Lecture Notes

On

Cyber Security

University Academy
Teaching | Training | Informative

By

Mr. Sandeep Vishwakarma

Assistant Professor

Dr. A.P.J. Abdul Kalam

Technical University,Lucknow

UNIT – 2

Application security:

Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Security is becoming an increasingly important concern during development as applications become more frequently accessible over networks.Actions taken to ensure application security are sometimes called countermeasures.

Database Security:

Database security is the protection of the database against intentional and unintentional threats that may be computer-based or non-computer-based. Database security is the business of the entire organization as all people use the data held in the organization's database and any loss or corruption to data would affect the day-to-day operation of the organization and the performance of the people. Therefore, database security encompasses hardware, software, infrastructure, people and data of the organization.

1. Threats to a Database:

A threat is any situation or event, either intentional or unintentional that may affect a system and organization. Whether the threat is intentional or unintentional, the impact may be the same. The threats may be caused by a situation or event that involves a person, action or circumstance that is likely to produce harm to someone or to an organization. The harm may be tangible like loss of hardware, software or data. The harm may also be intangible like loss of credibility or client confidence and trust. Threats to data security may be a direct and intentional threat to the database.
Those who gain unauthorized access to a database like computer hackers may steal or change the data in the database. And they would have to have special knowledge in order to do so.

2. Data Tampering

Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. The chances of data tampering are high in case of distributed environments as data moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes that data before retransmitting it.

3. Falsifying User Identities

In a distributed environment, it becomes more feasible for a user to falsify an identity to gain access to sensitive and important information. Criminals attempt to steal users' credit card numbers, and then make purc~1ases against the accounts. Or they steal other personal data, such as bank account numbers and driver's license numbers etc.

4. Password-Related Threats

In large systems, users must remember multiple passwords for the different applications and services that they use. Users typically respond to the problem of managing multiple passwords in several ways:

• They may select easy-to-guess password

• They may also choose to standardize passwords so that they are the same on all machines or websites.

Security Levels

To protect the database, we must take security measures at several levels:

• **Physical:** The sites containing the computer systems must be secured against armed or surreptitious entry by intruders.

• **Human:** Users must be authorized carefully to reduce the chance of any such user giving access to an intruder in exchange for a bribe or other favors .

•**Operating System**: No matter how secure the database system is, weakness in operating system security may serve as a means of unauthorized access to the database.

• **Network:** Since almost all database systems allow remote access through terminals or networks, software-level security within the network software is as important as physical security, both on the Internet and in networks private to an enterprise.

Data Security methods

Confidentiality

A secure system ensures the confidentiality of data. This means that it allows individuals to see only the data they are supposed to see. Confidentiality has several aspects like privacy of communications, secure storage of sensitive data, authenticated users and authorization of users.

Privacy of Communications

The DBMS should be capable of controlling the spread of confidential personal information such as health, employment, and credit records. It should also keep the corporate data such as trade secrets, proprietary information about products and processes, competitive analyses, as well as marketing and sales plans secure and away from the unauthorized people.

Authentication

One of the most basic concepts in database security is authentication, which is quite simply the process by which it system verifies a user's identity, A user can respond to a request to authenticate by providing a proof of identity, or an authentication token

Eg: If you have ever been asked to show a photo ID (for example, when opening a bank account), you have been presented with a request for authentication. You proved your identity by showing your driver's license (or other photo ID). In this case, your driver's license served as your authentication token.

Authorization

An authenticated user goes through the second layer of security, authorization. Authorization is the process through which system obtains information about the authenticated user, including

which database operations that user may perform and which data objects that user may access. Example: an authorization document.

E-mail Security:

Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise. Email is a popular medium for the spread of malware, spam, and phishing attacks, using sensitive information, open attachments or click on hyperlinks that install malware on the device.

Email security refers to the collective measures used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.An email service provider implements email security to secure subscriber email accounts and data from hackers - at rest and in transit.

The Need for Email Security:

Email security is a broad term that encompasses multiple techniques used to secure an email service. From an individual/end user standpoint, proactive email security measures include:

- Strong passwords
- Password rotations
- Spam filters
- Desktop-based anti-virus/anti-spam applications

Similarly, a service provider ensures email security by using strong password and access control mechanisms on an email server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber email address. It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.

It is very easy to spoof e-mail message and alter the name in the form field. All attacker srequires to modify information within the preference section of his/her mail & restart the application. This is the act of sending spoofed messages that pretend to originate from a source the user trusts and has a business relation with such as a bank.

