E-Commerce

E-Security

Module 4

Information system security

- Security refers to the policies, procedures and technical measures and to prevent unauthorised access,alteration,theft or physical damage to information systems.

- The main objective of information security are :
  - Availability objective
  - Confidentiality objective
  - Integrity objective

- **Availability objective**

  Information should be available and usable whenever it is required.

- **Confidentiality objective**

  This objective states that information should be available to only those who have the right to access it.

- **Integrity objective**

  As per this objective, information should be protected from unauthorised alteration and modification.

Security on the internet

- Web security is also known as “Cybersecurity”. It basically means protecting a website or web application by detecting, preventing and responding to cyber threats.

- It is a system of protection measures and protocols that can protect our website or web application from being hacked or entered by unauthorized personnel.

Network and web security risks

- Hacking
- Denial of service attack (DOS)
- Viruses
- Trojan horses
- Internet hoax
- Worms
- Spyware
- Adware
- Phishing

Hacking

- Hacking is unauthorized intrusion into a computer or a network.
- The person engaged in hacking activities is generally referred to as a hacker.
- A hacker is a person who gains unauthorised access to a computer network for profit, criminal mischief or personal pleasure.
- Types of hackers :
    - White hat hackers
    - Black hat hackers
    - Grey hat hackers

Denial of service attack (DOS)

- A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

- DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Viruses

- A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code.

- If this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

Trojan horses

- In computing, a Trojan horse is any malware which misleads users of its true intent.
- The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.
- Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems.
- Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems.

Internet hoax

- Internet hoaxes are stories that spread throughout the internet, often through email, forums, and blogs or showing images that are untrue or alteration of the truth.
- It is usually an email urging to pass this information to as many people to make aware of this information.
- The only purpose of hoax is to waste time.

Worms

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- It often uses a computer network to spread itself, relying on security failures on the target computer to access it.
- It will use this machine as a host to scan and infect other computers.
- Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time.

Spyware

- Spyware is unwanted software that gain our computing device, stealing internet usage data and sensitive information.
- Spyware is classified as a type of malware — malicious software designed to gain access to or damage your computer, often without your knowledge.
- Spyware aims to gather information about a person or organization and send such information to another entity in a way that harms the user; for example by violating their privacy or endangering their device's security.

Adware

- Adware, often called advertising-supported software by its developers, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process.
- The software may generate two types of revenue: one is for the display of the advertisement and another on a "pay-per-click" basis, if the user clicks on the advertisement.

Phishing

- Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication.

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy is called vulnerability.

- Internet attacks can be launched from anywhere in the world and the location of the attacker can easily be hidden.
- New web based attack types are coming out every day; this is causing businesses, communities and individuals to take security seriously now.

Types of vulnerability

- SQL injection
- Cross site scripting
- Broken authentication and session management
- Cross site request forgery attack
- Clickjacking attack
- Social engineering attack
- Website defacement
- Cyber industrial espionage
- Credit card fraud and theft of customer data

SQL injection

- SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.
- SQL injection is one of the most common web hacking techniques.

- SQL injection is a code injection technique that might destroy our database.
- If successful this allows the attacker to create, read, update, alter or delete data stored in the database.

Cross site scripting (XSS)

- It is a client-side code injection attack.
- The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.

- The actual attack occurs when the victim visits the web page or web application that executes the malicious code.
- The web page or web application becomes a vehicle to deliver the malicious script to the user's browser.

Broken authentication and session management

- If the user authentication system of a website is weak, hackers can take full advantage.
- Authentication systems involve passwords, session IDs, and cookies that can allow a hacker to access user's account from any computer.
- If a hacker exploits the authentication and session management system, they can operate with user's identity.

Cross site request forgery attack

- Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

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

- Cross-site request forgery, also known as **one-click attack** or **session riding** and abbreviated as **CSRF** is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.
- This attack happens when a user is logged into a session and a hacker uses this opportunity to send them a forged HTTP request to collect their cookie information.
- In most cases, the cookie remains valid as long as the user or the attacker stays logged into the account. This is why websites directs to logout of account when session is finished.

Clickjacking attack

- Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element.
- This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.
- The attacker is hijacking clicks that are not meant for the actual page, but for a page where the tracker wants take us.

Social engineering attack

- It happens when the user reveal private information in good faith, such as a credit card number, through common online interactions such as email, chat, social media sites etc.

Website defacement

- Website defacement is an attack on a website that changes the visual appearance of a website or a web page. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own.
- Visitors may be redirected to a website with an address quite similar to the company.

Cyber industrial espionage

- Cyber espionage is a form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.
- Espionage is “the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company.”

Credit card fraud and theft of customer data

- Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card.
- The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal.
- The most common types of fraud causing concern among merchants are identity theft.

