BCA

Semester: V

MIS and E-Business

E-commerce Security and Fraud Issues and Protection

Unit-4: E-commerce Security and Fraud Issues and Protection

Security

- Information security, or information systems security, refers to a variety of activities and methods that protect information systems, data, and procedures from any action designed to destroy, modify, or degrade the systems and their operations.
- Computer security in general refers to the risks and protection of data, networks, computer programs, computer power, and other elements of computerized information systems.
- It is a very broad field due to the many methods of attack as well as the many modes of defense.
- The attacks on and defenses for computers can affect individuals, organizations, countries, or the entire Web.
- Computer security aims to prevent, repair, or at least minimize the attacks.
- E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

Threat, attack and attacker

- Anything potential to cause harm to the computer system or organization.
- A threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.
- A threat can be either "intentional" or "accidental" or otherwise a circumstance, capability, action, or event.
- Unintentional threats fall into three major categories: human error, environmental hazards, and malfunctions in the computer system.
- 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.
- An attacker is the individual or organization performing these malicious activities.

Intentional Attacks and Crimes

- Intentional attacks are committed by cybercriminals.
- Types of **intentional attacks** include theft of data, inappropriate use of data (e.g., changing it or presenting it for fraudulent purposes), theft of laptops and other devices and equipment, and/or inserting computer programs to steal data, vandalism or sabotage directed toward the computer or its information system damaging computer resources, losses from malware attacks, creating and distributing viruses, and causing monetary losses due to Internet fraud.
- **Intentional crimes** carried out using computers and the Internet are called cybercrimes, which are done by cybercriminals (criminals for short) that include hackers and crackers. A hacker describes someone who gains unauthorized access to a computer system. A cracker (also known as a black hat hacker) is a malicious hacker with extensive computer experience who may be more damaging.

Basic EC Security Terminology

- **Business continuity plan:** A plan that keeps the business running after a disaster occurs. Each function the business should have a valid recovery capability plan.
- **Cybercrime:** Intentional crime carried out on by using the Internet.
- **Cybercriminal:** A person who intentionally carries out crimes over the internet.
- **Exposure:** An instance of being exposed to losses from an attack that exploits vulnerability (including estimate of damages).
- **Fraud:** Any business activity that uses deceitful practices or devices to deprive another of property or other rights.
- **Vulnerability:** Weakness or fault that can lead to an exposure.
- **Malware:** malicious code such as viruses, worms, Trojan horses, bots, backdoors, spyware, adware, etc.
- **Cyber vandalism:** Intentionally disrupting, defacing or destroying a Web site.

Vulnerable Points in an E-commerce Transaction

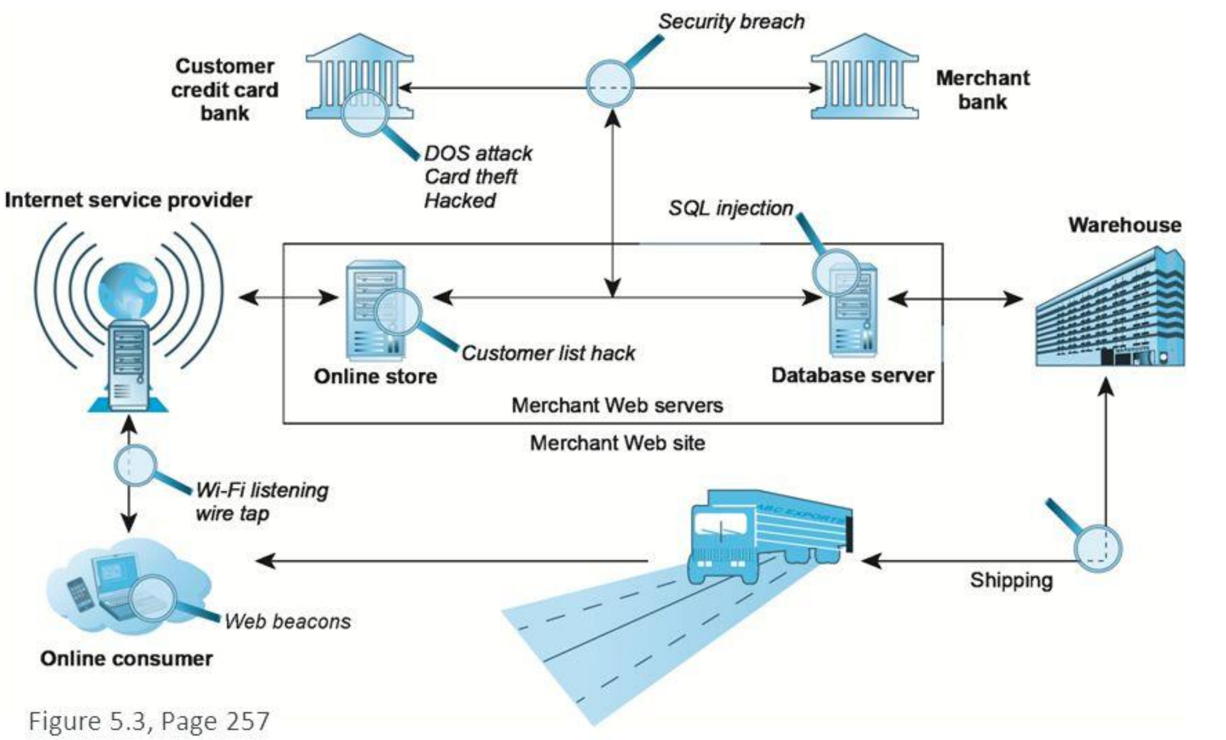
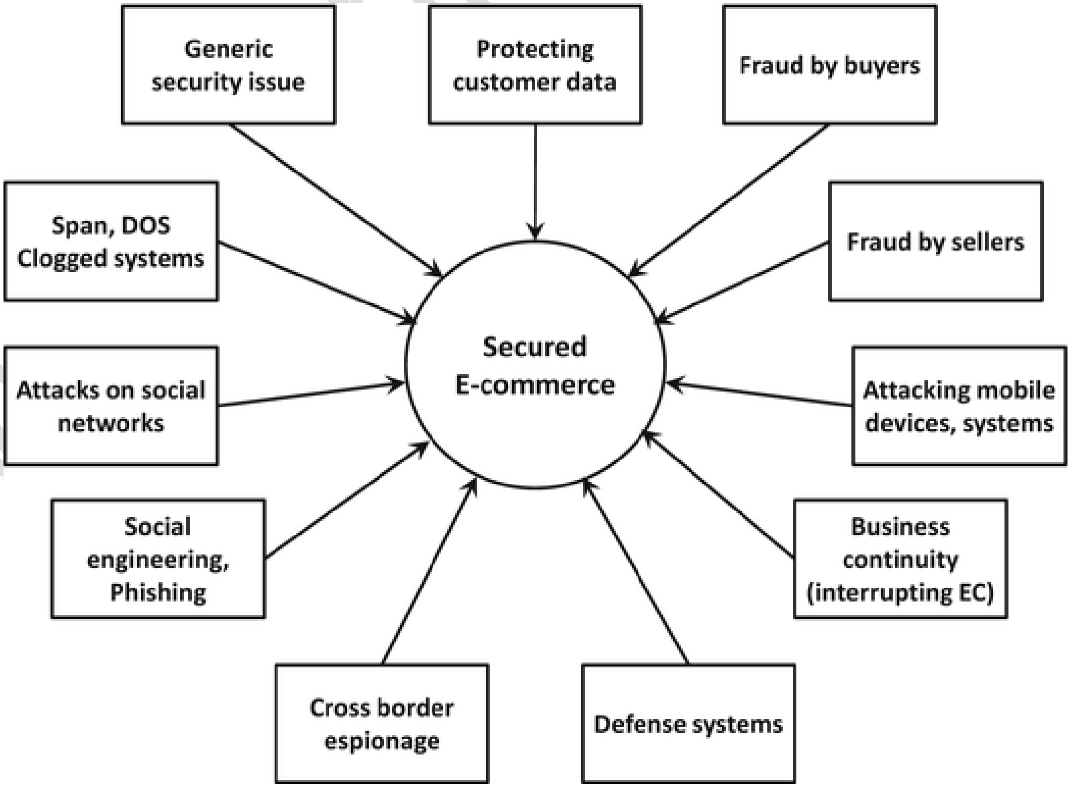


