others are working to crack the security systems. One of the most effective means of ensuring data security and integrity is encryption.

E- Payment Systems

E-commerce sites use electronic payment, where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing the paperwork, transaction costs, and labor cost. Being user friendly and less time-consuming than manual processing, it helps business organization to expand its market reach/expansion. Some of the modes of electronic payments are Credit Card, Debit Card, Smart Card, E-Money, Electronic Fund Transfer (EFT) etc.

4.4 Benefits and limitations of E-Commerce

Online shopping is extremely beneficial to the customers and sellers alike. It allows buyers and sellers to meet and conduct transactions from any corner of the globe. It adds to the transparency and convenience of doing business, and creates a level playing field. Customers now obtain extensive and detailed knowledge of the product or the nature of services at the fingertips, and can undertake a real-time comparative price study before finalizing the purchase. The support systems such as online, banking and brokerage services ensure security, and easy tracking.

The major advantages of E-commerce systems are summarized as follows.

- E-commerce helps organizations to reduce the cost to create process, distribute, retrieve and manage the information by digitizing.

- E-commerce improves the brand image of the company.
- E-commerce helps organizations to provide better customer service.
- E-commerce helps to simplify the business processes and makes them faster and efficient. E-commerce reduces the paper work.
- E-commerce increases the productivity of organizations. It supports "pull" type supply management. In "pull" type supply management, a business process starts when a request comes from a customer and it uses just-intime manufacturing way.
- It provides 24x7 support. Customers can enquire about a product or service and place orders anytime, anywhere from any location. E-commerce application provides users with more options and quicker delivery of products.
- E-commerce application provides users with more options to compare and select the cheaper and better options. A customer can put review comments about a product and can see what others are buying, or see the review comments of other customers before making a final purchase.
- E-commerce provides options of virtual auctions.
- It provides readily available information. A customer can see the relevant detailed information within seconds, rather than waiting for days or weeks. E-Commerce increases the competition among organizations and as a result, organizations provide substantial discounts to customer.
- Customers need not travel to shop a product, thus less traffic on road and low air pollution. E-commerce helps in reducing the cost of products, so less affluent people can also afford the products. E- commerce has enabled rural areas to access services and products, which are otherwise not available to them.
- E-commerce helps the government to deliver public services such as healthcare, education, social services at a reduced cost and in an improved manner.

With such many benefits of e-commerce, the major limitations of e- commerce are as follows:

- There can be lack of system security, reliability or standards owing to poor implementation of e-commerce.
- Special types of web servers or other software might be required by the vendor, setting the e-commerce environment apart from network servers.

Among all the major potential challenges to E-commerce, the security threats are

vital and crucial.

4.5 E-Commerce Security

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration as well as destruction.

- Security is a crucial feature
    - Most transactions take place in a fully automated way
    - Restricted data are transmitted through a public network
- Users must be sure that their money will not be lost or stolen.

4.5.1 Purpose of E-Commerce Security

1. **Integrity:** prevention against unauthorized data modification. It ensures info has not been tampered with. Is implemented by message digest or hashing

2. **Non-repudiation**: prevention against any one party on agreement after the fact. It means not to deny a sale or purchase Implemented with digital signatures.

3. **Authenticity:** authentication of data source. It is for ensuring that someone is who he or she claims to be is implemented with digital Signature.

4. **Confidentiality:** protection against unauthorized data disclosure. Confidentiality is provided by encryption /decryption.

5. **Privacy:** provision of data control and disclosure.

6. **Availability:** prevention against data delays or removal.

7. **Access Control**: It governs what resources a user may access on the system. It uses valid IDs and passwords.

4.6 E-Commerce Security Threats

Now a day's E-commerce threats are very common. Anyone with the capability, opportunity, and intent to do harm other can perform it without any fear. Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element. The potential people those may create threats may be Terrorists, insiders, disgruntled employees and hackers.

People using the internet for commercial transactions always remain at risk of their confidential information such as passwords, and credit card details stolen and their cash siphoned off, or their identity hijacked to undertake criminal activities. Hackers use various techniques such as spear phishing attacks, click jacking, brute force

attacks and more to extract personal user information for their nefarious ends.

Mainly three types of security threats are seen. These include denial of service, – unauthorized access, and –theft and fraud.

Denial of Service (DOS)

Two primary types of DOS attacks that disrupt the resources are spamming and viruses.

Spamming –Sending unsolicited commercial emails to individuals –E- mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it. –Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.

Viruses: These are self-replicating computer programs designed to perform unwanted events.

Worms: These are special viruses that spread using direct Internet connections.

Trojan Horses: disguised as legitimate software and trick users into running the program Security (unauthorized access) and illegally access to systems, applications or data

Passive unauthorized access –listening to communications channel for finding secrets. –May use content for damaging purposes

Active unauthorized access –Modifying system or data –Message stream modification

Changes intent of messages, e.g., to abort or delay a negotiation on a contract

Masquerading or spoofing –sending a message that appears to be from someone else.

Impersonating another user at the —name (changing the —From field) or IP levels (changing the source and/or destination IP address of packets in the network)

- **Sniffers**–software that illegally access data traversing across the network. •Software and operating systems' security holes Security (theft and fraud) •Data theft already discussed under the unauthorized access section

- **Fraud** occurs when the stolen data is used or modified.

- **Theft** of software via illegal copying from company's servers.

- **Theft** of hardware, specifically laptops.

4.7 Types of E-Commerce Authentication

Electronic authentication, also referred to as **e-authentication** is the process of establishing confidence in user identities electronically presented to an information system. In online environments, the username identifies the user, while the password authenticates that the user is who he claim to be. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce. The following are some of the authentication techniques.

- **One-time password/Single sign on** - It is process where a user's
- password and information is used for logon and then, becomes invalid after a set time.

- **Two-factor authentication** - This requires two forms of authentication before access can be granted to a user.

- **Multi-factor authentication** - Multi-factor authentication requires that the user uses a user id, password combined with any other form of authentication method as smartcard or biometric. Using this method decreases the likelihood that an unauthorized person can compromise your electronic security system, but it also increases the cost of maintaining that system.

- **Electronic access card/Smart card** - Smart cards are credit card- sized plastic cards that house an embedded integrated circuit. They can be used in electronic commerce for providing personal security, stored value and mobility. At the functional level, smart cards can be categorized as either memory cards or microprocessor cards. Memory cards, such as disposable pre-paid payphone cards or loyalty card, are the cheapest form of smart card. They contain a small amount of memory in the form of ROM (read only memory) and EEPROM (electrically erasable programmable read only memory). Microprocessor cards are more advanced than simple memory cards in that they contain a microprocessor CPU (central processing unit) and RAM (random access memory) in addition to ROM and EEPROM. The ROM contains the card's operating system and factory- loaded applications.

- **Security token** - It is an authentication device that has been assigned to a specific user by an appropriate administrator‖. It uses what the user has such as, Passport, driver's license etc. to identify them. ―Most security tokens also

incorporate two-factor authentication methods to work effectivelyǁ.

- **Keystroke dynamics** - It is an automated form of authentication based on something the user does. It authenticates the user based keyboard typing pattern.
- **Biometric** - Biometric based systems enable the automatic identification and/or authentication of individuals. Authentication answers the question: "Am I who I claim to be"? The system verifies the identity of the person by processing biometric data, which refers to the person who asks and takes a yes/no decision (1:1 comparison). On the other hand, identification answers to the question: "Who am I?". The system recognizes the individual who asks by distinguishing him from other persons whose biometric data is also stored in the database. In this case the system takes a l- of-n decision, and answers that the person who asks is X, if her/his biometric data is stored in the database or that there is no match at all. Although the identification function should be regarded as distinct from authentication from an application perspective, often systems using biometrics integrate both identification and authentication functions, since the former is a repetitive execution of the latter.

4.8 How to Minimize Security Threats?

Certain steps that have to be followed to minimize security threats are as follows.

1. Perform a risk assessment i.e. prepare a list of information assets and their value to the firm
2. Develop a security policy i.e a written statement should be created which deals with
   - What assets to protect from whom?
   - Why these assets are being protected?
   - Who is responsible for what protection?
   - Which behaviors are acceptable and unacceptable?
3. Develop an implementation plan i.e. a set of action steps to achieve security goals.
4. Create a security organization i.e. a unit to administer the security policy
5. Perform a security audit i.e. a routine review of access logs and evaluation of security procedures.

4.9 Making E-Commerce Secure

E-commerce may be the way ahead but it needs to be secure that customers will make transaction with confidence with challenge.

Your e-commerce website is your electronic shop. To make the most of it, you want it to be open 24 hours a day, seven days a week (24*7). But you also want people to use it and the key is to give people a sense of security. The ultimate truth is using an E-commerce web site is no more or no less secure than using a telephone and people no longer balk at handing over their credit card details over the phone. However, although it is mainly a matter of educating people to understand and to make everything as secure as possible at all times which is a necessity.

4.10 E-Commerce Security Applications

As with e-mail applications, several protocols, standards, and applications have been developed to provide security for Internet communications and E-Commerce transactions. Some of them are as follows.

4.10.1 Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) is a communications protocol standard for securing credit card transactions over insecure networks, specifically, the Internet. SET was not itself a payment system, but rather a set of security protocols and formats that enabled users to employ the existing credit card payment infrastructure on an open network in a secure fashion. However, it failed to gain attraction in the market. VISA now promotes the 3-D secure scheme.

The Secure Electronic Transaction (SET) specification was developed by MasterCard and Visa to provide secure e-commerce transactions by implementing authentication mechanisms while protecting the confidentiality and integrity of cardholder data. SET defines the following features:

- **Confidentiality** (using DES)
- **Integrity** (using digital signatures and RSA asymmetric system)
- **Cardholder authentication** (using digital signatures and X.509 digital certificates)
- **Merchant authentication** (using digital signatures and X.509 digital certificates)
- **Interoperability**(between different hardware and software manufacturers)

SET utilizes dual signatures by allowing two pieces of data to be linked and sent to two different entities. SET never won favour in the marketplace and has fallen into disuse.

4.10.1.1 How SET Works

Both cardholders and merchants must register with CA (certificate authority) first, before they can buy or sell on the Internet, which we will talk about later. Once registration is done, cardholder and merchant can start to do transactions, which involve 9 basic steps in this protocol, which is simplified.

1. Customer browses website and decides on what to purchase

2. Customer sends order and payment information, which includes 2 parts in one message:

      a) Purchase Order – this part is for merchant

      b) Card Information – this part is for merchant's bank only.

3. Merchant forwards card information (part b) to their bank

4. Merchant's bank checks with Issuer for payment authorization

5. Issuer sends authorization to Merchant's bank

6. Merchant's bank send authorization to merchant

7. Merchant completes the order and sends confirmation to the customer

8. Merchant captures the transaction from their bank

9. Issuer prints credit card bill (invoice) to customer

4.10.2 Dual Signature

An important innovation introduced in SET is the *dual signature*. The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit-card number, and the bank does not need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service. The message digest (MD) of the OI and the PI are independently calculated by the customer. The dual signature is the encrypted MD (with the customer's secret key) of the concatenated MD's of PI and OI. The dual

signature is sent to both the merchant and the bank.

The protocol arranges for the merchant to see the MD of the PI without seeing the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be verified using the MD of the OI or PI. It doesn't require the OI or PI itself. Its MD does not reveal the content of the OI or PI, and thus privacy is preserved.

4.10.3 Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP). Major web sites (including Google, YouTube, Facebook and many others) use TLS to secure all communications between their servers and web browsers.

The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications. When secured by TLS, connections between a client (e.g. a web browser) and a server (e.g. wikipedia.org) will have one or more of the following properties:

The connection is private because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated at the start of the session (see Handshake Protocol). The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. The negotiation of a shared secret is both secure (the negotiated secret is unavailable to eavesdroppers and cannot be obtained, even by an attacker who places himself in the middle of the connection) and reliable (no attacker can modify the communications during the negotiation without being detected).

The identity of the communicating parties can be authenticated using public key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server).

The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or

alteration of the data during transmission.

4.10.4 Secure Hypertext Transfer Protocol (S-HTTP)

HTTPS (also called HTTP over TLS, HTTP over SSL and HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

In its popular deployment on the internet, HTTPS provides authentication of the website and associated web server with which one is communicating, which protects against man-in-the middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. In practice, this provides a reasonable guarantee that one is communicating with precisely the website that one intended to communicate with (as opposed to an impostor), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

The HTTPS uniform resource identifier (URI) scheme has identical syntax to the standard HTTP scheme, aside from its scheme token. However, HTTPS signals the browser to use an added encryption layer of SSL/TLS to protect the traffic. SSL/TLS is especially suited for HTTP since it can provide some protection even if only one side of the communication is authenticated. This is the case with HTTP transactions over the Internet, where typically only the server is authenticated (by the client examining the server's certificate).