Network and web security

- The goal of security management is to minimize risk and ensure protection by limiting the impact of s security breach.

- Ensure the following points for better security :
  - Monitor network performance
  - Username and password
  - Use of firewall
  - Intrusion detection
  - Virus scanning software.

- **Monitor network performance**

  Network performance monitoring is a routine process to evaluate, analyzes, report and track on the performance of a computer network.

- **Username and password**

  Password protection allows only those with a authorized password to gain access to certain information.

- **Use of firewall**

  It is a network security system designed to prevent unauthorized access to or from a private network.

  It is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

  Firewalls can be implemented as both hardware and software, or a combination of both.

- **Intrusion detection**

  It is a system that monitors network traffic for suspicious activity and issues alerts when such an activity is discovered.

  While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected.

- **Virus scanning software.**

  It helps to scan and identify any malicious content and removes it from the system.

Transaction security and data protection

- The following measures can be adopted for data protection :
  - Encryption
  - Secure socket layer (SSL)
  - Secure hypertext transfer protocol (S-HTTP)
  - Trusted seals programs
  - Digital signature
  - Secure electronic transaction (SET)
  - Digital certificate

- **Encryption**

  It is the process of transforming plain text or data into cipher text that can not be read by anyone other than the sender and the receiver.

- **Secure socket layer (SSL)**

  The SSL protocol provides data encryption, server authentication, optional client authentication, and message integrity for TCP/IP connections.

- **Secure hypertext transfer protocol (S-HTTP)**

  It is a secure message oriented communications protocol designed for use in conjunction with HTTP.

  Generally, S-HTTP attempts to make HTTP more secure.

- **Trusted seals programs**

  A number of trustmark seals have been developed to provide assurance about web business practices and policies through the web interface.

- **Digital signature**

  A digital signature is a technique used to validate the authenticity and integrity of a message, software or digital document.

  It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security.

- **Secure electronic transaction (SET)**

  It will enable payment security for all involved, authenticate card holders and merchants, provide confidentiality for payment data and define protocols.

- **Digital certificate**

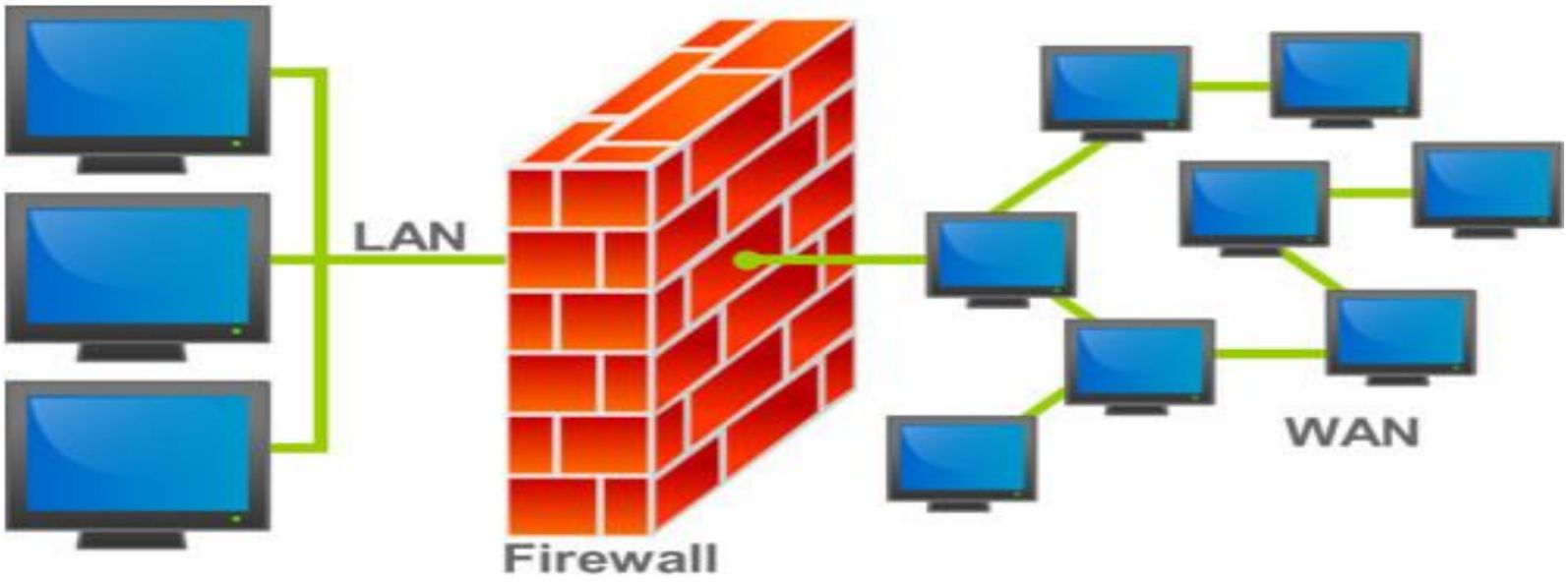
  It is a digital document issued by a trusted third party institution known as a certificate authority that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, the digital signature of the certification authority and other identifying information.

