ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

DCS-05 NETWORK CYBER SECURITY

BLOCK

1 NETWORK SECURITY

EXPERT COMMITTEE

DIPLOMA IN CYBER SECURITY

Course Writers

Chandrakant Mallick
Odisha State Open University, Sambalpur, Odisha
Bijay Kumar Paikaray
Centurion University of Technology and Management, Odisha

UNIT-1 NETWORK SECURITY MODEL AND NETWORK SECURITY THREATS

UNIT STRUCTURE

1.0 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.

1.1 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 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.

1.3 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.

1.4 First Layer of Network Security Model: The Physical Layer

1.4.1 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.

1.4.2 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.

1.5 Second Layer of Network Security Model: The VLAN Layer

1.5.1 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.

1.5.2 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.

1.6 Third Layer of Network Security Model: The ACL Layer

1.6.1 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.

1.6.2 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.

1.7 Fourth Layer of Network Security Model: The Software Layer

1.7.1 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.

1.7.2 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.

1.8 Fifth Layer of Network Security Model: The User Layer

1.8.1 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.

1.8.2 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.

1.9 Sixth Layer of Network Security Model: The Administrative Layer

1.9.1 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.

1.9.2 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.

1.10 Seventh Layer of Network Security Model: The IT Department Layer

1.10.1 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.

1.10.2 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.

1.11 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.

1.11.1 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.

1.11.1.1 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.

1.11.1.2 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?

1.12 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.

1.13 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.

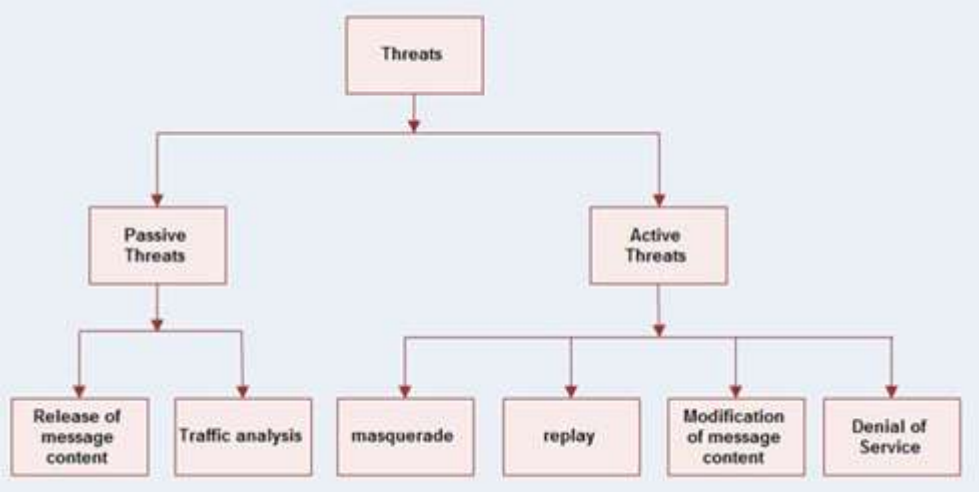


Fig: Types of Security Threats

(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.

1.14 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.

1.15 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.

1.16 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.

1.17 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.

1.18 Self-assessment Questions

1. Define a Network Security Model.
   ……
   ……
   ……
   ……
   ……
2. Why the Network Security Model is divided in to seven Layers?
   ……
   ……
   ……
   ……
   ……
3. Write the functions of Physical Layer in Network Security Model.
   ……
   ……
   ……
   ……
   ……
   ……
4. Write the functions of ACL Layer in Network Security Model.
   ……
   ……
   ……
   ……
   ……
   ……

5. Write the functions of User Layer in the Network Security Model.

……
……
……
……
……
……

6. How can you mitigate security threats?

……
……
……
……
……
……

1.19 Model Questions

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.

1.20 References & 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/network-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

UNIT-2 FIREWALLS

UNIT STRUCTURE

2.0 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.

2.1 Learning Objective

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 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.

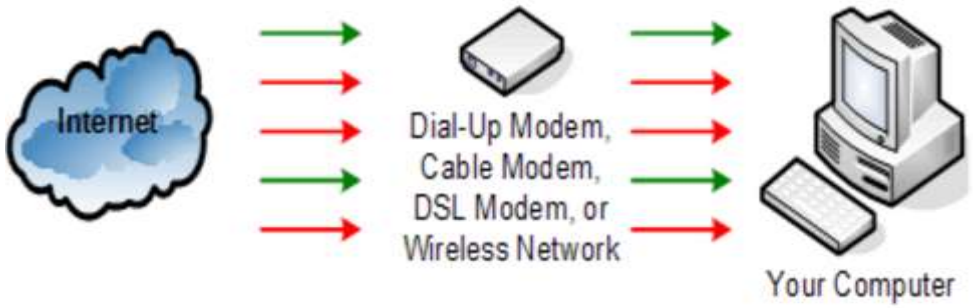


Fig: A firewall

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.

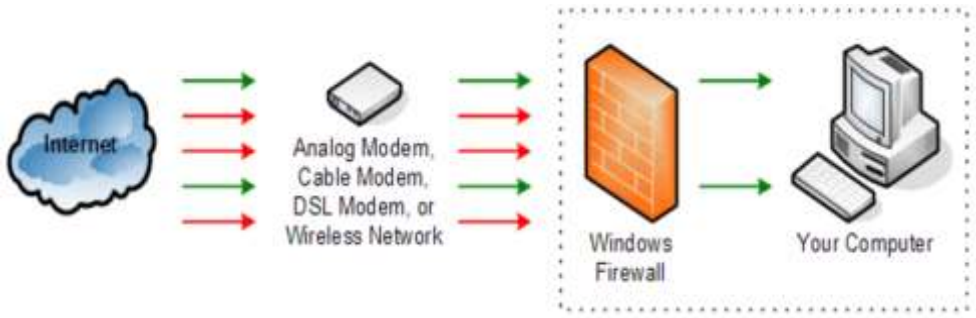


Fig: Firewall in an organization

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!

2.3 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.

2.4 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.

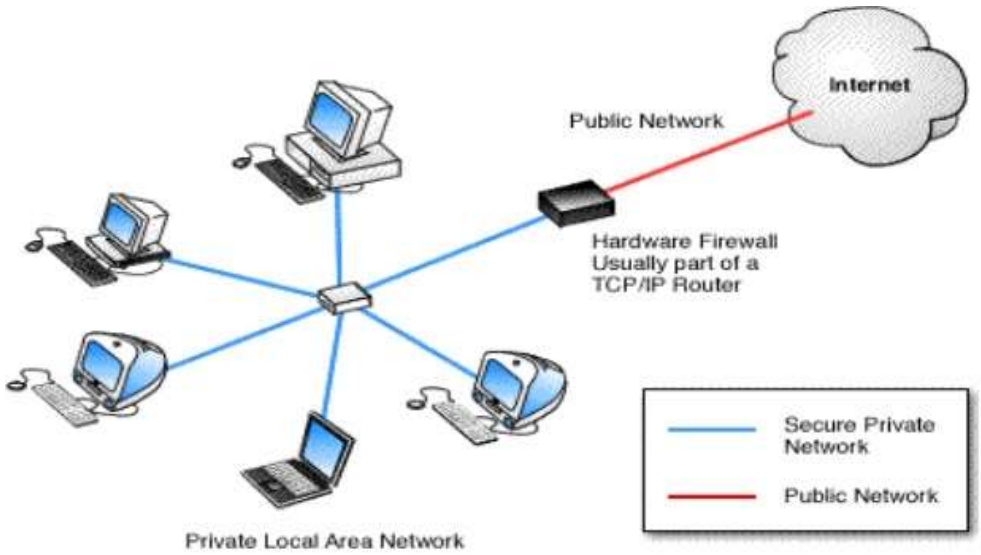


Fig: A software firewall

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.

2.5 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.

2.6 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.

2.7 Configuring Firewall in your Computer

2.7.1 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.