Internet Security:

The internet is a network of networks, connecting billions of computers located at various points. Networking helps users to gain a way to information resources like database and to other users.

Internet security is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol.

Internet security relies on specific resources and standards for protecting data that gets sent through the Internet. This includes a secure Web setup includes firewalls, which block unwanted traffic, and anti-malware, anti-spyware and anti-virus programs that work from specific networks or devices to monitor Internet traffic for dangerous attachments.

Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency's servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

Security and Network Security Goals

Networked systems (simple apps, complex networks, complete IT infrastructures) operate in environments involving different interconnected parties each with their own goals, which may not match with the goals of other parties of the system as whole. As such it is essential to consider, in addition to the functional requirements of systems (i.e. what the systems should achieve) also its security requirements.

Security requirements are expressed in terms of security attributes that express goals that one may want to achieve to call a system 'secure'. The most commonly used and widely accepted security attributes are Confidentiality, i.e. 'my information stays secret', Integrity, i.e. 'my information stays correct', and Availability, i.e. 'I can get at my information' (sometimes called the C-I-A triad.)

Backup

Having a backup these days is mandatory for any organization concerned with their information and data. A file backup is a copy of a file that is stored in a separate location from the original. Backing up is making copies of data which may be used to restore the original after a data loss event. This new copy of data is the Backup. You can have multiple backups of a file if you want to track changes to the file.

Why we Backup?

There are many reasons why your organization may want to back up their data. The primary reason is to recover data after its loss. The loss can occur by accidental deletion, a virus attack, or a software or hardware failure. If any of those things occur and your files are backed up, you can easily restore those files. Preventing events that result in loss of data is most desired, but backing up data provides the protection for data after a system failure. Individual computers being backed up are different than servers being backed up. Individual computer users can back up their own information when desired and using methods they desire, whereas data on organization servers need more formal backup procedures.

Types of backup:

Full Backup

Full backup is a method of backup where all the files and folders selected for the backup will be backed up. The advantage of this backup is restores are fast and easy as the complete list of files are stored each time. The disadvantage is that each backup run is time consuming as the entire list of files is copied again.

FTP Backup

This is a kind of backup where the backup is done via FTP (File Transfer Protocol) over the Internet to an FTP Server. Typically the FTP Server is located in a commercial data centre away from the source data being backed up.

Cloud Backup

This term is often used interchangeably with Online Backup and Remote Backup. It is where data is backed up to a service or storage facility connected over the Internet.

Offsite Backup

When the backup storage media is kept at a different geographic location from the source, this is known as an offsite backup. The backup may be done locally at first but once the storage medium is brought to another location, it becomes an offsite backup. Examples of offsite backup include taking the backup media or hard drive home, to another office building or to a bank safe deposit box.

Remote Backup

Remote backups are a form of offsite backup with a difference being that you can access, restore or administer the backups while located at your source location or other location. You do not need to be physically present at the backup storage facility to access the backups.

Archival storage of data:

This identifies the different steps involved in the data creation process, from data creation & retention for reuse or archiving. The decisions to retain data include:

- Effective use of storage resources for data which has long term value.
- Reduced volume of data making it easier to manage & maintain descriptive metadata records.
- Reduced storage costs.
- Efficient & effective file organization for quick use.

The data must be retain in order to satisfy:

- Needs in the present day
- Future need
- Compliance with policies

Disposal of data:

Confidential electronic and paper information must be disposed of securely to minimise the risk of unwanted disclosure. Confidential information is information which if improperly disclosed or lost could cause harm or distress. This includes personal data as defined by the Data Protection act, i.e. information about a living individual where that individual could be identified, and other valuable or sensitive information not in the public domain.

Disposal is an important part of records management. Properly done, it ensures that the organization retains records for as long as they are needed and then, when they are no longer needed, destroys them in an appropriate manner or disposes of them in some other way, e.g. by transfer to an archives service. A managed disposal process has several benefits:

● it avoids unnecessary storage costs incurred by using office or server space to maintain records no longer needed by the organization

● it supports compliance with the 5th data protection principle if records contain personal information (this principle requires organizations not to keep personal information for longer than necessary)1

● finding and retrieving information is quicker and easier because there is less to search

● responding to Freedom of Information (FOI) requests is more efficient.