  The certificate is signed with the private key of the certification authority.

The firewall

- In computing, a firewall is a network security system that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
- A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

- The aim of this wall is to protect the premises network from internet based attacks and to provide a single block point where security and auditing can be checked.


LAN
Firewall
WAN

Why firewalls ?

- Protection from vulnerabilities
- Managing and controlling network traffic
- Authentication access
- Acting as a intermediary
- Resource protection
- Recording and reporting of events
- Preventing access to information
- Enforcing policy
- auditing

- **Protection from vulnerabilities**

  Internet connection is vulneration to hackers who want to access financial and personal information.

- **Managing and controlling network traffic**

  This is the first and most basic function. It should be able to identify which data packets are coming through, which connection is established and also be able to control those traffic in the system.

- **Authentication access**

  The usage of packet filtering helps to restrict resource access from unexpected sources.

- **Acting as a intermediary**

  Instead of allowing computers connect directly to the internet, a firewall is modified into an intermediary device to the internet.

  The simplest mechanism for verification is asking users for a username and password whenever they want to access the system.

- **Resource protection**

  Important task of a firewall is to protect the network resource from outside threats.

- **Recording and reporting of events**

  Records all information about policy violated activities and reports it to administrator.

- **Preventing access to information**

  It also used to limit the activities of their users on the internet.

- **Enforcing policy**

  Firewall enforce the rules about which network traffic is allowed to enter or leave a network.

- **Auditing**

  If a security breach occurs, audit trails can be used to help determine what had happened.

Types of Firewall

- Packet filtering firewall
- Application level gateway
- Circuit level gateway

Benefits of firewall

- Monitors traffic
- Blocks trojans
- Stops hackers’
- Stops keyloggers

Limitations

- Cannot protect against attacks that bypasses the firewall
- The firewall may not protect fully against internal threats

Information security environment in india

Assignment

Legal and ethical issues

- Ethical issues deal with what is considered to be right and wrong.
- If anybody does something that is not legal, they are breaking the law, but if they do something unethical, they may not be breaking the law.

Ethical issues

- Web spoofing
- Cyber squatting
- Web tracking
- Identity theft

- **Web spoofing**

  It occurs when the attacker sets up a fake website which is almost same as the original website in order to attract consumers to give their credit card number or other personal information.

  Normally, the spoof website will adopt the design of the target website, and it sometimes has a similar URL.

- **Cyber squatting**

  It means an activity in which a person or firm register, purchase and uses the existing domain name, belonging to a well known organization, for the purpose of infringing its trademark.

  The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price.

- **Web tracking**

  Web tracking is the practice by which operators of websites collect, store and share information about visitors' activities on the World Wide Web.

- **Identity theft**

  Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

Legal issues

- Cyberstalking
- Application fraud on the internet
- Skimming
- Copyright

- **Cyberstalking**

  It is a criminal practice where an individual uses the internet to systematically harass or threaten someone.

  This crime can be committed through email,social media, chat rooms, instant messaging clients and any other online medium.

  A stalker may be an online stranger or a person whom the target knows.

- **Application fraud on the internet**

  The small investors are attracted by the promises of false profits by the stock promoters.

  The availability of emails and popup ads have paved the way for financial criminals to have access to many people.

- **Skimming**

  Skimming is the unauthorized capture and transfer of payment data to another source.

  For example, information that is electronically stored on the magnetic stripe of a credit card or debit card is illegally copied during an attempt to use an automatic teller machine (ATM).

- **Copyright**

  Copyright is a type of intellectual property that gives its owner the exclusive right to make copies of a creative work, usually for a limited time.

  Unfortunately, it is easy for the computer to create an exact copy of valuable software in seconds.

  Software piracy is widespread. It refers to the unauthorized duplication of computer software.

Internet gambling

Online gambling (or **Internet gambling**) is any kind of gambling conducted on the internet.

This includes virtual poker, casinos and sports betting.

Threat to children

- Children face additional challenges because of their natural characteristics like innocence, curiosity, etc.

Remedial measures

- Involvement of parent
- Keep computer in an open area
- Set rules and warn about dangers
- Talking with children
- Monitor computer activity
- Partitioning computer into separate account

The End

Thank You

Teacher : Jishna K

College of Applied Science, Thamarassery.