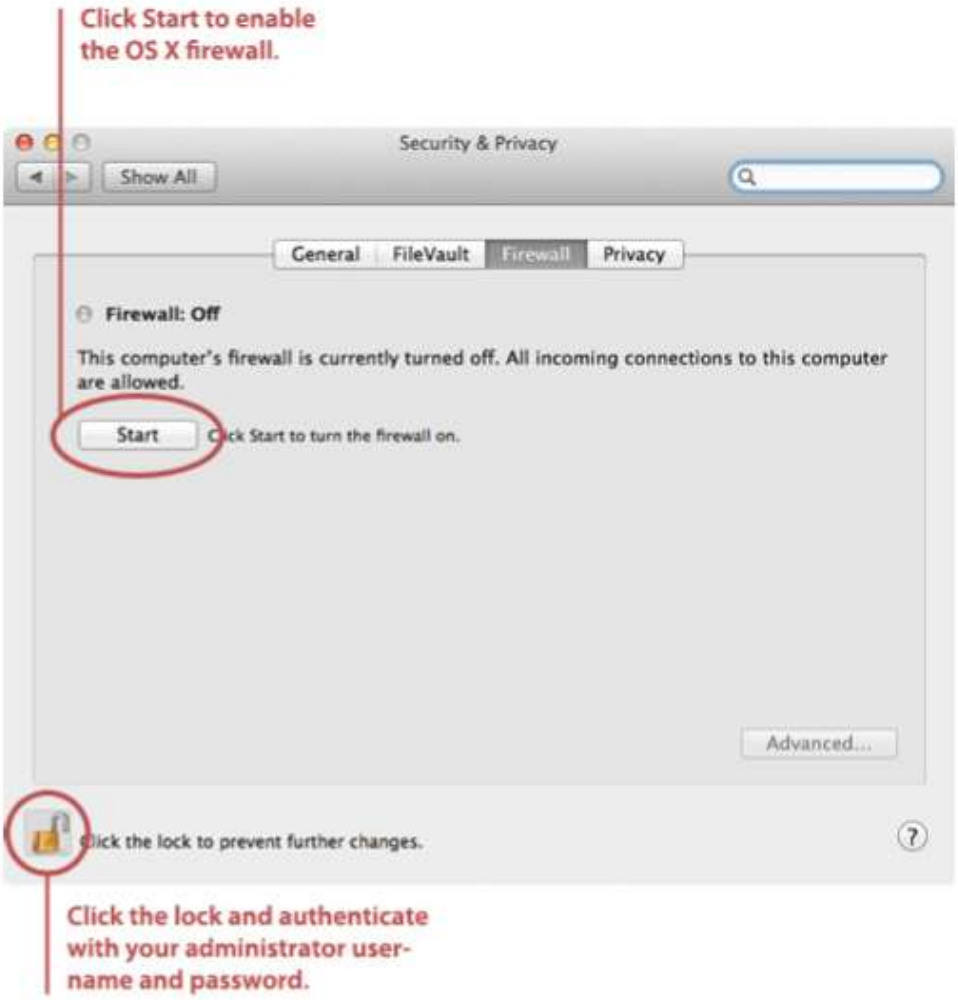
This all happens in a matter of seconds. Once your Mac has reassembled the packets, you'll see something, like an email message or web page.
A firewall can help prevent bad packets from entering your Mac. Hackers love to run automated applications that can scan thousands of computers (including your 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.

2.7.1.1 Turning on and Configuring the Mac OS X Firewall

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

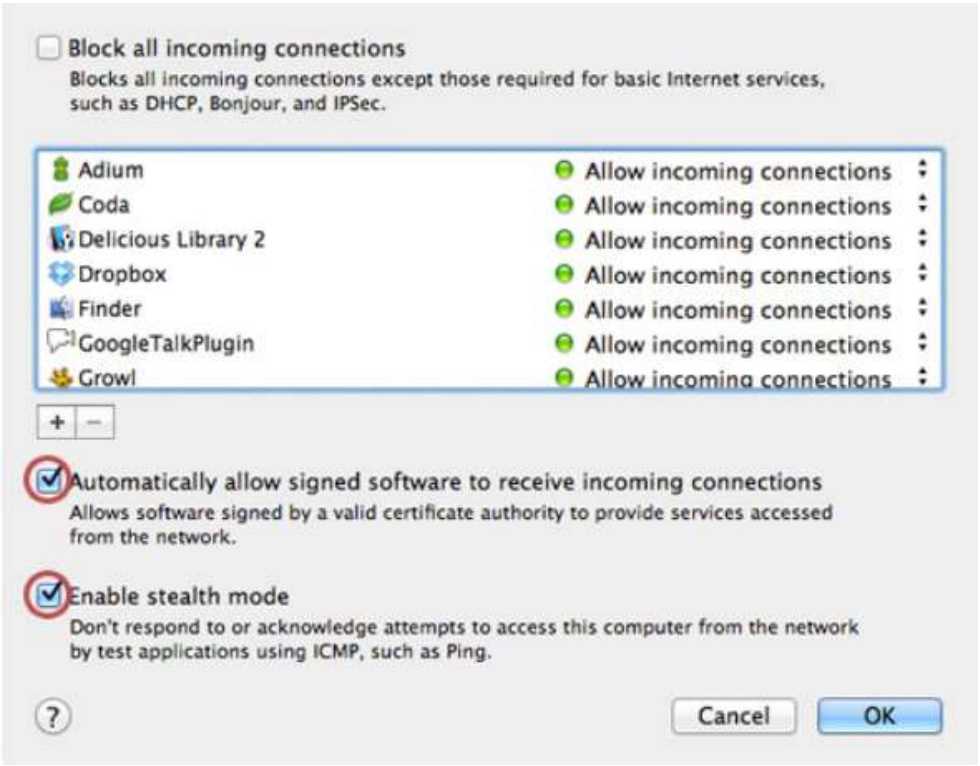
1. From the Apple menu, select System Preferences. The window shown below appears.

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!

2.7.2 Working with Windows Firewall in Windows 7

2.7.2.1 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:

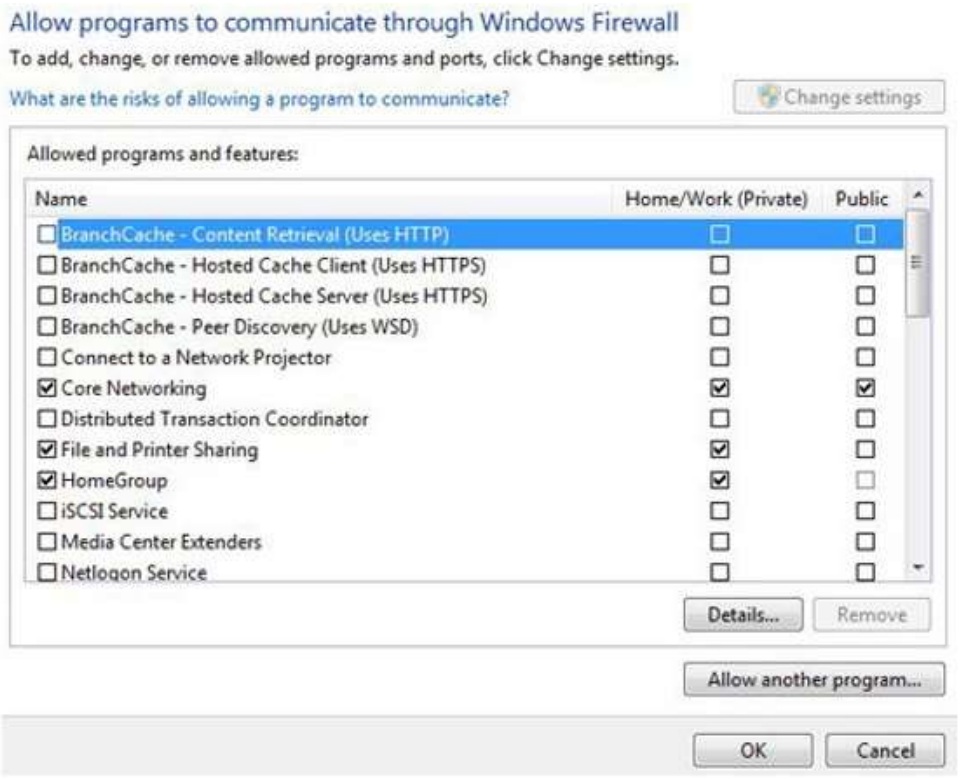
- Public
- Home/Work - private network
- Domain - used within a domain

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.