Figure 5.3, Page 257

Slide 5-9

E-Commerce security Concern


Generic security issue
Protecting customer data
Fraud by buyers
Span, DOS Clogged systems
Fraud by sellers
Secured E-commerce
Attacks on social networks
Attacking mobile devices, systems
Social engineering, Phishing
Business continuity (interrupting EC)
Cross border espionage
Defense systems

EC Security Requirements

- **Authentication** is a process used to verify (assure) the real identity of an EC entity, which could be an individual, software agent, computer program, or EC website. For electronic messages, authentication verifies that the sender/receiver of the message is who the person or organization claims to be (the ability to detect the identity of a person/entity with whom you are doing business).
- **Authorization** is the provision of permission to an authenticated person to access systems and perform certain operations in those specific systems.
- **Auditing:** When a person or program accesses a website or queries a database, various pieces of information are recorded or logged into a file. The process of maintaining or revisiting the sequence of events during the transaction, when and by whom, is known as auditing.
- **Availability:** Assuring that systems and information are available to the user when needed and that the site continues to function. Appropriate hardware, software, and procedures ensure availability.
- **Nonrepudiation:** Closely associated with authentication is nonrepudiation, which is the assurance that online customers or trading partners will not be able to falsely deny (repudiate) their purchase, transaction, sale, other obligation. Nonrepudiation involves several assurances, including providing proof of delivery from the sender and proof of sender and recipient identities and the identity of the delivery company.
- **Confidentiality:** For sender, intended receiver should understand message contents using encryption and decryption. For sender, intended receiver should understand message contents.
- **Integrity:** sender and receiver want to make sure that the message are not altered without detection.

Technical Malware attack

Hackers often use several software tools (which unfortunately are readily and freely available over the Internet together with tutorials on how to use them) in order to learn about vulnerabilities as well as attack procedures.

Malware (Malicious Software): Viruses, Worms, and Trojan Horses:

- Malware is a software program that, when spread, is designed to infect, alter, damage, delete, or replace data or an information system without the owner's knowledge or consent.
- Malware is a comprehensive term that describes any malicious program or software (e.g., a virus is a "subset" of malware).
- Malware attacks are the most frequent security breaches.
- Computer systems infected by malware take orders from the criminals and do things such as send spam or steal the user's stored passwords. (key logger)

Viruses

- A virus is programmed software inserted by criminals into a computer to damage the system; running the infected host program activates the virus. A virus has two basic capabilities.
- First, it has a mechanism by which it spreads.
- Second, it can carry out damaging activities once it is activated.
- Sometimes a particular event triggers the virus's execution.
- The problem is that existing virus protection systems may not work against new viruses, and unfortunately, new viruses are created all the time.

Worms

Unlike a virus, a worm can replicate itself automatically (as a "stand-alone" without any host or human activation). Worms use networks to propagate and infect a computer or handheld device and can even spread via instant messages or e-mail. In addition, unlike viruses that generally are confined within a target computer, a worm can infect many devices in a network as well as degrade the network's performance.

Trojan horse

A Trojan horse is a program that seems to be harmless or even looks useful but actually contains a hidden malicious code. Users are tricked into executing an infected file, where it attacks the host, anywhere from inserting pop-up windows to damaging the host by deleting files, spreading malware, and so forth. e.g., Zeus, W32.

Heartbleed

- Heartbleed is a flaw in OpenSSL, the open-source encryption standard used by majority of websites that need to transmit the data that users want to keep secure. It basically gives you a secure line when you're sending an e- mail or chatting on IM."
- The potential damage may be large. In theory, any data kept in the active memory can be pulled out by the bug. Hackers can even steal encryption keys that enable them to read encrypted messages. About 650 million websites may be affected. The only advice provided by experts is to change the online passwords.

Crypto Locker

Discovered in September 2013, Crocker is a ransomware Trojan bug. This malware can come from many sources including e-mail attachments and can encrypt files on your computer, so that you cannot read these files. The malware owner then offers to decrypt the data in exchange for a Bitcoin or similar untraceable payment system.

- **A denial-of-service (DoS) attack** is "a malicious attempt to make a server or network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet."
- This causes the system to crash or become unable to respond in time, so the site unavailable. One of the most popular types of DoS attacks occurs when a hacker "floods" the system by overloading the system with "useless traffic" so user is prevented from accessing their e-mail, websites, etc.
- A DoS attack is a malicious attack caused by one computer and one Internet connection as opposed to a distributed denial-of-service **(DDoS)** attack, which involves many devices and multiple Internet connections. For example, the attack on the Dyn(closing case) was done by thousands of computers taken hostage by the hackers.

Page hijacking or pagejacking is illegally copying website content so that a user can be misdirected to a different website. Social media accounts are sometimes hijacked for the purpose of stealing the accountholder's personal information. For example, Justin Bieber's 50 million followers fell victim to this method when Bieber's Twitter account was hijacked in March 2014.

Botnets

A botnet (also knowered b as "zombie army") is a malicious software that criminals distribute to infect a large number of hijacked Internet-connected computers controlled by hackers. These infected computers then form a "botnet," causing the personal computer to "perform unauthorized attacks over the Internet" without the user's knowledge. Unauthorized tasks include sending spam and e- máil messages, attacking computers and servers, and committing other kinds of fraud, causing the user's computer to slow down. Each attacking computer is considered computer robot. A botnet made up of 75,000 systems infected, in 2010, with Zeus Trojan contaminated computers.

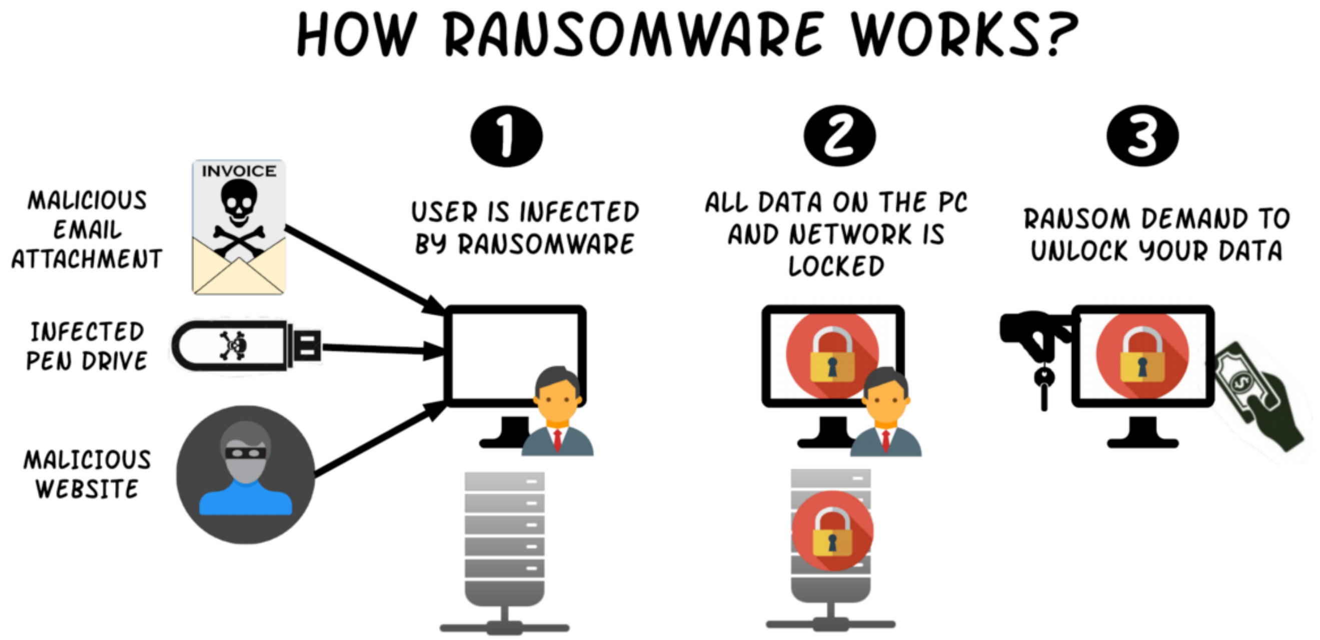
Malvertising

Malvertising is a malicious form of Internet advertising used to spread malware. Malvertising is accomplished by hiding malicious code within relatively safe online advertisements.