Making disposal decisions

Making disposal decisions is about deciding two things:
- how long records should be kept, i.e. their retention period
- what should happen at the end of that period

Implementing disposal decisions

Making a disposal decision is an important first step but to realize the benefits identified above you need to implement the decisions in a timely and effective way. This means monitoring retention periods and taking appropriate disposal action when they come to an end. This disposal action will be one of the following:
- destruction of records
- transfer of records to an in-house or external archives service
- a further review of records (if necessary)
- transfer of records to a successor body (if applicable).

Benefits of disposal schedules

The main benefits of disposal schedules are:
- clear instructions on what happens to records when they are no longer needed to support the business
- definitive periods of time for which records should be kept and remain accessible
- consistency in retention of records across the organization
- evidence of compliance with legal and regulatory requirements for the retention of records

Contents of disposal schedules

The disposal schedule should provide sufficient information for the records covered by each disposal class to be identified and the disposal decision put into effect. What details should be included will vary from organization to organization and will depend on factors such as:

- Technology – whether the records are in physical or digital format or a hybrid of both (this will determine whether the format of each disposal class needs to be specified in the schedule)
- Location – if records are held on several sites or in several systems it may be necessary precisely to specify where they are stored
- Storage arrangements – if records are moved off-site or off-line, it may be necessary to specify when this should take place
- The size of the organization – if the organization is large enough to be broken down into separate business units, the creating business unit or, alternatively, the function should be specified.

Network Security

Information security is a critical need for individuals as well as society and all countries around the world. Since invented, computer network has brought along tremendous effectiveness in every aspect of life. Besides that users also have to face threats from all kinds of attack from hackers. Network security includes protection methods for all information that is stored and transferred through a system network. This is also a special field of interest and a difficult and complex work at the same time.

Network Security Methods

Due to a lack of absolute security solutions a network should be contemporarily constructed with multilayers to form a barrier against violating activities. The act of information security in the network focuses on protecting data stored on computers, especially on servers.

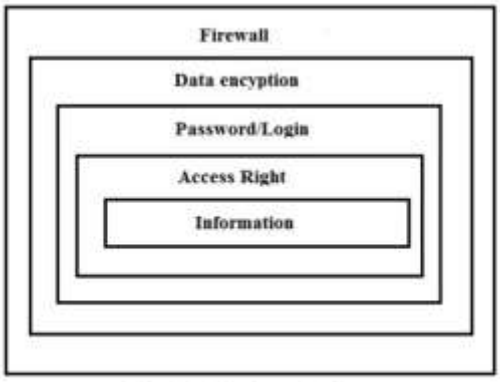


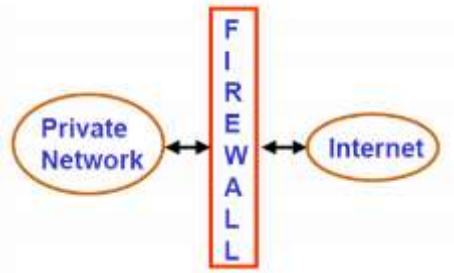
Figure 1. Network security layers

Network servers commonly have many security layers in order to enhance the ability to protect data and information. The innermost layer of protection is Access Right. This layer controls network resources (information) and rights (what users can do with those resources). This control applies to partitions, folders and files. The next layer restricts account access including usernames and passwords (Password/Login). This is a commonly used method of protection due to its simplicity, economical and highly effective. The administrator has full responsibility to control and manage the activities of other users. The third layer uses a data encryption method (Data Encryption). Data is encrypted with a certain algorithm so that even in case of data loss,

hackers will not be able to read it without an encryption key. The outermost layer (Firewall) prevents intrusions, filters unwanted outgoing or incoming information packets.

Firewall

Firewalls can be understood as a piece of software running on an individual's PC, notebook or host. It is designed to allow or restrict data transferred on a network based on a set of rules. A firewall is used to protect a network from intrusions and concurrently allow legitimate data pass through. Usually a firewall should have at least two network traffics, one for private network and one for public network activities such as the Internet. At that time it acts as a gate controlling outgoing/incoming data streams of an intranet.



Firewall Characteristics

Lists the following design goals for a firewall:

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this chapter. 3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

Lists four general techniques that firewalls use to control access and enforce the site's security policy. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four:

• **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

• **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

- **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPsec.
- • **Behavior control:** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

VPN:

A Virtual Private Network is a connection method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet. Virtual Private Networks are most often used by corporations to protect sensitive data. However, using a personal VPN is increasingly becoming more popular as more interactions that were previously face-to-face transition to the Internet. Privacy is increased with a Virtual Private Network because the user's initial IP address is replaced with one from the Virtual Private Network provider. Subscribers can obtain an IP address from any gateway city the VPN service provides

A virtual private network (VPN) allows the provisioning of private network services for an organization or organizations over a public or shared infrastructure such as the Internet or service provider backbone network. The shared service provider backbone network is known as the *VPN backbone* and is used to transport traffic for multiple VPNs, as well as possibly non-VPN traffic.