2.7.2.2 Configuring Windows Firewall

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

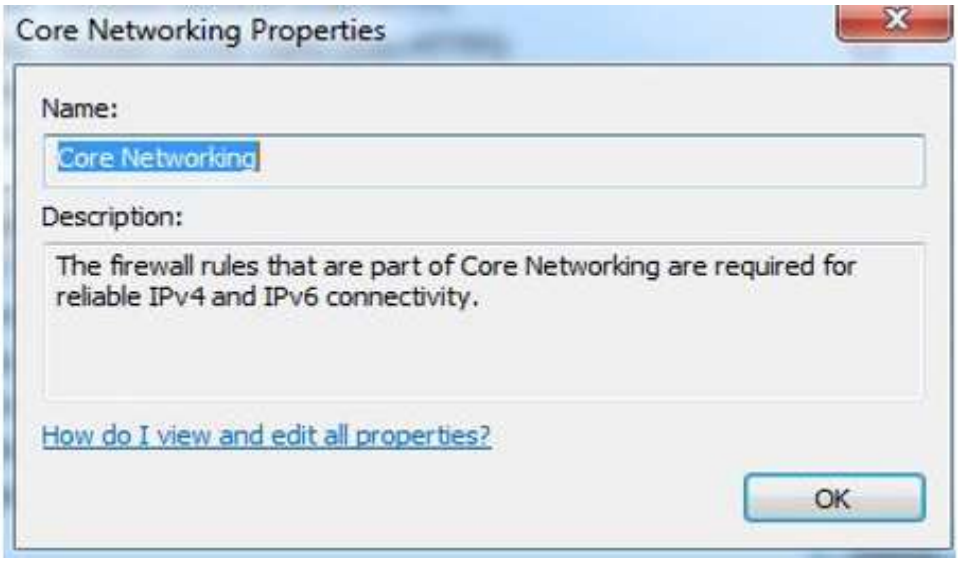
By default, Windows Firewall is enabled for both private (home or work) and public networks. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature trough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

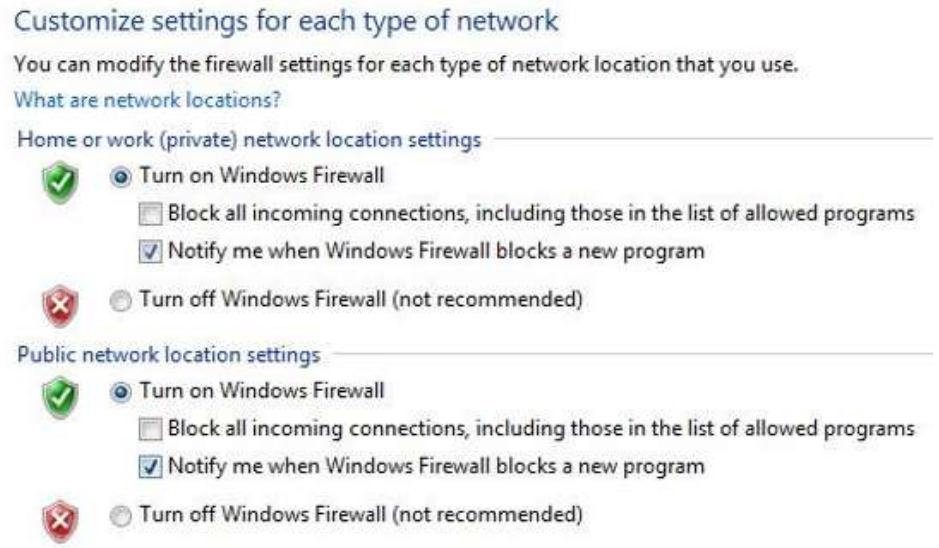
Add a Program

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.

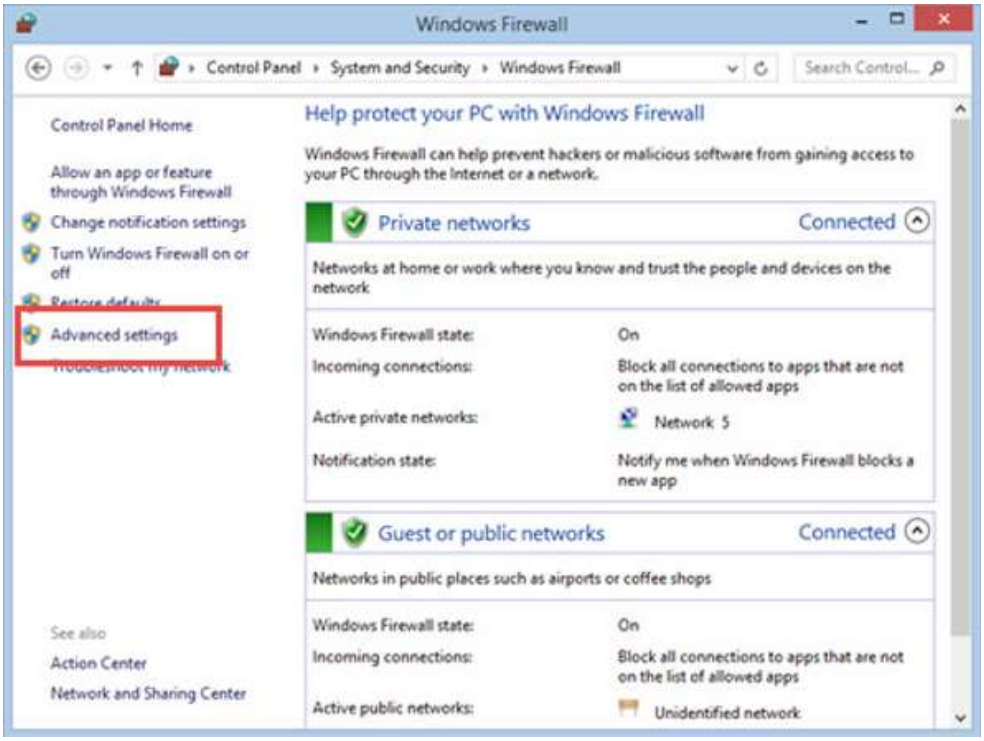
2.7.3 How to Start & Use the Windows Firewall with Advanced Security

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

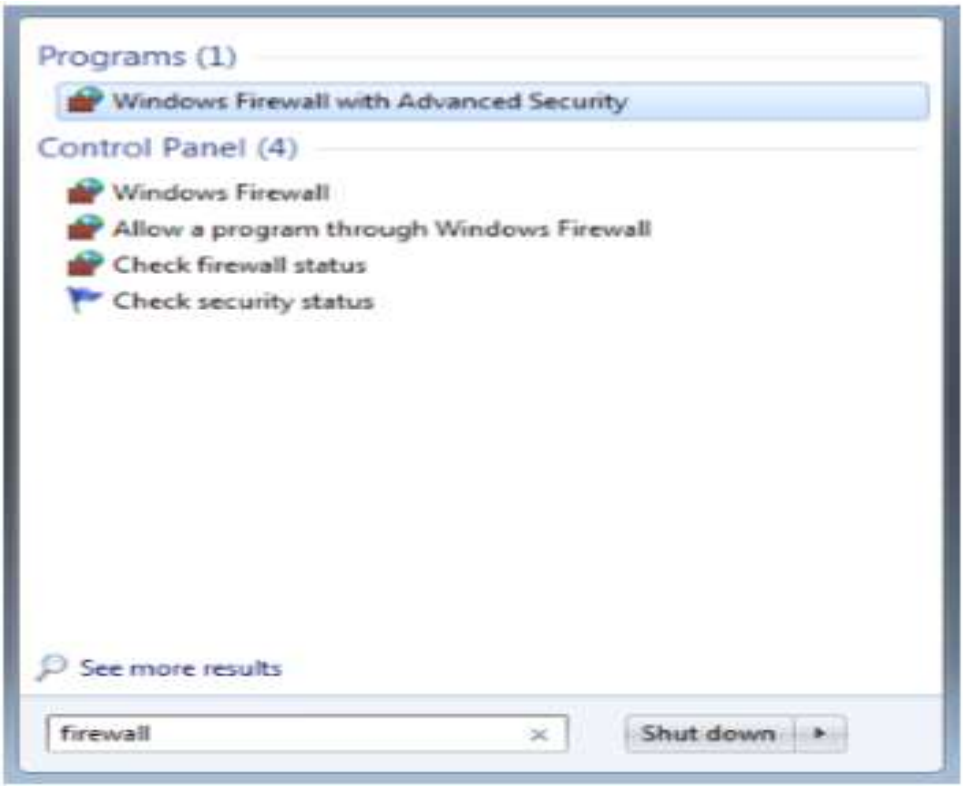
their properties, create new rules or disable existing ones. In this tutorial we will share how to open the Windows Firewall with Advanced Security, how to find your way around it and talk about the types of rules that are available and what kind of traffic they filter.

2.7.3.1 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.



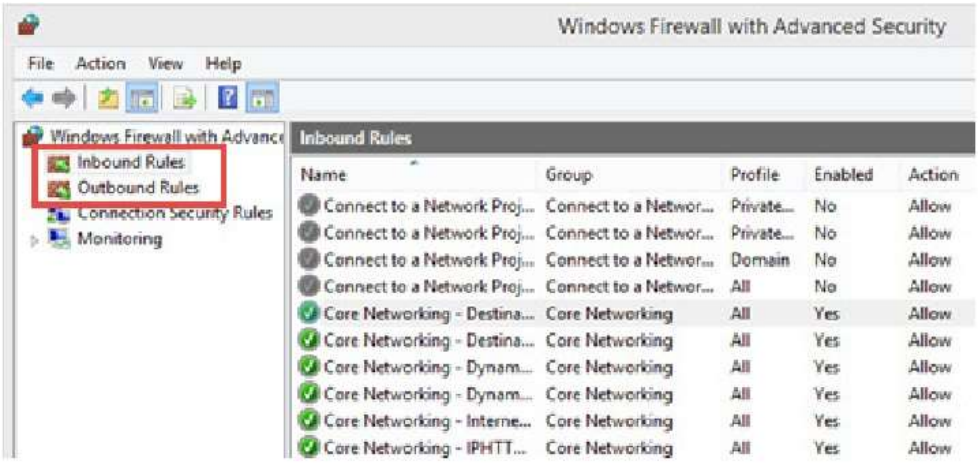
In Windows 8.1, Windows Firewall with Advanced Security is not returned in search results and you need to use the first method shared above for opening it.

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.

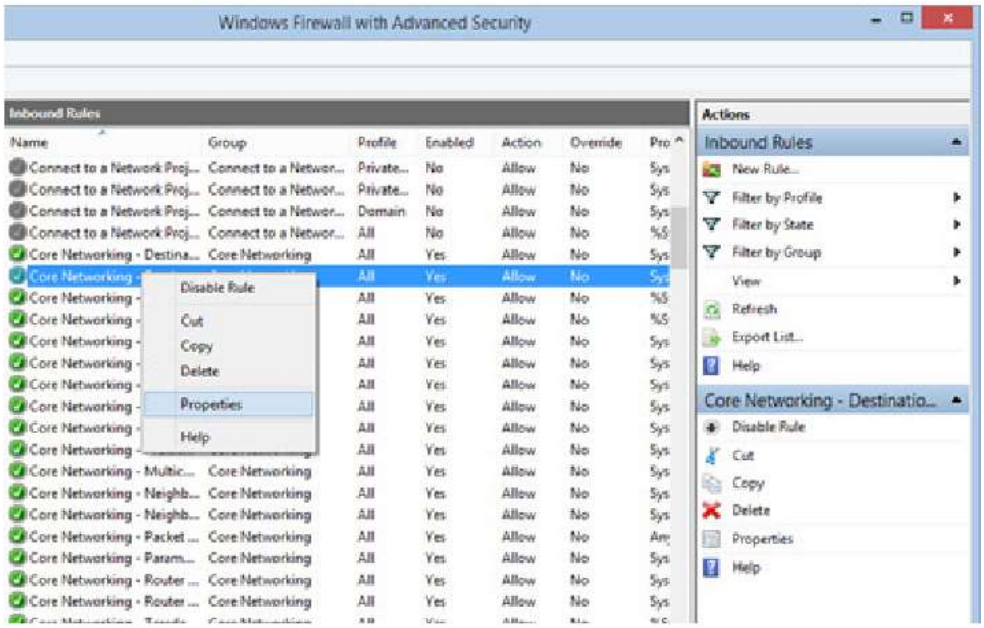
2.7.3.2 What Are The Inbound & Outbound Rules?

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.

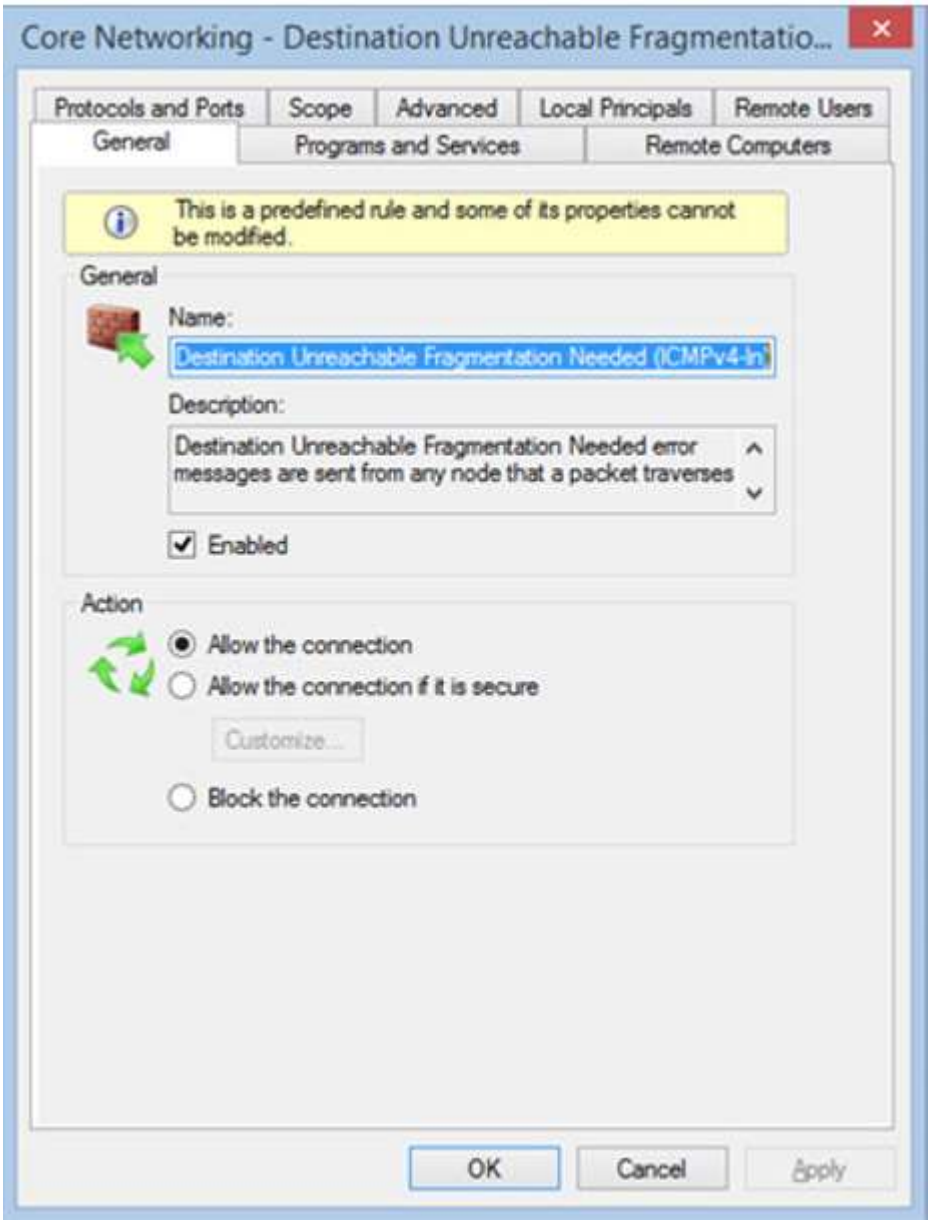
These rules can be configured so that they are specific to: computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to. In the Windows Firewall with Advanced Security, 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.