Note that hackers are targeting ads to hide malware at accelerating rates. For example, in 2013, Google disabled ads from over 400,000 sites that were hiding malware. A final word: If you get an e-mail that congratulates you on winning a large amount of money and asks you to "Please view the attachment," don't!

Ransomware

Attacker encrypt and lock digital files by using malware and demand a ransom before the system is unlocked it. A method of attack where the attacker encrypts files so the victim cannot open them unless they pay a ransom.


HOW RANSOMWARE WORKS?
MALICIOUS EMAIL ATTACHMENT
INVOICE
INFECTED PEN DRIVE
MALICIOUS WEBSITE
1
USER IS INFECTED BY RANSOMWARE
2
ALL DATA ON THE PC AND NETWORK IS LOCKED
3
RANSOM DEMAND TO UNLOCK YOUR DATA

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires and get to know about the conversation. It is also called wiretapping applied to the computer networks.

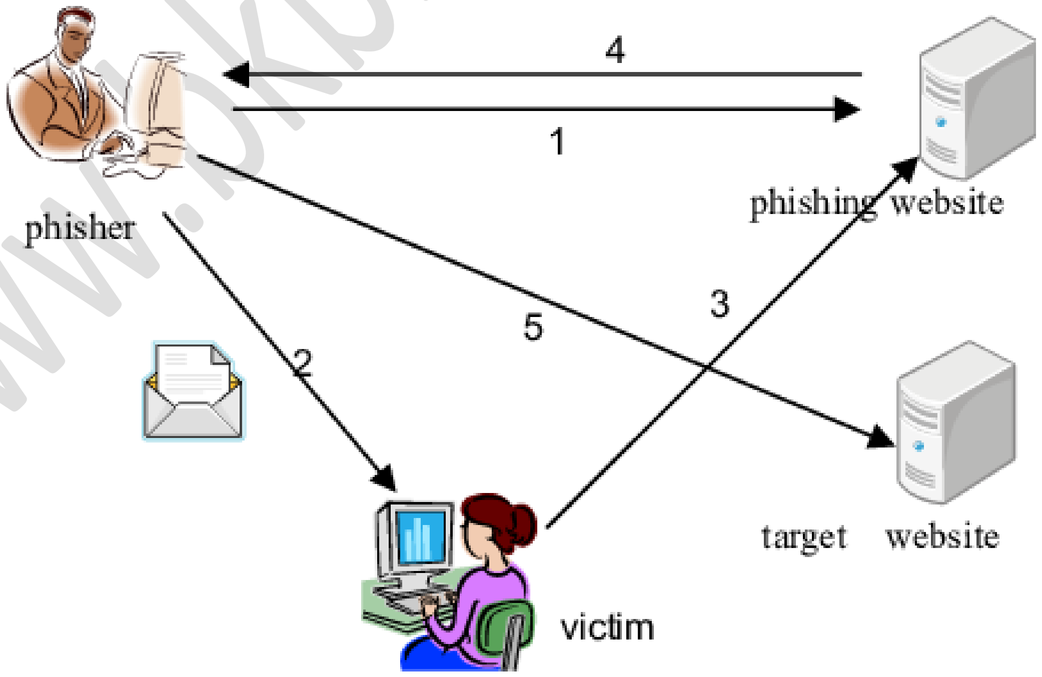
A **packet analyzer** is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. Packet capture is the process of intercepting and logging traffic.

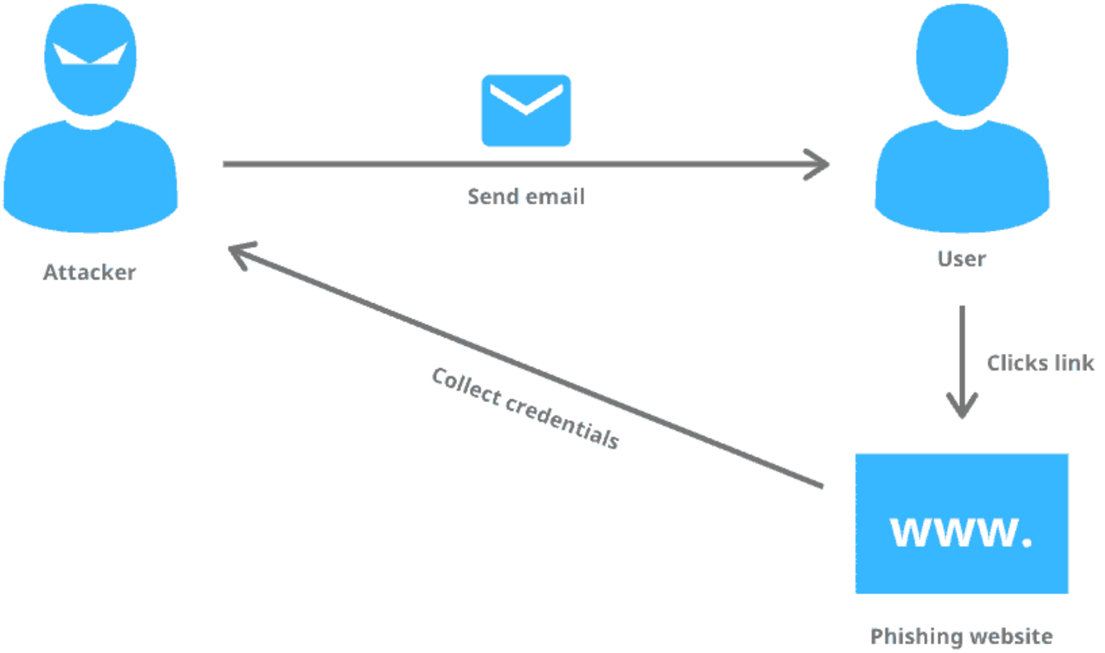
Non-Technical malware attack

- Software and systems knowledge are used to perpetrate technical attacks. Insufficient use of antivirus and personal firewalls and unencrypted communication are the major reasons for technical vulnerabilities.
- Nontechnical organizational attacks are those where the security of a network or the computer is compromised (e.g., lack of proper security awareness training). We consider financial fraud, spam, social engineering, that includes phishing, and other fraud methods, as nontechnical.
- Many nontechnical methods also use some malware in their attacks. The goals of social engineering are to gain unauthorized access to systems or information by persuading unsuspected people to disclose personal information that is used by criminals to commit fraud and other crimes.

Social Engineering and Fraud

- **Social engineering** refers to a collection of methods where criminals use human psychology to persuade or manipulate people into revealing their confidential information, or their employment information, so they can collect information for illegal activities.
- The hacker may also attempt to get access to the user's computer in order to install malicious software that will give hackers control over the person's computer.
- **Social phishing** is a fraudulent process of acquiring confidential information, such as credit card or banking details, from unsuspecting computer users.
- A phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, well-known, popular company, bank, school, or public institution.
- The user is instructed to enter a corrupted website, where he or she may be tricked into submitting confidential information (e.g., being asked to "update" information). Sometimes phishers install malware to facilitate the extraction of information.





Pharming

- Similar to phishing, pharming is a scam where malicious code installed on a computer is used to redirect victims to bogus (fake) websites without the victims' knowledge or consent.
- Pharming can be more dangerous than phishing since users have no idea that they have been redirected to a fake website.
- **Identity theft** is crime. It refers to wrongfully obtaining and using the identity of another person in some way to commit crimes that involve fraud or deception (e.g., for economic gain). Victims can suffer serious damages.

Identity Fraud

Identity fraud refers to assuming the identity of another person or creating a fictitious person and then unlawfully using that identity to commit a crime. Typical activities include:

- Opening a credit card in the victim's name.
- Making a purchase a false identity (e.g., using another's identity to buy goods).
- Business identity theft is using another's business name to obtain credit or to get into a partnership
- Posing as another to commit a crime
- Conducting money laundering (e.g., organized crime) using a fake identity

Spam Attacks:

- E-mail spam, also known as junk e-mail or just spam, occurs when almost identical messages are e-mailed to many recipients in bulk (sometimes millions of unsolicited e-mails).
- Spammers can purchase millions of e-mail addresses and then format the addresses, cut and paste the messages, and press "send." Mass e-mail software that generates, sends, and automates spam e-mail sending is called Ratware.
- The situation is better today (2017) due to improved filtering of junk mail.
- According to Symantec, most of messages on corporate networks are e-mail spam. Nearly 58% of spam came from botnets; the worst botnet was called Dotnet.

- **Spyware** is a tracking software that is installed by criminals, without the user's consent, in order to gather information about the user and direct it to advertisers or other third parties.
- Once installed the spyware program tracks and records the user's movements on the Internet. Spyware may contain malicious code redirecting Web browser activity.
- Spyware can also slow surfing speeds and damage a program's functionality. Spyware usually is installed when you download freeware or shareware.

EC defense Strategy

EC security needs to address by the organization. An EC security framework that defines the high level categories of assurance and their controls is presented. The major categories are regulatory, financial, and marketing operations. Only the key areas are listed in bellow:

1. Defending access to computing systems, data flow, and EC transactions.

This includes three topics: Access control (including biometrics), encryption of contents, and public key infrastructure (PKI). This line of defense provides comprehensive protection when applied together: Intruders that circumvent the access control will face encrypted material even if they pass a firewall.

2. Defending EC networks.

This includes mainly protection by firewalls. The firewall isolates the corporate network and computing devices from the Internet that are poorly secured. To make the Internet more secure, we can use virtual private networks. In addition to these measures, it is wise to use intrusion detection systems. A protected network means securing the incoming e-mail, which is usually unencrypted. It is also necessary to protect against viruses and other malware that are transmitted via the networks.

3. General, administrative, and application controls. These are a variety of safeguards that are intended to protect computing assets by establishing guidelines, checking procedures, and so forth.

4. Protection against social engineering and fraud. Several defense methods are used against spam, phishing, and spyware.

5. Disaster preparation, business continuity, and risk management. These topics are managerial issues that are supported by software.

6. Implementing enterprise-wide security programs. To deploy the abovementioned defense implementation strategy.

7. Conduct a vulnerability assessment and a penetration test.

8. Back up the data.

Access Control

Access control determines who (person, program, or machine) can legitimately use the organization's computing resources (which resources, when, and how).

Authorization and Authentication

Access control involves authorization (having the right to access) and authentication, which is also called user identification (user ID), i.e., proving that the user is who he or she claims to be. Each user has a distinctive identification that differentiates it from other users. Typically, user identification is used together with a password.

Authentication

After a user has been identified, the user must be authenticated. Authentication is the process of verifying the user's identity and access rights. Verification of the user's identity usually is based on one or more characteristics that distinguish one individual from another.

Biometrics System

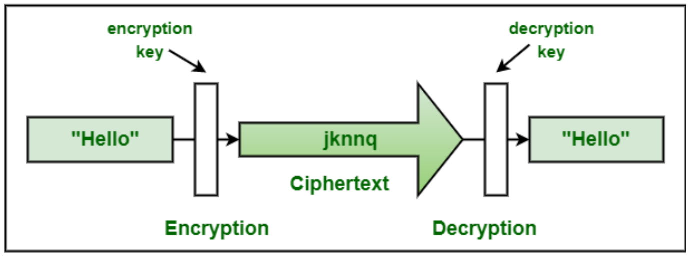
A biometric authentication is a technology that measures and analyzes the identity of people based on measurable biological or behavioral characteristics or physiological signals. Biometric systems can identify a previously registered person by searching through a database for a possible match based on the person's observed physical, biological, or behavioral traits, or the system can verify a person's identity by matching an individual's measured biometric traits against a previously stored version. Examples of biometric features include fingerprints, facial recognition, DNA, palm print, hand geometry, iris recognition, and even odor/scent. Behavioral traits include voice ID, typing rhythm (keystroke dynamics), and signature verification.

A brief description of some of these follows:

- **Thumbprint or fingerprint.** A thumb- or fingerprint (finger scan) of users requesting access is matched against a template containing the fingerprints of authorized.
- **Retinal scan.** A match is sought between the patterns of the blood vessels in the retina of the access seekers against the retinal images of authorized people stored in a source database.
- **Voice ID (voice authentication).** A match is sought between the voice pattern of the access seekers and the stored voice patterns of the authorized people.
- **Facial recognition**. Computer software that views an image or video of a person and compares it to an image stored in a database (used by Amazon.com and Alibaba).
- **Signature recognition.** Signatures of access seekers are matched against stored authentic signatures.

Encryption and PKI (Public Key Infrastructure)

- The word "cryptography" derives from the Greek word for "secrete writing".
- Cryptography is a process associated with changing **plaintext** (ordinary text, or clear text) into **cipher text** (a process called **encryption**), and then backs again (known as **decryption**).
- It is the conversion of into a secret code for protection of privacy using a specific algorithm and secret key.
- It is used to protect e-mail messages, credit card information, and corporate data.
- The primary goal of cryptography is to conceal (hide) data to protect it against unauthorized third-party access by applying encryption.
- The more theoretical or mathematical effort is required for an unauthorized third party to recover data, the stronger is the encryption.



Cryptography

Encryption and decryption in cryptography

- **Encryption** is the process of transforming plain text or data into cipher text that cannot be read by anyone outside of the sender and the receiver.
- **Decryption** is the process of taking encrypted text or other data and converting it back into original text that we can read and understand.
- The purpose of encryption is to (a) secure stored information (b) To secure information transmission.
- **Plaintext** is ordinary text or clear text which is able to read and understand by computer and human being.
- **Cipher text**- text that has been encrypted and thus cannot be read by anyone besides the sender and the receiver.
- A **key** is a piece of information that allows only those that hold it to encode and decode a message.

How does algorithm work?

- **Substitution cipher -** every occurrence of a given letter is replaced systematically by another.

"HELLO" → "JGNNQ"

- **Transposition cipher**- the ordering of the letters in each word is changed in systematic way

“HELLO” → "OLLEH"

General Requirement of encryption and decryption

- Consider an e-commerce scenario where Alice, a purchasing agent, wants to order some products from Bob, her supplier.
- Requirements for the transaction:

1. Alice wants to be sure that she is really dealing with Bob and not an impostor (**authentication**).
2. Bob wants to know that Alice is really Alice and not an impostor (**authentication**), because Alice gets special Prices as negotiated.
3. Alice wants to keep the order secret from her competitors; and Bob does not want other customers to see Alice's special prices (**privacy**).
4. Alice and Bob both want to be sure that crackers cannot change the price or quantity (**integrity**).
5. Bob wants to ensure that Alice cannot later claim that she did not place the order (**non-repudiation**).

Benefits of encryption and decryption

- Allows users to carry data on their laptops, mobile devices, and storage devices (e.g., USB flash drives)
- Protects backup media while people and data are offsite
- Allows for highly secure virtual private networks
- Enforces policies regarding who is authorized to handle specific corporate data
- Ensures compliance with privacy laws and government regulations and reduces the risk of lawsuits
- Protects the organization's reputation and secrets

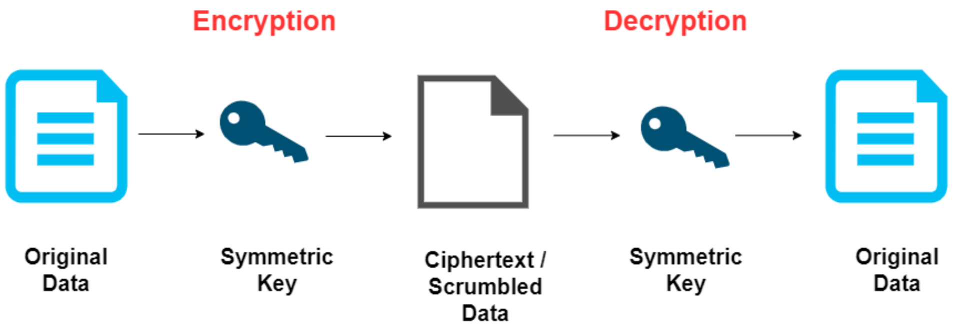
Type of Cryptography

- There are several ways of classifying cryptographic algorithms.
- According to number of keys used for encryption and decryption, can be classified into 3 types:

1. **(Secret/Symmetric)** Key Cryptography: Uses a single key for both encryption and decryption.
2. **(Public/Asymmetric)** Key Cryptography: Uses one key for encryption and another for decryption.
3. **Hash function or Algorithm.**

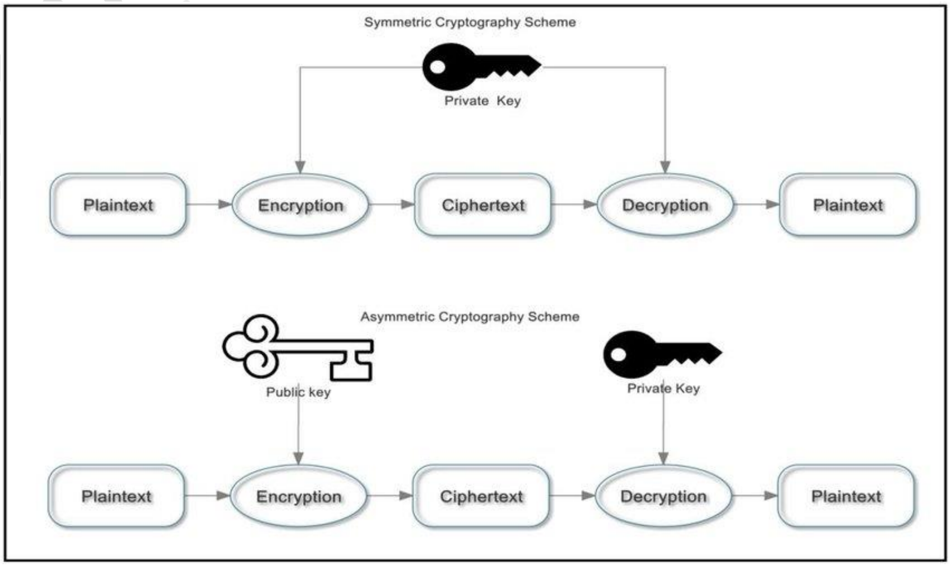
Secret/Symmetric Cryptography

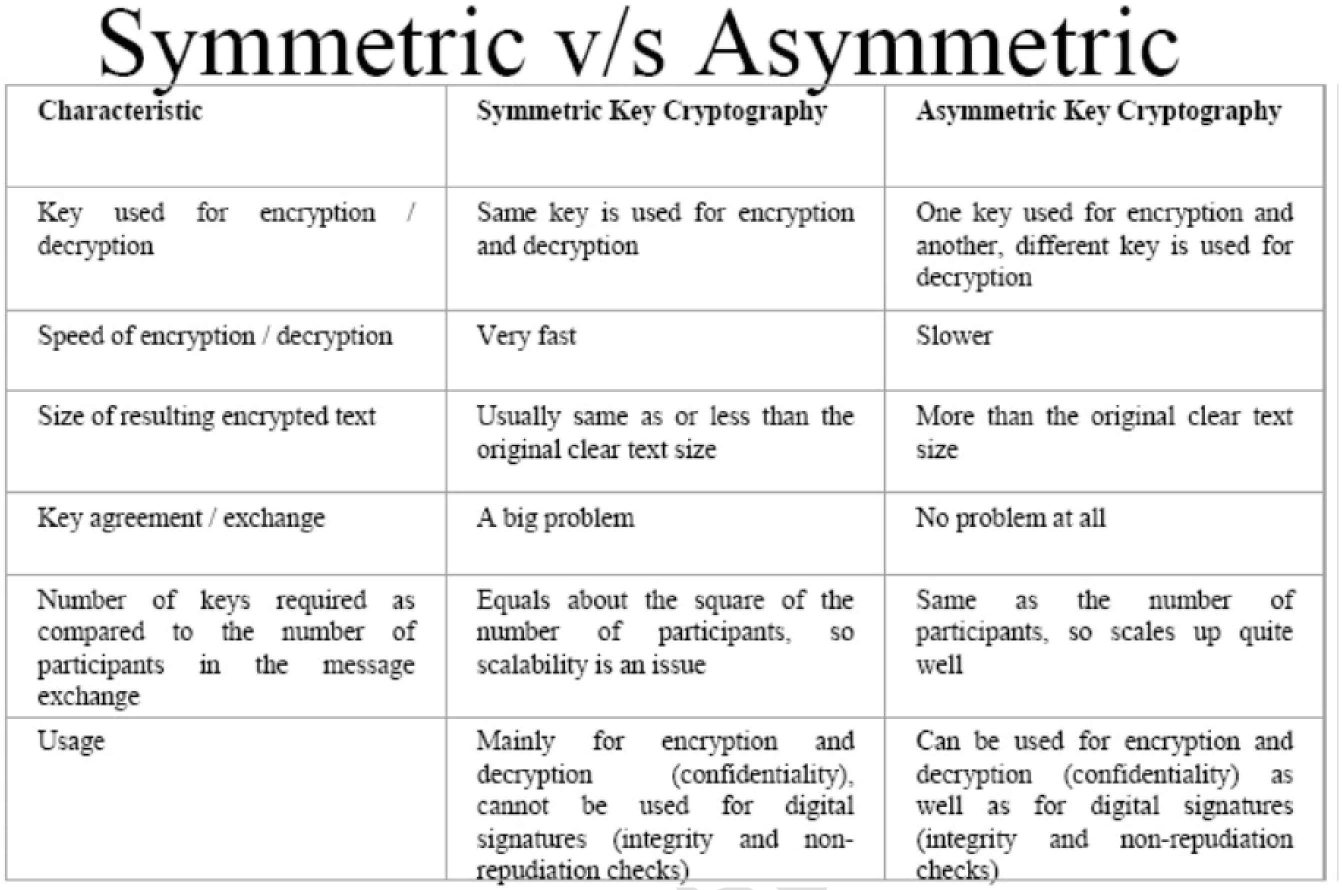
- The message (plaintext) is encrypted into cipher text using a key.
- The resulting cipher text is sent to the recipient, who will decrypt it using the same key.
- Hence, the same key must be known to both parties.
- The best known secret-key system is the Data Encryption Standard (DES). This method is easy and fast to implement but has weaknesses;
- The algorithm that is used to encode the message is easier for attackers to understand, enabling them to more easily decode the message.



Public/Asymmetric Cryptography

- The **public key** can only be used to encrypt the message and the **private key** can only be used to decrypt it.
- This allows a user to freely distribute his or her public key to people who are likely to want to communicate with him or her without worry of compromise because only someone with the private key can decrypt a message.
- To secure information between two users, the sender encrypts the message using the **public key** of the receiver. The receiver then uses the **private key** to decrypt the message.
- The best-known public-key cryptosystem is RSA, named after its inventors: Rivest, Shamir, and Adleman.





Symmetric v/s Asymmetric

Characteristic	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key used for encryption / decryption	Same key is used for encryption and decryption	One key used for encryption and another, different key is used for decryption
Speed of encryption / decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size	More than the original clear text size
Key agreement / exchange	A big problem	No problem at all
Number of keys required as compared to the number of participants in the message exchange	Equals about the square of the number of participants, so scalability is an issue	Same as the number of participants, so scales up quite well
Usage	Mainly for encryption and decryption (confidentiality), cannot be used for digital signatures (integrity and non-repudiation checks)	Can be used for encryption and decryption (confidentiality) as well as for digital signatures (integrity and non-repudiation checks)

Digital Signature or E-signature

- A digital signature is an electronic signature that can be used to **authenticate** the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged (**Integrity**).
- Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily **repudiate** it later.
- A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.
- Digital Signatures are a cryptographic technique and are one of the most important application of asymmetric public-key cryptography.

Digital Signatures features

- Easily transportable.
- Cannot be imitated by someone
- Can be automatically generated.

How does Digital Signature Work?

Digital signature technology ensures the process of digitally signing documents is easy and secure. They provide a platform for sending and signing documents online and work with the appropriate Certificate Authorities to provide trusted digital certificates.

The Certificate Authority you are using determines what kind of information you may be required to provide. There can also be set regulations and rules on to whom you send documents for signing and the way in which you send them.

When you receive a document for signing via email, you must authenticate as per the Certificate Authority's requirements and then proceed to sign the document by filling out an online form.

How do digital signatures work?

The mathematical algorithm generates a public key and a private key that is linked to each other. When a signer electronically signs a document, the mathematical algorithm generates data pertaining to the signed document by the signer, and the data is then encrypted. This data is also called a cryptographic hash. A hash function is a fixed-length string of numbers and letters generated from a mathematical algorithm. This generated string is unique to the file being hashed and is a one-way function, a computed hash cannot be reversed to find other files that may generate the same hash value. The signer has sole access to the private key and this private key is used to encrypt the document data. The encrypted information or encrypted hash is then transmitted and can be decrypted only by the signer's public key.

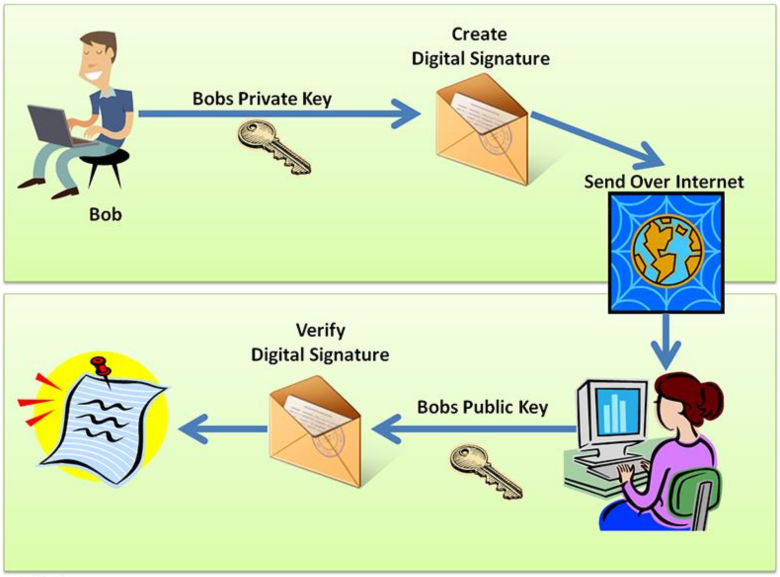
The receiver who receives the document also receives a copy of the signer's public key which is used to decrypt the signature. A cryptographic hash is again generated on the receiver's side. Both cryptographic hashes are checked to validate their authenticity.

The document is considered genuine if they match.

Certificate Authority who are Trust Service Providers (TSP) provides digital certificates to ensure that the keys generated and documents signed are created in a secure environment.

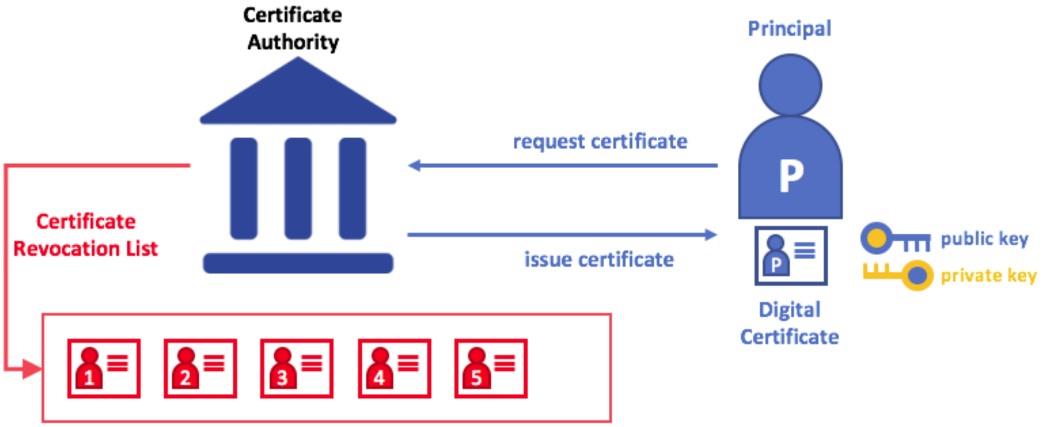
Digital certificates help to validate the holder of a certificate. Digital certificates contain the public key of the sender and are digitally signed by a Certificate authority.

Public key infrastructure (PKI) includes regulations, protocols, rules, people, and systems that aid the distribution of public keys and the identity validation of users with digital certificates and a certificate authority.



What is Digital Certificate and Certification authority?

- Digital certificate a digital document issued by a certification authority that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority, and other identifying information.
- A digital certificate is a digital document issued by a trusted third-party institution known as a Certification authority (CA) that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority (the name of the CA encrypted using the CA's private key), and other identifying information.
- **Certification authorities** that issue, verify, and guarantee digital certificates that are used in e-commerce to assure the identity of transaction partners.
- **Public key infrastructure (PKI**) refers to the CAs and digital certificate procedures that are accepted by all parties. When you sign into a "secure" site, the URL will begin with "https" and a closed lock icon will appear on your browser. This means the site has a digital certificate issued by a trusted CA. It is not, presumably, a spoof site.



Digital certificate and e-commerce site

- Here are several ways the certificates are used in e-commerce. Before initiating a transaction, the customer can request the signed digital certificate of the merchant and decrypt it using the merchant's public key to obtain both the message digest and the certificate as issued. If the message digest matches the certificate, then the merchant and the public key are authenticated. The merchant may in return request certification of the user, in which case the user would send the merchant his or her individual certificate. There are many types of certificates: personal, institutional, Web server, software publisher, and CAs themselves.

All forms of encryption have limitations

It is not effective against insiders

Protecting private keys may also be difficult because they are stored on insecure desktop and laptop computers

Additional technology solutions exist for securing channels of communications, networks, and servers/clients

Digital signatures VS Digital certificate

- **Digital signatures** are electronically generated and can be used to ensure the integrity and authenticity of some data, such as an e-mail message and protect against non-repudiation
- **Digital certificate** is a form of an electronic credential for the Internet. Similar to a driver's license, employee ID card, a Digital certificate is issued by a trusted third party to establish the identity of the certificate holder. The third party who issues the Digital Certificate is known as the Certifying Authority (CA).

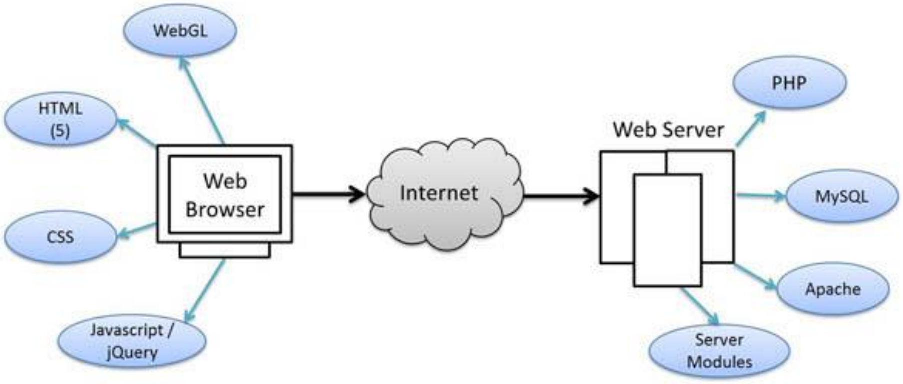
Third party authentication

- Someone who may be indirectly involved but is not a principal party to an arrangement, contract, deal, lawsuit, or transaction. Third party authentication work is to confirm the identify on the behalf of first and second party to make any transaction.

Secure Sockets Layer (SSL)

- The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- E-commerce web sites use SSL (Secure Sockets Layer) to protect important information such as credit card numbers as they travel across the network.
- SSL creates a private communication path between the web browser and the web server, encrypting all information that goes between the systems.
- Most common web browsers have SSL support built in and e-commerce companies can purchase or get freely available web servers that support SSL.
- SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text-leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.
- More specifically, SSL is a security protocol. Protocols describe how algorithms should be used; in this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

How does (SSL) work?



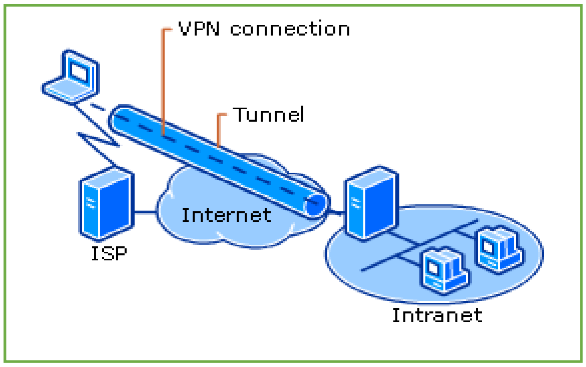
1. Browser connects to a server (website) secured with SSL (https). Browser requests that the server identify itself.
2. Server sends a copy of its SSL Certificate, including the server's public key.
3. Browser checks the certificate root against a list of trusted CAs and that the certificate is unexpired unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
4. Server decrypts the symmetric session key using its private key and sends back acknowledgement encrypted with the session key to start the encrypted session.
5. Server and Browser now encrypt all transmitted data with the session key.

Securing e-commerce networks: Virtual private network (VPN)

- A virtual private network (VPN) is a computer network that uses the Internet to provide remote offices or individual users with secure access to their organization's network by creating an encrypted path to that network.
- Virtual private networks help distant colleagues work together, much like desktop sharing.
- VPNs use both authentication and encryption to secure information from unauthorized persons. Authentication prevents spoofing and misrepresentation of identities. A remote user can connect to a remote private local network using a local ISP.
- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.
- It allows remote users to securely access internal networks via the Internet, using the Point-to-Point Tunneling Protocol (PPTP).

Virtual private network (VPN)

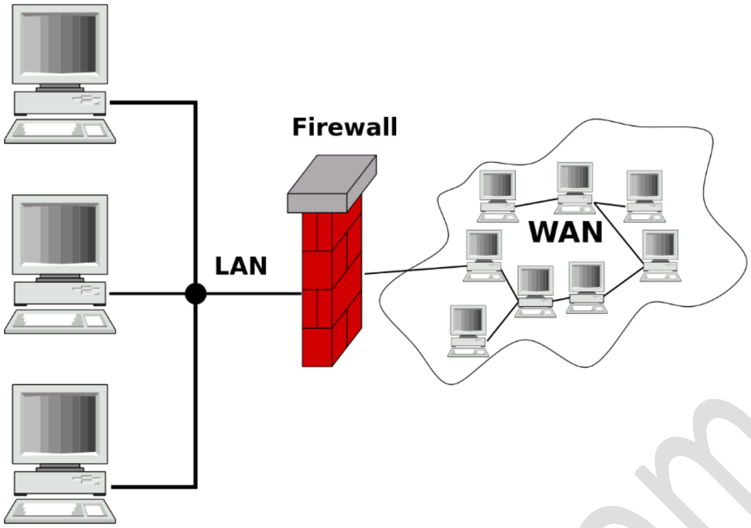
- A virtual private network (VPN) is a secure way of connecting to a private Local Area Network at a remote location, using the Internet or any unsecure public network to transport the network data packets privately, using encryption. The VPN uses authentication to deny access to unauthorized users, and encryption to prevent unauthorized users from reading the private network packets. The VPN be used to send any kind of network traffic securely, including voice, video or data.



Securing e-commerce networks: Firewall

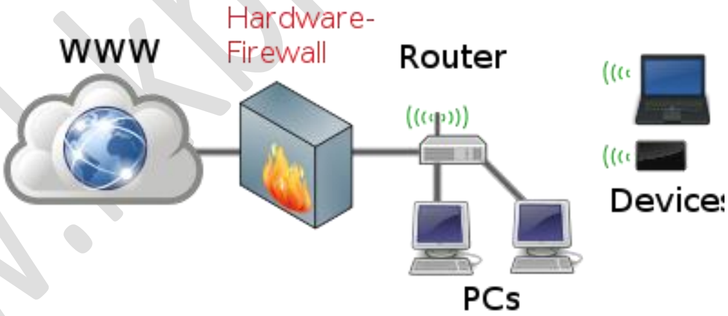
- **A firewall** is a hardware or software designed to permit or deny network transmissions based upon a set of rules and is frequently used to **protect networks from unauthorized access** while permitting legitimate communications to pass.

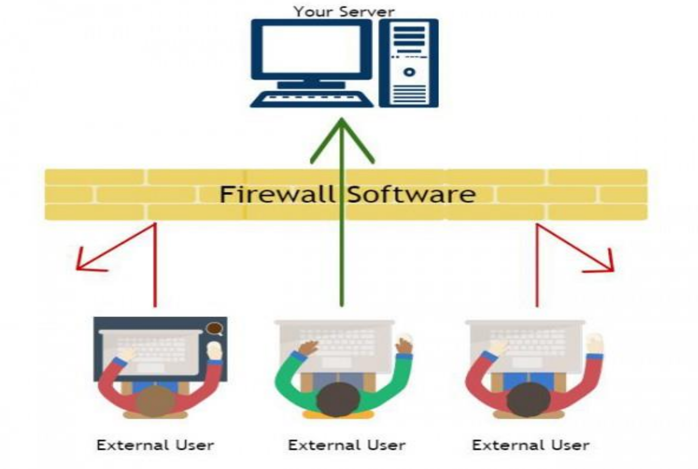
- A Firewall is hardware, Software or a combination of both which is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer.



Hardware V/S Software firewall

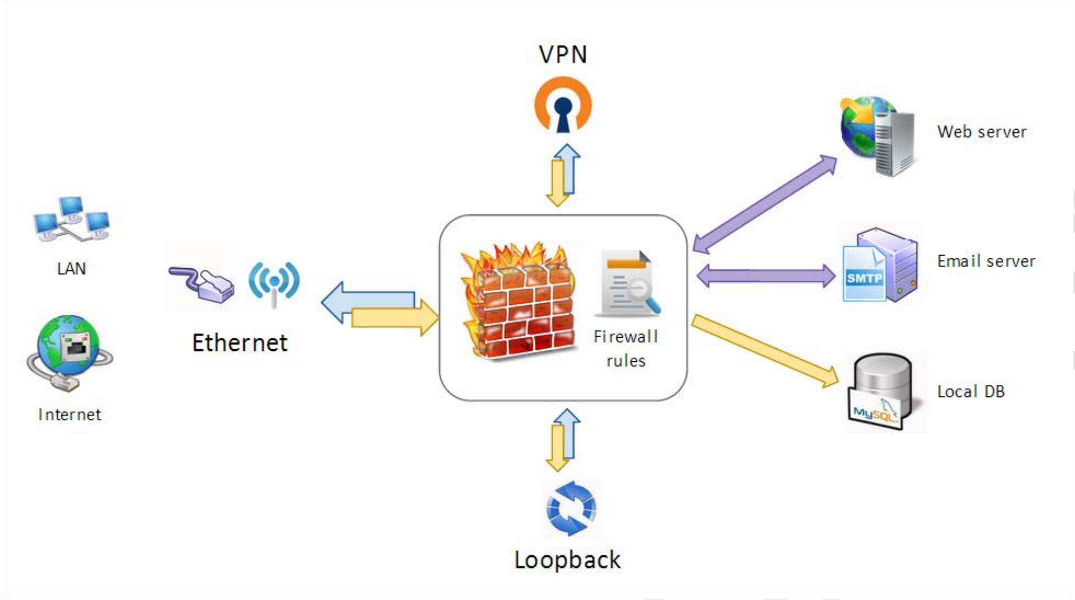
- Hardware Firewalls
  - Protect an entire network
  - Implemented on the router level
  - Usually more expensive, harder to configure.
- Software Firewalls
  - Install in a single computer and protect all
  - Usually less expensive, easier to configure





How does a software firewall work?

- Inspects each individual "packet" of data as it arrives at either side of the firewall.
- Determines whether it should be allowed to pass through or if it should be blocked.



Firewall rules

Allow- traffic that flows automatically it has been deemed.
Block- traffic that blocked because it has been deemed dangerous to your computer.
Ask- asks user weather or not the traffic is allowed to pass through.

What Can a Firewall Do?

- ***Focus for security decisions:*** Stop hackers from accessing your computer.
- ***Can enforce security policy:*** Protects your personal information.
- ***Limits your exposure:*** Blocks "pop up" ads and certain cookies
- ***Can log Internet activity efficiently:*** Determines which programs can access the Internet
- ***Cannot protect against internal threats:*** For example, an angry employee deleting files Or, an employee cooperating with an outside attacker
- ***Cannot protect against attacks that bypass the firewall***
- ***Can't protect against completely new threats***
- ***Can't protect against viruses:*** Different operating systems and applications inside the network need to scan all incoming data...impractical, perhaps impossible.

Types of firewalls

1. ***Packet-filtering Router***

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (Discard or forward)

Advantages:

- Transparency to users
- High speed

Disadvantages:

- Difficulty of setting up packet filter rules
- Lack of Authentication

2. *Application-level gateway*

- Also called proxy server.
- Acts as a relay of application-level traffic
  - User contacts gateway through an application (eg, telnet or FTP)
  - User must authenticate and provide name of remote host
  - Gateway connects to remote host and relays data back to the user
- If code for an application is not implemented, gateway will not support that application
- May be configured to support only certain features of an application

Advantages:

- Higher security than packet filters
- Only need to scrutinize a few allowable applications
- Easy to log and audit all incoming traffic

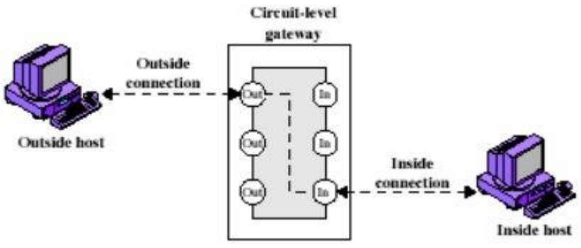
Disadvantages:

- Additional processing overhead on each connection (gateway as splice point).

3. *Circuit-level Gateway*

- Stand-alone system or Specialized function performed by an Application-level Gateway
- Sets up two TCP connections
- The gateway typically relays TCP segments from one connection to the other without examining the contents
- The security function consists of determining which connections will be allowed.

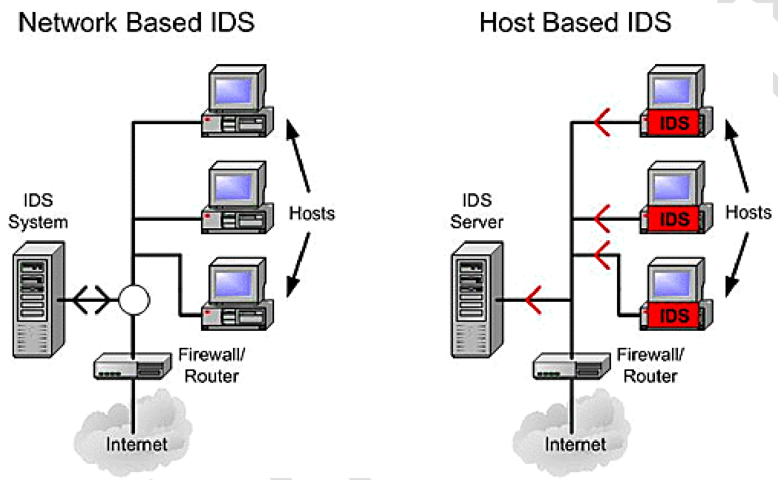
Circuit level gateway



(c) Circuit-level gateway

Characteristics of firewall

- ***Service control***
  Determines the types of Internet services that can be accessed, inbound or outbound.
- ***Direction control***
  Determines the direction in which particular service requests are allowed to flow.
- ***User control***
  Controls access to a service Cording to which user is attempting to access it
- ***Behavior control***
  Controls how particular services are used (e.g. filter e-mail)
- ***All traffic from inside to outside must pass through the firewall.***
- ***Only authorized traffic will be allowed to pass.***



Intrusion Detection Systems (IDS)

- An intrusion detection system (IDS) is a device composed of software and/or hardware designed to monitor the activities of computer networks and computer systems in order to detect and define unauthorized and malicious attempts to access, manipulate, and/or disable these networks and systems.
- 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. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.
- A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Types of IDS:

Network Intrusion Detection System (NIDS):

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

Host Intrusion Detection System (HIDS):

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or, deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

Protocol-based Intrusion Detection System (PIDS):

Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

Application Protocol-based Intrusion Detection System (APIDS):

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

Hybrid Intrusion Detection System:

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Intrusion prevention System (IPS)

- Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity.
- Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

Comparison of IPS with IDS:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

Parameters of Comparison	**IDS**	**IPS**
Full-Form	Intrusion Detection Systems.	Intrusion Prevention Systems.
Launched on	The IDS was launched between 1984 to 1986.	The IPS was launched in the mid-2000s.
Definition	The IDS is the system that detects the files passing through the gateway for any malware.	The IPS are the software that detects and even solves the malware detected according to the ruleset provided.
Type	The IDS is a passive type of software.	The IPS is active software.
Working	The IDS working involves the detection and notifies of the malware and errors.	The IPS doesn't require the involvement of humans or other software as it solves the problem on its own.
Performance	The IDS doesn't affect the performance of the network.	The IPS slow down the network because of the detection process.
Communication	The communication of the IDS is out of the band.	The IDS involves inline communication.
Advantage	The IDS doesn't interfere in the working of the network thus, has no influence and problems by the IDS.	The IDS have advantages as they automatically update the errors without including the other software.

Types of IPS:

1. Network-based intrusion prevention system (NIPS):
   It monitors the entire network for suspicious traffic by analyzing protocol activity.
2. Wireless intrusion prevention system (WIPS):
   It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
3. Network behavior analysis (NBA):
   It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.
4. Host-based intrusion prevention system (HIPS):
   It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Assignment Questions

1. How you define network security?
2. Explain the Network security goal with example. 3. Differentiate between authorization and authentication.
3. Why firewall is required in organization.
4. What are the limitation of firewall?
5. What is DDOS attack?
6. Explain the working mechanism of Anti-virus software.
7. What is VPN? Write three applications of VPN.
8. Explain the public/private cryptography in detail.
9. What is digital signature?

10. How does digital signature work?
11. Define the term 'Certification authority' e-commerce.
12. What is PKI?
13. Explain the limitation of encryption.
14. Differentiate between digital signature and digital certificate.
15. What is SSL? Explain the working mechanism of SSL in e-commerce web site.
16. Explain EC security requirement in details.
17. Explain basic terminology of EC Security.
18. What is technical attack? Explain five technical attack on EC Application.
19. What is ransomware? Explain defense technic of ransomware.
20. What is digital signature? Explain the requirements of digital signature in secure transaction.
21. Explain the working mechanism of digital signature.
22. What is CA? Explain the working mechanism of CA.
23. Explain working mechanism of Secure Sockets Layer (SSL)
24. Explain the Securing e-commerce networks.
25. How does a VPN work and how does it benefit users?
26. List the basic types of firewalls and briefly describe each, commerce.
27. What do you mean by Third party authentication in e-commerce?
28. Define biometric systems and list five of their methods.
29. Define access control.
30. Briefly describe the major types of IDSs.
31. How does one protect against spam?
32. How does one protect against pop-ups?
33. How does one protect against phishing, spyware, and advertising?
34. How does one protect against ransomware?

The End