VPN (Virtual Private Network) is a generic term used to describe a communication network that uses any combination of technologies to secure a connection tunneled through an otherwise unsecured or untrusted network. Instead of using a dedicated connection, such as leased line, a "virtual" connection is made between geographically dispersed users and networks over a shared or public network, like the Internet. Data is transmitted as if it were passing through private connections.

VPN Devices

Before describing the various VPN technologies and models, it is useful to first describe the various customer and provider network devices that are relevant to the discussion.

Devices in the customer network fall into one of two categories:

• **Customer (C) devices**—C devices are simply devices such as routers and switches located within the customer network. These devices do not have direct connectivity to the service provider network. C devices are not aware of the VPN.

• **Customer Edge (CE) devices**—CE devices, as the name suggests, are located at the edge of the customer network and connect to the provider network.

• **Service Provider (P) devices**—P devices are devices such as routers and switches within the provider network that do not directly connect to customer networks. P devices are unaware of customer VPNs.

• **Service Provider Edge (PE) devices**—PE devices connect directly to customer networks via CE devices. PE devices are aware of the VPN in PE-based VPNs, but are unaware of the VPN in CE-based VPNs.

There are three types of PE device:
— Provider Edge routers
— Provider Edge switches
— Provider Edge devices that are capable of both routing and switching

Why do I need a VPN?

- **Hide your IP address**
  Connecting to a Virtual Private Network often conceals your real IP address.
- **Change your IP address**
  Using a VPN will almost certainly result in getting a different IP address.
- **Encrypt data transfers**
  A Virtual Private Network will protect the data you transfer over public WiFi.
- **Mask your location**
  With a Virtual Private Network, users can choose the country of origin for their Internet connection.
- **Access blocked websites**
  Get around website blocked by governments with a VPN.

Intrusion detection:

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents.

Different types of intrusion detection systems

Intrusion detection systems come in different flavors and detect suspicious activities using different methods, including the following:

- A network intrusion detection system (NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.
- Host intrusion detection systems (HIDS) run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. HIDS have an

advantage over NIDS in that they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that originates from the host itself, as when the host has been infected with malware and is attempting to spread to other systems.

- Signature-based intrusion detection systems monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software.

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.

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.

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.
- **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.

1. Security threat

Whenever an individual or an organization creates a web site or has a web presence, they are vulnerable to security attacks. Security attacks are mainly aimed at stealing, altering or destroying personal and confidential information, stealing the hard drive space, illegally accessing passwords to get to the private account information from the online banking services.

In network security, the three common terms used are as follows:

■ **Vulnerability**—A weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves.

■ **Threats**—The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.

■ **Attacks**—The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktops.

1.1 Vulnerabilities

Vulnerabilities in network security can be summed up as the "soft spots" that are present in every network. The vulnerabilities are present in the network and individual devices that make up the network. Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses:

■ Technology weaknesses

■ Configuration weaknesses

Security policy weaknesses **(in unit 1notes)**

1.2 Threats (cover from active attacks in unit1)

1.3Attacks Four primary classes of attacks exist:

■ Reconnaissance

■ Access

■ Denial of service

■ Worms, viruses, and Trojan horses

Reconnaissance:

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities (see Figure 1-13). It is also known as information gathering and, in most cases, it precedes an actual access or denial-of-service (DoS) attack. Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows.

Access System:

Access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems to which one does not have authority to access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Denial of Service (DoS) :

Denial of service implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack simply involves running a hack or script. The attacker does not need prior access to the target because a way to access it is all that is usually required. For these reasons, DoS attacks are the most feared.

Virues:

A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.

A virus can be spread by opening an email attachment, clicking on an executable file, visiting an infected website or viewing an infected website advertisement. It can also be spread through infected removable storage devices, such USB drives. Once a virus has infected the host, it can infect other system software or resources modify or disable core functions or applications, as well as copy, delete or encrypt data. Some viruses begin replicating as soon as they infect the host, while other viruses will lie dormant until a specific trigger causes malicious code to be executed by the device or system.