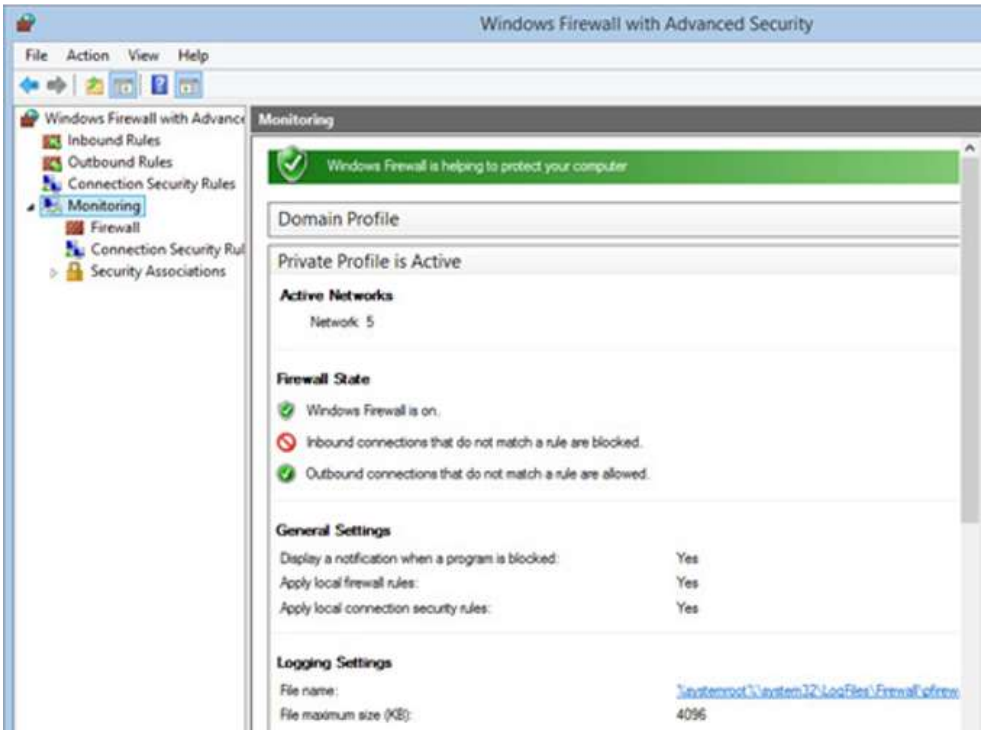
2.7.3.3 What are the Connection Security Rules?

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.

2.7.3.4 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.

2.8 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.

2.9 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.

2.10 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.

2.11 Self-assessment Questions

1. What do you understand by firewalls? Name different types of it.
   .....
   .....
   .....
   .....
   .....
2. Differentiate between software based firewall and hardware based firewall.
   .....
   .....
   .....
   .....
   .....

2.12 Model Questions

1. How can you prevent your network from anonymous attack using firewall?
2. When and where to implement hardware based firewall?
3. Describe the steps to configure firewall in Windows-7.
4. How to turn on and configure the Mac OS X Firewall?

2.13 References and 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.

UNIT-3 INTRUSION DETECTION SYSTEM AND INTRUSION PREVENTION SYSTEM

UNIT STRUCTURE

3.0 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.

3.1 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 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

3.3 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.

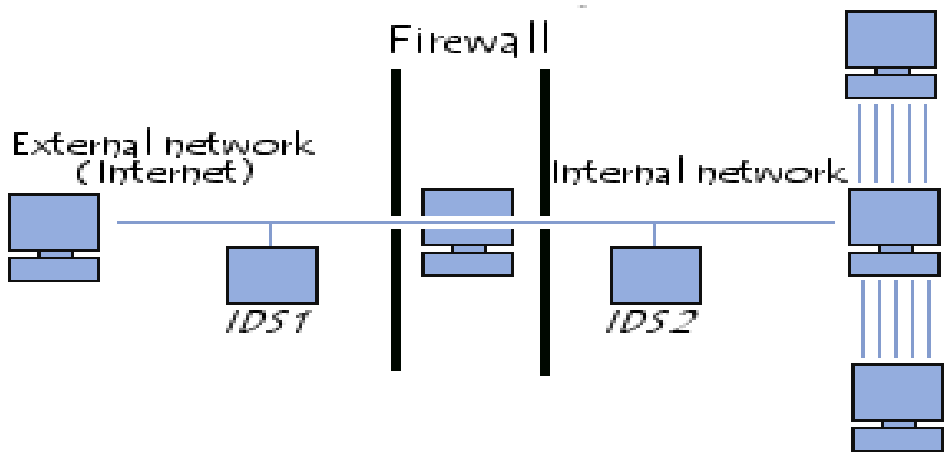


Fig: An Intrusion Detection System

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

3.4 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.

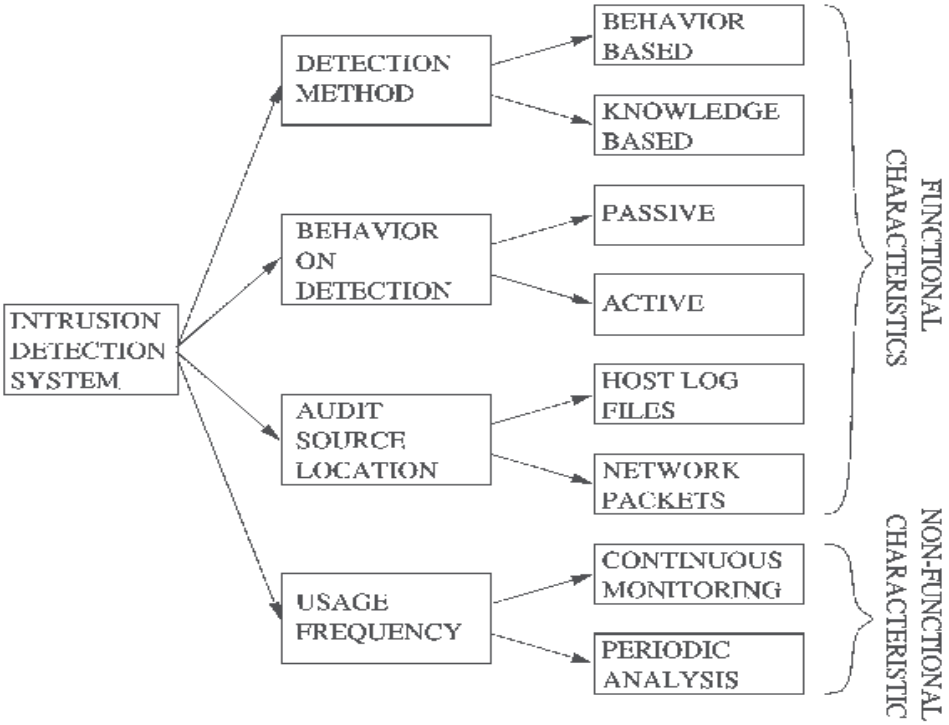


Fig: The characteristics of IDS

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).

3.5 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).

3.5.1 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

3.5.2 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.

3.5.3 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

3.5.4 IDS Based on Intrusion Detection Techniques:

3.5.4.1 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.

3.5.4.2 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.

3.6 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.

3.7 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.

3.8 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.

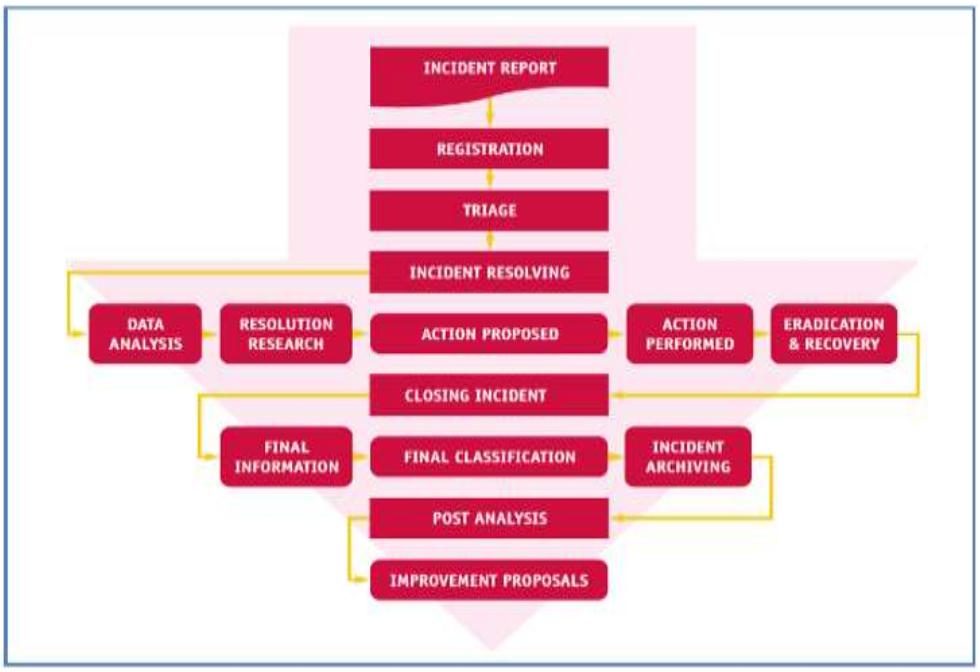
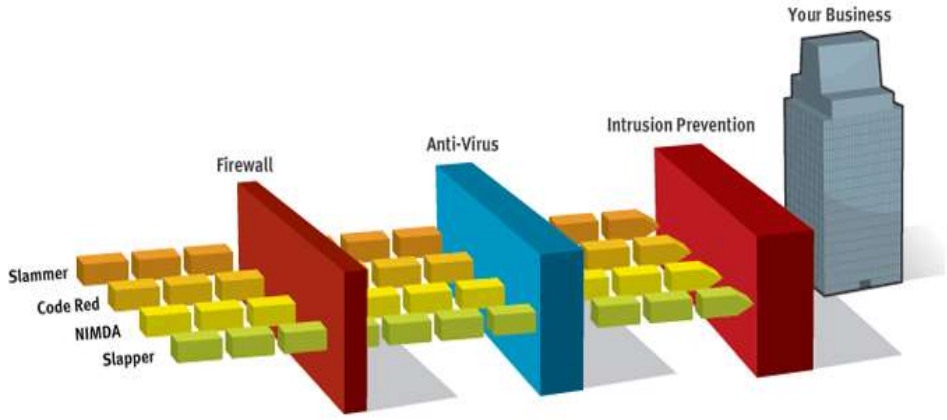


Fig: This diagram workflow of incident handling process

3.9 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

3.10 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.

3.11 Types of IPS

3.11.1 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.

3.11.1.1 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.

3.11.2 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."

3.11.3Network 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.

3.12 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.

3.13 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!

3.14 Self-assessment Questions

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?
   .....
   .....
   .....
   .....

3.15 Model Questions

1. What is a Honeypot?
2. What are the steps to install IDS in an organization?
3. Make diagram of IDS Components?
4. Give examples of Misuse & Anomaly Detection IDS?
5. What is DMZ?

3.16 References & 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.

UNIT-4 PUBLIC KEY INFRASTRUCTURE(PKI)

UNIT STRUCTURE

4.0 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.

4.1 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 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.

4.3 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.

4.4 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.

4.5 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."

4.6 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.

4.7 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.

4.7.1 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.

4.7.2 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.

4.7.3 Hierarchical Trust Model

4.7.3.1 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.

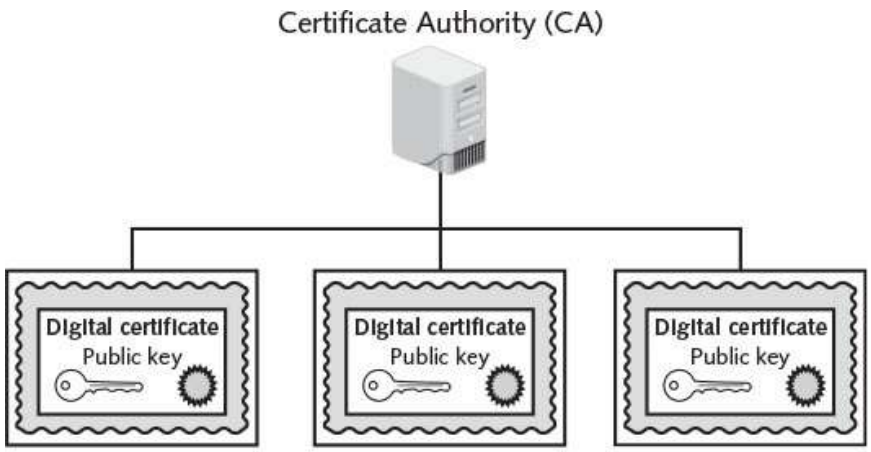


Fig: Hierarchical Trust Model

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?

4.7.4 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.

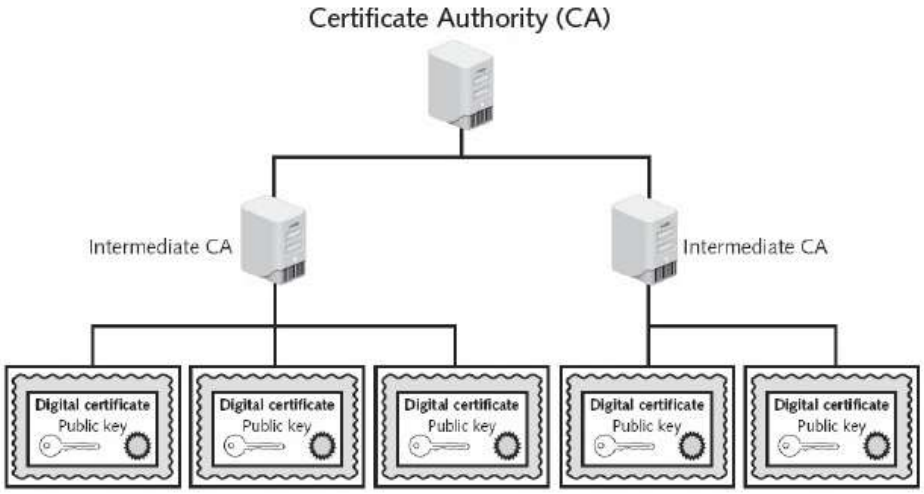


Fig: Distributed Trust Model

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.

4.7.5 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 s. 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.

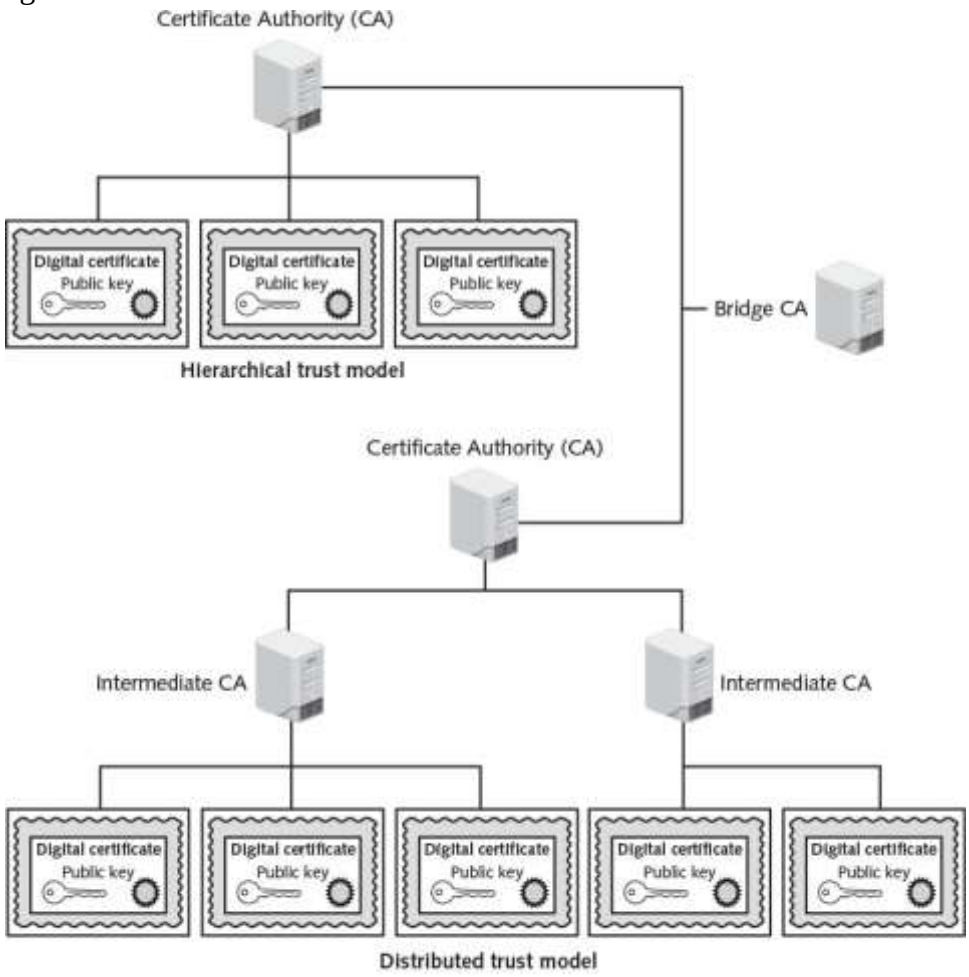


Fig: Distributed trust Model

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.

4.8 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.

4.8.1 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.

4.8.2 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.

4.8.3 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.

4.9 Key Management

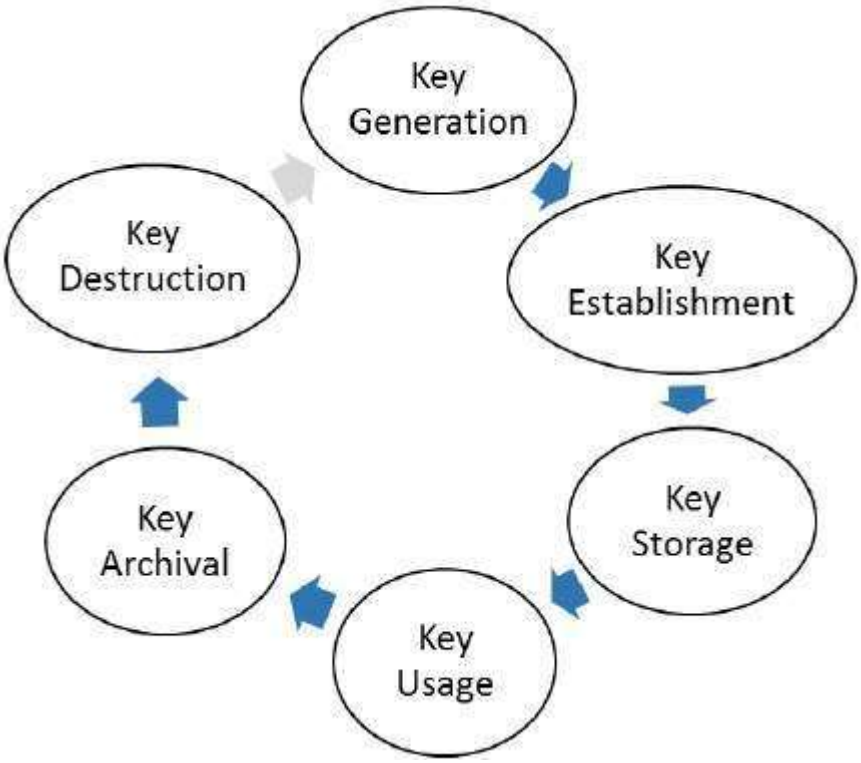
It goes without saying that the security of any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the

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.

4.9.1 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.

4.9.2 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.

4.9.3 Key-Handling Procedures

Certain procedures can help ensure that keys are properly handled. These procedures include:

4.9.3.1 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.

4.9.3.2 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.

4.9.3.3 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.

4.9.3.4 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.

4.9.3.5 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.

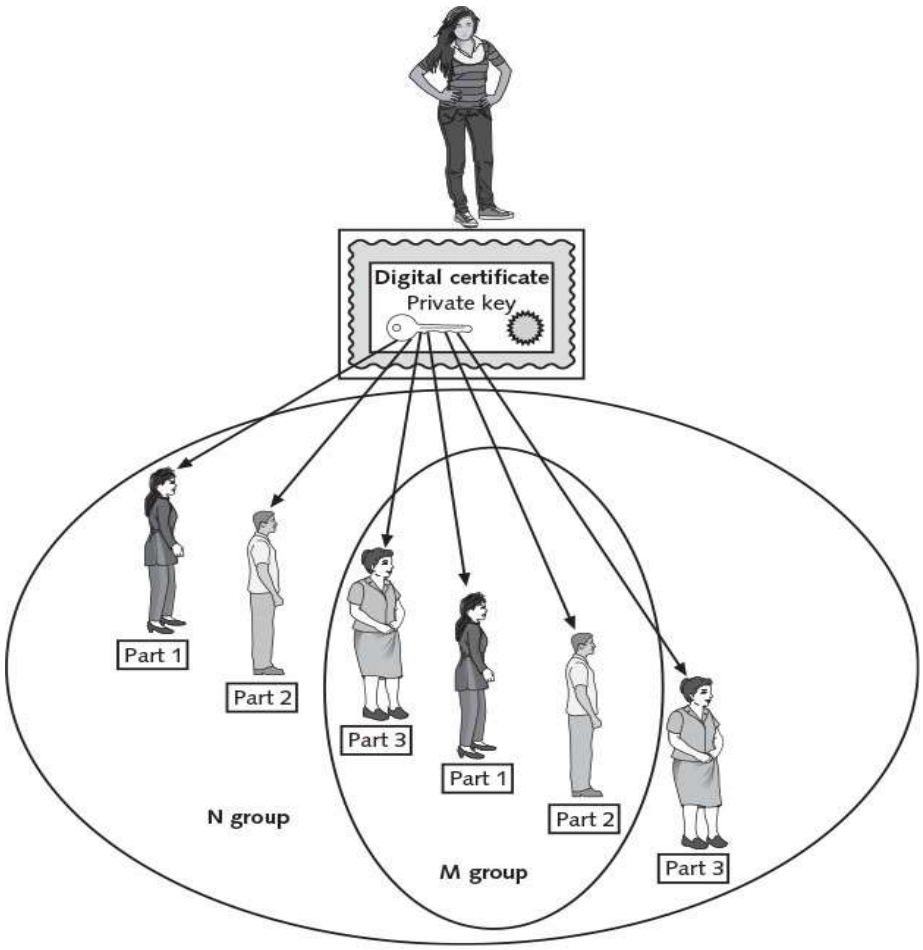


Fig: M-of-N Control

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.

4.10 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.

4.10.1 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.

4.10.2 Challenges

Several challenges IT organizations face when trying to control and manage their encryption keys are:

1. Complex Management: Managing a plethora of encryption keys in the millions.
2. Security Issues: Vulnerability of keys from outside hackers/malicious insiders.
3. Data Availability: Ensuring data accessibility for authorized users.
4. Scalability: Supporting multiple databases, applications and standards.
5. Governance: Defining policy driven, access, control and protection for data.

4.10.3 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.

4.11 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.

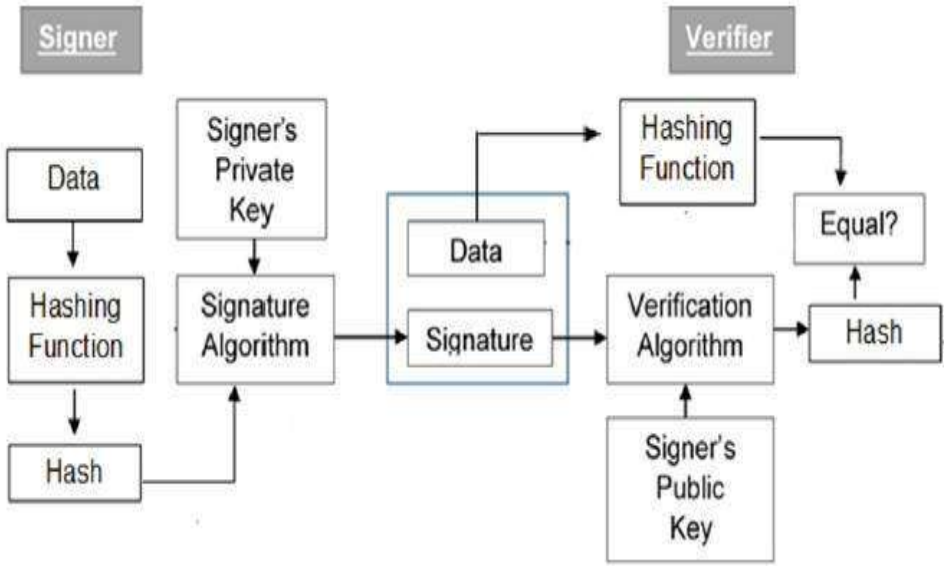
Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

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.

4.12 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.

4.13 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.

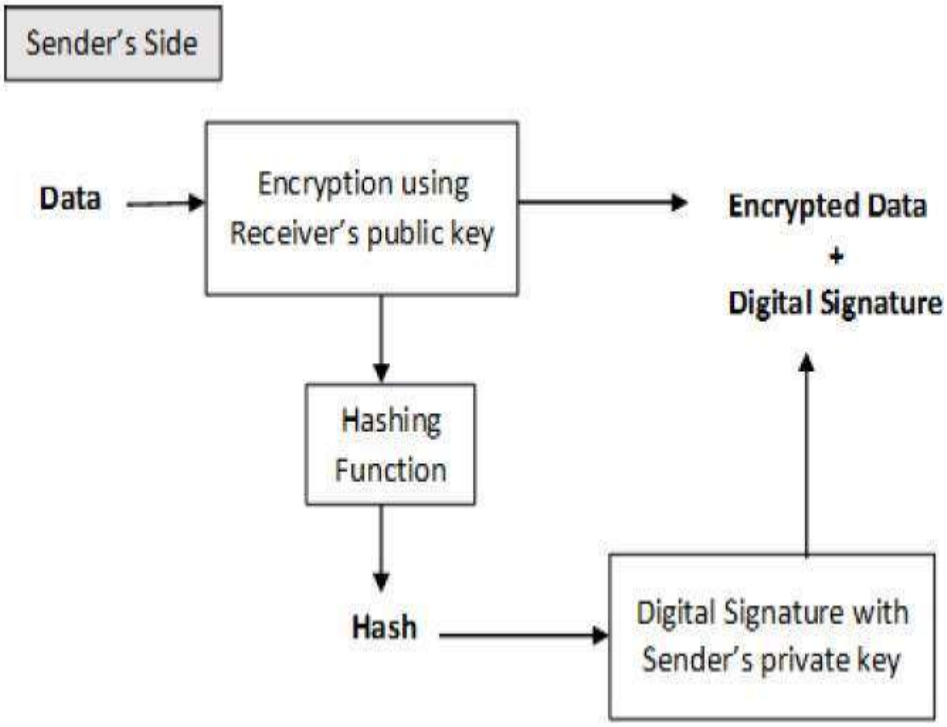
4.14 Encryption with Digital Signature

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 −



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.

4.15 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.

4.15. Self-assessment Questions

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?
   ……
   ……
   ……
   ……
   ……

4.16 Model Questions

1. What are the two specific requirements of key management for public key cryptography?
2. Explain the process of digital signature
3. Write a short note on Key Management.
4. Discuss how Digital Signature provides non-repudiation of message authentication and data integrity

4.17 References & 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_infrastructure.htm

ANSWER TO SELF-ASSESSMENT QUESTIONS (UNIT-1)

1. Define a Network Security Model.

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.

2. Why the Network Security Model is divided in to seven Layers?

The main purpose of dividing the Network Security Model in to seven layers is:

- To divide the complexity of design into small tasks in order to reduce the design complexity.
- The benefits of the layered models are modularity and clear interfaces, i.e. open architecture and comparability between the different providers' components.

3. Write the functions of Physical Layer in Network Security Model.

The function of physical layer is to provide 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 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.

4. Write the functions of ACL Layer in Network Security Model.

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. The key to creating strong ACLs is to focus on both inbound (ingress) ACLs as well as outbound (egress) ACLs

5. Write the functions of User Layer in the Network Security Model.

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.

6. How can you mitigate security threats?

Since the attack is directed at the software layer, this is the layer that has been compromised. We will need to go through the following activities to mitigate the attack.

a) Initial Mitigation

- Remove the infected host form the network
- Determining what malware is running on the system by running root kit detectors as well as checking anti-virus software.
- Also look if the attacker may have infected any other hosts at the same time.
- Identify the specific VLAN the host resided on.
- Mitigate the threats from the hosts infected.
- 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.

b) Long-Term Mitigation

- Push out the update in order to mitigate this type of attack from happening again.
- Make sure all machines are updated with the most current patches.
- Look 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.
- Look at the VLAN layer to see if something should be changed in the VLANs which can prevent a network wide outbreak.

ANSWER TO SELF-ASSESSMENT QUESTIONS (UNIT-2)

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

Types of Firewall

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

c. **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.

d. **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.

e. **Proxies:** 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". Firewalls often have such functionality to hide the true address of hosted protected. Hiding the addresses of protected devices has become an increasingly important defence against network reconnaissance.

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

Hardware Firewalls

A hardware firewall sits between the local network of computers and the Internet. The firewall will inspect all the data that comes in from the Internet, passing along the safe data packets while blocking the potentially dangerous packets. In order to properly protect a network without hindering performance, hardware firewalls require expert setup, and so may not be a feasible solution for companies without a dedicated IT department. For businesses with many computers, however, being able to control network security from one single device simplifies the job.

Software Firewalls

Software firewalls are installed on individual computers on a network. Unlike hardware firewalls, software firewalls can easily distinguish between programs on a computer. This lets them allow data to one program while blocking another. Software firewalls can also filter outgoing data, as well as remote responses to outgoing requests. The major downside to software firewalls for a business is their upkeep: they require installation, updating and administration on each individual computer.

ANSWER TO SELF-ASSESSMENT QUESTIONS (UNIT-3)

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

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.

It 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).

Types of Intrusion-Detection systems

Network based Intrusion Detection System (NIDS): - identifies intrusions by examining network traffic and monitors multiple hosts. NIDS gain access to network traffic by connecting to a hub, network

switch configured for port mirroring, or network tap. An example of a NIDS is Snort.

Host-based Intrusion Detection System (HIDS): - consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/ACL databases) and other host activities and state.

Hybrid Intrusion Detection System: - combines one or more approaches. Host agent data is combined with network information to form a comprehensive view of the network. An example of a Hybrid IDS is Prelude.

2. Differentiate between Network based IDS and host based IDS.

Host Based IDS	Network Based IDS
▸ It has narrow in scope as it watches only **specific** host activities)	▸ Broad in scope as it watches **all** network activities.
▸ Better for detecting attacks from the **inside**	▸ Better for detecting attacks from the **outside**
▸ **More expensive** to implement	▸ **Less expensive** to implement
▸ OS-specific	▸ OS-independent
▸ Detects local attacks before they hit the network	▸ Detects network attacks as payload is analyzed
▸ Verifies success or failure of attacks	▸ Detects unsuccessful attack attempts

3. How an IDS is different from an IPS?

IDS and IPS are originally developed for addressing requirements of lacking in most firewalls. IDS are basically used to detecting the threats or intrusions in network segment. But IPS is focused on identifying those threats or intrusions for blocking or dropping their activities.

The purpose of intrusion detection is to provide monitoring, auditing, forensics, and reporting of network malicious activities. Preventing network attacks

- Identifying the intruders
- Preserving logs in case the incident leads to criminal prosecution

The IPS is specified to provide protection for assets, resources, data, and networks.

- IPS stops the attack itself

- IPS changes the security environment

The best example of security gate in term of difference of IDS and IPS is, An IDS works like a patrol car within the border, monitoring activities and looking for abnormal situations. But an IPS operates like a security guard at the gate of allowing and denying access based on credentials and some predefined rule set, or policy. No matter how strong the security at the gate is, the patrols continue to operate in a system that provides its own checks.

ANSWER TO SELF-ASSESSMENT QUESTIONS (UNIT-4)

1. What is PKI? What are the components of PKI environment?

The PKI environment is made up of five components:

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

b) **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.

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

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

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

2. What are the key reasons to deploy Public Key Infrastructure in a company?

According to Microsoft, the key reasons to deploy Public Key Infrastructure are here:

- 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.

3. What is digital signature? Why digital signature is important?

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.

Importance of Digital Signature

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.