4.11   Let us Sum Up

E-Commerce or Electronics Commerce is a methodology of modern business, which addresses the requirements of business organizations. It can be broadly defined as the process of buying or selling of goods or services using an electronic medium such as the Internet.

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised. The essential requirements for safe e-payments/transactions are Confidentiality Integrity Availability Authenticity Non-Reputability Audit ability. Major security measures to ensure e-commerce security include the following:

Encryption: Sender's machine of the information encrypts the data using a secret code and only the specified receiver's machine can decrypt the data using the same or a different secret code.

Digital Signature -Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.

Security Certificates: Security certificate is a unique digital id used to verify the identity of an individual website or user.

4.12   Further Readings

1. Fundamentals of Information Security (PGDCS-01), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e-Governance and Cyber Security.

2. Cyber Security Techniques (PGDCS-02), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e- Governance and Cyber Security

3. Cyber Attacks and Counter Measures: User Perspective, (PGDCS- 03), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

4. Information System (PGDCS-06), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security.

5. Niranjanamurthy M, DR. Dharmendra Chahar , The study of E- Commerce Security Issues and Solutions, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013

6. https://www.tutorialspoint.com/e_commerce/e_commerce_tutorial.pdf

7. Wikipedia: https://en.wikipedia.org/wiki/E-commerce.

4.13   Assignments

1. What do you mean by e-commerce? What are the advantages and disadvantages of e-commerce?

2. Name the types of Ecommerce Authentication techniques.

3. How to Minimize Security Threats?

4. What are the E-Commerce Security Applications

5. Write short notes on Secure Hypertext Transfer Protocol (S- HTTP).

6. What are different threats to E-Commerce security?

7. Name the types of Ecommerce Authentication techniques.

8. How can you make your E-Commerce transactions Secured?

9. Discuss the working of Secure Electronic Transaction (SET)

10. Write Brief notes on Secure Sockets Layer (SSL)

Block-4
Wireless Network Security

Unit 1: Wireless Network Security 1

Unit Structure

1.1 Learning Objectives

After going through this unit you should be able to

1. Define a wireless network.
2. Identify the components of wireless networks
3. Explain the security issues in wireless networks

1.2 Introduction

In this unit we will explain the important factor in the growth of a country that is a good communication infrastructure and will sees how wireless networks have an important role to play in the development of a country like India. Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile phones and tablets also great benefits. However, wireless networking has many security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. So there should have proper Management of Operational and Technical issues and recommendations for the secure deployment of wireless network security**.**

In this unit will introduce the benefits, components and security issues in wireless networks**.**

1.3 Wireless Network

Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the expensive process of introducing cables into buildings or as a connection between different equipment locations. The basis of wireless systems is radio waves, an implementation that takes place at the physical level of network structure.

Wireless networks use radio waves to connect devices such as laptops to the Internet, the business network and applications. When laptops are connected to Wi-Fi hot spots in public places, the connection is established to that business's wireless network.

There are four main types of wireless networks:

    1   Wireless Local Area Network (LAN): Links two or more devices using a

wireless distribution method, providing a connection through access points to the wider Internet.

2   Wireless Metropolitan Area Networks (MAN): Connects several wireless LANs.

3   Wireless Wide Area Network (WAN): Covers large areas such as neighboring towns and cities.

4   Wireless Personal Area Network (PAN): Interconnects devices in a short span, generally within a person's reach.

Table: Comparison of Wireless Network Types

Type	Coverage	Performance	Standards	Applications
Wireless PAN	Within reach of a person	Moderate	Wireless PAN Within reach of a person Moderate Bluetooth, IEEE 802.15, and IrDa Cable replacement for peripherals	Cable replacement for peripherals
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet
Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G,4G	Mobile access to the Internet from outdoor areas

1.3.1 WLAN

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method (often

spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local overage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards.
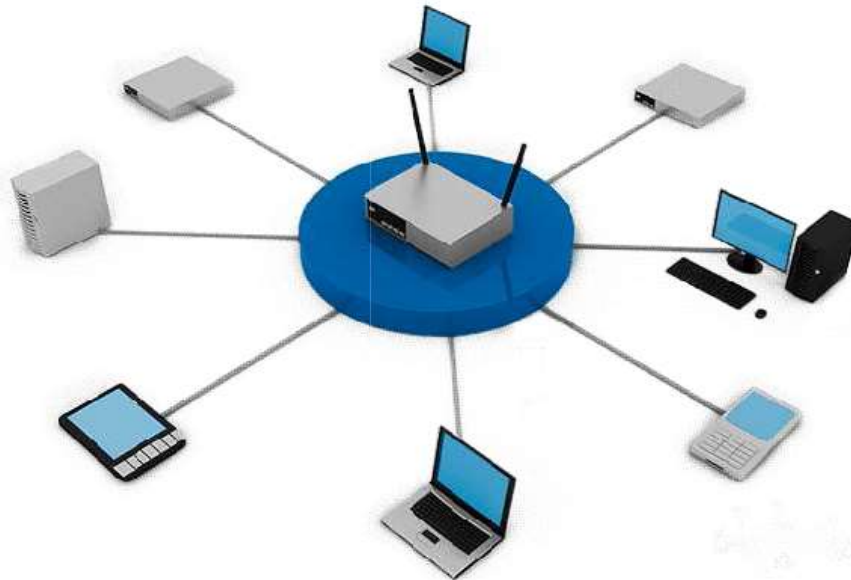
The other factors why WLANs are becoming more acceptable are:

1   No need to be connected physically with each other through any medium such as cables. You can roam around freely in office, premises, home or around..

2   WLANs are cost effective. Cabling all the way in the offices, hotels etc. are not needed. So it's cheap and provides same quality of service.

3   Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.

4   Less interruption and easy trouble shooting in case of failures as compared to cabled networks.

5   More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.

1.3.1.1 Major issues with WLAN

Having said that, WLAN are also as prone to various attacks as their counterpart wired LNAs are. Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation. No need to be in contact of physical wires to hack can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly. Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), De-authentication attacks, War driving etc. This chapter is not focused on attacks, we shall mainly concentrate on best practices- how to install and use WLAN securely which can thwart a number of above mentioned attacks.

1.3.1.2 Secure WLAN

Wireless Security mainly depends on these 3 factors:

- How much is your wireless network secured in terms of encryption being used?
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks. These are also for users how to remain safe while surfing. **Wi-Fi at home**

Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it?

Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor's and Internet Service provider do not provide any security settings by default and leave the customer to find for herself. So make sure, your network is secured from being maliciously used. There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

1.   Use most secure possible encryption: The first and most necessary step-use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords

it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel.

Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access -2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.

2.   **Use Firewall:** All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.

3.   **Have a monitoring system in place:** There's a saying- prevention is better than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.

4.   **Don't use default credentials:** Every wireless router comes with a set of default username/password. Sometimes, people don't change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/ " ".

5.   **Disable Auto-connect feature:** Some devices or the computers/laptops have 'Let this tool manage your wireless networks' or 'Connect automatically to available network'. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as 'HotSpot', 'SecureConnect', 'Govt Networks' etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.

6.   **Don't use public Wi-Fi spots to surf sensitive websites:** Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from

your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi. Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked

7. **Change the default SSID:** Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So he may be an obvious target to explore further to see if he still uses the default passwords as well?

8. **Restrict access by assigning static IP addresses and MAC filtering:** Disable automatic IP assigning feature and use private static IPs to the legitimate devices you 115 want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering- router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network.

9. **Turn off your router when not in use:** Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

1.4 Wireless Network Components

A wireless **network** is "**unsecured**" if you can access the Internet using the **network** without entering a password or **network** key. For example, a "hotspot" is a wireless **network** that is open and available for the public to use.

Depending on network budget or customers, instead of using wired network cards, it can use wireless ones. Most laptops already have a wireless card built-in so it may not have to acquire one. Many new desktop computers now have built-in wireless capability. A wireless NIC appears as its wired counterpart.

1.4.1 Firewall

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Network firewalls are frequently used to prevent unauthorized Internet users

from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Fig: Firewall

1.4.2 Wireless Access Point

In computer networking, a **wireless access point** (WAP) is a networking hardware device that allows a Wi-Fi compliant device to connect to a wired network. The WAP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. This is an area in which you can access the wireless network. An example of this device would be a wireless router.

Fig: Wireless Access Point

1.4.3 Modem

A modem (modulator-demodulator) is a network hardware device that

modulates one or more carrier wave signals to encode digital information for transmission and demodulates signals to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals, from light emitting diodes to radio. A common type of modem is one that turns the digital data of a co puter into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Fig:

1.4.4 Server

In information technology, a server is a computer program that provides services to other computer programs (and their users) in the same or other computers.

The computer that a server program runs in is also frequently referred to as a server (though it may be used for other purposes as well).

In the client/server programming model, a server is a program that awaits and fulfills requests from client programs in the same or other computers.

A given application in a comp ter may function as a client with requests for services from other programs and also as a *server* of requests from other programs.

Specific to the Web, a Web server is the computer program (housed in a computer) that serves requested HTML pages or files. A Web *client* is the requesting program

associated with the user. The Web browser in your computer is a client that requests HTML files from Web servers. This is your connection to the internet. A server is also considered the main computer of a network as it runs the rest of the computers in the network.

Fig: Server

1.4.5 Switch

In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. In the traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties. On an Ethernet local area network (LAN), a switch determines from the physical device (Media Access Control or MAC) address in each incoming message frame which output port to forward it to and out of. In a wide area packet-switched network such as the Internet, a switch determines from the IP address in each packet which output port to use for the next part of its trip to the intended destination.

Fig: Switch

1.4.6 USB Network Adapter

Besides the wireless network cards that can be installed inside the computer, it can use external cards. These are installed using a USB port.

Fig: USB Network Adapter

1.4.7 Hub

A hub is rectangular box that is used as the central object on which computers and other devices are connected. To make this possible, a hub is equipped with small holes called ports. It can be equipped with 4, 8, 12, 16, 32 ports.

Fig: HUB

1.4.8 Routers: Wired or Wireless

Like a hub, a router is another type of device that acts as the central point among computers and other devices that are part of a network Security.

1.4.9 Station (STA): A STA is a wireless endpoint device, also called a client device. STAs enable end users to gain access and utilize resources provided by wireless networks. Examples include laptop computers, personal digital assistants,

mobile phones and other consumer electronic devices with IEEE 802.11 capabilities.

1.4.10 Access Point (AP): An AP logically connects STAs with a distribution system (DS), which is typically an organization's wired network. APs can also logically connect wireless STA with each other without accessing a distribution system. Wireless APs provide users with a mobile capability by allowing users to freely move within a APs coverage area while maintaining connectivity between the user's client device and the AP. APs can also be linked together using wired infrastructure to allow users to "roam" between APs within a building or campus.

The IEEE 802.11 standard also defines the following two WLAN design structures or configurations, as follows:

1.4.11 Ad Hoc Mode: The ad hoc mode does not use APs. Ad hoc mode is sometimes referred to as infrastructure less because only peer-to-peer STAs are involved in the communications. This mode of operation is possible when two or more STAs are able to communicate directly to one another. Examples are laptops, mobile phones, PDAs, printers and scanners being able to communicate with each other without an AP. One of the key advantages of ad hoc WLANs is that theoretically they can be formed anytime and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance. However, an ad hoc WLAN cannot communicate with external networks. A further complication is that an ad hoc network can interfere with the operation of an AP-based infrastructure mode network that exists within the same wireless space.

1.4.12 Infrastructure Mode: In infrastructure mode, an AP logically connects STAs to each other or to a distribution system (DS), which is typically an organization's wired network. The DS is the means by which STAs can communicate with the organization's wired LANs and external networks such as the Internet. Infrastructure mode is the most commonly used mode for WLANs.

1.5 Wireless Security

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. Wireless

technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. WEP is an old IEEE

802.11 standard from 1999, which was out dated in 2003 by WPA, or Wi- Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

Wireless devices communicate through radio transmissions, without physical connections and without network or peripheral cabling. Wireless systems include local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices that do not process or store information. Other wireless devices being widely used include infrared (IR) devices such as remote controls, cordless computer keyboards, mouse devices, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver.

Authentication: Only clients who know a shared secret may connect to the network.WEP was the first cryptographic protocol developed for Wi-Fi to enable privacy and authentication. WEP, however, was not secure after all. To rectify the security issues with WEP, the Wi-Fi Alliance pushed a new cryptographic protocol, WPA. Since then, a common practice of securing a WPA enabled network with passwords has been discovered to be vulnerable to an offline dictionary-attack. Even though WPA itself is thought to be secure, apart from the dictionary-attack, it was a quick fix to the problems in WEP.

1.5.1 Use of Wi-Fi

Wireless technologies have become inexpensive, user- friendly and available to a large number of people and companies. In dense urban areas, access points belonging to different individuals are so closely spaced that their coverage areas

overlap. With its popularity and the availability to anyone within range, many individuals detect Wi-Fi networks as a hobby. War drivers bring their laptops and Wi-Fi gear1With WEP, anyone participating in the network can eavesdrop on other conversations in the network in their cars. With the aid of a Global Positioning System (GPS) receiver and an antenna, they explore areas and map the locations and coverage areas of access points. Some do it for the fun, and some with the intent to exploit vulnerable Wi-Fi networks. War bikers and war walkers do the same by other means of transportation.

1.5.2 Service Set Identification (SSID)

Service set identification (SSID) a series of 0 to 32 octets. It is used as a unique identifier for a wireless LAN. Since this identifier must often be entered into devices manually by a human user, it is often a human-readable string and thus commonly called the "network name". An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. A network administrator often uses a public SSID that is set on the access point and broadcast to all wireless devices in range. Some newer wireless access points disable the automatic SSID broadcast feature in an attempt to improve network security.

1.6 Types of Wireless Security

Wireless security is of two types: WEP and WPA.

WEP: WEP stands for Wired Equivalent Privacy. WEP was designed to provide the same level of security as wired networks. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

When using WEP, all clients and APs on a wireless network use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. Since the 802.11 standard does not specify a key management protocol.15

The shared key can be used for client authentication. This requires a four step process between the AP and the client. This process is as follows:

1. The client makes an authentication request to the AP.

2. The AP returns a challenge phrase to the client.

3. The client encrypts the challenge phrase using the shared symmetric key and transmits it to the AP.

4. The AP then compares the client's response with its phrase; if there is a match, the client is authorized otherwise the client is rejected.

Security problems with WEP include the following:

1. **The use of static WEP keys:** Many users in a wireless network potentially sharing the identical key for long periods of time, is well- known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key.

2. **Caffe Latte attack**: The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.16

3. **WEP provides no cryptographic integrity protection.** However, the 802.11 MAC protocol uses a no cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of no cryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text.12

4. **Authentication is not enabled; only simple SSID identification occurs.** Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.

5. **Device authentication is simple shared-key challenge-response.** One-way challenge-response authentication is subject to —man-in the-middlell attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

1.7 WPA Security problems

WPA also implements something called the Extensible Authentication Protocol (EAP) for authorizing users. Instead of authorizing computers based solely on their MAC address, WPA can use several other methods to verify each computer's identity. This makes it more difficult for unauthorized systems to gain access to the wireless network. Security problems with WPA include the following:

5. **Weak Password:** Pre-shared key WPA and WPA2 remain vulnerable to password cracking attacks if users rely on a weak password or passphrase. To protect against a brute force attack, a truly random passphrase of 20 characters (selected from the set of 95 permitted characters) is probably sufficient. Brute forcing of simple passwords can be attempted using the Air crack Suite starting from the four-way authentication handshake exchanged during association or periodic re-authentication.

6. **WPS PIN recovery:** Most recent models have this feature and enable it by default. Many consumer Wi-Fi device manufacturers had taken steps to eliminate the potential of weak passphrase choices by promoting alternative methods of automatically generating and distributing strong keys when users add a new wireless adapter or appliance to a network. These methods include pushing buttons on the devices or entering an 8-digit PIN. The Wi-Fi Alliance standardized these methods as Wi-Fi Protected Setup; however the PIN feature as widely implemented introduced a major new security flaw. The flaw allows a remote attacker to recover the WPS PIN and, with it, the router's WPA/WPA2 password in a few hours.

1.7.1 Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2)

Wi-Fi Protected Access (WPA) is a security standard that improves on older security standards by authenticating network users and providing more advanced encryption techniques. Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two most common security protocol and security certification programs developed by the Wi-Fi Alliance to secure wireless computer network. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

Difference between WPA & WPA2

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

1.8 Wireless Security Policy

- **Secure communications:** Encrypt data that travels on the network, and unthenticate users to be sure you know who is using the WLAN.Cisco supports all industry-standard encryption and authentication methods for the broadest client device compatibility.

- **Use strong encryption:** As soon as you install your network, set up the strongest wireless encryption you can. Wired Equivalent Privacy (WEP) encryption is adequate, but WPA and WPA2 give you stronger options.

- **Change the default network name:** When you set up your network equipment, change the default name to make it more difficult for hackers to find. Do not choose your company name, company phone number, or other information about your company that is easy to guess or find on the Internet. Use VLANs or MAC address control lists combined with encryption to restrict user access.

- Implement Cisco secure guest access features to allow visitors to connect to the network or Internet while keeping your business network and resources separate and secure.

- Be sure that management ports are secured.

- Physically hide or secure access points to prevent tampering. In many buildings, Cisco access points can be installed in the plenum space above the ceiling, providing optimal coverage in a secure location.

- Use video surveillance cameras to monitor your office building and site for suspicious activity.

1.9 Let us Sum up

In this unit we have discussed about the importance of a wireless network, its components and explained the security issues in different wireless networks. We have compared the performances of different network types. We have also

discussed wireless security concepts and types of wireless security. Finally we have outlined the wireless security policies.

1.10   Further Readings

1. N. Poorinma, S.Gowri, r. Abinaya, "Issues and the Advantages of Wireless Network", 2015 IJEDR, NC3N 2015, ISSN: 2321-9939.
2. https://en.wikibooks.org/wiki/Introduction_to_Computer_Informatio n_Systems/Security
3. Post-Graduate Diploma in Cyber Security Practical Handbook of Internet Security for Beginners (PGDCS-04)
4. Certificate in e-Governance and Cyber Security Cyber Security Techniques (PGDCS-02)

1.11   Assignments

1. What are different wireless components?
2. Discuss different design structures or configurations of WLAN according to IEEE 802.11 standard?
3. What do you mean by Wireless security? What are common types of Wireless security?
4. What is the security problems associated with WPA?
5. Discuss the policies on maintaining Wireless Security.
6. What is the security problems associated with WEP?
7. What is firewall?
8. Explain about the Wireless Security Policy.
9. Write the Wi-Fi protect process.

Unit 2: Security Issues in Wireless Networks

2

Unit Structure

2.1 Learning Objectives

After going through this unit you should be able to

1. Identify the Vulnerabilities, Threats and Attacks in Wireless Networks
2. Know about the different type of wireless security issues.
3. Note the Wireless Security Tips.
4. Know the Wireless Attacks Detection Techniques.

2.2 Introduction

The need for security on any network is apparent: the prevention of eavesdropping and the desire for authentication has been the main focus of many network administrators. However, the problems that already exist are added to when you add wireless networking to the equation. As wireless networking becomes more popular, the flawed security of most of those networks becomes more apparent. Several organizations have devised ways to secure their wireless networks from intruders. However, there is currently no wireless security implementation that everyone agrees is always suitable, regardless of what network it is to be used on. Some implementations are satisfactory for some environments, and there is work underway to create future solutions. Meanwhile, some wireless users make the situation more difficult as they advertise existing vulnerable networks. In this unit we will cover the Vulnerabilities, Threats and Attacks in Wireless Networks, Security issues in wireless networks and the process of Securing Wireless Transmissions, Securing Wireless Access Points, and Securing Wireless Client Devices etc.

2.3 Wireless Vulnerabilities, Threats and Countermeasures

The wireless networks consist of four basic components: The transmission of data using radio frequencies; Access points that provide a connection to the organizational network and/or the Client devices (laptops, PDAs, etc.); and users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

2.4 Security Concerns for Wireless Networks in Businesses

Working in reverse, in using customer networks, you are giving up security in two regards: you're connecting to a network that may or may not require a password that anyone can obtain. You have no way to ascertain the security of the network or even verify and validate that it is truly the network and not an "Evil Twin". You have no way to make sure no one can intercept and read and/or modify your data. Furthermore, while not dangerous yet still annoying, the stores can also monitor your connections and dependent upon the fine print you click "OK" in order to connect, they could query your device and get data about you. This data could be the apps you have installed, location data, and others. The same also applies for applications you install (Walmart Savings Catcher, Macy's App, etc.). These stores also have NO legal obligation or responsibility to protect your device or data on their network. Moral obligations and responsibilities are a different story.

2.4.1 Public Wireless Security Issues

Public Wireless networks (for this, those with a Pre-Shared Key) are not much safer, if at all. While they may not have the same intentions as retail stores, there is no level of assurance or legal obligation for them to secure your device or data. Again, you have no way to make sure no one can intercept and read and/or modify your data. You should question why this network exists, especially if the connection is free. You are probably the "product" via data mining (like retail stores above) or via advertising.

2.4.2 Security Concerns with Wireless Networks

Open Wireless networks are bastions for malicious intent. While some people genuinely want to share and others are ignorant as to the possible outcomes or the ability to secure the networks, others blatantly leave the networks open. Again, you have no way to make sure no one can intercept and read and/or modify your data. If you are connecting to a network that is named after an establishment, you should check to verify they even have a Wireless network before connecting. Many attackers will name their networks after establishments to get people to connect so they can steal their data.

2.5 About Wireless Attacks Issues

2.5.1 War Driving

This is the act of driving around neighborhoods and areas to enumerate what wireless networks exist, what type of encryption (if any) is used, password (if known), and any other pertinent information. This information may chalk or painted to the street or sides walk or posted to various websites. Some websites, like SkyHook ask their users for this. Be cautious when you see various cars sitting outside your house for long periods of time (unless you live near a Pokemon Gym or a Pokestop).

2.5.2 Cracking Attacks

Just like anything else using Passwords, there are desires and ways to crack those passwords to gain access. Without password attacks, there would be no Have I Been Pwned and other similar sites. Very much like other password attacks, there are the simplistic attacks (brute force) and the complex attacks. While brute force will eventually work, there are methods to minimize the impact if compromised. These mitigating factors are mentioned below in the Wireless Security Tips. One tool, or rather a suite of tools, used to crack Wireless (WEP, WPA1, and WPA2) passwords is Aircrack-ng. It is the replacement for Airsnort. You will also need the airmon-ng, airodump-ng, and aireplay-ng tools (hence the suite) as well as a wireless card set to to "Monitor Mode" (like promiscuous mode) to steal the handshake file and replay handshake to get the file to crack. Once you have the file, you can use your favorite password list (mine is a custom list with rockyou.txt as a base) to attempt to crack the key. Note: The key MUST be in the dictionary for this attack to work. See mypasswords blog post for guidance on how to make a complex and difficult password.

2.5.3 Denial of Service

A Denial of Service (DoS) attack is more of a nuisance than a true technical attack. Think of it as an extreme brute force attack that overwhelms something, in this case, a Wireless network or assets/nodes on it. My broad over generalization of it being a nuisance vice technical is an exaggeration; sometimes the vectors of attack for DoS are very technical. Many technologies, namely web servers and websites, have DoS protective measures, as the internet can connect to them if they are public facing.

2.5.4 Karma Attacks (as seen on S2.E6 of Mr. Robot)

The NANO and TETRA Pineapple Wireless Auditing Platforms

Karma was a tool that was used to sniff, probe, and attack Wireless networks using Man-in-the-Middle (MITM) methods. It has since fell from support as Karma but now exists as several other products. For the scope of this blog post, I will be focusing on the current incarnation known as Karmetasploit a portmanteau of Karma and Metasploit. Once the run control file is obtained and everything properly configured, the attacker will use airmon-ng and airbase-ng (relative of all the other airX-ng tools) to establish itself as a wireless access point (AP). This is what perpetrates the Wireless version of the Evil Twin attack. Note: A femtocell was used to do the same thing on Mr. Robot S2.E6. Femtocells target cellular communications vice Wireless and are carrier specific in addition to being specific for 3G, 4G, or LTE as well as GSM or CDMA/WCDMA. In perpetrating the actual attack, the attacker will open metasploit and input the Karma run control file then wait for users to connect. Once they connect, the attacker has visibility into what the victim is doing and browsing as well as the capability to interrogate the victim machine and extract cookies, passwords, and hashes.

2.6 Wireless Security Tips

Now that you're (hopefully) going to avoid using unsecure Wireless, I would like to present to you ways to be secure and maintain your confidentiality, integrity, and availability. We'll discuss a few myths as well as a couple steps to both protect your wireless network as well as protect you on other wireless networks. Keep in mind that there is not and will never be a 100% solution (aside from the obvious of never connecting).

2.6.1 Wireless Myth Busting

The biggest myth I hear is that by not broadcasting your Wireless network name or Service Set Identifier (SSID) attackers will not see your network and thus will not attack it. The SSID is sent in every single packet transmitted wirelessly. Below is the output of a program called inSSIDer that enumerates these networks and their SSIDs, encryption types, and channels. Below is a screen shot of an inSSIDer capture that shows my test network and all types of encryption? You can also see which channel(s) a network is operating on. Note: I edited the SSIDs and MACs out of extreme caution and respect for my neighbors.

The second myth I hear is that MAC filtering works for preventing unauthorized access to wireless networks. This works under a single condition: the attacker does not know and cannot ascertain the MAC address of a client on the network. This is less effective now due to Karma attacks. 802.1x deals with this and is commonly called "Port Security" or Port-based Network Access Control (PBNAC). It also works on wired networks.

2.6.2 Wireless Encryption

In the early days of Wireless, it was more challenging to encrypt the wireless transmission than it was the wired. This led to the creation of WEP, Wired Equivalent Privacy. WEP was great for its time, but with the evolution of computers and the reduced cost of processing power, it was quickly defeated. Below is a summary of wireless encryption protocols:

- Wired Equivalent Privacy (WEP): Deprecated; 64 bit key - 40 bit key and 24 bit Initialization Vector (IV); used Rivest Cipher 4 (RC4); although not as common, also had 128, 152, and 256 bit versions as well;

- Wireless Protected Access (WPA): Deprecated; began implementation of 802.1i standard; used Temporal Key Integrity Protocol (TKIP; which changes the encryption key per packet) vice Cyclic Redundancy Checking (CRC); also use a fixed encryption key for all users' authentication

- Wireless Protected Access Version 2 (WPA-3): Current Standard; implementation of 802.1i standard; eliminated TKIP in favor of CCMP (CCM Protocol; CCM is a mouthful) which enables the use of the Advanced Encryption Standard also use a fixed encryption key for all users' authentication

Both WPA and WPA2 have the following characteristics:

- PSK (Personal)
- Enterprise
- Wireless Protected Setup
- EAP

Using an encrypted network is awesome with this caveat: it depends on how the encryption is implemented. If it is enterprise, then you are more protected because it has multiple keys and does not share them with multiple hosts. Personal (PSK) encryption is better than nothing, but anyone with access can decrypt packets.

2.7 Wireless Network Attacks

Wireless forensics is a sub-discipline of network forensics. The main goal of wireless forensics is to provide the methodology and tools required to collect and analyze (wireless) network traffic that can be presented as valid digital evidence in a court of law. The evidence collected can correspond to plain data or, with the broad usage of Voice-over-IP (VoIP) technologies, especially over wireless, can include voice conversations. Analysis of wireless network traffic is similar to that on wired networks; however there may be the added consideration of wireless security measures. Wireless networks have entered in a paramount way in the day to day life of people as well as enterprises. The wireless have added convenience of mobility and thus introduced risks on the traditional networks.

2.7.1 Accidental association

Unauthorized access to company wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as "accidental association". When a user turns on a computer and it latches on to a wireless access point from a neighboring company's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

2.7.2 Malicious association

"Malicious associations" are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops are known as "soft APs" and are

created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point. Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant Trojans. Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1x authentications do help with protection but are still vulnerable to cracking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the cracker is just trying to take over the client at the Layer 2 level.

2.7.3 Ad-hoc networks

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-topeer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

2.7.4 Non-traditional networks

Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These nontraditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

2.7.5 Identity theft (MAC spoofing)

Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorized computers with specific MAC IDs to gain access and utilize the network. However, a number of programs exist that have network "sniffing" capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

2.7.6 Man-in-the-middle attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the

traffic. One type of man-in-the- middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack". This attack forces AP connected computers to drop their connections and reconnect with the cracker's soft AP. Man-in-the-middle attacks are enhanced by software such as LAN jack and AirJack, which automate multiple steps of the process. What once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

2.7.7 Denial of service

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

2.7.8 Network injection

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as "Spanning Tree" (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

2.7.9 Caffe Latte attack

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

2.8 Wireless Attacks Detection Techniques

Now that we have a good idea of various attacks in a wireless system, we should now look into certain ways that can be employed to detect certain attacks. These detection techniques can be categorized in following three basic forms:

a) Wireless Access point monitoring
b) Wireless client/node monitoring
c) Wireless traffic monitoring

Wireless Access Point Monitoring

In this the wireless network keeps a list of authorized access points and hardware using the net with information like respective SSID, MAC address and other channel information recorded earlier. The monitoring agent/component would continuously listen to wireless frames like beacons, frame probes; responses and authentications etc. sent out by every Access Points and compare these with the previously recorded information. The monitoring device must listen to every possible channel and record all packets for this technique to be effective. To detect Man-in-the-middle attack, such a monitoring component needs to detect that whether there is a sudden introduction of an AP on another channel previously not present. Though the SSID, MAC address might be spoofed (see previous section) by the attacker in the process of setting up the rouge AP, the channel information in which the genuine AP was operating from has been changed which provides an alert on a possible MitM attack.

Wireless Client/Node Monitoring

The access point monitoring is much simpler, in the wireless client monitoring a list of allowed clients' needs to be maintained. This adds up to lot of administrative overheads, however, some of the clients aspects can be recorded and monitored. Like, list of blacklisted clients can be maintained and any movements from these nodes can generate alerts for analysis. Also, all wireless clients with an unauthorized MAC address (MAC address ranges 143 which have not been allocated out yet) are automatically denied access and an alert send off. Also, clients sending probes with typical nicknames can also be recorded and alert generated. One more area where monitoring might be applied is WEP (encrypted) traffic is being used to send/receive, no station should be reusing the same WEP Initialization Vector (used to generate keys) over and over again within a very short period of time (WepWedgie and other cracking tools use this).

For wireless clients that are legitimate, there is a sequence number field within the IEEE 802.11 header which can be tracked for abrupt changes. Certain times when impersonation attacks are being carried out, the attacker will be able to read the MAC / IP address of the victim, but it will not be able to continue with the sequence

number used previously by the victim, thus by monitoring the sequence number in these client generated packets impersonation attacks can be easily detected.

General Wireless Traffic Monitoring

To detect DoS attacks, Wireless traffic can be monitored for attempts to flood the network using de-authentication, de-association, authentication, association, erroneous authentication. Frequency and Signal-To-Noise Ratio monitoring could help signal an oncoming RF based DOS attack on your wireless network. Failures in authentication as well as association can also be monitored and reported.

2.9 Network Auditing

Wireless network auditing is an important part of WLAN security policy. The network needs to be regularly audited for rouge hardware. In this method the network is scanned and mapped for all access points and WLAN nodes. Then this is compared with previous network map. Commonly available network mapping tools like nets tumbler and wavelan-tool can be used to do this. Specialized tools such as Air snort can be used for WEP cracking and auditing the network for weak keys, key reuse and WEP security settings. These methods include the same tests as those carried out by hackers for breaking into the network.

2.9.1 Safety First

The unprotected WLANs are many. Wireless traffic is easily recorded. Passive eavesdroppers can gather proprietary information, logins, passwords, intranet server addresses, and valid network and station addresses. Intruders can steal Internet bandwidth, transmit spam, or use your network as a springboard to attack others. They can capture and modify traffic to masquerade as you, with financial or legal consequences. Even a low-tech attacker can disrupt your business by launching wireless packet floods against your APs, nearby servers, next-hop wired network or Internet uplink.

Fortunately, these risks are not yet heavily exploited. Jupiter Media Research recently reported that 26 percent of surveyed businesses had experienced at least one type of WLAN attack in the past year. However, most of these incidents were problems waiting to happen: rogue APs, stations associating with the wrong AP and war driving. Serious security breaches--like wired network intrusion, theft of confidential data and forgery--were far less common, according to the survey.

In short, early adopters have been lucky. The cost of downtime and cleanup can be

an order of magnitude greater than the cost of prevention. Now is the time to start playing catch-up with WLAN security.

2.9.2 Policy

If you don't know what you're defending and why, your security measures are just shots in the dark. It's critical to identify business assets that must be protected and the impact of damage, theft or loss.

For wireless, as with dial-up and DSL, your policy should define access requirements. Who needs access to what and when? If your company already has a remote access policy for travelers and telecommuters, expand it to incorporate wireless. If you have no such policy, create one. Remember to include scenarios that are unique to wireless, like employees at public hot spots (see "Hot Spots Give Security Managers the Chills") or office visitors.

Consider how wireless changes the rules for office visitors. Few companies offer Ethernet access to visiting customers or business partners. Jacks in public areas are typically disabled or latched to known addresses. But wireless laptops and PDAs can easily associate with nearby APs or other wireless stations. This is both a threat and an opportunity. Security policies should define rules for "walled garden" guest access. For example, you may prohibit peer-to-peer networking while permitting logged guest sessions through specific APs with limited destinations, protocols, duration and bandwidth. If guest access is banned, your policy must state this so that steps can be taken to prevent visitor intrusion.

2.9.3 Taking Stock

Before you plot out access point deployment, conduct a site survey using a WLAN discovery tool such as NetStumbler. What you learn might surprise you. According to a recent Gartner report, at least one in five companies find APs deployed without IT department permission. Commodity pricing, retail distribution and setup wizards have made it trivial for employees to install rogue APs, which can expose corporate assets to outsiders and interfere with WLAN performance. Find and eliminate rogue APs from the start--or safely incorporate them into your wireless network design.

You may find nearby APs and stations that don't belong to you. Survey public areas (parking lots, hallways, lobbies) just beyond the physical boundaries of your facility, including upstairs and downstairs. Neighboring MAC addresses should be recorded, along with network name (SSID) and channel. This list will be used to avoid cross-

channel interference and eliminate false-positive intrusion alerts.

2.9.4 WLAN Meets LAN

Consider how new WLAN segments will be integrated with and reuse components of your wired infrastructure. Your network topology, device placement and current security measures all have direct impact on wireless LAN security.

Restrict AP placement in your network topology. Wireless applications require protected access to the intranet and/or Internet, affecting routers,

firewall rules and VPN policies. Wireless APs are untrusted entities and should always sit outside the firewall or within a DMZ--never inside the firewall.

Think in terms of a three-interface firewall--intranet on the inside, APs (and other public servers) on the DMZ, and Internet on the outside interface. Circumstances dictate whether your APs should sit on the DMZ or outside.

A DMZ can protect the WLAN from Internet threats while protecting the wired intranet from WLAN threats. However, for example, if your firewall doesn't let VPN tunnels originate in the DMZ, you may need to place your AP on the outside interface instead.

However, WLANs require more bandwidth per user than v.90 or even residential broadband. Smart APs can offload VPN processing, placing fewer demands on the firewall.

2.9.5 802.11 Security

You have an increasing choice of options for authentication and encryption, from several emerging technologies to VPNs. Depending on the size of your enterprise and the level of risk WLAN opens up, you may want to start with the security 802.11 offers out of the box.

Basic 802.11 securities deter accidental association or casual eavesdropping. In most WLAN products, however, these security features are disabled by default. Disabled means the WLAN operates in "open system" mode--any station can join because they know the network's Service Set Identifier (SSID) or by capturing beacon frames broadcast by APs.

2.9.6 802.1X

Many APs can be configured with a list of MAC addresses to allow or block. But MAC addresses can be forged. To address this, IEEE 802.1X provides a standard,

multivendor framework for combining port-level access control with some type of authentication.

2.9.7 Alternative WLAN Network Topologies

802.1X applies the Extensible Authentication Protocol (EAP) to LANs-- wired and wireless--defining messages to be exchanged between LAN stations (supplicants), APs (authenticators) and backend authentication servers. Think of 802.1X as an on/off switch that blocks everything but EAP until the authentication server accepts the supplicant's access request.

Encryption keys are supplied dynamically to authorized stations on a per- session basis.

2.9.8 Wireless Protected Access

Wireless is the brand given to 802.11 products certified by the Wireless Alliance, a consortium organized to promote 802.11 products and interoperability among them. Wireless Protected Access (WPA) is a security enhancement for current-generation WLAN hardware. WPA incorporates just the stable parts of the 802.11i advanced security standard, which is still a work in progress. WPA products can interoperate with the older WEP products.

2.9.9 VPNs

If your company already has a remote access VPN, consider using it for WLAN security. Reuse makes the most sense when security policy is consistent for WAN and LAN access--the same credentials can be used for authentication; the same encryption algorithms can be used for confidentiality.

2.9.10 WLANs Present Their Own Set of VPN Issues

There is more data to encrypt on a high-speed WLAN. Additional gateways may be needed to support wireless encryption, particularly when using 802.11a/g at link speeds up to 54 Mbps.

Tunnels are bound to IP addresses. WLAN stations roam between APs, changing IP address. Broken tunnels can be reestablished, but service disruption is often noticeable. In smaller WLANs, several APs can share the same DHCP scope. VLANs can help, up to a point. In larger WLANs, wireless gateways can provide tunnel persistence when stations roam.

Client deployment can be costly and difficult to mandate. Reusing deployed clients is

one thing, adding new clients and policies quite another. VPN tunnels, WEP/TKIP and 802.1X address different problems. Consider a business partner using a guest WLAN. A tunnel controls access to the visitor's own network; 802.1X controls access to the guest WLAN. A tunnel prevents eavesdropping from end to end; WEP/TKIP prevents eavesdropping on the air link only.

2.9.11 The Many Facets of Wireless

When considering wireless, it's important to realize that there are many kinds of wireless technologies, aimed at different devices and usage environments:

Wireless Personal Area Networks (WPANs) use very short-range wireless technology to replace cables connecting PCs with peripherals, phones with headsets, etc. The most popular WPAN is Bluetooth (IEEE 802.15), which reaches about 30 feet, at speeds up to 780 Kbps.

2.9.12 Portals and 'Mobile VPNs'

Portals frequently control access to public hot spots and guest networks (wired or wireless). Outbound HTTP requests are redirected to a login page, where the user authenticates via SSL before access is granted to the network.

2.9.13 Hot Spots Give Security Managers the Chills

For several years, road warriors have used Internet cafés to check e-mail. Wireless hot spots make this more convenient. Workers use hot spots to make productive use of time spent waiting in airports and hotel lobbies.

Hot spots are found in 1.67 million access locations across the United States. With cellular carriers buying their way into the hot spot market, things are likely to change. By 2007, Analysis Re-search predicts 21 million people in the U.S. will use hot spots. Cometa Networks-an AT&T, IBM Global Services and Intel partnership-wants to make wireless connectivity ubiquitous by building a national hot spot network, are placing APs within a five-minute walk in cities and a five-minute drive elsewhere.

2.10 Let us Sum up

In this unit we have provided an overview of the security problems in wireless networks and focusing on security issues of wireless network. We have describe about how to securing wireless transmission and how to protect it confidentiality. Wireless networks have entered in a paramount way in the day to day life of people as well as enterprises. The wireless networks have added convenience of mobility and thus introduced risks on the traditional networks.

2.11   Further Readings

1. Wireless Networks: Security Problems and Solutions, SANS Institute 2002

2. Jie Gao, Department of Computer Science, Stony Brook University, Stony Brook, NY 11794, USA, jgao@cs.sunysb.edu, April 24, 2007

3. R. Rathika, D. Sowmyadevi, Wireless Sensor Network Security: Vulnerabilities, Threats and Countermeasures, IJARCSSE, Volume 6, Issue 1, January 2016 ISSN: 2277 128X.

4. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, Wireless Network Security: Vulnerabilities, Threats and Countermeasures, International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.

5. Post-Graduate Diploma in Cyber Security Cyber Attacks and Counter Measures: User Perspective (PGDCS-03).

2.12   Assignments

1. What is malicious association?

2. What is network auditing?

3. Write about wireless network attacks.

4. How to secure wireless client devices?

5. Discuss about different type of wireless attack issues.

6. Discuss about the tips to Wireless Network Security.

7. Write the sort notes about Wireless Encryption.

8. What are the different types of Wireless Network Attacks?

9. What are the public wireless security issues?

Unit 3: Securing a Wireless Network

<div style="text-align:right">**3**</div>

Unit Structure

3.1 Learning Objectives

After going through this unit you should be able to

1. Know the security risks posed by wireless computer networks.
2. To provide guidance for establishing secure wireless networks.
3. To know the suggested management, operational and technical countermeasures to help mitigate security risks specific to wireless computing technologies.
4. Authentication of secure wireless networks with attacks.

3.2 Introduction

Wireless Networking (Wireless) has made it so easy for anyone to use Internet on your computer, mobile phones, tablets and other wireless devices anywhere in the house without the clutter of cables.

With traditional wired networks, it is extremely difficult for someone to steal your bandwidth but the big problem with wireless signals is that others can access the Internet using your broadband connection even while they are in a neighboring building or sitting in a car that's parked outside your apartment.

3.3 Securing Wireless Signal Transmissions

The nature of wireless communications creates three basic threats: Interception, Alteration and Disruption.

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

3.3.1 Protecting the Wireless Transmissions

Two types of countermeasures exist for reducing the risk of eavesdropping on wireless transmissions. The first involves methods for making it more difficult to

locate and intercept the wireless signals. The second involves the use of encryption to preserve confidentiality even if the wireless signal is intercepted.

Signal-Hiding Techniques

In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that organizations can take to make it more difficult to locate their wireless access points. The easiest and least costly include the following: Turning off the service set identifier (SSID) broadcasting by wireless access points, Assign cryptic names to SSIDs, Reducing signal strength to the lowest level that still provides requisite coverage or Locating wireless access points in the interior of the building, away from windows and exterior walls. More effective, but also more costly methods for reducing or hiding signals include: Using directional antennas to constrain signal emanations within desired areas of coverage or Using of signal emanation-shielding techniques, sometimes referred to as TEMPEST, 1 to block emanation of wireless signals.

Encryption

The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. This is especially important for organizations subject to regulations.

3.3.2 Preventing Alteration of Intercepted Communications

Interception and alteration of wireless transmissions represents a form of "man-in the middle" attack. Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users.

3.3.3 Reduce the Risk of Denial-of-Service Attacks

Wireless communications are also vulnerable to denial-of-service (DoS) attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Careful site surveys can identify locations where signals from other devices exist; the results of such surveys should be used when deciding where to locate wireless access points. Regular periodic audits of wireless networking activity and performance can identify problem areas; appropriate remedial actions may include removal of the offending devices or measures to increase signal strength and coverage within the problem area.

3.4 Securing Wireless Access Points

Insecure, poorly configured wireless access points can compromise confidentiality by

allowing unauthorized access to the network.

3.4.1 Countermeasures to Secure Wireless Access Points

Organizations can reduce the risk of unauthorized access to wireless networks by taking these three steps:

1. Eliminating rogue access points;
2. Properly configuring all authorized access points; and
3. Using 802.1 xs to authenticate all devices.

1 Eliminate Rogue Access Points

The best method for dealing with the threat of rogue access points is to use 802.1 xs on the wired network to authenticate all devices that are plugged into the network. Using 802.1x will prevent any unauthorized devices from connecting to the network.

2 Secure Configurations of Authorized Access Points

Organizations also need to ensure that all authorized wireless access points are securely configured. It is especially important to change all default settings because they are well known and can be exploited by attackers.

3 Use 802.1 xs to authenticate all devices

Strong authentication of all devices attempting to connect to the network can prevent rogue access points and other unauthorized devices from becoming insecure backdoors. The 802.1x protocol discussed earlier provides a means for strongly authenticating devices prior to assigning them IP addresses.

3.5 Securing the Wireless Client

An essential step in wireless security is locking down the client device used to access the wireless network. If a laptop or other endpoint is compromised, then the device can be used to gain entry into the network, regardless of other wireless security measures that may be in place. By the way, this is true whether a client is used to access the network over wireless or wired. Mobile clients, like laptops, are inherently used in some unfriendly places outside the corporate network, and can become infected with malicious software.

One way hackers have gained access to corporate wireless networks is to hack the laptop of an employee while they are sitting in an airport or coffee shop. There are a couple of well-known attacks that can be launched at a wireless NIC, which can result in learning the corporate wireless security key.

Whether accessing a wired or wireless network, it is a best practice to implement

host-based security on clients, including anti-virus and host intrusion protection such as Cisco Security Agent (CSA). With CSA, attempts to install software or execute harmful calls in the operating system can be intercepted and prevented.

Another important measure is to insure that clients accessing the network are "healthy," meaning that they have not been compromised, have the correct anti-virus software running, and are otherwise compliant with the company's security policy. Enforcement of all these measures can be difficult, but with Cisco Clean Access (CCA) solution, the wireless network can challenge endpoints to prove compliance and "health" before being permitted on the network.
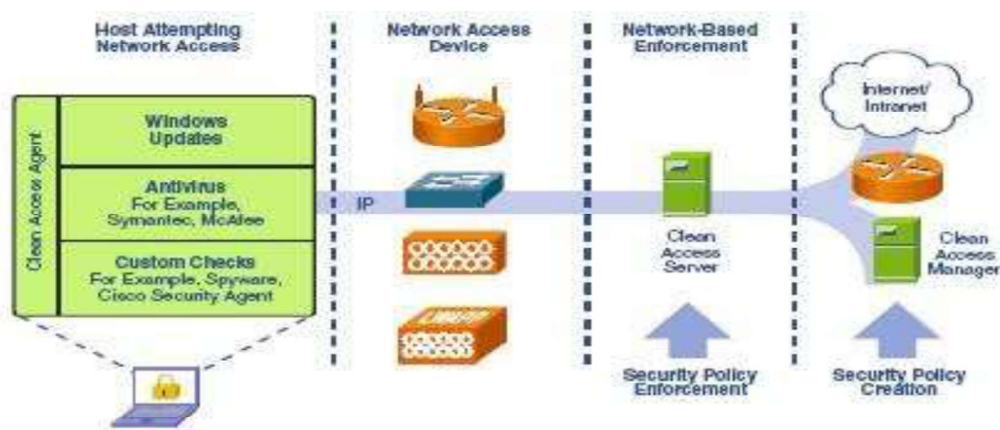
3.6 Securing Wireless Communications

The next step to securing the wireless network (which is where most people start and often stop) is securing the actual wireless communications over the air between the client device and the wireless access point. There are two best practices to follow: authentication and encryption.

Authentication of wireless clients by the network insures that only authorized devices are allowed to join the wireless network. The best practice for authentication is to implement Extensible Authentication Protocol (EAP) and Flexible Authentication via Secure Tunnel (FAST). Using a set of credentials on the client device, the wireless network can authenticate the endpoint against the credentials stored in the corporate identity database. If a match is not achieved, access to the wireless network is denied. (Wired networks are implementing an equivalent technique via 802.1x.)
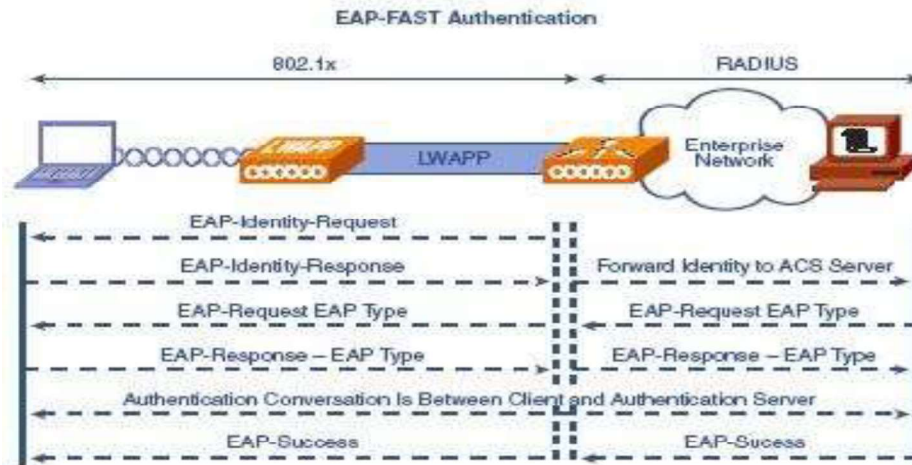
Just as important as the network authenticating a wireless client is for the wireless client to authenticate the network to which it is connecting. "Imposter" access points can be setup posing as legitimate corporate wireless network access points. If only the SSID is used to determine the network authenticity, this is trivial to imitate. The wireless client needs to use additional factors and credentials to authenticate that the access point it is trying to connect to be really a corporate network access point. This mutual authentication is also part of the EAP-FAST authentication process.

3.7 Securing Wireless Client Devices

Two major threats to wireless client devices are

(1) Loss or Theft

(2) Compromise.

Loss or theft of laptops and PDAs is a serious problem. Laptops and PDAs often store confidential and proprietary information. Consequently, loss or theft of the devices may cause the organization to be in violation of privacy regulations involving the disclosure of personal identifying information it has collected from third parties. Another threat to wireless client devices is that they can be compromised so that an attacker can access sensitive information stored on the device or use it to obtain unauthorized access to other system resources.

3.8 Vulnerabilities of wireless networks, devices and protocols.

There are a number of vulnerabilities in the security protocols listed above. We describe some of these vulnerabilities in the following sections.

3.8.1 Insertion attacks

Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review.

- **Unauthorized Clients –** An attacker tries to connect a wireless client, typically a laptop or PDA, to an access point without authorization. Access points can be configured to require a password for client access. If there is no password, an intruder can connect to the internal network simply by enabling a wireless client to communicate with the access point.

- **Unauthorized or Renegade Access Points –** An organization may not be aware that internal employees have deployed wireless capabilities on their network in the form of an unauthorized access point, attached to the wired network.. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources through the rogue access point.

3.8.2 Interception and Monitoring of Wireless Traffic

As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be within range of an access point (approximately 300 feet for 802.11b) for this attack to work, whereas a wired attacker can be anywhere there is a functioning network connection. The advantage for a wireless interception is that a wired attack requires the placement of a monitoring agent on a compromised system. All a wireless intruder needs is access to the network data stream traveling over public air waves.

There are two important considerations to keep in mind with the range of 802.11b access points. First, directional antennae can dramatically extend either the transmission or reception ranges of 802.11b devices. Therefore, the 300 foot maximum range attributed to 802.11b only applies to normal, as-designed installations. Enhanced equipment also enhances the risk. Second, access points transmit their signals in a circular pattern, which means that the 802.11b signal almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings, or even through floors in multistory buildings. Some of the monitoring techniques:

- **Wireless Packet Analysis –** Attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of
these tools capture the first part of the connection session, where the data would typically include the username and password. An intruder can then masquerade as a

legitimate user by using this captured information to hijack the user session and issue unauthorized commands.

- **Broadcast Monitoring –** If an access point is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcast out over the wireless network. Because the Ethernet hub broadcasts all data packets to all connected devices including the wireless access point, an attacker can monitor sensitive data on the wireless network, not even intended for any wireless clients.

- **Access Point Clone (Evil Twin) Traffic Interception –** The

  availability of WiFi in coffee shops, airports and other high-traffic areas led to the evolution of the Evil Twin Network. The Evil Twin is essentially a wireless version of a phishing scam users think they're connecting to a genuine hot spot but are actually connecting to a rogue access point set up by a phisher. Once connected, the attacker serves up pages mimicking actual websites. Banking, EBay or PayPal sites are the websites of choice. All the attacker needs is the hardware for an access point (with a higher signal strength than the target network) and off-the-shelf software tools like Karma 10 which is a set of wireless sniffing tools to discover clients and their preferred/trusted networks by passively listening for 802.11 Probe Request frames.

3.8.3 Jamming

Denial of service attacks are also easily applied to wireless networks, where legitimate traffic cannot reach clients or the access point because illegitimate traffic overwhelms the frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency (or the other frequencies in which WiFi operates), corrupting the signal until the wireless network ceases to function. In addition, cordless phones, baby monitors and other devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. These denials of service attacks can originate from outside the work area serviced by the access point, or can inadvertently arrive from other WiFi devices installed in other work areas that degrade the overall signal.

3.8.4 Client-to-Client Attacks

Two wireless clients can talk directly to each other, bypassing the access point. Users therefore need to defend clients not just against an external threat but also against each other.

- File Sharing and Other TCP/IP Service Attacks – Wireless clients

running TCP/IP services such as a Web server or file sharing are open to the same exploits and Misconfiguration as any user on a wired network.

- DOS (Denial of Service) – A wireless device floods another wireless client with bogus packets, creating a denial of service attack. In addition, duplicate IP or MAC addresses, both intentional and accidental, can cause disruption on the network.

3.8.5 Attacks against Encryption

The 802.11, Wired Equivalent Privacy (WEP) standard, described above, was intended to make a WLAN as secure as an unsecured wired network. Not long after WEP was developed, a series of independent research studies began to expose its cryptographic weaknesses. The first practical attack on WEP was identified by researchers11 Scott Fluhrer, Itsik Mantin and Adi Shamir who found that, even with WEP enabled, third parties with a moderate amount of technical expertise and resources could breach WLAN security.

Three key difficulties were identified:

- WEP uses a single, static shared key. It remains the same unless a network administrator manually changes it on all devices in the WLAN, a task that becomes ever more daunting as the size of the WLAN increases.

- At the time of its introduction, WEP employed a necessarily short 40-bit encryption scheme. The scheme was the maximum allowed by US export standards at that time. In 1997, the US government deemed the export of data cryptography to be as threatening to national security as the export of weapons of mass destruction. By necessity, WiFi security had to be weak if the specification was to be adopted as an international standard and if products were to be freely exported.

- Other technical problems contributed to its vulnerability, including attacks that could lead to the recovery of the WEP key itself. Attacks based on Fluhrer, Mantin and Shamir's paper have come to be known as "FMS Attacks". Shortly after the FMS paper was released, the following tools to automate WEP cracking were developed:

- WEPCrack
- AirSnort

In response to the weaknesses in WEP new security mechanisms were developed.

- Cisco developed the Lightweight Extensible Authentication Protocol (LEAP)

- WiFi protected access (WPA) was developed to replace WEP. It had 2 sub-parts-
- WPA-PSK (Pre-Shared key)
- WPA-Radius

In March 2003, Joshua Wright12 disclosed that LEAP was vulnerable to dictionary attack. A short time later Wright released ASLEAP, a tool to automate attacks against LEAP. Cisco released EAP-FAST as a replacement for LEAP about a year after Wright's initial disclosure to them. In November 2003 Robert Moskowitz of ISCA Labs detailed potential problems with WPA when deployed using a Pre-Shared Key in his paper "Weakness in Passphrase Choice in WPA Interface".

In November 2004 Joshua Wright released CoWPAtty which could perform an automated dictionary attack process against WPA-PSK

Attacks against WEP

Even with chopping attacks, a large number of packets still need to be captured by an attacker. The easiest way to do this is by re-injecting packets back into the network to generate unique initialization vectors.

Attacks against WPA

WPA Pre shared keys with pass-phrases shorter than 21 characters is vulnerable to dictionary attacks. This is an offline attack and not as easy to identify in real time as attacks against WEP.

3.9   Misconfiguration

Many access points ship in an unsecured configuration in order to emphasize ease of use and rapid deployment. Unless administrators understand wireless security risks and properly configure each unit prior to deployment, these access points will remain at a high risk for attack or misuse. The following section examines three leading access points, one each from Cisco, Lucent and 3Com. Although each vendor has its own implementation of 802.11b, the underlying issues should be broadly applicable to products from other vendors.

- **Server Set ID (SSID) –** SSID is a configurable identification that allows clients to communicate with an appropriate access point. With proper configuration, only clients with the correct SSID can communicate with access points. In effect, SSID acts as a single shared password between access points and clients. Access points come with default SSIDs. If not changed, these units are easily compromised. Here are common default SSID's:

Manufacturer	Default SSID
Cisco	tsunami
3Com	101
Lucent/Cabletron	Roam About Default Network Name
Addtron	WLAN
Intel	intel
Linksys	linksys

SSIDs go over the air as clear text if WEP is disabled, allowing the SSID to be captured by monitoring the network's traffic. Another common vulnerability regarding the SSID is setting it to something meaningful such as the AP's location or department, or setting them to something easily guessable.

By default, the Access Point broadcasts the SSID every few seconds in what are known as 'Beacon Frames'. While this makes it easy for authorized users to find the correct network, it also makes it easy for unauthorized users to find the network name. This feature is what allows most wireless network detection software to find networks without having the SSID upfront.

- **Wired Equivalent Privacy (WEP) –** WEP can be typically configured as follows:
  - o No encryption
  - o 40 bit encryption
  - o 128 bit encryption

Most access point's ship with WEP turned off. Although 128 bit encryption is more effective than 40 bit encryption, both key strengths are subject to WEP's known flaws.

- **SNMP Community Passwords –** Many wireless access points run SNMP agents. If the community word is not properly configured, an intruder can read and potentially write sensitive data on the access point. If SNMP agents are enabled on the wireless clients, the same risk applies to them as well. By default, many access points are read accessible by using the community word, "public". 3Com access points allow write access by using the community word, "comcomcom". Cisco and Lucent/Cabletron require the write community word to be configured by the user or administrator before the agent is enabled.

- **Client Side Security Risk –** Clients connected to access point store sensitive information for authenticating and communicating to the access point. This information can be compromised if the client is not properly configured. Cisco client software stores the SSID in the Windows registry, and the WEP key in the firmware, where it is more difficult to

access. Lucent/Cabletron client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry, but it is encrypted using an undocumented algorithm. 3Com client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry with no encryption.

- **Installation –** By default, all three access points are optimized to help build a useful network as quickly and as easily as possible. As a result, the default configurations minimize security.

3.10   Securing Wireless Networks

3.10.1   Use of Encryption

The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn't have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on.

3.10.2   Use anti-virus, anti-spyware software, and a firewall

Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

3.10.3   Turn off identifier broadcasting

Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

3.10.4   Change the identifier on your router from the default

The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters

long: The longer your password, the harder it is for hackers to break.

3.10.5 Change your router's pre-set password for administration

The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. The longer the password, the tougher it is to crack.

3.10.6 Allow only specific computers to access your wireless network

Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

3.10.7 Turn off your wireless network when you know you won't use it

Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

3.10.8 Don't assume that public "hot spots" are secure

Many cafés, hotels, airports, and other public establishments offer wireless networks for their customers' use.

3.11 Wireless Network Security protocols

One of the biggest concerns for wireless users is making sure their router and wireless network are secure. I think we all know by now that, when it comes to technology, there is no such thing as being 100 percent secure. Once you send data over a wireless signal, you've already potentially exposed your data to hackers, and once you've set up a router, Wireless signal leeches are always a possibility.

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

Wireless security is the prevention of unauthorized access or damage to computers

using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA). WEP is a notoriously weak security standard. WEP is an old IEEE 802.11 standard from 1999, which was out dated in 2003 by WPA, or Wireless Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

Wireless devices communicate through radio transmissions, without physical connections and without network or peripheral cabling. Wireless systems include local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices that do not process or store information. Other wireless devices being widely used include infrared (IR) devices such as remote controls, cordless computer keyboards, mouse devices, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver.

3.12   Authentication of Wireless Network

Only clients who know a shared secret may connect to the network.WEP was the first cryptographic protocol developed for Wireless to enable privacy and authentication. WEP, however, was not secure after all. To rectify the security issues with WEP, the Wireless Alliance pushed a new cryptographic protocol, WPA. Since then, a common practice of securing a WPA enabled network with passwords has been discovered to be vulnerable to an offline dictionary-attack. Even though WPA itself is thought to be secure, apart from the dictionary-attack, it was a quick fix to the problems in WEP.

3.13   Use of Wi-Fi

Wireless technologies have become inexpensive, user- friendly and available to a large number of people and companies. In dense urban areas,

access points belonging to different individuals are so closely spaced that their coverage areas overlap. With its popularity and the availability to anyone within range, many individuals detect Wi-Fi networks as a hobby. War drivers bring their laptops and Wi-Fi gear1With WEP, anyone participating in the network can eavesdrop on other conversations in the network in their cars. With the aid of a

Global Positioning System (GPS) receiver and an antenna, they explore areas and map the locations and coverage areas of access points. Some do it for the fun, and some with the intent to exploit vulnerable Wi-Fi networks. War bikers and war walkers do the same by other means of transportation.

3.10.9 Security problems with WEP include the following

1.   The use of static WEP keys: Many users in a wireless network potentially sharing the identical key for long periods of time, is well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key.

2.   Caffe Latte attack: The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

3.   WEP: WEP provides no cryptographic integrity protection. However, the 802.11 MAC protocol uses a no cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of no cryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged.

4.   Authentication is not enabled: only simple SSID identification occurs. Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.

5.   Device authentication is simple shared-key challenge-response. One- way challenge-response authentication is subject to ―man-in the-middle‖ attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

3.14   Let us Sum up

Although Wi-Fi technologies have significantly improved their security capabilities, many of the features and abilities are available only in newer equipment for IT-

managed infrastructure. Meanwhile, cellular data networks rely on a completely separate security architecture that emphasizes protection of the radio link and does not provide end-to-end encryption. By using an SSL VPN, you can secure all forms of wireless communication, both externally and internally. Moreover, this approach accommodates a wide range of user equipment. Nevertheless, it's too soon to tell whether WNS encryption problems will turn out to be a tempest in a teapot or seriously exploited vulnerabilities.

3.15   Further Readings

1. Using Wireless Technology Securely, Produced 2006 by US-CERT, a government organization. Updated 2008.

2. Jeff Bilger, Holly Cosand, Noor-E-Gagan Singh, Joe Xavier, "Security and Legal Implications of Wireless Networks, Protocols, and Devices".

3. Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks" June 30, 2012.

4. http://www.cisco.com/web/services/news/ts_newsletter/tech/chalktalk /archives/200802.html

3.16   Assignments

1. Describe about securing wireless signal transmission.

2. What is an insertion attack?

3. Write about the Use of Wi-Fi in network.

4. Explain about Jamming signal.

5. Write about Authentication of Wireless Network.

6. What are the methods for securing wireless transmissions?

7. What are the processes for securing wireless networks?

8. Write about Client-to-Client Attacks.

9. What is Misconfiguration

10. How to secure wireless client devices?

Unit 4: Mobile Device Security 4

Unit Structure

4.1 Learning Objectives

After going through this unit you should be able to

1. Know the use of security software on MOBILE.
2. Develop a sense of responsibility to store personal data, private photos, Internet banking information or even company data.
3. Know how to protect smart phones which are know a days are more costly.

4.2 Introduction

Smartphone's are the future of modern communications. According to a survey carried out by IDC there are over 1.6 billion smart phones running Android in current use. Classic telephone functions are becoming less relevant. For example, the inclusion of high-quality cameras means that smart phones are being used more and more to take photos. Additionally, users are employing services like Facebook, WhatsApp and Email to run their lives from their smart phones. This means that smart phones are being targeted by criminals, who try to infect devices and/or steal sensitive data, e.g. by phishing attacks. As modern smart phones are often expensive to buy, they are also an attractive target for thieves. As it is not possible to physically prevent them from being stolen, they must be made less attractive to thieves. Consequently, many of today's security products contain not only malware protection, but also highly developed theft-protection functions, such as anti theft software, which make the device less attractive to thieves (e.g. by locking the device), and help the owner to find it again.

4.3 Mobile Device Security

Prior to the widespread use of smart phones, the dominant paradigm for computer and network security in organizations was as follows. Corporate IT was tightly controlled. User devices were typically limited to Windows PCs. Business applications were controlled by IT and either run locally on endpoints or on physical servers in data centers. Network security was based upon clearly defined perimeters that separated trusted internal networks from the un-trusted Internet. Today, there have been massive changes in each of these assumptions. An organization's networks must accommodate the following.

Growing use of new devices: Organizations are experiencing significant growth in

employee use of mobile devices. In many cases, employees are allowed to use a combination of endpoint devices as part of their day-to- day activities.

Cloud-based applications: Applications no longer run solely on physical servers in corporate data centers. Quite the opposite, applications can run anywhere on traditional physical servers, on mobile virtual servers, or in the cloud. Additionally, end users can now take advantage of a wide variety of cloud-based applications and IT services for personal and professional use. Facebook can be used for an employee's personal profiles or as a component of a corporate marketing campaign. Employees depend upon Skype to speak with friends abroad or for legitimate business video conferencing. Drop box and Box can be used to distribute documents between corporate and personal devices for mobility and user productivity.

De-parameterization: Given new device proliferation, application mobility and cloud-based consumer and corporate services, the notion of a static network perimeter is all but gone. Now there are a multitude of network perimeters around devices, applications, users, and data. These perimeters have also become quite dynamic as they must adapt to various environmental conditions such as user role, device type, server virtualization mobility, network location and time-of-day.

External business requirements: The enterprise must also provide guests, third-party contractors, and business partners network access using various devices from a multitude of locations.

The central element in all of these changes is the mobile computing device. Mobile devices have become an essential element for organizations as part of the overall network infrastructure. Mobile devices such as smart phones, tablets, and memory sticks provide increased convenience for individuals as well as the potential for increased productivity in the workplace. Because of their widespread use and unique characteristics, security for mobile devices is a pressing and complex issue. In essence, an organization needs to implement a security policy through a combination of security features built into the mobile devices and additional security controls provided by network components that regulate the use of the mobile devices.

4.3.1 Security Threats

Mobile devices need additional, specialized protection measures beyond those implemented for other client devices, such as desktop and laptop devices that are

used only within the organization's facilities and on the organization's networks.

Major security concerns for mobile devices:

Lack of Physical Security Controls: Mobile devices are typically under the complete control of the user, and are used and kept in a variety of locations outside the organization's control, including off premises. Even if a device is required to remain on premises, the user may move the device within the organization between secure and no secured locations. Thus, theft and tampering are realistic threats.

The security policy for mobile devices must be based on the assumption that any mobile device may be stolen or at least accessed by a malicious party. The threat is twofold: A malicious party may attempt to recover sensitive data from the device itself, or may use the device to gain access to the organization's resources.

Use of Untrusted Mobile Devices In addition to company-issued and company controlled mobile devices; virtually all employees will have personal smart phones and/or tablets. The organization must assume that these devices are not trust worthy. That is, the devices may not employ encryption and either the user or a third party may have installed a bypass to the built-in restrictions on security, operating system use, and so on.

Use of Un-trusted Networks If a mobile device is used on premises; it can connect to organization resources over the organization's own in-house wireless networks. However, for off-premises use, the user will typically access organizational resources via Wi-Fi or cellular access to the Internet and from the Internet to the organization. Thus, traffic that includes an off- premises segment is potentially susceptible to eavesdropping or man-in- the-middle types of attacks. Thus, the security policy must be based on the assumption that the networks between the mobile device and the organization are not trustworthy.

Use of Applications Created by Unknown Parties: By design, it is easy to find and install third-party applications on mobile devices. This poses the obvious risk of installing malicious software. An organization has several options for dealing with this threat, as described subsequently.

Interaction with Other Systems a common feature found on smart phones and tablets is the ability to automatically synchronize data, apps, contacts, photos, and so on with other computing devices and with cloud-based storage. Unless an organization has control of all the devices involved in synchronization, there is

considerable risk of the organization's data being stored in an unsecured location, plus the risk of the introduction of malware.

Use of Un-trusted Content: Mobile devices may access and use content that other computing devices do not encounter. An example is the Quick Response (QR) code, which is a two-dimensional barcode. QR codes are designed to be captured by a mobile device camera and used by the mobile device. The QR code translates to a URL, so that a malicious QR code could direct the mobile device to malicious Web sites.

Use of Location Services: the GPS capability on mobile devices can be used to maintain knowledge of the physical location of the device. While this feature might be useful to an organization as part of a presence service, it creates security risks. An attacker can use the location information to determine where the device and user is located, which may be of use to the attacker.

4.4 Mobile Device Security Strategy

With the threats listed in the preceding discussion in mind, we outline the principal elements of a mobile device security strategy. They fall into three categories: device security, client/server traffic security, and barrier security

Mobile Device Security Elements
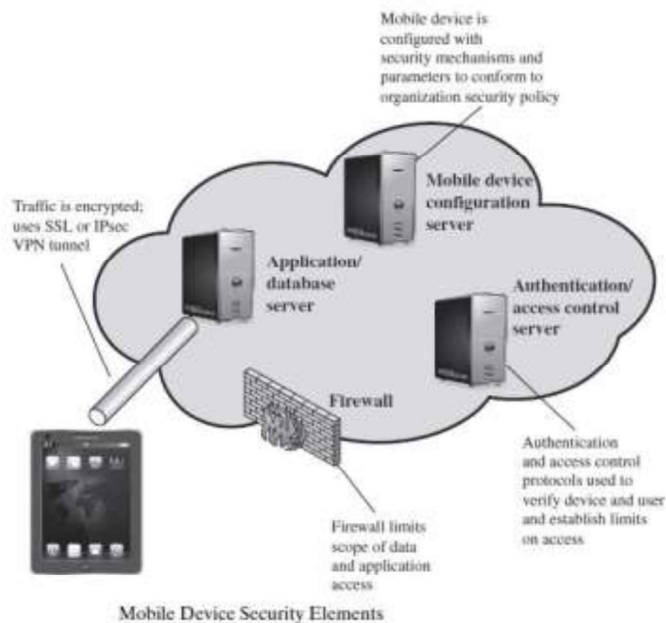
Device Security: A number of organizations will supply mobile devices for employee use and pre configure those devices to conform to the enterprise security policy. However, many organizations will find it convenient or even necessary to adopt a bring your- own-device (BYOD) policy that allows the personal mobile devices of employees to have access to corporate resources. IT managers should be able to inspect each device before allowing network access. IT will want to establish configuration guidelines for operating systems and applications. For example, "rooted" or "jail-broken" devices are not permitted on the network, and mobile devices cannot store corporate contacts on local storage. Whether a device is owned by the organization or BYOD, the organization should configure the device with security controls, including the following:

- Enable auto-lock, which causes the device to lock if it has not been used for a given amount of time, requiring the user to re-enter a four- digit PIN or a password to re-activate the device.

- Enable password or PIN protection. The PIN or password is needed to unlock the device. In addition, it can be configured so that e-mail and other data on the device are encrypted using the PIN or password and can only be retrieved with the PIN or password.

- Avoid using auto-complete features that remember user names or passwords.

- Enable remote wipe.

- Ensure that SSL protection is enabled, if available.

- Make sure that software, including operating systems and applications, is up to date.

- Install antivirus software as it becomes available.

- Either sensitive data should be prohibited from storage on the mobile device or it should be encrypted.

- IT staff should also have the ability to remotely access devices, wipe the device of all data, and then disable the device in the event of loss or theft.

- The organization may prohibit all installation of third-party applications,

- Implement white listing to prohibit installation of all unapproved applications, or implement a secure sandbox that isolates the organization's data and applications from all other data and applications on the mobile device. Any application that is on an approved list should be accompanied by a digital signature and a public-key certificate from an approved authority.

- The organization can implement and enforce restrictions on what devices can synchronize and on the use of cloud-based storage.
- To deal with the threat of untrusted content, security responses can include training of personnel on the risks inherent in untrusted content and disabling camera use on corporate mobile devices.
- To counter the threat of malicious use of location services, the security policy can dictate that such service is disabled on all mobile devices.

Traffic Security: Traffic security is based on the usual mechanisms for encryption and authentication. All traffic should be encrypted and travel by secure means, such as SSL or IPv6. Virtual private networks (VPNs) can be configured so that all traffic between the mobile device and the organization's network is via a VPN.

A strong authentication protocol should be used to limit the access from the device to the resources of the organization. Often, a mobile device has a single device-specific authenticator, because it is assumed that the device has only one User. A preferable strategy is to have a two-layer authentication mechanism, which involves authenticating the device and then authenticating the user of the device.

Barrier Security: The organization should have security mechanisms to protect the network from unauthorized access. The security strategy can also include firewall policies specific to mobile device traffic. Firewall policies can limit the scope of data and application access for all mobile devices. Similarly, intrusion detection and intrusion prevention systems can be configured to have tighter rules for mobile device traffic.

4.5   Mobile Device Security Process

Mobile devices face a number of threats that pose a significant risk to corporate data. Like desktops, smart phones and tablet PCs are susceptible to digital attacks, but they are also highly vulnerable to physical attacks given their portability. Here is an overview of the various mobile device security threats and the risks they pose to corporate assets.

Eavesdropping – Carrier-based wireless networks have good link-level security but lack end-to-end upper-layer security. Data sent from the client to an enterprise server is often unencrypted, allowing intruders to eavesdrop on users' sensitive communications.

Unauthorized access – Users often store login credentials for applications on their mobile devices, making access to corporate resources only a click or tap away. In this manner unauthorized users can easily access corporate email accounts and applications, social media networks and more.

Theft and loss – Couple mobile devices' small form factor with PC-grade processing power and storage, and you have a high risk for data loss. Users store a significant amount of sensitive corporate data–such as business email, customer databases, corporate presentations and business plans–on their mobile devices. It only takes one hurried user to leave their iPhone in a taxicab for a significant data loss incident to occur.

Unlicensed and unmanaged applications – Unlicensed applications can cost your company in legal costs. But whether or not applications are licensed, they must be updated regularly to fix vulnerabilities that could be exploited to gain unauthorized access or steal data. Without visibility into end users' mobile devices, there is no guarantee that they are being updated.

4.5.1 Theft protection

Along with malware protection, theft protection is one of the most important security features for an Android security product. It allows the user to run commands remotely on a lost or stolen phone. These principally concern protection of the user's private data and the recovery of the device. The commands are sent via web interface or text message.

4.5.2 Lock

The lock function prevents unauthorized access by locking the device. There should be no means of bypassing the lock screen. Some manufacturers use the same PIN for the lock screen as for the text- message commands. This can be a problem, if text messages are displayed on the lock screen (which is the default Android setting). A thief could thus easily see the PIN and so unlock the device. We feel that manufacturers who use such a mechanism should urgently find and offer an alternative.

Another problem noted with some products is the ability to open the Android notification bar. This enables a thief not only to activate aero plane mode, thus rendering commands from the product's web interface useless, but also to switch to the guest account. Even if functions such as making phone calls are disabled in this

mode, it is still possible to use the phone for some other functions. Google's own recommendation to allow only trusted people to use the phone in guest mode makes this point clear. In our evaluation, we also considered the opportunity to use a customizable lock screen. This could be employed e.g. to display the user's contact details when the device is locked, which might be used by an honest finder to contact the owner and arrange to return the phone. We also feel it is important that it should always be possible to use the phone to make emergency calls (e.g. fire brigade, police, and ambulance). Just a few products provide the option to take pictures with the front-facing camera when the phone is locked. This makes it possible to photograph and thus identify a thief. In our tests, we discovered that not all features of all products work in a satisfactory fashion. In some cases, we were able to unlock the device by reading the text message with the PIN on the lock screen. Other products allowed the notification bar to be opened, thus giving access to the guest account. In some apps, it was not possible to make an emergency call. On the other hand, we have to praise all manufacturers for their respective products' behavior when the device is restarted.

4.5.3 Locate

A Locate function allows the position of the phone to be determined when it has been lost or stolen. This could be valuable if the owner has simply forgotten where he/she left the phone. Some manufacturers of mobile security software warn explicitly against trying to track down a thief oneself, and recommend contacting the police instead. Differences between the locate functions of different products are usually quite small. All allow a single location to be determined.

Android version and its text-message app Hangouts. Browser history and bookmarks were not removed by some products. We have stressed the importance of deleting the Google Account details, so that access to mails, calendar, call history and contacts is prevented. It is also important to remove the user's files.

4.5.4 SIM Protection

A SIM Protection feature saves metadata to the user's SIM card. This makes it possible to recognize if a thief has swapped the SIM card, in order to use the phone to make calls. Most products will lock the device as soon as the SIM-card change is registered. The user does not need to send a command; the function works automatically. Some security apps inform a trusted person, whose details were

entered during product setup, that the SIM card has been changed. This might help the owner to identify or contact the thief.

4.5.5 Malware protection

This component scans the mobile phone for malicious software, which it deletes or quarantines. For this function to work effectively, it has to be kept up-to-date. When travelling abroad, users need to be careful that automatic updates and cloud scans do not incur high roaming costs from the mobile service provider.

4.5.6 Windows products

The perfect mobile-security product does not yet exist. As with Windows products, we recommend drawing up a short list after reading about the advantages and disadvantages of each product in our review. A free trial version of each candidate product can then be installed and tested for a few days; this should make the decision easier. Especially with Android security products, new versions with improvements and new functions are constantly being released. By participating in this test, the manufacturers have shown their commitment to providing customers with quality security software. As this report shows, we have found some degree of malfunction in many of the tested products. The manufacturers of the affected products have taken these problems very seriously and are already working on solutions. As the core functions of all the products we tested reached a very good level, we are happy to present our "Approved Award" to all participating manufacturers. We have noticed a significant improvement in the overall standard of the products since last year's test.

4.5.7 Battery usage

Testing the battery usage of a device might appear at first glance to be very straightforward. If one goes into more detail, the difficulties become apparent. Particularly with mobile phones, the usage patterns of different users are very varied. Some use the multimedia functions extensively, others view a lot of documents, while some use only the telephone functions. We need to differentiate between power users, who take advantage of all of the possible functions in the device, and traditional users who merely make and receive phone calls.

4.6   Protection Against Android Malware

Methods of attacking mobile devices are getting more and more sophisticated. Fraudulent applications attempt to steal users' data or money. To reduce the risk of this happening, follow the advice given here. Only download apps from Google Play or reputable app makers own stores. Avoid third-party stores and side loading. Another indication of untrustworthy apps is irrelevant access rights. For example, an app that measures the speed at which you are travelling has no need to access your phone book or call log. Of course, even if an app does this, it is not a clear- cut indication that it is malicious, but it makes sense to consider whether it is genuine and should be used. A look at the reviews in the app store is also a guide; avoid apps with bad or dubious reviews. If you Root your smart phone, you will have more functionality on the phone, but equally the opportunity for malicious apps to take control will also increase. Another point to consider is the warranty. It is not legally clear-cut whether the warranty is still valid if the phone is rooted. In many cases, the warranty will be considered null and void.

Android Security

Android Security is the range of security features built into the Android operating system, and thus preinstalled on every Android device. It includes theft-protection functionality, and the ability to verify apps online.

Locate

This function locates a lost or stolen device and displays its position using Google Maps. This is done automatically when the user logs on to the web interface. Only a single location is provided each time, continuous tracking is not possible.

Installation

Installation is not necessary, as the features are already built into the operating system. On our test device, the functions were activated by default. Users can see the status of the Android security features and enable/disable them by going to Google Settings\Security.

Theft Protection

Android includes theft protection with the most important functions. They are controlled by web interface: This requires a Google Account, which is of course a requirement for many Android features. Text-message commands are not provided.

Ring

This function plays a melody at full volume for 5 minutes. It can be used to locate a mislaid mobile phone at home, for instance. The command does not lock the device. The on/off button on the phone can be used to stop the phone ringing.

Lock

The Lock function uses the Android lock screen to lock the phone. This makes it inaccessible to unauthorized persons. The unlock password for the lock screen can be set in the web interface. We liked the fact that it is possible to define a message in the web interface, which will be displayed on the lock screen. This would allow the owner to provide an honest finder with contact details. Additionally, a phone number can be entered.

Wipe

This function deletes the user's personal data from the smart phone. When the command has been received, the phone is reset to factory settings.

Verify Apps

Android includes several settings to prevent malicious attacks. Prior to installing an application downloaded outside of the Play store, Google's Safe Browsing feature will scan the app and warn of any potential threats. Android Security allows the user to check installed apps regularly, whereby it will warn of any potentially malicious ones found.

Updates

We could not find any information relating to updates for malware signatures.

Help

No significant help functions are provided.

De-Installation

The Android Device Manager, which includes Android Security, cannot be uninstalled, only disabled.

License

The protection features are already installed with the operating system and can be used free of charge without restriction.

Summary

Android Security provides the user with basic theft-protection and malware-

protection functionality. In our test, these features impressed us as stable and well thought-out, and they represent a usable, simple alternative to external security products.

Ahn Lab V3 Mobile Security

Ahn Lab V3 Mobile Security is a comprehensive security product. Even the Free version provides the most important functions. The Premium version includes additional functions such as app lock and URL scan.

URL Scan

The URL scan protects the user while surfing the Internet. It has to be activated before it can be used. In a well-designed dialog box, the user is taken through the configuration. AhnLab has to be made the default program for surfing the Internet (although it is not itself a browser). Any browser of the user's choice can be used.

Privacy Advisor

Privacy Advisor alerts the user to apps that demand specific permissions. The apps are shown in pre-defined categories, such as "Access to Contacts". All apps with this permission will be listed.

Installation

We installed Ahn Lab V3 Mobile Security from the Google Play Store. Once the license agreement has been accepted, the scope of malware scans can be configured. As well as installed apps, the user can also scan all files. Detection of PUAs (potentially unwanted programs) can additionally be enabled at this stage. After this, updates can be set to run only via Wi-Fi, or additionally via a mobile data connection. A scan is then started, and the installation is complete.

Malware Scan

This function allows the device to be checked for malicious software. In addition to real- time protection, on-demand scans can be run. The malware signatures are updated before each scan. Tapping an app in the list will display all its current permissions.

Privacy Cleaner

Privacy Cleaner deletes files that potentially contain personal data. Browser logs and the cache can be removed by the feature.

Application Lock

Application Lock allows installed apps to be protected with a PIN, which has to be

entered before an app can be run. This might be useful e.g. if a child is going to use the phone.

Lock Device

Text-message command: #lock <PIN> This function locks the device by sending a text message with the PIN. AhnLab have overlooked an important point here. In the Android version used for the test, text messages are shown on the lock screen by default, meaning that a thief would be able to see the PIN and so unlock the phone. This would not be a major problem if it were possible to use a different PIN or lock pattern for the lock screen.

Hidden Gallery

The Hidden Gallery can be used to hide specific photos and videos on the device. These are moved into a hidden folder, and can then only be viewed if the PIN is entered.

Call Block

This component can reject calls from unwanted callers. This involves creating a blacklist of unwanted numbers. We liked the fact that it is possible to block numbers according to a pattern (e.g. a particular dialing code).

Track Location

Text-message command: #locates <PIN>. This command determines the smart phone's location. The sender's phone will receive in reply the device's current co-ordinates and a direct link to Google Maps. These two pieces of information are sent as two separate text messages.

Anti-Theft

A wizard is again provided to configure the feature. AhnLab needs to be registered as a device administrator. Next, a trusted phone number has to be entered, which will be used to contact the owner in the event that the SIM card is exchanged. In the final step, a personalized message can be entered, which will be displayed on the lock screen.

4.7   Encryption for mobile devices

Encrypting data at rest and in motion helps prevent data loss and successful eavesdropping attempts on mobile devices. Carrier networks have good encryption of the airlink, but the rest of the value chain between the client and enterprise server remains open unless explicitly managed. Contemporary tablet PCs and smartphones can secure Web and email with SSL/TLS, Wi-Fi with WPA2 and corporate data with mobile VPN clients. The primary challenge facing IT organizations is ensuring proper configuration and enforcement, as well as protecting credentials and configurations to prevent reuse on unauthorized devices.

Data at rest can be protected with self-protecting applications that store email messages, contacts and calendars inside encrypted containers. These containers separate business data from personal data, making it easier to wipe business data should the device become lost or stolen.

4.8   Authentication and authorization for mobile devices

Authentication and authorization controls help protect unauthorized access to mobile devices and the data on them. Ideally, Craig Mathias, principal with advisory firm Farpoint Group, says IT organizations should implement two-factor authentication on mobile devices, which requires users to prove their identity using something they know–like a password– and something they have–like a fingerprint. In addition to providing robust authentication and authorization, Mathias says two-factor authentication can also be used to drive a good encryption implementation. Unfortunately, two-factor authentication technology is not yet widely available in mobile devices. Until then, IT organizations should require users to use native device-level authentication (PIN, password).

4.9   Remote wipe for mobile device security

Authentication and encryption help prevent data loss in the case of mobile device theft or loss, but physical security can be further fortified with remote wipe and "phone home" capabilities. Native remote lock, find and wipe capabilities can be used to either recover a lost mobile device or permanently delete the data on them. Be careful, however, if you choose to use these functionalities. Experts recommend defining policies for these technologies and asking users to sign a consent form. Remote wipe could put the user's personal data at risk and "phone home" or "find

me" services can raise privacy concerns.

4.10 Mobile device management

When experts and IT professionals talk about securing mobile devices, the conversation often turns to mobile device management systems, and for good reason. Most mobile device management products include basic security functionality. They also enable centralized visibility, policy configuration, application provisioning and compliance reporting for any mobile device that accesses network resources – regardless of who owns it. These functions are key security controls and their centralized management makes them practical. For example, most mobile device management systems feature Exchange ActiveSync policies, which allow you to deny corporate mail access by unencrypted devices. Others offer more extensive and transparent control to enable IT organizations to enroll and secure iPads, for example, without relying on iTunes or Exchange.

4.11 Let us Sum up

Today's mobile devices are a mixed bag when it comes to security. On the one hand, these platforms have been designed from the ground up to be more secure— they raise the bar by leveraging techniques such as application isolation, provenance, encryption, and permission-based access control. On the other hand, these devices were designed for consumers, and as such, they have traded off their security to ensure usability to varying degrees. These tradeoffs have contributed to the massive popularity of these platforms, but they also increase the risk of using these devices in the enterprise.

While mobile devices promise to greatly improve productivity, they also introduce a number of new risks that must be managed by enterprises. We hope that by explaining the security models that undergird each platform, and the environment these devices participate in, we have discussed, you will be able to more effectively derive value from these devices and also more effectively manage this risks they introduce.

4.12 Suggested Readings

1. https://www.av-comparatives.org/wp- ontent/uploads/2015/09/avc_mob_2015_en.pdf

2. https://www.sophos.com/en-us/security-news-trends/security- trends/malware-goes-mobile.aspx

3. Babu B., S., & Venkataram, P. Wireless and Mobile Security 1st Edition. Mcgraw Hill Education.

4.13 Assignments

1. Discuss about mobile device security.

2. What are the Mobile device security threats?

3. Explain about the Mobile device policies.

4. How to do the Mobile device management

5. Discuss about android malware.

6. What are the steps for SIM protection?

7. Write about the malware protection in mobile.

8. Discuss about Security Threats in mobile security.

9. What are the theft protections for mobile phones?