Types of Computer Viruses:

A **computer virus** is one type of malware that inserts its virus code to multiply itself by altering the programs and applications. The computer gets infected through the replication of malicious code.

Computer viruses come in different forms to infect the system in different ways. Some of the most common viruses are:

Boot Sector Virus – This type of virus infects the master boot record and it is challenging and a complex task to remove this virus and often requires the system to be formatted. Mostly it spreads through removable media.
Direct Action Virus – This is also called non-resident virus, it gets installed or stays hidden in the computer memory. It stays attached to the specific type of files that it infect. It does not affect the user experience and system's performance.

Resident Virus – Unlike direct action viruses, resident viruses get installed on the computer. It is difficult to identify the virus and it is even difficult to remove a resident virus.

Multipartite Virus – This type of virus spreads through multiple ways. It infects both the boot sector and executable files at the same time.

Polymorphic Virus – These type of viruses are difficult to identify with a traditional anti-virus program. This is because the polymorphic viruses alters its signature pattern whenever it replicates.

Overwrite Virus – This type of virus deletes all the files that it infects. The only possible mechanism to remove is to delete the infected files and the end-user has to lose all the contents in it. Identifying the overwrite virus is difficult as it spreads through emails.

Spacefiller Virus – This is also called "Cavity Viruses". This is called so as they fill up the empty spaces between the code and hence does not cause any damage to the file.

Worms:

An Internet worm is type of malicious software (malware) that self-replicates and distributes copies of itself to its network. These independent virtual viruses spread through the Internet, break into computers, and replicate without intervention from and unbeknownst to computer users.
A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.
To spread, worms either exploit vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided. More advanced worms leverage encryption, wipers, and ransom ware technologies to harm their targets.

Trojan horse:

A Trojan is also known as Trojan horse. It is a type of malicious software developed by hackers to gain access to target users' systems. Users are typically tricked by some attractive social media adds who then directed to malicious website thereby loading and executing Trojans on their systems. Cyber-criminals use Trojans to spy on the victim user, gain illegal access to the system to extract sensitive data.

These actions can include:

- Deletes Data
- Copies data

- Modifies Data
- Blocks Data

Trojan horse is not able to replicate itself, nor can it propagate without an end user's assistance. This is why attackers must use social engineering tactics to trick the end user into executing the Trojan. Typically, the malware programming is hidden in an innocent-looking email attachment or free download. When the user clicks on the email attachment or downloads the free program, the malware that is hidden inside is transferred to the user's computing device. Once inside, the malicious code can execute whatever task the attacker designed it to carry out.

Characteristics of a Trojan horse

When a Trojan horse becomes active, it puts sensitive user data at risk and can negatively impact performance. Once a Trojan has been transferred, it can:

- Give the attacker backdoor control over the computing device.
- Record keyboard strokes to steal the user's account data and browsing history.
- Download and install a virus or worm to exploit vulnerability in another program.
- Install ransomware to encrypt the user's data and extort money for the decryption key.
- Activate the computing device's camera and recording capabilities.

Bombs:

A logic **bomb** is a piece of code inserted into an operating system or software application that implements a malicious function after a certain amount of time, or specific conditions are met. Logic**bombs** are often used with **viruses**, worms, and trojan horses to time them to do maximum damage before being noticed.

Some logic bombs can be detected and eliminated before they execute through a periodic scan of all computer files, including compressed files, with an up-to-date anti-virus program.

Trapdoors:

A computer trapdoor, also known as a back door, provides a secret -- or at least undocumented -- method of gaining access to an application, operating system or online service. Programmers write trapdoors into programs for a variety of reasons. Left in place, trapdoors can facilitate a range of activities from benign troubleshooting to illegal access.

TrapDoor does not spread automatically using its own means. It needs the attacking user's intervention in order to reach the affected computer. The means of transmission used include, among others, floppy disks, CD-ROMs, email messages with attached files, Internet downloads, FTP, IRC channels, peer-to-peer (P2P) file sharing networks, etc.

Spoofing mean?

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.

Email spoofing is one of the best known spoofs. Since core SMTP fails to offer authentication, it is simple to forge and impersonate emails. Spoofed emails may request personal information and may appear to be from a known sender. Such emails request the recipient to reply with an account number for verification. The email spoofer then uses this account number for identity theft purposes, such as accessing the victim's bank account, details changing contact etc.

The attacker (or spoofer) knows that if the recipient receives a spoofed email that appears to be from a known source, it is likely to be opened and acted upon. So a spoofed email may also contain additional threats like Trojans or other viruses. These programs can cause significant computer damage by triggering unexpected activities, remote access, deletion of files and more.

