Computer system security notes 3RD SEM CS/IT/ME/EC /CIVIL

UNIT-1

COMPUTER SYSTEM SECURITY-Computer security basically is the protection of**computer systems** and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your **computer system**

internal architectural design comes in different types and sizes, but the basic structure remains same of all computer systems. hardware and software there are two component of computer system security

market place vulnerability-Software vulnerabilities and "exploits" are used to get remote access to both stored information and information generated in real time. When most people use the same software, as is the case in most of countries today given the monopolistic nature of internet content and service providers, one specific vulnerability can be used against thousands if not millions of people. In this context, criminals have become interested in such vulnerabilities.

. **Cyber security** refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access

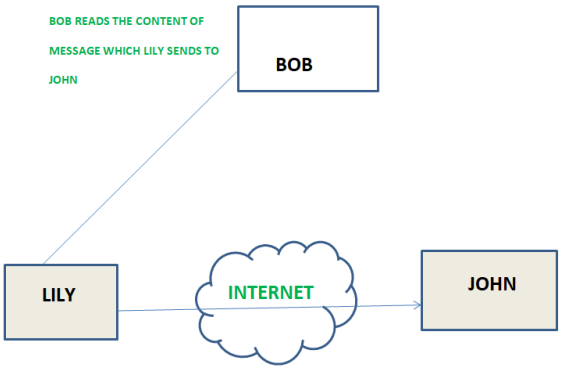
Attacks- In computers and computer networks an **attack** is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. ... A cyber attack can be employed by nation-states, individuals, groups, society or organizations. A cyber attack may originate from an anonymous source.

Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1-The release of message content –

Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or

confidential information. We would like to prevent an opponent from learning the

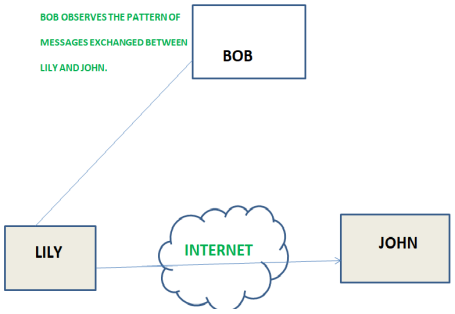


contents of

2-Traffic analysis –

Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.

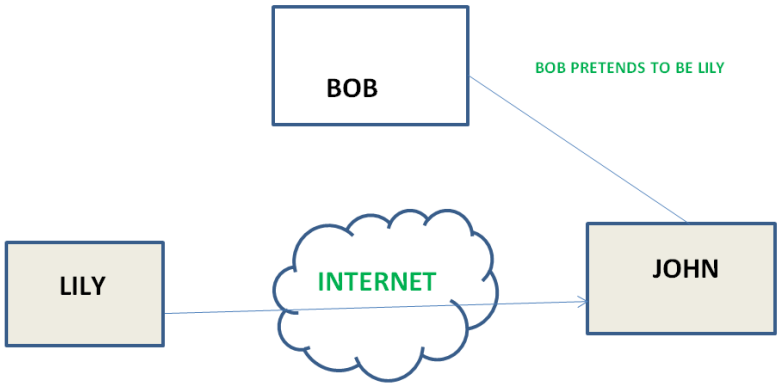
The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



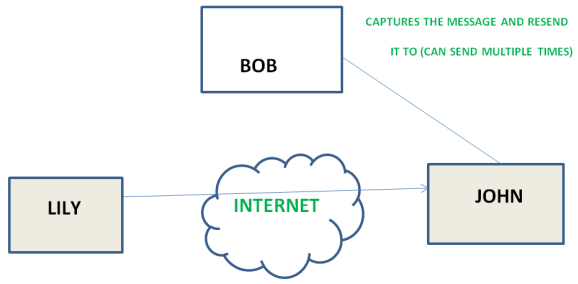
Active attacks: An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following

1-Masquerade –

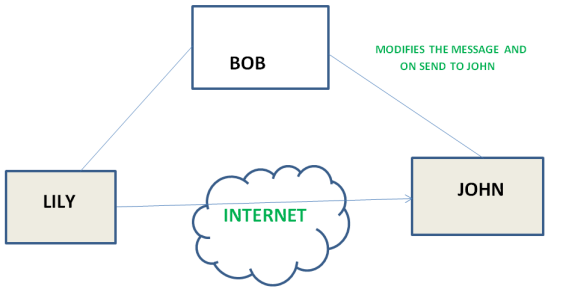
Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.



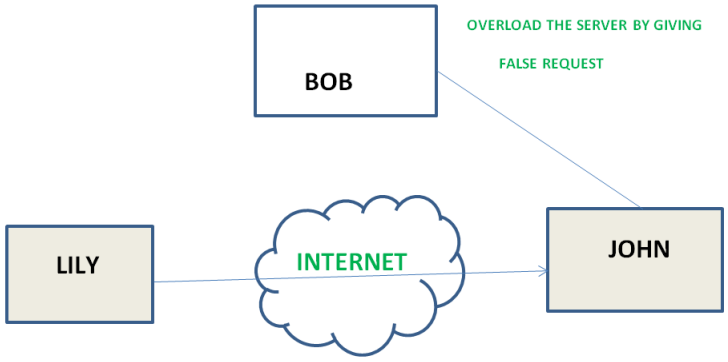
2-Replay –
It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.



3-Modification of messages –
It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.



4-Denial of Service It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance



hijacking -Hijacking is a type of network security attack in which the attacker takes control of a communication - just as an airplane hijacker takes control of a flight - between two entities and masquerades as one of them.one type of hijacking (also known as a man in the middle attack), the perpetrator takes control of an established connection while it is in progress. The

attacker intercepts messages in a public key exchange and then retransmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before retransmitting them.**Browser hijacking** is a form of unwanted software that modifies a web **browser**'s settings without a user's permission, to inject unwanted advertising into the user's**browser**. A **browser hijacker** may replace the existing home page, error page, or search engine with its own.
Session hijacking of controller attack is one of the most common ways of information leakage Software-Defined Networking is facing, which brings a serious threat to cyber security. However, the existing defense technologies mainly focus on how to detect attacks and reduce the attack success rate. The paper proposes a method from another perspective to minimize the cost that the network undertakes and find an optimal defender's strategy when an attack is unavoidable in some case. The main work is as follows. First of all, we models the scenario of attack and defense as a Stackelberg Games, and prove the optimal strategy is equal to the SSE (Strong Stackelberg Equilibrium)

Difference between active and passive attack

Basic	Active attack tries to change the system resources or affect their operation.	Passive attack tries to read or make use of information from the system but does not influence system resources.
Modification in the information	Occurs	does not take place
Harm to the system	Always causes damage to the system.	Do not cause any harm.
Threat to	Integrity and availability	Confidentiality
Attack awareness	The entity (victim) gets	The entity is unaware of the attack.

	informed about the attack.	
Task performed by the attacker	The transmission is captured by physically controlling the portion of a link.	Just need to observe the transmission.

ERROR-404.

ANS. The **HTTP 404**, **404 Not Found**, **404**, **Page Not Found**, or **Server Not Found** error message is a Hypertext Transfer Protocol (HTTP) standard response code, in computer network communications, to indicate that the browser was able to communicate with a given server, but the server could not find what was requested. Further, when the requested information is found but access is not granted, the server may return a 404 error if it wishes to not disclose this information, as well.[1]

The website hosting server will typically generate a "404 Not Found" web page when a user attempts to follow a broken or dead link; hence the 404 error is one of the most recognizable errors encountered on the World Wide Web

confidentiality is a set of rules that limits access to information, **integrity** is the assurance that the information is trustworthy and accurate, and **availability** is a guarantee of reliable access to the information by authorized people. the terms of confidentiality, integrity and availability .

Information Security is not all about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electrical one. Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.
During First World War, Multi-tier Classification System was developed keeping in mind sensitivity of information. With the beginning of Second World War formal alignment of Classification System was done. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data.

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

1. **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
2. **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an

employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.

3. **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management.
   Denial of service attack is one of the factor that can hamper the availability of information.

The need for Information security:

1. **Protecting the functionality of the organisation:**
   The decision maker in organisations must set policy and operates their organisation in compliance with the complex, shifting legislation, efficient and capable applications.

2. **Enabling the safe operation of applications:**
   The organisation is under immense pressure to acquire and operates integrated, efficient and capable applications. The modern organisation needs to create an environment that safeguards application using the organisations IT systems, particularly those application that serves as important elements of the infrastructure of the organisation.
3. **Protecting the data that the organisation collect and use:**
   Data in the organisation can be in two forms that are either in rest or in motion, the motion of data signifies that data is currently used or processed by the system. The values of the data motivated the attackers to seal or corrupts the data. This is essential for the integrity and the values of the organisation's data. Information security ensures protection od both data in motion as well as data in rest.

UNIT-4

CRYPTOGRAPHY

. *Cryptography is the art and science of making a cryptosystem that is capable of providing information security.*

Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

Cryptography – Benefits

Cryptography is an essential information security tool. It provides the four most basic services of information security −

- **Confidentiality** − Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Authentication** − The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Data Integrity** − The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
- **Non-repudiation** − The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

Cryptography – Drawbacks

Apart from the four fundamental elements of information security, there are other issues that affect the effective use of information −

- A strongly encrypted, authentic, and digitally signed information can be **difficult to access even for a legitimate user** at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.
- **High availability,** one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system.
- Another fundamental need of information security of **selective access control** also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.
- Cryptography does not guard against the vulnerabilities and **threats that emerge from the poor design of systems,** protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.
- Cryptography comes at cost. The cost is in terms of time and money −
    - Addition of cryptographic techniques in the information processing leads to delay.
    - The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.
- The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

Security Services of Cryptography

The primary objective of using cryptography is to provide the following four

fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.

Confidentiality

Confidentiality is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as **privacy** or **secrecy**.

Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

Data Integrity

It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.

Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Authentication service has two variants −

- **Message authentication** identifies the originator of the message without any regard router or system that has sent the message.
- **Entity authentication** is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

Non-repudiation

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this trans

Components of a Cryptosystem

The various components of a basic cryptosystem are as follows −

- **Plaintext.** It is the data to be protected during transmission.
- **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

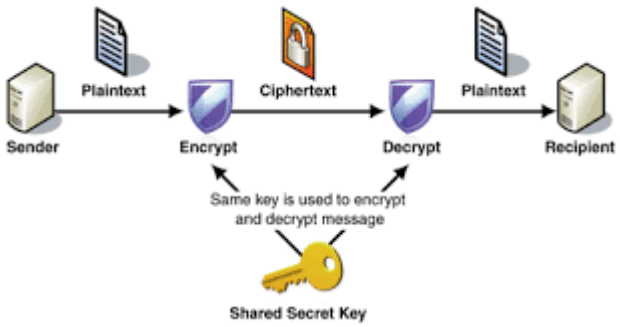
An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system −

- Symmetric Key Encryption
- Asymmetric Key Encryption

- **Symmetric encryption** uses a single key that needs to be shared among the people who need to receive the message.. Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the keyPersons using symmetric key encryption must share a common key prior to exchange of information.

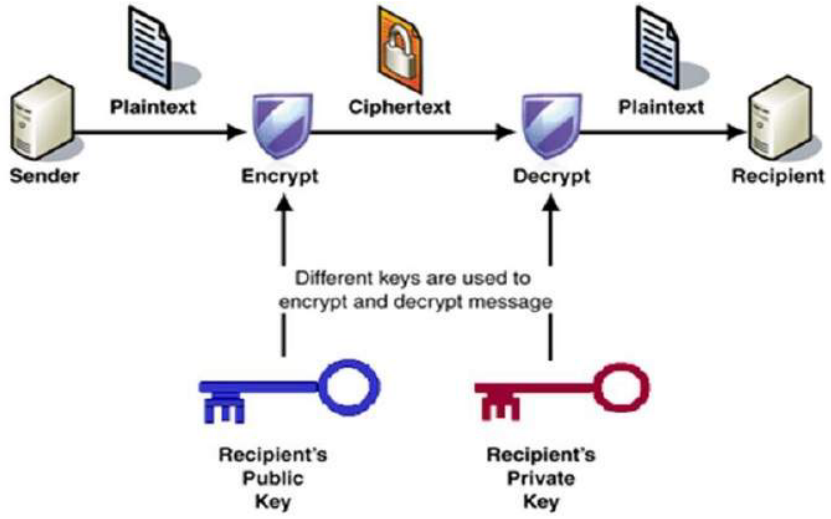


- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of **n** people, to enable two-party communication between any two persons, the number of keys required for group is **n × (n – 1)/2**.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

so that it can be used

The Asymmetric Key Encryption

The asymmetric encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration



- Every user in this system needs to have a pair of dissimilar keys, **private key** and **public key**. These keys are mathematically related – when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.
- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
- When *Host1* needs to send data to *Host2,* he obtains the public key of *Host2* from repository, encrypts the data, and transmits.
- *Host2* uses his private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
- Processing power of computer system required to run asymmetric algorithm is higher

Difference between block and stream cipher

S.NO	BLOCK CIPHER(ENCRYPTION)	STREAM CIPHER(DECRYPTION)
1.	Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plaint text into cipher text by taking 1 byte of plain text at a time.
2.	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3.	The complexity of block cipher is simple.	While stream cipher is more complex.
4.	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5.	In block cipher, reverse encrypted text is hard.	While in stream cipher, reverse encrypted text is easy.
6.	The algorithm modes which are used	The algorithm modes which are

in block cipher are: ECB (Electronic Code Book) and CBC (Cipher Block Chaining).

used in stream cipher are: CFB (Cipher Feedback) and OFB (Output Feedback).

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.

Digital Signature is a process that guarantees that the contents of a message have not been altered in transit. When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your public and private key pair.

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.

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.

Difference between Connection-oriented and Connection-less Services:

S.NO	CONNECTION-ORIENTED SERVICE	CONNECTION-LESS SERVICE
1.	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
3.	Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
4.	Connection-oriented Service is feasible.	Connection-less Service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give the guarantee of reliability.
7.	In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.

TLS

TLS is a cryptographic protocol that provides end-to-end communications security over

networks and is widely used for internet communications and online transactions

Network security entails securing data against attacks while it is in transit on a network. To achieve this goal, many real-time security protocols have been designed. There are popular standards for real-time network security protocols such as S/MIME, SSL/TLS, SSH, and IPsec. As mentioned earlier, these protocols work at different layers of networking model.

In the last chapter, we discussed some popular protocols that are designed to provide application layer security. In this chapter, we will discuss the process of achieving network security at Transport Layer and associated security protocols.

For TCP/IP protocol based network, physical and data link layers are typically implemented in the user terminal and network card hardware. TCP and IP layers are implemented in the operating system. Anything above TCP/IP is implemented as user process.

Need for Transport Layer Security

Let's discuss a typical Internet-based business transaction.

Bob visits Alice’s website for selling goods. In a form on the website, Bob enters the type of good and quantity desired, his address and payment card details. Bob clicks on Submit and waits for delivery of goods with debit of price amount from his account. All this sounds good, but in absence of network security, Bob could be in for a few surprises.

- If transactions did not use confidentiality (encryption), an attacker could obtain his payment card information. The attacker can then make purchases at Bob's expense.
- If no data integrity measure is used, an attacker could modify Bob's order in terms of type or quantity of goods.
- Lastly, if no server authentication is used, a server could display Alice's famous logo but the site could be a malicious site maintained by an attacker, who is masquerading as Alice. After receiving Bob's order, he could take Bob's money and flee. Or he could carry out an identity theft by collecting Bob's name and credit card details.

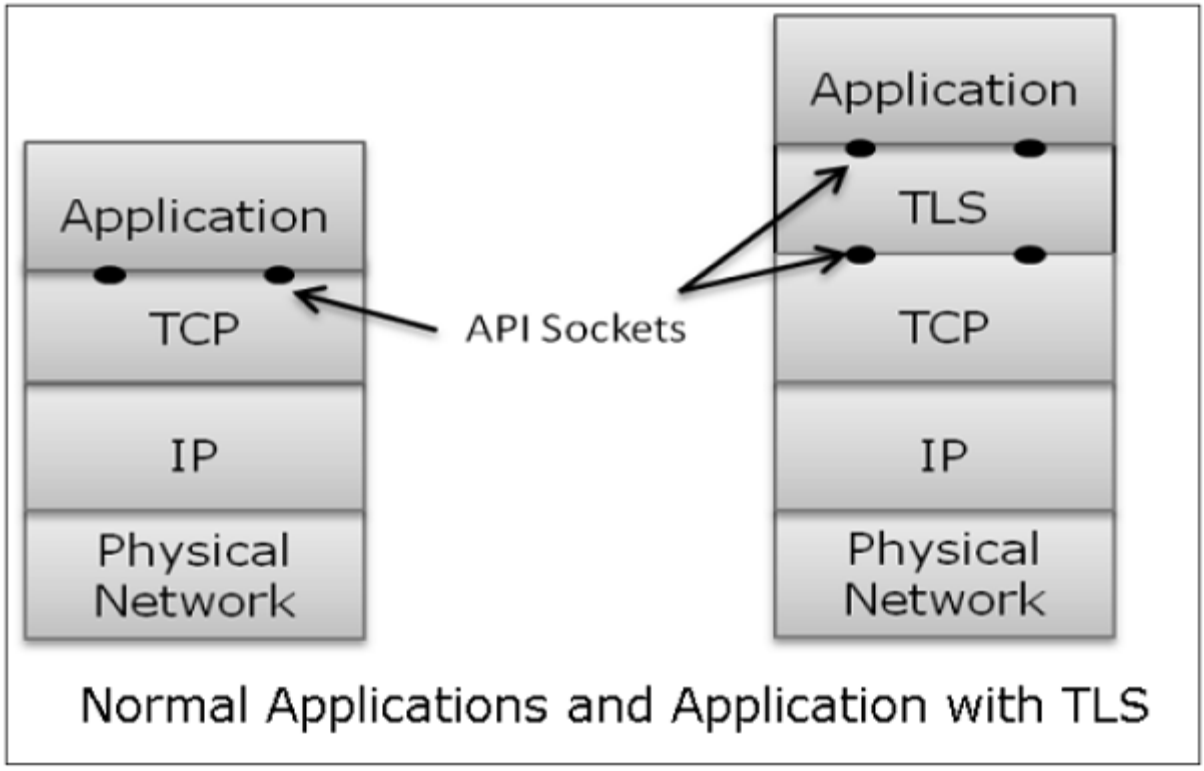
Transport layer security schemes can address these problems by enhancing TCP/IP based network communication with confidentiality, data integrity, server authentication, and client authentication.

The security at this layer is mostly used to secure HTTP based web transactions on a network. However, it can be employed by any application running over TCP.

Philosophy of TLS Design

Transport Layer Security (TLS) protocols operate above the TCP layer. Design of these protocols use popular Application Program Interfaces (API) to TCP, called “sockets" for interfacing with TCP layer.

Applications are now interfaced to Transport Security Layer instead of TCP directly. Transport Security Layer provides a simple API with sockets, which is similar and analogous to TCP's API.



In the above diagram, although TLS technically resides between application and transport layer, from the common perspective it is a transport protocol that acts as TCP layer enhanced with security services.

TLS is designed to operate over TCP, the reliable layer 4 protocol (not on UDP protocol), to make design of TLS much simpler, because it doesn't have to worry about 'timing out' and 'retransmitting lost data'. The TCP layer continues doing that as usual which serves the need of TLS.

EMAIL SECURITY:- E-mail Hacking

Email hacking can be done in any of the following ways:

Spam

Virus

Phishing

Spam

E-mail spamming is an act of sending Unsolicited Bulk E-mails (UBI) which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

Virus

Some emails may incorporate with files containing malicious script which when run on your computer may lead to destroy your important data.

Phishing

Email phishing is an activity of sending emails to a user claiming to be a legitimate enterprise. Its main purpose is to steal sensitive information such as usernames, passwords, and credit card details.

Such emails contains link to websites that are infected with malware and direct the user to enter details at a fake website whose look and feels are same to legitimate one.

E-mail Spamming and Junk Mails

Email spamming is an act of sending Unsolicited Bulk E-mails (UBI) which one has not asked for. Email spams are the junk mails sent by commercial companies as an advertisement of their products and services.

Spams may cause the following problems:

- It floods your e-mail account with unwanted e-mails, which may result in loss of important e-mails if inbox is full.
- Time and energy is wasted in reviewing and deleting junk emails or spams.
- It consumes the bandwidth that slows the speed with which mails are delivered.
- Some unsolicited email may contain virus that can cause harm to your computer.

Blocking Spams

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server. Here in this tutorial, we will discuss various protocols such as SMTP, POP, and IMAP.

SMPTP

SMTP stands for Simple Mail Transfer Protocol. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.
- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

IMAP

IMAP stands for Internet Mail Access Protocol. It was first proposed in 1986. There exist five versions of IMAP as follows:

1. Original IMAP
2. IMAP2
3. IMAP3
4. IMAP2bis
5. IMAP4

Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

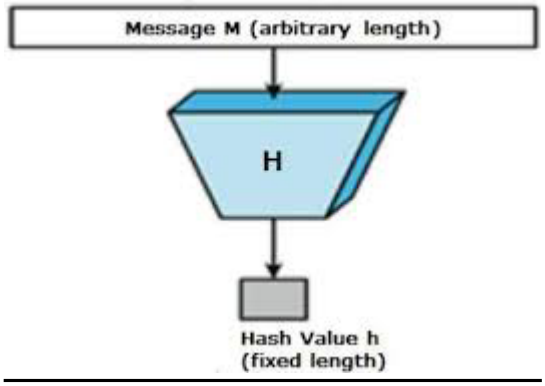
DIFFERENCE BETWEEN IPV4 AND IPV6

IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection	In IPv6 end to end connection integrity is

integrity is Unachievable	Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 in decimal	Address Representation of IPv6 is in hexadecimal

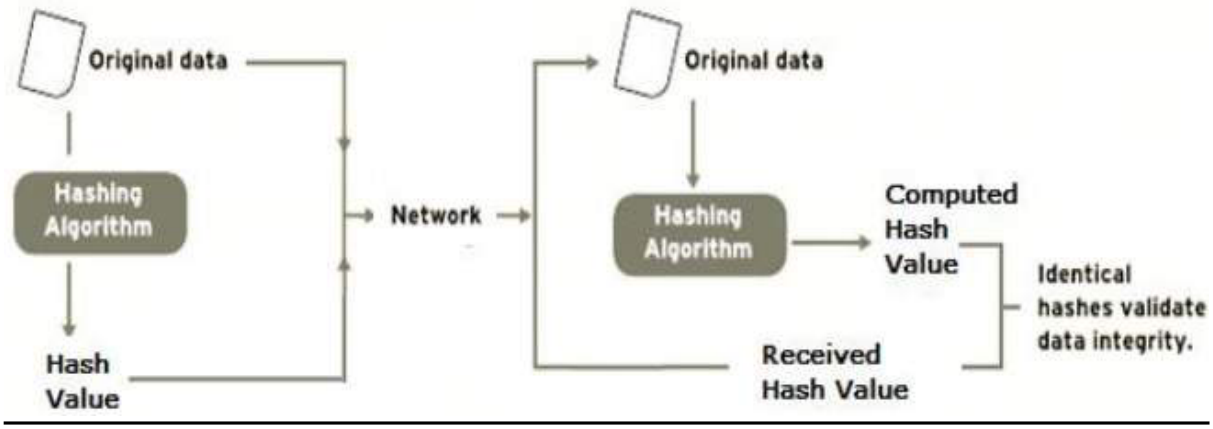
hash function takes a group of characters (called a key) and maps it to a value of a certain length (called a **hash** value or **hash**). ... **Hashing** is done for indexing and locating items in databases because it is easier to find **the** shorter **hash** value than **the** longer string

A **hash function** is a mathematical **function** that converts an input value into a compressed numerical value – a **hash** or **hash** value



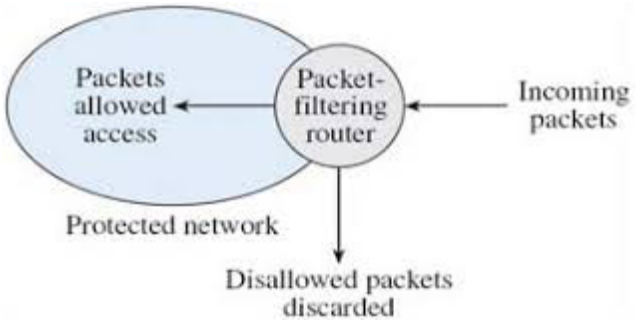
Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data.

The process is depicted in the following illustration –The integrity check helps the user to detect any changes made to original file. It however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver. This integrity check application is useful only if the user is sure about the originality of file.



UNIT -5

Packet filtering is a **firewall** technique used to control network access by monitoring outgoing and incoming **packets** and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports



Techopedia explains *Packet Filtering*

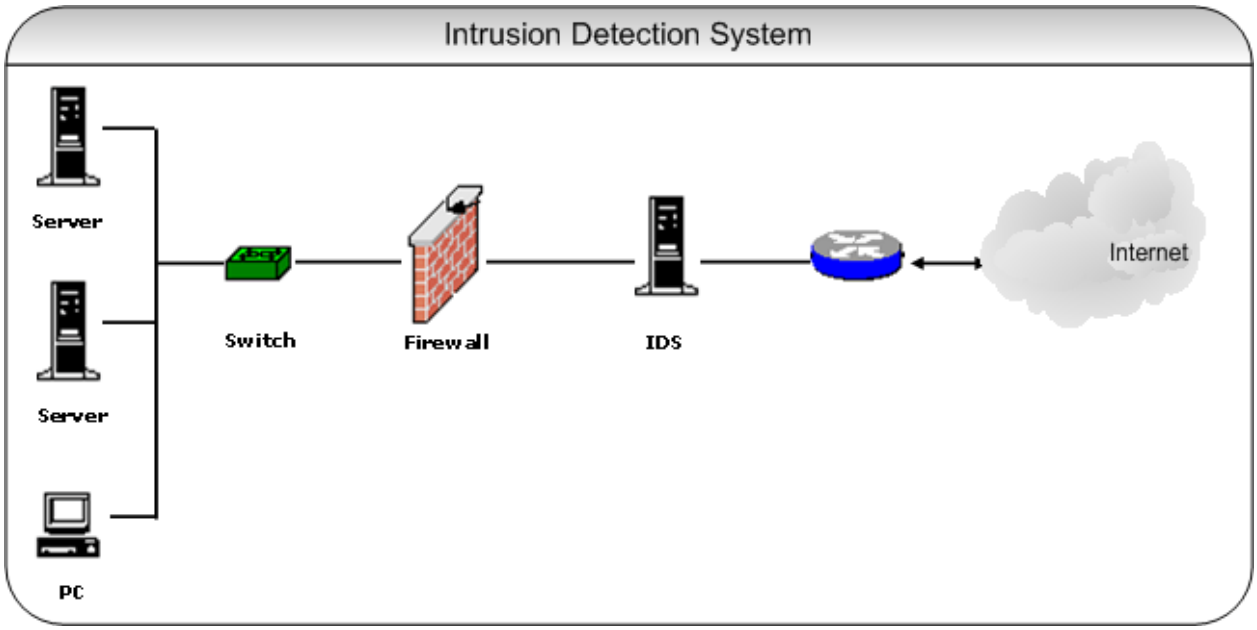
During network communication, a node transmits a packet that is filtered and matched with predefined rules and policies. Once matched, a packet is either accepted or denied.

Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified. Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Packet filters also verify source and destination port addresses.

Some packet filters are not intelligent and unable to memorize used packets. However, other packet filters can memorize previously used packet items, such as source and destination IP addresses.

Packet filtering is usually an effective defense against attacks from computers outside a local area network (LAN). As most routing devices have integrated filtering capabilities, packet filtering is considered a standard and cost-effective means of security.

An **Intrusion Detection System** (IDS) is a **system** that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a **system** for harmful activity or policy breaching



Intrusion detection systems (IDS) can be classified into different ways. The major classifications are Active and passive IDS, Network Intrusion detection systems (NIDS) and host Intrusion detection systems (HIDS)

Active and passive IDS

An active Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Prevention System (IDPS). Intrusion Detection and Prevention System (IDPS) is configured to automatically block suspected attacks without any intervention required by an operator. Intrusion Detection and Prevention System (IDPS) has the advantage of providing real-time corrective action in response to an attack.

A passive IDS is a system that's configured to only monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. A passive IDS is not capable of performing any protective or corrective functions on its own.

Network Intrusion detection systems (NIDS) and Host Intrusion detection systems (HIDS)

Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and

monitors all traffic on that segment.

A Host Intrusion Detection Systems (HIDS) and software applications (agents) installed on workstations which are to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host Intrusion detection systems (HIDS) can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network. Host based IDS systems are used to monitor any intrusion attempts on critical servers.

The drawbacks of Host Intrusion Detection Systems (HIDS) are

• Difficult to analyse the intrusion attempts on multiple computers.

• Host Intrusion Detection Systems (HIDS) can be very difficult to maintain in large networks with different operating systems and configurations

• Host Intrusion Detection Systems (HIDS) can be disabled by attackers after the system is compromised.

Knowledge-based (Signature-based) IDS and behavior-based (Anomaly-based) IDS

A knowledge-based (Signature-based) Intrusion Detection Systems (IDS) references a database of previous attack signatures and known system vulnerabilities. The meaning of word signature, when we talk about Intrusion Detection Systems (IDS) is recorded evidence of an intrusion or attack. Each intrusion leaves a footprint behind (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.). These footprints are called signatures and can be used to identify and prevent the same attacks in the future. Based on these signatures Knowledge-based (Signature-based) IDS identify intrusion attempts.

The disadvantages of Signature-based Intrusion Detection Systems (IDS) are signature database must be continually updated and maintained and Signature-based Intrusion Detection Systems (IDS) may fail to identify a unique attacks.

A Behavior-based (Anomaly-based) Intrusion Detection Systems (IDS) references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Higher false alarms are often related with Behavior-based Intrusion Detection Systems (IDS

Network-based Intrusion Detection System (NIDS) mean?

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

Network-based Intrusion Detection System (NIDS)

Intrusion detection systems (IDSs) are available in different types; the two main types are the host-based intrusion system (HBIS) and network-based intrusion system (NBIS). Additionally, there are IDSs that also detect movements by searching for particular signatures of well-known threats.

An IDS compliments, or is part of, a larger security system that also contains firewalls, anti-virus software, etc. A NIDS tries to detect malicious activity such as denial-of-service attacks, port scans and attacks by monitoring the network traffic.

Difference between firewall and IDS

1

Firewall	**IDS**
A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications.	An Intrusion Detection System (IDS) is hardware device installed on the netwo (HIDS) to detect and report intrusion a network.
A firewall can block an unauthorized access to network (E.g. A watchman standing at gate can block a thief)	An IDS can only report an intrusion; it c (E.g. A CCTV camera which can alert a cannot stop it)
A firewall cannot detect security breaches for traffic that does not pass through it (E.g. a gateman can watch only at front gate. He is not aware of wall-jumpers)	IDS is fully capable of internal security information from a variety of system a resources and analyzing the symptom problems
Firewall doesn't inspect content of permitted traffic. (A gateman will never suspect an employee of the company)	IDS keeps a check of overall network
No man-power is required to manage a firewall.	An administrator (man-power) is requi

Firewall	IDS
	threats issued by IDS
Firewalls are most visible part of a network to an outsider. Hence, more vulnerable to be attacked first. (A gateman will be the first person attacked by a thief!!)	IDS are very difficult to be spotted in a (especially stealth mode of IDS).

Data link layer **is** the protocol **layer** in a program that handles the moving of data into and out of a physical **link** in a network. ... Data bits are encoded, decoded and organized in the data **link layer**, before they are transported as frames between two adjacent nodes on the same LAN or WAN

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

DNSSEC (DNS) stands for Domain Name System **Security** Extensions, and it is a technology used to protect information on the Domain Name System (**DNS**) which is used on IP networks. It provides authentication for the origin of the **DNS** data, helping to safeguard against attacks and protect data integrity

DNS is **important** because it links the domain name to the IP. ... Internet criminals can exploit these weaknesses and are capable of creating false **DNS** records. These fake records can trick users into visiting fake websites, downloading malicious software, or worse. Thus, DNSSEC was created to save the day.

Domain Name System **Security** Extensions (DNSSEC)**is** a suite of extensions to the **DNS** standard, which uses digital signatures to validate the authenticity of **DNS** responses. DNSSEC prevents attacks that inject false information into **DNS** resolvers, such as **DNS** spoofing,

cache poisoning and man in the middle attacks

. **IPSec(IP SECURITY)** which works at the network layer is a framework consisting of protocols and algorithms for protecting data through an un-trusted network such as the internet. IPSec provides data security in various ways such as encrypting and authenticating data, protection against masquerading and manipulation. IPSec is a complex framework consisting of many settings, which is why it provides a powerful and flexible set of security features that can be used.

Difference between MAC Address and IP Address

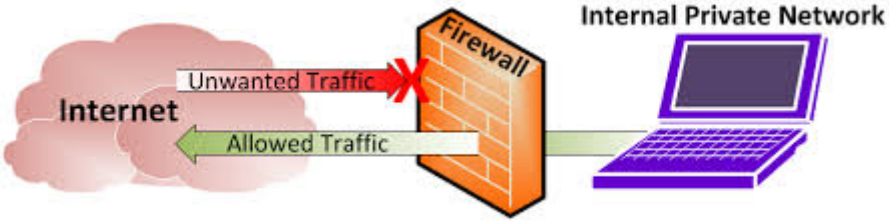
Both MAC Address and IP Address are used to uniquely defines a device on the internet. NIC Card's Manufacturer provides the MAC Address, on the other hand Internet Service Provider provides IP Address.
The main difference between MAC and IP address is that, MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network. While IP address are used to uniquely identifies the connection of network with that device take part in a network.

Let's see the difference between MAC Address and IP Address:

S.NO	MAC ADDRESS	IP ADDRESS
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or six byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.

5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.

firewall is a **network security** device that monitors incoming and outgoing network traffic and permits or blocks data **packets** based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.



Types of Firewalls

Proxy firewall

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

Stateful inspection firewall

Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Unified threat management (UTM) firewall

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention

and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.
See our UTM devices.

Next-generation firewall (NGFW)

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.
According to Gartner, Inc.’s definition, a next-generation firewall must include:

Internet, sometimes called simply "the Net," is a worldwide system of computer networks -- a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers

Although the Internet is one of man's greatest creations, it also has many disadvantages, several of which are listed in the following sections.

Bullying, trolls, stalkers, and crime

Anyone who has spent time on the Internet has encountered trolls or abusive people. Another issue that has increased over the years is cyberbullying.

With people sharing information on the Internet, stalkers may experience less difficulty finding personal information about others through various means.

Hidden places on the Internet and the deep web can also be a place for criminals to conduct business without as much fear of being caught. A global audience also gives criminals more

ways to solicit their goods.

- Computer crime information and a list of the types of computer crime.

Pornographic and violent images

In our digital age, there is a nearly an infinite amount of content on the Internet. While there are amazing resources, such as Wikipedia, less desirable content also exists. Consequently, users can accidentally come across violent or pornographic images that they may not want to view.

Addiction, time waster, and causes distractions

Surfing and playing games on the Internet can quickly become very addictive. Doing so can lead to spending a lot of frivolous time on the Internet, instead of doing something productive. On this same note, the Internet can hamper workplace productivity as well.

Never being able to disconnect from work

The Internet is great for giving its users the ability to work from anywhere. However, you may be expected to be available to work at any time of the day, even if you had not previously agreed to be available.

For example, you may be at home and get a notification that you have received an important work-related e-mail and then end up working on the content of that e-mail without getting paid.

Identity theft, hacking, viruses, and cheating

With access to billions of computers, computer hackers and malicious users can hack accounts and steal personal information that could be used for identity theft. The Internet also connects all computers to each other, so hackers can scan millions of computers and quickly identify what computers are vulnerable to attack.

The Internet also enables students to cheat on their studies, or find others on the Internet to do their homework.

- How to protect yourself while on the Internet.

Spam and advertising

It's great that the Internet can facilitate reaching a much wider audience than traditional advertising methods (e.g., newspaper, TV, and radio). However, because digital advertising can be sent on a massive scale, you might see more spam in your inbox than junk mail in real life.

- How to stop spam.

Affects focus and patience

The sites we use on the Internet every day have an "instant gratification" effect. They also present an endless menu of things to think about and experience at any moment, on demand. Getting information this way rewards fast-paced thinking that shifts focus quickly, which affects your interactions in general, making you more impatient and less focused on your activities. Try to balance this natural effect with time away from social media and focused on more productive real-life activities like exercise or cleaning.

Depression, loneliness, and social isolation

Social networking sites can also lead to depression as many people tend to compare their lives with others. The Internet and online games facilitate communication with others. Although you may find new connections around the world, you may also find yourself disconnecting from those in your real life.

Health issues and obesity

As with watching TV, spending too much time on the computer surfing the Internet or playing games can also lead to obesity and an unhealthy lifestyle.

A computer also requires a lot of repetitive

movement that can lead to carpal tunnel syndrome. For example, moving your hand from your keyboard to a mouse and typing are all repetitive actions, which can cause injuries. Taking breaks, keeping the proper posture, and understanding computer ergonomics can all help delay or prevent these injuries.

- How to protect your eyes when using a computer.

Buying things that you don't need

The Internet reduces the barriers for consumers to make purchases, so users may find themselves purchasing products without putting much thought into whether they should. Also, for some people, buying items on the Internet can become so addictive that it causes serious debt.

UNIT-3

Threats to Information Security

In Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest. **Software attacks** means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behave differently.

Malware is a combination of 2 terms- Malicious and Software. So Malware

basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the **basis of Infection** Method are following:

1. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. Ther Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms –** Worms are also self replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will for example consume hard disk space thus slowing down the computer.
3. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.

   Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

   They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.
4. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need of human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

Malware on the **basis of Actions:**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on computer's desktop or inside individual programs. They come attached with free to use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware –** It is a program or we can say a software that monitors your

activities on computer and reveal collected information to interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection.

One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

3. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
4. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
5. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
6. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

.

- **Technology with weak security –** With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follows Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices
- **Social media attacks –** In this cyber criminals identify and infect a cluster of websites that persons of a particular organisation visit, to steal information.
- **Mobile Malware –**There is a saying when there is a connectivity to Internet there will be danger to Security. Same goes to Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus in the device.
- **Outdated Security Software –** With new threats emerging everyday, updation in security software is a pre requisite to have a fully secured environment.
- **Corporate data on personal devices –** These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.
- **Social Engineering –** is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example email or message from your friend, that was probably not sent by your friend. Criminal can access your friends device and then by accessing the contact list he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definately

check the link or attachment in the message, thus unintentionally infecting the computer.

access control

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings as well as alarms and lockdown capabilities to prevent unauthorized access or operations.

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication, which requires two or more authentication factors, is often an important part of layered defense to protect access control systems.

These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or IP address. Directory services and protocols, including the Local Directory Access Protocol (LDAP) and the Security

Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.

Organizations use different access control models depending on their compliance requirements and the security levels of information technology they are trying to protect.

Types of access control

The main types of access control are:

- **Mandatory access control (MAC)**: A security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel, grants or denies access to those resource objects based on the information security clearance of the user or device. For example, Security Enhanced Linux is an implementation of MAC on the Linux operating system.
- **Discretionary access control (DAC):** An access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.
- **Role-based access control (RBAC):** A widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- executive level, engineer level 1 -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed

using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.

- **Rule-based access control:** A security model in which the system administrator defines the rules that to govern access to resource objects. Often these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and role-based access control to enforce access policies and procedures.
- **Attribute-based access control (ABAC):** A methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

Use of access control

The goal of access control is to minimize the risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information and intellectual property.

Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services. After some high-profile breaches, technology vendors have shifted away from single sign-on systems to unified access management, which offers access controls for on-premises and cloud environments.

Implementing access control

Access control is a process that is integrated into an organization's IT environment. It can involve identity and access management systems.

These systems provide access control software, a user database, and management tools for access control policies, auditing and enforcement.

Windows NT -- Access Control

Windows NT supports multiple file systems, but the protection issues we will consider are only associated with one: NTFS. In NT there is the notion of an item, which can be a file or a directory. Each item has an owner. An owner is usually the thing that created the item. It can change the access control list, allow other accounts to change the access control list and allow other accounts to become owner. Entries in the ACL are individuals and groups. Note that NT was designed for groups of machines on a network, thus, a distinction is made between local groups (defined on a particular workstation) and global groups (domain wide). A single name can therefore mean multiple things.

NTFS is structured so that a file is a set of properties, the contents of the file being just one of those properties. An ACL is a property of an item. The ACL itself is a list of entries: (user or group, permissions). NTFS permissions are closer to extended permissions in UNIX than to the 9 mode bits. The permission offer a rich set of possibilities:

- R -- read
- W -- write
- X -- execute
- D -- delete
- P -- modify the ACL
- O -- make current account the new owner ("take ownership")

UNIX uses access control lists. A user logs into UNIX and has a right to start processes that make requests. A process is "bigger" than a subject, many domains may correspond to a single process. Each process has an identity(uid). This uid is obtained from the file that stores user passwords: /etc/passwd. An entry in /etc/passwd

The main differences between Windows and Unix are as follows:

1.Unix is a Command Line User Interface and Windows is Graphic User Interface operating system.

2. Unix is command based and Windows is menu based operating system.

3. Windows is event driven whereas this feature is absent in Unix operating system.

4. File system in Unix is (STD.ERR,STD.IO), and in Windows it is (FAT32,NTFS).

5. In Unix multiprocessing is possible whereas it is not possible in Windows.

6. In terms of security, Unix is more secure than Windows as we can restrict the permission of each user.

7. Windows operating system support plug and play and this feature is not available in Unix.

8. Windows is licensed operating system and Unix is free source operating system.

Browser isolation is a cybersecurity model used to physically isolate an internet users web browser and their browsing activity away from the local machine and network, it is the underlying model and technology that supports a remote browsing platform. According to Gartner, more than 50% of enterprises will actively begin to isolate their internet browsing to reduce the impact of cyber attacks over the next three years (Gartner BIT Report 2016). Gartner are also recommending browser isolation technologies as one of the most effective ways that an enterprise can reduce web based attacks. With this in mind, lets take a closer look at exactly what browser isolation is and why remote browser isolation is being adopted so quickly by security conscious organizations.

Browser isolation was an invention borne out of necessity, our current security tools (anti-virus, firewall, intrusion detection and prevention) are failing to protect us from malware, ransomware and browser based cyber attacks. Browser based attacks are increasing in frequency, with Gartner estimating that 98% of external information security attacks are carried out over the public internet and of those attacks 80% of them are targeted directly at end users through their browsers as they use the internet normally.

Over time and beneath the weight of regular cyberattacks many organizations realized that their browsers (along with all of the associated browsing activity and risk) do not really need to be connected to their internal networks and infrastructure. In fact they realized that letting their users browse the internet from their work machines (or their internal networks) was a bad idea from a cybersecurity perspective.

Web security also known as "Cyber security**" involves protecting website or** web **application by detecting, preventing and responding to attacks. Websites and** web **applications are just as prone to** security **breaches as physical homes, stores, and government locations.**

The Three Security Goals Are Confidentiality, Integrity, and Availability

All information security measures try to address at least one of three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs (see Figure 2.1). Information security professionals who create policies and procedures (often referred to as governance models) must consider each goal when creating a plan to protect a computer system.

Frame busting and clickjacking prevention

Clickjacking allows an attacker to trick your users into clicking parts of your interface without their consent. A simple way to describe describe this is, an attacker will embed your application in their site as an iframe. On top of the iframe they can show a completely different interface. You're thinking you're clicking buttons on your own interface, while in fact you are hitting the 'Delete my account' button in for example GMail.

Because this technique completely operates with frames, it can be circumvented by using a 'Frame busting' technique. As a bonus, this will also disallow for example Digg to steal and monetize your content.

Rendering-

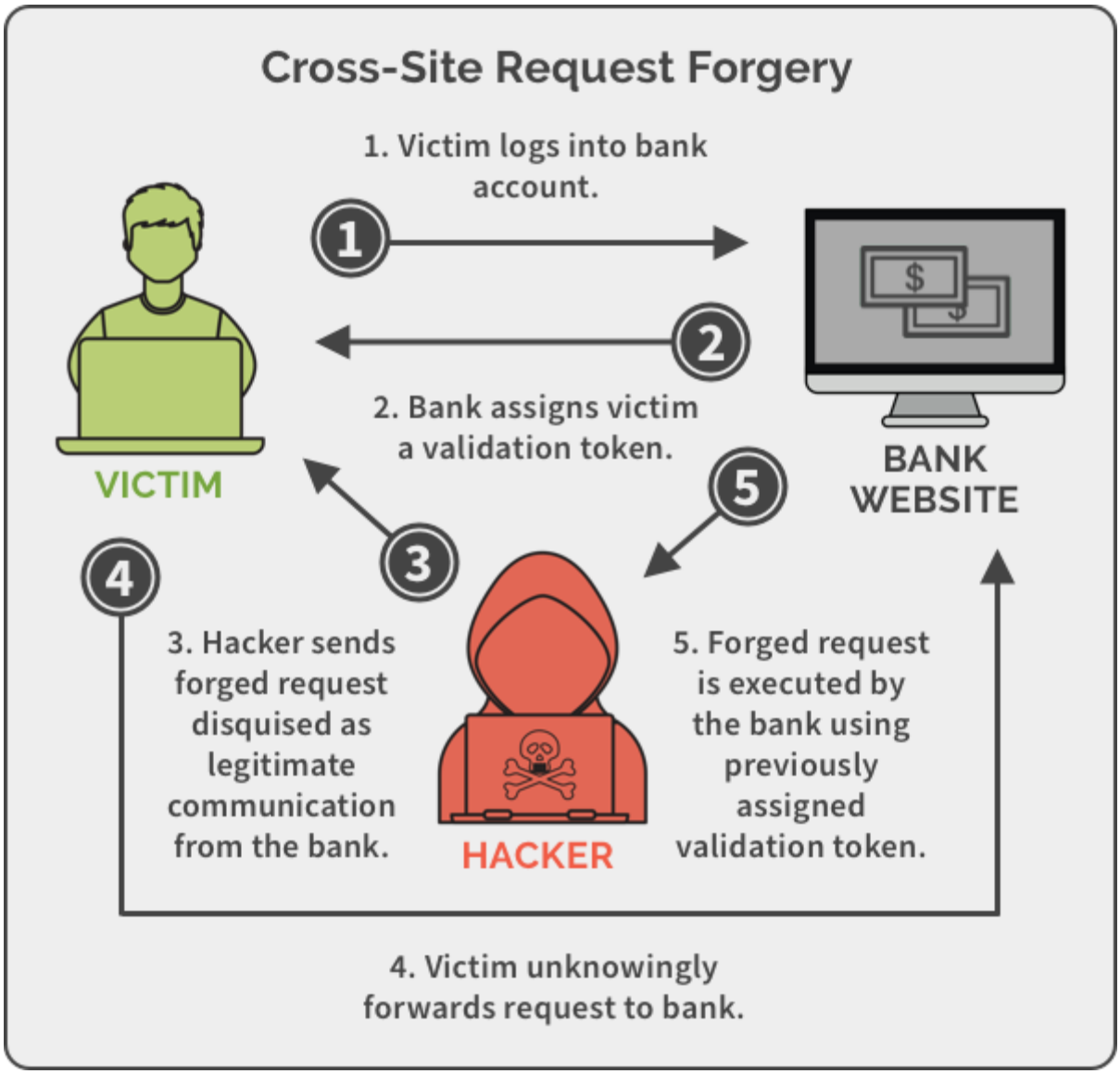
Rendering is the process involved in the generation of a two-dimensional or three-dimensional image from a model by means of application programs. Rendering is mostly used in architectural designs, video games, and animated movies, simulators, TV special effects and design visualization. The techniques and features used vary according to the project. Rendering helps increase efficiency and reduce cost in design.

There are two categories of rendering: pre-rendering and real-time rendering. The striking difference between the two lies in the speed at which the computation and finalization of images takes place.

- **Real-Time Rendering:** The prominent rendering technique using in interactive graphics and gaming where images must be created at a rapid pace. Because user interaction is high in such environments, real-time image creation is required. Dedicated graphics hardware and pre-compiling of the available information has improved the performance of real-time rendering.
- **Pre-Rendering:** This rendering technique is used in environments where speed is not a concern and the image calculations are performed using multi-core central processing units rather than dedicated graphics hardware. This rendering technique is mostly used in animation and visual effects, where photorealism needs to be at the highest standard possible.

cross-site request forgery (CSRF)

In this section, we'll explain what cross-site request forgery is, describe some examples of common CSRF vulnerabilities, and explain how to prevent CSRF attacks.



What is CSRF?

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.

What is the impact of a CSRF attack?

In a successful CSRF attack, the attacker causes the victim user to carry out an action unintentionally. For example, this might be to change the email address on their account, to change their password, or to make a funds transfer. Depending on the nature of the action, the attacker might be able to gain full control over the

user's account. If the compromised user has a privileged role within the application, then the attacker might be able to take full control of all the application's data and functionality.

How does CSRF work?

For a CSRF attack to be possible, three key conditions must be in place:

- **A relevant action.** There is an action within the application that the attacker has a reason to induce. This might be a privileged action (such as modifying permissions for other users) or any action on user-specific data (such as changing the user's own password).
- **Cookie-based session handling.** Performing the action involves issuing one or more HTTP requests, and the application relies solely on session cookies to identify the user who has made the requests. There is no other mechanism in place for tracking sessions or validating user requests.
- **No unpredictable request parameters.** The requests that perform the action do not contain any parameters whose values the attacker cannot determine or guess. For example, when causing a user to change their password, the function is not vulnerable if an attacker needs to know the value of the existing password.

Cross-site scripting

Description

Cross-site scripting is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy

Cross-site scripting (**XSS**) is a security breach that takes advantage of dynamically generated Web pages. In an **XSS** attack, a Web application is sent with a **script** that activates when it is read by an unsuspecting user's browser or by an application that has not protected itself against **cross-site scripting**.

Unit-2

Software-based **Fault Isolation** (SFI) is a **software**-instrumentation technique at the machine-code level for establishing logical protection domains within a process. ... In SFI, protection domains stay within the same process, incurring low overhead when switching between domains.

Definition of: fault **isolation**. fault **isolation**. Determining the cause of a problem.

Also known as "fault diagnosis," the term may refer to hardware or software, but always deals with methods that can **isolate** the component, device or software module causing the **error**.

A **VM** is an **isolated** environment with access to a subset of physical resources of the computer system. Each **VM** appears to be running on the bare hardware, giving the appearance of multiple instances of the same computer, though all are supported by a single physical system.

A kernel-mode rootkit alters components within the computer operating system's core, known as the kernel. Some of these rootkits resemble device drivers or loadable modules, giving them unrestricted access to the target computer. These rootkits avoid detection by operating at the same security level as the OS. Examples include FU, Knark, Adore, Rkit and Da IOS.

Bootkit

A bootkit is a type of kernel-mode rootkit that infects the master boot record, volume boot record or boot section during computer startup. The malware loader persists through the transition to protected mode when the kernel has loaded and is thus able to subvert the kernel. Examples include Olmasco, Rovnix and Stoned Bootkit.

User-mode Rootkit

The user-mode rootkit replaces executables and system libraries and modifies the behavior of application programming interfaces. It alters the security subsystem and displays false information to administrators of the target computer. It can intercept system calls and filter output in order to hide processes, files, system drivers, network ports, registry keys and paths, and system services. Examples of this type of rootkit include Vanquish, Aphex and Hacker Defender.

Virtual Rootkit

A virtual, or hypervisor, rootkit hosts the target OS as a virtual machine, enabling it to intercept hardware calls made by the original OS. The rootkit does not have to modify the kernel to subvert the operating system. So far, this type of rootkit is only a proof of concept.

Firmware Rootkit

A firmware rootkit uses device or platform firmware to create a persistent malware image in the router, network card, hard drive or the basic input/output system (BIOS). The rootkit is able to remain hidden because firmware is not usually inspected for code integrity. These rootkits can be used for legitimate purposes, such as anti-theft technology preinstalled in BIOS images by the vendor, but they can also be exploited by cybercriminals. Examples include Cloaker and

VGA rootkit.

Rooting out Rootkits

So what can IT administrators due to counter the threats posed by rootkits?

Preventing Rootkit Infections

In their chapter in the Information Security Management Handbook, Sixth Edition, Volume 2, security researchers E. Eugene Schultz and Edward Ray recommend that enterprises consider the following measures to prevent rootkit infections:

- using intrusion detection and prevention tools such as rootkit scanners
- applying vulnerability patches in a timely manner
- configuring systems according to security guidelines and limiting services that can run on these systems
- adhering to the least privilege principle
- deploying firewalls that can analyze network traffic at the application layer
- using strong authentication
- performing regular security maintenance
- limiting the availability of compiler programs that rootkits exploit

Detecting Rootkits

Once an infection takes place, things get tricky. The researchers caution that detecting and removing a rootkit is difficult. However, a rootkit can be detected by trained investigators and analysis tools, such as rootkit scanners, which uncover clues to the presence of the rootkit. Major security firms, such as Symantec, Kaspersky Lab and Intel Security (McAfee), offer rootkit scanners to enterprise customers.

Some of the telltale signs that a rootkit is present include unexplained changes in target systems, strange files in the home directory of root or unusual network activity.

Cryptographer and computer programmer Thomas Pornin noted that the rootkit needs to maintain an entry path for the attacker, creating an opportunity for detection. In a post on *Information Security Stack Exchange*, Pornin recommends that IT administrators reboot the computer on a live CD or USB key and then inspect the hard disk. "If the same files do not look identical, when inspected from the outside (the OS booted on a live CD) and from the inside, then this is a rather definite sign of foul play," he wrote.

Another contributor to the Information Security Stack Exchange who goes by the moniker user2213 explained that another way to detect a rootkit is to use spurious device codes on devices that do not normally respond to the codes. "If you get anything other than the relevant 'Not implemented' error code on your system, something strange is going on."

User2213 also suggested mounting the system drive on a different PC to see if an incorrect file system size or unexpected files come up. This could be an indication of a rootkit. "Unfortunately, there aren't generic red flags for rootkits in general -- the battle is more cat-and-mouse," the writer noted.

Removing Rootkits

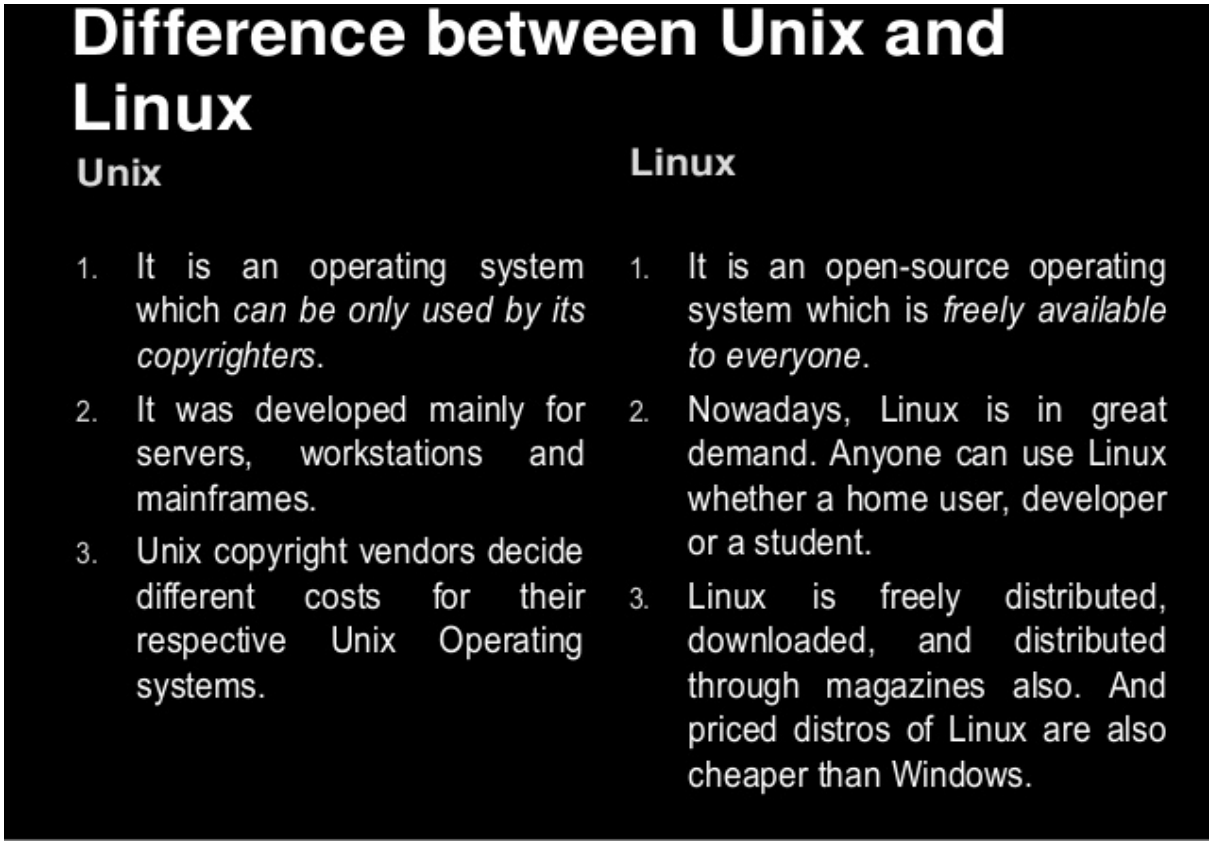
Removing a rootkit is a challenge because it runs with a full set of system privileges, which means it could have done anything to the system. Schultz and Ray recommend making an image backup and then rebuilding the compromised system using the original installation media; otherwise, the malicious code or unauthorized changes could continue even after the rootkit is "deleted." Security patches then need to be installed and a vulnerability scan performed.

In sum, the best strategy to deal with rootkit threats is to stop the rootkit from infecting computers in your network through security best practices such as patch management and regular maintenance, and specialized tools such as rootkit scanners and firewalls. Should your computers become infected anyway, you need to rebuild the compromised computer from the ground up to ensure that the rootkit is eradicated.

A **rootkit** is a malicious software that allows an unauthorized user to have privileged access to a computer and to restricted areas of its software.
A **rootkit** may contain a number of malicious tools such as keyloggers, banking credential stealers, password stealers, antivirus disablers, and bots for DDoS attacks.

Buffer Overflow Attack

A **buffer** is a temporary area for data storage. When more data (than was originally allocated to be stored) gets placed by a program or system process, the extra data overflows. It causes some of that data to leak out into other buffers, which can corrupt or overwrite whatever data they were holding.
In a **buffer-overflow attack,** the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user; for example, the data could trigger a response that damages files, changes data or unveils private information.
Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user's input. There are two types of buffer overflows: stack-based and heap-based. Heap-based, which are difficult to execute and the least common of the two, attack an application by flooding the memory space reserved for a program. Stack-based buffer overflows, which are more common among attackers, exploit applications and programs by using what is known as a stack:



Confinement is a mechanism for enforcing the **principle** of least privilege. The problem is that the **confined** process needs to transmit data to another process. ... The **confinement** mechanism must distinguish between transmission of authorized data and the transmission of unauthorized data.

Unix is a computer Operating System which is capable of handling activities from multiple users at the same time. The development of Unix started around 1969 at AT&T Bell Labs by Ken Thompson and Dennis Ritchie

The Unix operating system is a set of programs that act as a link between the computer and the user.

The computer programs that allocate the system resources and coordinate all the details of the computer's internals is called the **operating system** or the **kernel**.

Users communicate with the kernel through a program known as the **shell**. The shell is a command line interpreter; it translates commands entered by the user and converts them into a language that is understood by the kernel.

The main concept that unites all the versions of Unix is the following four basics −

- **Kernel** − The kernel is the heart of the operating system. It interacts with the

hardware and most of the tasks like memory management, task scheduling and file management.

- **Shell** − The shell is the utility that processes your requests. When you type in a command at your terminal, the shell interprets the command and calls the program that you want. The shell uses standard syntax for all commands. C Shell, Bourne Shell and Korn Shell are the most famous shells which are available with most of the Unix variants.
- **Commands and Utilities** − There are various commands and utilities which you can make use of in your day to day activities. **cp**, **mv**, **cat** and **grep**, etc. are few examples of commands and utilities. There are over 250 standard commands plus numerous others provided through 3rd party software. All the commands come along with various options.
- **Files and Directories** − All the data of Unix is organized into files. All files are then organized into directories. These directories are further organized into a tree-like structure called the

n Unix, there are three basic types of files −

- **Ordinary Files** − An ordinary file is a file on the system that contains data, text, or program instructions. In this tutorial, you look at working with ordinary files.
- **Directories** − Directories store both special and ordinary files. For users familiar with Windows or Mac OS, Unix directories are equivalent to folders.
- **Special Files** − Some special files provide access to hardware such as hard drives, CD-ROM drives, modems, and Ethernet adapters. Other special files are similar to aliases or shortcuts and enable you to access a single file using different names.

Chroot on Unix operating systems is an operation that changes the apparent root directory for the current running process and its children. A program that is run in such a modified environment cannot name files outside the designated directory tree

Confinement

The confinement problem deals with preventing a process from taking disallowed actions. Consider a client/server situation: the client sends a data request to the server; the server uses the data, performs some function, and sends the results (data) back to the client. In this case the confinement problem deals with preventing a server from leaking information that the user of that service considers confidential. Access control affects the function of the server in **2 ways Goal of service provider** 1. **The server must ensure** that the resources it accesses on behalf of the client include only those resources that the client is authorized to access. Goal of the service user

2. The server must ensure that it does not reveal the client's data to any other entity not authorized to see the client's

DEFINITION

threat modeling

Threat modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. In this context, a threat is a potential or actual adverse event that may be malicious (such as a denial-of-service attack) or incidental (such as the failure of a storage device), and that can compromise the assets of an enterprise.

The key to threat modeling is to determine where the most effort should be applied to keep a system secure. This is a variable that changes as new factors develop and become known, applications are added, removed, or upgraded, and user requirements evolve. Threat modeling is an iterative process that consists of defining enterprise assets, identifying what each application does with respect to these assets, creating a security profile for each application, identifying potential threats, prioritizing potential threats, and documenting adverse events and the actions taken in each case.

Threat modeling methodologies for IT purposes

Conceptually, a threat modeling practice flows from a methodology. Numerous threat modeling methodologies are available for implementation. Typically, threat modeling has been implemented using one of four approaches independently, asset-centric, attacker-centric, and software-centric. Based on volume of published online content, the four methodologies discussed below are the most well known.

STRIDE methodology

The STRIDE approach to threat modeling was introduced in 1999 at Microsoft, providing a mnemonic for developers to find 'threats to our products'.[9] STRIDE, Patterns and Practices, and Asset/entry point were amongst the threat modeling approaches developed and published by Microsoft. References to "the" Microsoft

methodology commonly mean STRIDE and Data Flow Diagrams.

P.A.S.T.A.

The Process for Attack Simulation and Threat Analysis (PASTA) is a seven-step, risk-centric methodology.[10] It provides a seven-step process for aligning business objectives and technical requirements, taking into account compliance issues and business analysis. The intent of the method is to provide a dynamic threat identification, enumeration, and scoring process. Once the threat model is completed security subject matter experts develop a detailed analysis of the identified threats. Finally, appropriate security controls can be enumerated. This methodology is intended to provide an attacker-centric view of the application and infrastructure from which defenders can develop an asset-centric mitigation strategy.

Trike

The focus of the Trike methodology[11] is using threat models as a risk-management tool. Within this framework, threat models are used to satisfy the security auditing process. Threat models are based on a “requirements model.” The requirements model establishes the stakeholder-defined “acceptable” level of risk assigned to each asset class. Analysis of the requirements model yields a threat model from which threats are enumerated and assigned risk values. The completed threat model is used to construct a risk model based on asset, roles, actions, and calculated risk exposure.

VASTE

VAST is an acronym for Visual, Agile, and Simple Threat modeling.[12] The underlying principle of this methodology is the necessity of scaling the threat modeling process across the infrastructure and entire SDLC, and integrating it seamlessly into an Agile software development methodology. The methodology seeks to provide actionable outputs for the unique needs of various stakeholders: application architects and developers, cybersecurity personnel, and senior executives. The methodology provides a unique application and infrastructure visualization scheme such that the creation and use of threat models do not require specific security subject matter expertise.

Generally accepted IT threat modeling processes

All IT-related threat modeling processes start with creating a visual representation of the application and / or infrastructure being analyzed. The application / infrastructure is decomposed into various elements to aid in the analysis. Once completed, the visual representation is used to identify and enumerate potential threats. Further analysis of the model regarding risks associated with identified threats, prioritization of threats, and enumeration of the appropriate mitigating controls depends on the methodological basis for the threat model process being utilized.

Vulnerability: a software defect with security consequences

Threat: a potential danger to the software

Attack: an attempt to damage or gain access to the system

Exploit: a successful attack Trust Boundary: where the level of trust changes for data or code

---

Confidentiality

Confidentiality refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data. Imagine your bank records. You should be able to access them, of course, and employees at the bank who are helping you with a transaction should be able to access them, but no one else should. A failure to maintain confidentiality means that someone who shouldn't have access has managed to get it, through intentional behavior or by accident. Such a failure of confidentiality, commonly known as a *breach*, typically cannot be remedied. Once the secret has been revealed, there's no way to un-reveal it. If your bank records are posted on a public website, everyone can know your bank account number, balance, etc., and that information can't be erased from their minds, papers, computers, and other places. Nearly all the major security incidents reported in the media today involve major losses of confidentiality.
So, in summary, a breach of confidentiality means that someone gains access to information who shouldn't have access to it.

Integrity

Integrity refers to ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine. Imagine that you have a website and you sell products on that site. Now imagine that an attacker can shop on your web site and maliciously alter the prices of your products, so that they can buy anything for whatever price they choose. That would be a failure of integrity, because your information—in this case, the price of a product—has been altered and you didn't authorize this alteration. Another example of a failure of integrity is when you try to connect to a website and a malicious attacker between you and the website redirects your traffic to a different website. In this case, the site you are directed to is not genuine.

Availability

Availability means that information is accessible by authorized users. If an attacker is not able to compromise the first two elements of information security (see above) they may try to execute attacks like denial of service that would bring down the server, making the website unavailable to legitimate users due to lack of availability.