Email virus:

An email virus is a virus that is sent with or attached to email communications. While many different types of email viruses work in different ways, there also are a variety of methods used to counteract such challenging cyber attacks.

Email viruses are often connected with phishing attacks in which hackers send out malicious email messages that look as if they are originated from legitimate sources, including the victim's bank, social media, internet search sites or even friends and co-workers. The attacker's goal, in these cases, is to trick users into revealing personal information, such as the victim's usernames, full names and addresses, passwords, Social Security numbers or payment card numbers.

Macro Virus:

A macro virus is a computer virus that replaces a macro, which is what enables a program to work and instigates a designated group of actions and commands. When these actions and commands are replaced by a virus, this can cause significant harm to a computer.

Malicious Software (Malware):

Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, Trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.

Malicious software (malware) is any software that gives partial to full control of your computer to do whatever the malware creator wants. Malware can be a virus, worm, trojan, adware, spyware, root kit, etc. The damage done can vary from something slight as changing the author's name on a document to full control of your machine without your ability to easily find out. Most malware requires the user to initiate it's operation. Some vectors of attack include attachments in e-mails, browsing a malicious website that installs software after the user clicks ok on a pop-up, and from vulnerabilities in the operating system or programs. *Malware is not limited to one operating system.*

Spam:

Spam is electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup.

Spam refers to the use of electronic messaging systems to send out unrequested or unwanted messages in bulk.

In addition to wasting people's time with unwanted email, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers.

Denial-of-Service Attack (DoS)

A denial-of-service attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources.

In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

A DoS attack can be done in a several ways. The basic types of DoS attack include:

1. Flooding the network to prevent legitimate network traffic
2. Disrupting the connections between two machines, thus preventing access to a service
3. Preventing a particular individual from accessing a service.
4. Disrupting a service to a specific system or individual
5. Disrupting the state of information, such resetting of TCP sessions

Difference between Hackers & attackers:

A computer hacker is any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.

An attacker is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Thus an attacker is the individual or organization performing these malicious activities.

E-Commerce Threats:

The exchange or buying and selling of commodities on a large scale involving transportation from place to place is known as commerce. E-Commerce is the application of technology toward the automation of business transaction and workflows, delivery of information, products or services, buying and selling of products over internet.

E-commerce is taking advantage of distance selling the great advantages offered by new information technologies, such as the extension of the offer , the interactivity and immediacy of purchase, with the difference that you can buy and sell to whom you want , and where and when they want. There are increased opportunities to enhancing the business efficiency and reducing the incurred costs by the computer applications of e-commerce as it enables a tighter integration with the several linkages.

The medium of electronic that is referred as the internet has the power and tendency for reducing actual time of transactions and the overall processing time radically. One of the critical issues in e-commerce success is security. Security is directly related to the issue of trust and confidence between buyer and seller and extremely sensitive personal information.

Security is the component that affects e-commerce which includes Computer Security, Data Security and other areas. Security is one of the concern which is affecting customer and organizations trade. Web application which is offering online payment system (net banking, credit card, debit card, PayPal or other token) are at more risk from being targeted and there is big loss if data is being hacked. The e-commerce website those offering online payment are giving guidelines for securing systems and networks available for the ecommerce system

There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are phishing attacks, money thefts, data misuse, hacking, credit card frauds and unprotected services.

Malicious code threats-These code threats typically involve viruses, worms, Trojan horses.

Inaccurate management-One of the main reason to e-commerce threats is poor management. When security is not up to the mark it poses a very dangerous threat to the networks and systems. Also security threats occur when there are no proper budgets are allocated for purchase of anti-virus software licenses.

Price Manipulation-Modern e-commerce systems often face price manipulation problems. These systems are fully automated; right from the first visit to the final payment getaway. Stealing is the most common intention of price manipulation. It allows an intruder to slide or install a lower price into the URL and get away with all the data.

Wi-Fi Eavesdropping-It is also one of the easiest ways in e-commerce to steal personal data. It is like a "virtual listening" of information which is shared over a Wi-Fi network which is not encrypted. It can happen on public as well as on personal computers.

Ways to prevent e-commerce threats

Encryption-It is the process of converting a normal text into an encoded text which cannot be read by anyone except by the one who sends or receives the message.

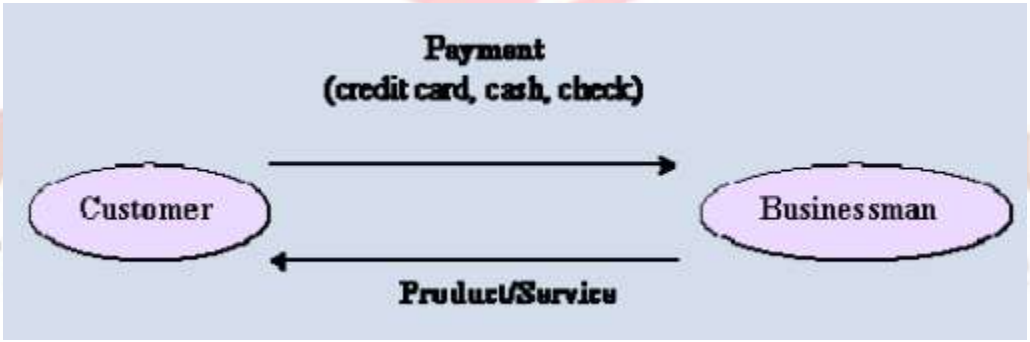
Having digital certificates

It is a digital certificate which is issued by a reliable third party company. A digital certificate contains the following things the name of the company, the most important digital certificate serial number, expiry date and date of issue.

Perform a security audit-a routine examination of the security procedures of the firm.

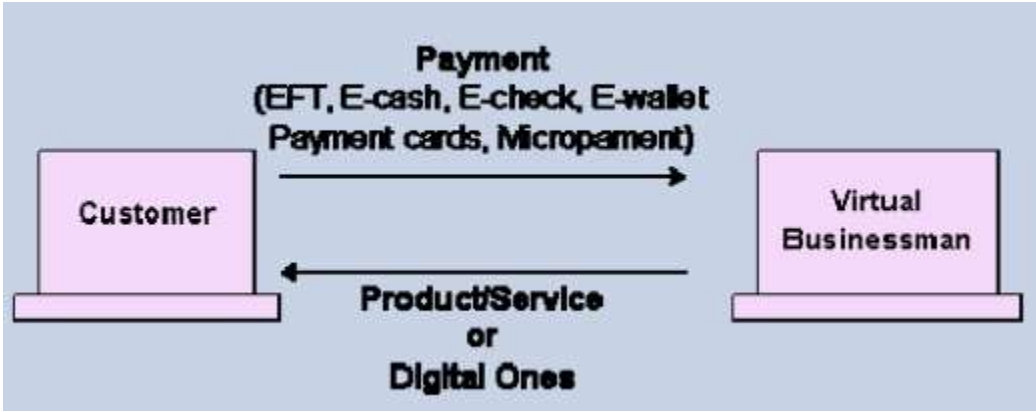
ELECTRONİC PAYMENT SYSTEMS (EPS)

Issues of trust and acceptance play a more significant role in the e-commerce world than in traditional businesses as far as payment systems are concerned. Traditionally, a customer sees a product, examines it, and then pays for it by cash, check, or credit card. In the e-commerce world, in most cases the customer does not actually see the concrete product at the time of transaction, and the method of payment is performed electronically.



Traditional payment scheme

EPSs enable a customer to pay for the goods and services online by using integrated hardware and software systems. The main objectives of EPS are to increase efficiency, improve security, and enhance customer convenience and ease of use. Although these systems are in their immaturity, some significant development has been made. There are several methods and tools that can be used to enable EPS implementation.



Electronic payment scheme

While customers pay for goods/services by cash, check, or credit cards in conventional businesses, online buyers may use one of the following EPSs to pay for products/services purchased online:

• **Electronic funds transfer (EFT):** EFT involves electronic transfer of money by financial institutions.

• **Payment cards :** They contain stored financial value that can be transferred from the customer's computer to the businessman's computer.

• **Credit cards** : They are the most popular method used in EPSs and are used by charging against the customer credit.

• Smart cards: They include stored financial value and other important personal and financial information used for online payments.

• **Electronic money (e-money/e-cash):** This is standard money converted into an electronic format to pay for online purchases.

• **Online payment:** This can be used for monthly payment for Internet, phone bills, etc.

• **Electronic wallets (e-wallets) :** They are similar to smart cards as they include stored financial value for online payments.

• **Micro-payment systems :** They are similar to e-wallets in that they include stored financial value for online payments; on the other hand, they are used for small payments, such as kurus in Turkey .

• **Electronic gifts :** They are one way of sending electronic currency or gift certificates from one individual to another. The receiver can spend these gifts in their favorite online stores provided they accept this type of currency.

Although these groups appear to be separate, there is some overlap among them. When the industry matures, this duplication in naming and function ought to be renamed. For example, e-wallets can be classified as payment cards when they are used to store credit card information or as e-money when they store electronic currency.

Types of E-payment system:-

1) **Credit cards:-** A Credit card is a piece of plastic, 3-1/8inches by 2-1/8 inches in size, that carries information that allow you to make purchase now pay for them later . (Kaur

M,2012).[2]Credit cards from visa maser card or any other network allow you to pay for purchase or services by borrowing from the credit card company. To purchase goods from merchant who accept credit card such as merchant has credit card reader to purchase the payment transaction to withdraw cash from ATM. You then repay by making monthly payment toward the amount borrowed ,that is you don't have to repay the whole borrowed amount in fill at one go.

2) **Debit Card:-** Debit card is a prepaid card and also known as ATM card. An individual has to open an account with the issuing bank which gives debit card with a personal id number, when he makes a purchase he enter his pin number on shop pin pad. When the card is slurped through the electronic terminal it dial the acquire a banking system either master card or visa card that validate the pin and finds out from the issuing bank whether to accept or decline the transaction the customer can never overspend because the system reject any transaction which exceeds the balance in his account the bank never face a default because the amount spent is debited immediately from the customer account With almost every bank account you are issued a debit card.
3) **Electronic cash:-** Similar to regular cash, e-cash enables transactions between customers without the need for banks or other third parties. When used, e-cash is transferred directly and immediately to the participating merchants and vending machines. Electronic cashes a secure and convenient alternative to bills and coins. E-cash usually operates on a smartcard, which includes an embedded microprocessor chip. The microprocessor chip stores cash value and the security features that make electronic transactions secure. when e cash created by one bank is accepted by other reconciliation must occur without any problem cash must be storable and receivable. Most E-cash is transferred directly from the customer's desktop to the merchant's site. Therefore, e-cash transactions usually require no remote authorization or personal identification.
4) **Digital signature:** Digital signatures are basically "enciphered data" created using cryptographic algorithms. The algorithms define how the enciphered data is created for a particular document or message. Standard digital signature algorithms exist so that no one needs to create these from scratch. Digital signature algorithms were first invented in the 1970's and are based on a type of cryptography referred to as "Public Key Cryptography".

   A digital signature scheme is just like a message authentication scheme except for an asymmetry in the key structure. The key **sk** used to generate signatures (in this setting the tags are often called signatures) is different from the key **pk** used to verify signatures. Furthermore **pk** is public, in the sense that the adversary knows it too. So while only a signer in possession of the secret key can generate signatures, anyone in possession of the corresponding public key can verify the signatures.

   Functional Standards for Authentication of Electronic Records:

   Authentication: the process of assuring that an electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.

   Digital Certificate: An attachment to an electronic message used for security purposes, which enables a user sending a message via an unsecured network.

   Electronic: relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. For the purposes of this standard, "electronic" is not meant to encompass activities involving facsimile transmission.

Digital signature is a mechanism by which a message is authenticated i.e. proving that a message is effectively coming from a given sender, much like a signature on a paper document. For instance, suppose that Alice wants to digitally sign a message to Bob. To do so, she uses her private-key to encrypt the message; she then sends the message along with her public-key (typically, the public key is attached to the signed message). Since Alice's public-key is the only key that can decrypt that message, a successful decryption constitutes a Digital Signature Verification, and meaning that there is no doubt that it is Alice's private key that encrypted the message.

PUBLIC-KEY CRYPTOGRAPHY:

Public-key cryptography is also known as asymmetric-key cryptography, to distinguish it from the symmetric-key cryptography. Encryption and decryption are carried out using two different keys. The two keys in such a key pair are referred to as the public key and the private key. With public key cryptography, all parties interested in secure communications publish their public keys.

Note: Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

The most important properties of public key encryption scheme are − Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme. Each receiver possesses a unique decryption key, generally referred to as his private key. Receiver needs to publish an encryption key, referred to as his public key. Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver.

Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only. Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the cipher text and the encryption public key. Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

A public-key encryption scheme has six ingredients

- **Plaintext**: This is the readable message or data that is fed into the algorithm as input.
- **Encryption algorithm**: The encryption algorithm performs various transformations on the plaintext.
- **Public and private keys**: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
- **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts. Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext