Unit VI

Chapter 6

Introduction to Cyber Security

Syllabus

Introduction to Cyber Security : Basic cyber security concepts, Layers of security, Vulnerability, Threat, Harmful acts-malware, Phishing, MiM attack, DOS attack, SQL Injection, **Internet Governance :** Challenges and constraints, Computer criminals, Assets and Threat, Motive of attackers, Software attacks, Hardware attacks, **Cyber Threats :** Cyber warfare, Cyber crime, Cyber stalking, Cyber terrorism, Cyber espionage, Comprehensive cyber security policy.

Chapter Contents

Chapter Contents

6.1 Introduction to Cyber Security :

Cyber security is the most worried matter as cyber threats and attacks are increasing.

Attackers are using more sophisticated methods to target the systems and causes impact on individuals, small-scale businesses or large organization.

All IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

Cyber Security is designed to protect networks and devices from external threats.

In the businesses, Cyber Security professionals are hired to protect their confidential information, maintain employee productivity, and improve customer confidence in products and services.

- The main goal of cyber security is the use of *authentication mechanisms*.

Definition of cyber security :

Cyber security is the process of protecting critical systems and sensitive information from digital attacks.

Cyber security defends computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

It is also known as information technology security or electronic information security.

The word cyber security is made up of two words one is cyber and other is security.

Cyber is related to the technology which contains systems, network and programs or data.

Security is the protection which includes systems security, network security, application and information security.

Importance of cyber security :

Today, Internet is playing very important role in every days life which makes hacker to exploit in more possible ways.

Therefore, maintaining the internet speed is as important as maintaining its security.

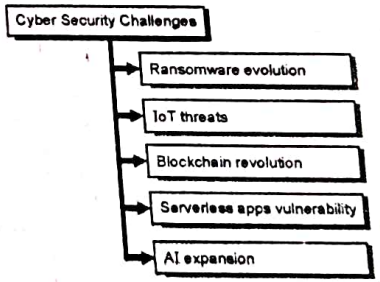
- Most of the commercial transactions, business deals, private information, human interests and emotions are processing through internet.
- Cyber security is one of the fast growing fields, not only in IT sectors but also in health, banking, educational, military, government and public sectors as well.
- Even governments of every country introducing new cyber security laws and policies to order prevent confidentiality, integrity and availability of the data and services.
- Cyber security is very important to secure data of companies.
- To prevent accidental insider attacks, it is necessary to train employees with proper knowledge and following security policies.
- Every company recruits cyber analysts for the company's security can help not only in identifying threat but also in event response process.
- The cyber security professionals plays important role in the incident investigation and implementing countermeasures to prevent attacks.
- Following are the reasons why cyber security is so important in the digital world :
  1. Cyber attacks can be expensive for businesses to continue.
  2. In addition to financial damage suffered, a data breach can also causes countless reputational damage.
  3. Cyber-attacks these days are becoming increasingly critical. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Due to the above reasons, cyber security has become an important part of the business or an individual.
- The focus now is on developing appropriate response plans to minimize the damage in the event of a cyber attack.

Why do cyber attacks happen ?

- The cyber attacks happen because criminals are interested in :
  1. Customers financial details (e. g credit card data).
  2. Sensitive personal data.
  3. Customers email addresses and login credentials.
  4. Customer databases.
  5. Clients lists.
  6. IT infrastructure.
  7. IT services (e.g. the ability to accept online payments).
  8. Intellectual property (e.g. trade secrets or product designs).
  9. Financial details of businesses.

6.2 Challenges to Cyber Security :

- Today cyber security is the main component of the country's overall national security and economic security strategies.
- The recent important cyber security challenges are as shown in Fig. 6.2.1.



(G-2892) **Fig. 6.2.1 : Cyber Security Challenges**

- The Cyber Security Challenges are as follows :
  1. Ransomware Evolution
  2. IoT Threats
  3. Blockchain Revolution
  4. Server-less Apps Vulnerability
  5. AI Expansion

1. Ransomware Evolution :

- Ransomware is a type of malware which locks the information on a victim's computer and payment is demanded before the ransomed data is unlocked.
- Access rights returned to the victim after successful payment.
- Ransomware is the nuisance of cyber security, data professionals, IT and executives.
- Day by day, ransomware attacks are growing rapidly in the areas of cybercrime.
- Business leaders and IT professionals need to have a powerful recovery strategy against the malware attacks in order to protect their organization.
- The strategy involves proper planning to recover corporate and customer's data and application.
- DRaaS solutions are the best protection against the ransomware attacks.
- With DRaaS solutions we can automatically back up our files, easily identify which backup is clean, and launch a fail-over with the press of a button when malicious attacks corrupt our data.

2. IoT Threats :

- Internet of Things (IoT) is a system of interconnected physical devices which can be accessible through the internet.
- The physical devices in IoT have a unique identifier (UID) and have the capability of transferring data over a network without any requirements of the human-to-human or human-to-computer interaction.
- The firmware and software running on IoT devices make consumer and businesses highly vulnerable to cyber-attacks.
- So every organization needs to work with cyber security professionals to make sure the security of their password policies, session handling, user verification, authentication and security protocols to help in risk managment.

3. Blockchain Revolution :

- Blockchain technology is the most important development in computing era.
- The blockchain technology allows crypto currencies like Bitcoin.
- It is global platform which allows two or more parties to do a transaction or do business without need of a third party for trust establishment.

- What blockchain systems will offer in regards to cyber security is difficult predict.
- The cyber security professionals can make some educated predictions regarding blockchain.
- There will be a tension but also balancing integrations with traditional, proven, cyber security approaches as the cyber security context emerges application and utility of blockchain.

4. Serverless Apps Vulnerability :

- Serverless apps depend on third-party cloud infrastructure or on a back-end service like google cloud function, Amazon web services (AWS) lambda etc.
- The serverless apps invite the cyber attackers to spread threats easily because the users access the application locally or off-server on their device.
- Therefore the user should take care for the security precautions while using serverless application.
- The serverless apps cannot do anything to keep the attackers away from our data.
- The serverless application will not help if an attacker gains access to our data through vulnerability such as leaked credentials, a compromised insider or by any other means.
- It is possible to run software with the application that provides best possibility to beat the cybercriminals.
- The size of the serverless application is small. It helps software developers to launch their applications easily and quickly.
- The web-services and data processing tools are examples of the serverless apps.

5. AI Expansion :

- Artificial Intelligence (AI) is the science and engineering of making intelligent machines, especially intelligent computer programs.
- The formation of intelligent machines with AI can work and react like humans.
- Artificial intelligence includes activities like speech recognition, learning, planning, problem-solving, etc.
- When the malicious attack starts, AI has the ability to protect and defend an environment which mitigates the impact.
- AI takes instant action against the malicious attacks at an instant when a threats impact a business.
- AI is considered as a future protective control that will allow our business to stay ahead of the cyber security technology curve.

6.3 Principles of Cyber Security :

- Let us now classify the principles related to security as this will help us understand the attacks on security better.
- The principles of security are : confidentiality, integrity, authentication and non-repudiation. Let us take an example to understand them.
- Assume that a person A wants to send a cheque worth Rs. 10,000/- to person B by putting the check inside an envelope.
- A would like to ensure that only B must get the envelope, and even if someone else gets it, he must not understand the details of the check. This is the principle of **confidentiality.**
- A and B would want to make sure that no one should be able to tamper with the contents of the cheque. This is the principle of **Integrity**.
- Next principle is **authentication** where B would like to be sure that the cheque has indeed come from A, and not from someone else posing as A.
- The next important aspect is that A should not refuse having written the cheque, after B deposits it in the bank.
- In such incident, the law will use A's signature on the cheque to disallow him to refute this claim, and settle the dispute. This is the principle of **non-repudiation**.
- These are the four major principles of security. In addition to these four, there are two more, **access control** and **availability**, which are linked to the overall system as a whole.

Security Goal :

- The three network security goals are :
  1. Confidentiality
  2. Integrity
  3. Availability

6.4 CIA Triad :

- The three letters in "CIA triad" stand for confidentiality, integrity and availability. The CIA triad is a widely used information security model.
- The aim of CIA triad model is to guide organizations about efforts and policies for the data security.

1. Confidentiality :

- The meaning of message confidentiality or privacy is that the sender and the receiver expect confidentiality and only the intended receiver should be able to decode the transmitted message correctly.
- To all others, the message must look like garbage..

2. Integrity :

- The meaning of message integrity is that the received data at the receiver must exactly be the same as were sent. The transmitted data must not changes during the transmission, neither accidentally nor maliciously.
- The message integrity is important for all the monetary exchanges occurring over the Internet.

3. Availability :

- The information should not be available to any unauthorized person but it should be always available to an authorized entity.

6.5 Layers of Cyber Security :

- Fig. 6.5.1 shows the seven layer architecture of cyber security.

Layer 7	The human layer
Layer 6	Perimeter security
Layer 5	Network security
Layer 4	Endpoint security
Layer 3	Application security
Layer 2	Data security
Layer 1	Mission critical assets

(G-2986) Fig. 6.5.1 : Layers of cyber security

- The following are seven layers of cyber security :
  1. Mission-Critical Assets
  2. Data Security
  3. Endpoint Security
  4. Application Security
  5. Network Security
  6. Perimeter Security
  7. The Human Layer

Layer 1 : Mission-Critical Assets :

- This is the data that is very critical to protect. Th businesses faces the malicious forces daily.
- An example of mission-critical assets in the Healthcar industry is Electronic Medical Record (EMR) software. I the financial sector, it is customer's financial records.

Layer 2 : Data Security :

- Data security controls will protect both the transfer an the storage of data.
- There should be backup security measure to prevent th loss of data. Data security needs the use of encryptio and archiving.
- Data security is an important focus for all businesses as breach of data can have horrible consequences.

Layer 3 : Application Security :

- Application security involves the security features th control access to an application and that application access to your mission critical assets.
- This layer includes the internal security of the applicatio itself.
- Most of the time, applications are designed with securi measures which provides protection when the app is use.

Layer 4 : Endpoint Security :

- Endpoint security controls protect the connectio between the devices and the network.
- This layer makes sure that the endpoints of user device are not exploited by breaches.
- This layer protects mobile devices, desktops, an laptops.
- This layer allows protection either on a network or in th cloud depending on the needs of a business.

Layer 5 : Network Security :

- Network security layer controls protect the business's network.
- The main goal of this layer is to prevent unauthorised access to the network.
- It is important to regularly update all systems on the business network with the essential security patches, including encryption.
- It is always best to disable unused interfaces for the further protection against any threats.

Layer 6 : Perimeter Security :

- Perimeter security layer makes sure that both the physical and digital security methods protect a overall business.
- It includes firewalls that protect the business network against external forces.

Layer 7 : The Human Layer :

- *The human layer is a very important layer, in spite of being known as the weakest link in the cyber security chain.*
- *It includes management controls and phishing simulations as an example.*
- *The aim of human management control is to protect the part which is critical to a business in terms of security.*
- This layer controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

6.6 Vulnerability :

Definition :

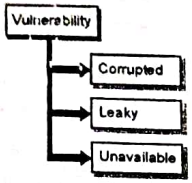
- Vulnerability is defined as the weakness in an information system, system processes or internal controls of an organization.
- It can be exploited by one or more attackers.

Examples of Vulnerabilities :

- Following are some examples of vulnerability :
  1. Due to a weakness in a firewall, malicious hackers can enter into a computer network.
  2. Lack of security cameras.
  3. Unlocked doors at businesses.
- With these weaknesses, anyone can harm a business or its assets.

6.6.1 Categories of Vulnerabilities :

- Fig. 6.6.1 shows the categories of vulnerabilities :

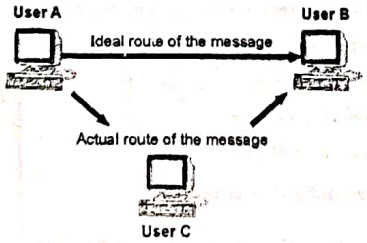


(G-2987) Fig. 6.6.1 : Categories of vulnerabilities

- The categories of vulnerability are as follows :
  1. Corrupted (Loss of integrity)
  2. Leaky (Loss of confidentiality)
  3. Unavailable or very slow (Loss of availability)

1. Corrupted (Loss of integrity) :

- We can say that the integrity of the message is lost, when the contents of a message are changed after the sender sends it, but before it reaches the desired recipient.
- Fig. 6.6.2 shows an example of loss of a message Integrity.



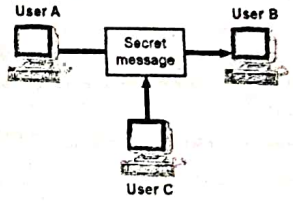
(G-2922) Fig. 6.6.2 : Loss of message integrity

- As shown in Fig. 6.6.2, user A sends a message to the user B.
- User C interfere with a message originally sent by user A to user B.

- User C somehow manages to access the message and makes changes in its contents and send the changed message to user B.
- In this case user A does not know about the message change whereas user B does not know that the contents of the message were changed after user A had sent it.
- This type of attack is known as **modification.**

2. Leaky (Loss of confidentiality) :

- Fig. 6.6.3 shows an example of compromising the confidentiality of a message.

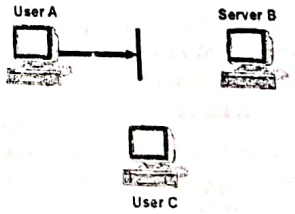


(G-2921) Fig. 6.6.3 : Loss of confidentiality

- As shown in Fig. 6.6.3, user A sends a message to the user B.
- Another unauthorized user C gets access to this secret message without permission of users A and B, which is not desired and this defeats the purpose of confidentiality.
- This type of attack is known as **interception.**
- Interception will cause loss of message confidentiality.

3. Unavailable or very slow (Loss of availability) :

- Fig. 6.6.4 shows the concept of attack on availability.

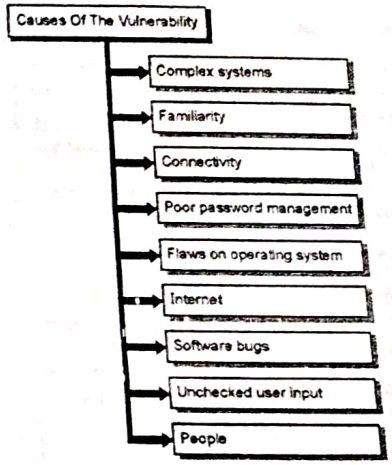


(G-2924) Fig. 6.6.4 : Attack on availability

- As shown in Fig. 6.6.4, an authorized user A cannot be able to contact the server B due to the intentional actions of unauthorized user C.
- This would defeat the principle of availability. Such an attack is known as **interruption.**
- The availability of resources becomes in danger due to Interruption.

6.6.2 Causes of the Vulnerability :

- The following are the causes of Vulnerabilities :



(G-2990) Fig. 6.6.5 : Causes of the vulnerability

1. Complex Systems :

- If the system is complex, it increases the probability of misconfigurations, flaws, or unintended access.

2. Familiarity :

- Cyber attackers may be known with common code, operating systems, hardware, and software which lead to known vulnerabilities.

3. Connectivity :

- The devices connected to the internet becomes more prone to vulnerabilities.

4. Poor Password Management :

- If the password used is weak and reused, it leads fro one data breach to several.

5. Flaws on Operating System :

- The flaws in the Operating systems and unsecured OS can give users full access and become a target for viruses and malware.

6. Internet :

- The internet can be installed automatically on computers because internet is full of spyware and adware.

7. Software Bugs :

- Programmers sometimes accidentally, leave an exploitable bug in the software that leads to system vulnerability.

8. Unchecked user input :

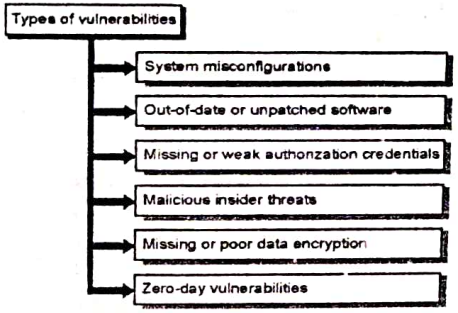
- If website or software assumes that all input by user is safe, it can run unintended SQL injection.

9. People :

- The biggest threat to the majority of organizations is social engineering. That means, humans can be one of the biggest causes of vulnerability.

6.6.3 Types of Vulnerabilities :

- Following are some of the most common types of cyber security vulnerabilities :



(G-2984)**Fig. 6.6.6 : Types of vulnerabilities**

1. System Misconfigurations :

- The network assets having different security controls or vulnerable settings can result in system misconfigurations.
- Cybercriminals commonly search networks for system misconfigurations.
- The network misconfigurations are increasing due to the rapid digital transformation.
- Therefore, it is important to work with experienced security professionals when implementing new technologies.

2. Out-of-date or Unpatched Software :

- Cybercriminals exploit unpatched vulnerabilities to carry out attacks and steal valuable data.
- In order to minimize these types of risks, it is necessary to establish a patch management schedule so that all the latest system patches are implemented as soon as they are released.

3. Missing or Weak Authorization Credentials :

- A common method of attackers use is to gain access to systems and networks through brute force like guessing credentials of employee.
- So it is important that employees should be educated on the best practices of cyber security so that their login credentials are not easily exploited.

4. Malicious Insider Threats :

- Unknowingly or with malicious intention, employees who have access to critical systems can share information that allows cybercriminals to breach a network.
- Insider threats can be very difficult to trace since all actions will appear legitimate.
- To help such types of threats, one should invest in network access control solutions, and divide the network according to employee seniority and expertise .

5. Missing or Poor Data Encryption :

- In case of poor or missing encryption, it becomes easy for attackers to intercept communication between systems and breach a network .
- In case of poor or unencrypted information, cyber adversaries are able to remove critical information and insert false information onto a server. This can weaken an organization's cyber security compliance efforts and lead to substantial fines from regulatory bodies.

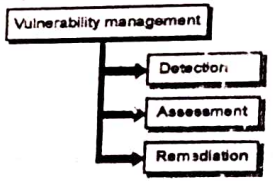
6. Zero-day Vulnerabilities :

- Zero-day vulnerabilities are specific software vulnerabilities known to the attacker but have not yet been identified by an organization or user.
- This means, there are no available fixes or solutions since the vulnerability has not yet been detected or notified by the system vendor.
- These are dangerous attacks as there is no way to defend against them until after the attack has been carried out.
- Hence, it is important to remain careful and continuously monitor your systems for vulnerabilities in order to minimize zero-day attacks.

6.7 Vulnerability Management :

Definition :

- Vulnerability management is the process which consists of identification, classification, remediation, and improvement of security vulnerabilities.
- Fig. 6.7.1 shows the three important elements of vulnerability management.



(G-2983)**Fig. 6.7.1 : Elements of vulnerability management**

- The vulnerability management consists of :
  1. Vulnerability detection
  2. Vulnerability assessment
  3. Vulnerability remediation

6.7.1 Vulnerability Detection :

- Vulnerability detection includes the following three methods :
  1. Vulnerability scanning
  2. Penetration testing
  3. Google hacking

1. Cyber Security Vulnerability Scan :

- Cyber Security Vulnerability Scan is done to search vulnerabilities in computers, applications or networks.
- A scanner (software) is used to scan the vulnerabilities.
- A scanner discovers and identifies the vulnerabilities that occur from misconfiguration and flawed programming within a network.
- Some vulnerability scanning tools are SolarWinds Network Configuration Manager (NCM), ManageEngine Vulnerability Manager Plus, Rapid7 Nexpose, Acunetix, Probely, TripWire IP 360 etc.

2. Penetration Testing :

- Penetration testing or pen testing is the testing of an IT asset for security vulnerabilities that an attacker could potentially exploit.
- Penetration Testing can be manual or automated.
- It also test security policies, employee security awareness, the ability to identify and respond to security incidents, and devotion to compliance requirements etc.

3. Google Hacking :

- Google hacking makes a use of a search engine in order to locate security vulnerabilities.
- Google Hacking is achieved through advanced search operators in queries.
- Advanced search operators in queries can locate hard-to-find information or data that has been accidentally exposed due to the misconfiguration of cloud services.
- These targeted queries are used to locate sensitive data that is not for public exposure.

6.7.2 Vulnerability Assessment :

- After a detection of vulnerability, it goes through the vulnerability assessment process.
- Vulnerability assessment process is a process which systematically reviews security weaknesses in an information system.
- This process highlights when a system is prone to any known vulnerabilities as well as it classifies the severity levels, and recommends appropriate remediation or mitigation if required.

The assessment process includes :

1. Identify
2. Verify
3. Mitigate
4. Remediate

1. **Identify vulnerabilities :**

It analyzes network scans, firewall logs, pen test results, and vulnerability scan which results to find irregularity that might highlight vulnerabilities prone to cyber-attacks.

2. **Verify vulnerabilities :**

- It decides whether an identified vulnerability could be exploited and it classifies its severity to understand the level of risk.

3. **Mitigate vulnerabilities :**

- It comes up with suitable countermeasures and measures their effectiveness if a patch is not available.

4. **Remediate vulnerabilities :**

- Wherever possible, it updates affected software or hardware.

6.7.3 Vulnerability Remediation :

- The vulnerability remediation process is a workflow which fixes or neutralizes detected weaknesses.
- It includes following steps :
  1. Find
  2. Prioritize:
  3. Fix
  4. Monitor

1. **Find :**

- It continuously monitors software inventory to be aware of which software components are being used and what needs immediate attention will significantly prevent malicious attacks.

2. **Prioritize :**

- The organizations must have prioritization policies.
- First, the risk of the vulnerabilities needs to be calculated going through the system configuration, the likelihood of an occurrence, its impact, and the security measures that are in place.

3. **Fix :**

- After knowing, the security vulnerabilities that require immediate attention, it is time to map out a timeline and work plan for the fix.

4. **Monitor :**

- Monitor projects and code for newly discovered vulnerabilities, with real-time alerts and notifications through all the relevant channels.

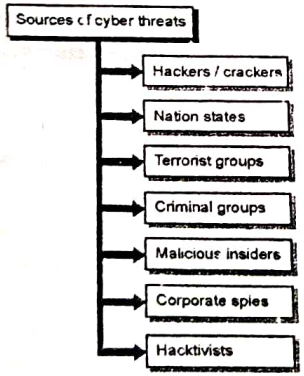
6.8 Threat :

Definition :

- A cyber security threat is malicious and intentional attack by an individual or organization in order to gain unauthorized access to another individual's or organization's network to damage, interrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive information.
- As per the definition taken from RFC 2828, Internet Security Glossary, we may define a threat as a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- Examples of common types of security threats include Malware, Phishing, MIM Attack, DOS Attack, SQL Injection etc.

6.8.1 Sources of Cyber security Threats :

- It is important to know the threat attackers and understand their tactics, techniques, and procedures in order to respond effectively to a cyber attack.
- Fig. 6.8.1 shows some of the common sources of cyber threats.



(G-2985) **Fig. 6.8.1 : Sources of cyber threats**

1. **Hackers / Crackers :**

- The motivation behind hacking is personal gain, revenge, aggravation, financial gain and political activism.
- They explore various cyber techniques to breach defenses and develop vulnerabilities in a computer system or network.
- Hackers or crackers develop new types of threats for the pleasure of challenge or bragging rights in the hacker community.

2. **Nation States :**

- Cyber attacks by a nation states can cause harmful impact. They can disrupt communications, military activities and everyday life.

3. **Terrorist Groups :**

- The terrorist do cyber attacks to destroy, get into, or exploit critical infrastructure to threaten national security, compromise military equipment, disturb the economy, and cause mass losses.

4. **Criminal Groups :**

- The aim of criminal groups is to get into systems or networks for financial gain. Criminal groups use phishing, spam, spyware, and malware attacks to conduct identity theft, online fraud, and system extortion.

5. **Malicious Insiders :**

- Malicious Insiders can be an employee, third-party vendors, contractors, or other business associates.
- Malicious Insiders have valid access to enterprise assets but they misuse that access to steal or destroy information for financial or personal gain.

6. **Corporate Spies :**

- Corporate spies do industrial or business spying.
- The motive behind the corporate spies is to make a profit or disturb a competitor's business by attacking critical infrastructure, stealing trade secrets, and gaining access.

7. **Hacktivists :**

- The reason behind the cyber attacks by the hacktivists is political cause rather than financial gain.
- Hacktivists target industries, organizations or individuals who don't support with their political ideas and plans.

6.8.2 Comparison of Treat and Vulnerability :

- Table 6.8.1 gives the difference between Treat and Vulnerability.

Table 6.8.1 : Comparison of Treat and Vulnerability

Sr. No	Threat	Vulnerability
1.	Threat take advantage of vulnerabilities in the system and can steal and damage data	Vulnerability is the weakness in hardware, software, or designs, which might allow cyber threats to happen.
2.	Can't be controlled	Can be controlled.
3.	It may or may not be intentional.	Generally, unintentional.
4.	Can be blocked by managing the vulnerabilities.	Vulnerability management is a process of identifying the problems, then categorizing them, prioritizing them, and resolving the vulnerabilities in that order
5.	Threat can be detected by anti-virus software and threat detection logs.	Vulnerability can be detected by penetration testing hardware and many vulnerability scanners.

6.9 Security Attacks :

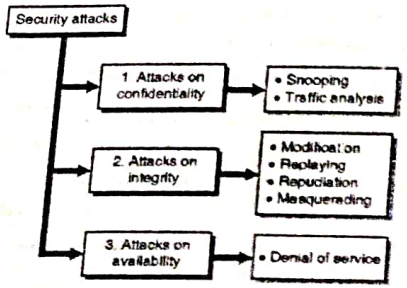
Definition :

- As per the definition taken from RFC 2828, Internet Security Glossary, we may define an attack on security as an assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Classification of attacks :

- The three goals of information security can get threatened by the security attacks.

– Fig. 6.9.1 shows classification of attacks.



(G-2338) **Fig. 6.9.1 : Classification of security attacks**

A. Attacks on Confidentiality :

1. Snooping :

– Snooping is defined as an unauthorized access to the information or as an unauthorized interception of the information. Snooping can be prevented by making the information non-intelligible to the unauthorized entity.

2. Traffic analysis :

– Even after making the data non-intelligible, an attacker can collect some other information such as email addresses of the sender or receiver by monitoring the online traffic.

B. Attacks on Integrity :

– The four types of attacks on integrity are modification, masquerading, replaying and repudiation.

1. Modification :

– In this type of attack, the attacker modifies the intercepted data to make it beneficial to himself.

2. Masquerading :

– Masquerading is also called as spoofing. In this type of attack, the attacker impersonates somebody else. For example, stealing the PIN of a credit card and pretending to be the customer.

3. Replaying :

– In this type of attack, the attacker obtains a copy of the message sent by a user and tries to replay it for his own benefit. This type of attack is often seen in the messages related to the bank transactions.

4. Repudiation :

– In this type of attack either the authorized sender or the authorized receiver is involved.

– The sender of a message may later on deny that he has sent that message or the receiver after actually receiving the message, may deny that he has received the message.

C. Attacks on Availability :

– The only one type of attack on the availability is the denial of service.

Denial of Services (DoS) :

– In this type of attack, a system may be slowed down or totally interrupted by the attackers. This could be done by using various strategies such as :

1. By flooding the server with bogus requests.
2. By intercepting and deleting the server's response to client.
3. By intercepting and deleting the client's request to the server.

6.10 Cyber Attacks (Harmful Acts) :

Definition :

– A cyber attack is a malicious attack by internet frauds or criminals.

– An intention behind the Cyber attack is to destroy the valuable data or to make trouble in the network operation.

– The idea behind such attacks is to expose sensitive data, to delete data or demand money.

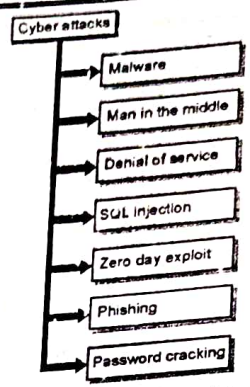
– Cyber attacks are very common now a days. They hit the internet every day.

– In order to exploit the system and break the valuable data, Malicious criminals launch cyber attacks into the computer or network

– Cyber attacks are of different types depending on the method used and the motivation behind the attack.

6.11 Types of Cyber Attacks :

– Fig. 6.11.1 shows the common types of cyber Attacks.



(G-2905) **Fig. 6.11.1 : Types of cyber Attacks**

6.11.1 Malware :

– The meaning of the term malware is malicious software.

– Malware is a file or code delivered over a network which infects, explores, steals or conducts almost any behavior of host computer.

– Malware is designed to gain access of computer or installed into the computer without the permission of the user.

– Malware software monitors the user's actions and keystrokes silently and gathers all confidential information of user.

– The unwanted tasks are performed in the host computer for the benefit of a third party. Malwares degrades the performance of the host computer.

6.11.2 Man-in-the-middle Attack (MITM) :

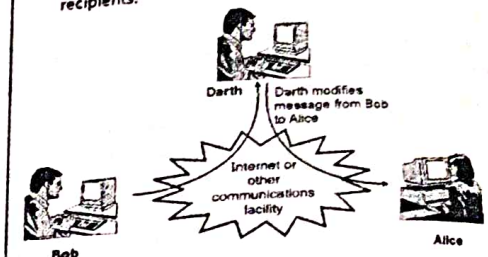
– This attack allows an attacker to intercepts the communication between the client and server.

– Due to this, an attacker can read, insert and modify the data in the intercepted connection.

– In modification, the original data sent by the authentic user is disrupted or modified by the attacker to make it non meaningful for the receiver.

– Usually the content sequence in the message is changed.

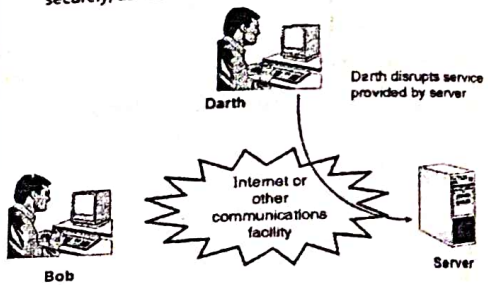
– Thus in modification of message as shown in Fig. 6.11.2, the attacker modifies the contents of message after sender sends it but before it reaches to indented recipients.



(G-2857) **Fig. 6.11.2 : Modification of messages**

6.11.3 Denial-of-service Attack :

– In the denial of service attack, an attacker makes the network unavailable for the user to communicate securely, as shown in Fig. 6.11.3.



(G-2858) **Fig. 6.11.3 : Denial of service**

– It is generally done by interrupting in the network connection between the users or making some services unavailable for user or disrupts the entire network by overloading it with unwanted messages.

– This slows down the network and becomes unavailable for users.

6.11.4 SQL Injection :

– It this attack, some data will be injected into a web application to manipulate the application and get the required information.

- A structured query language (SQL) injection attack targets the database of a website and tricks the server into providing access to modify the data by unauthorized criminals.

6.11.5 Zero-day Exploit :

- A zero-day (0-day) exploit is a cyber attack that targets a software vulnerability which is unknown to the software vendor or to antivirus vendors.
- The Zero-day exploit attack follows the announcement of network vulnerability.
- The attacker observes the vulnerability and uses this duration of time to exploit a large number of computers in the network.
- A typical target for a zero-day exploit includes government departments, large enterprises, large number of home users who use a vulnerable system, such as a browser or operating system.

6.11.6 Phishing :

- Phishing attack tries to steal sensitive information of uses like user login credentials and credit card number.
- The phishing attacks steals the identity and the personal information like username, password, and credit card number etc. of the user that can steal money from the user account.
- In Vishing (voice phishing) attack, a telephone is used as a medium for identity theft.
- In Smishing (Sms phishing) attack, a sms is used to attract the customers.

6.11.7 Password Cracking :

- In this type of attack, attackers try to crack the password of a user by trying out all possibilities or using tools.
- John the ripper, hashcat aid the criminals etc. are the password cracking tools.
- These attacks are typically possible through the use of software that expedites cracking or guessing passwords.

6.12 Internet Governance :

Definition :

- Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, standards, rules, decision-making procedures, and programs that shape the evolution and use of the internet.

Internet Governance Issues :

- Some of the key governance issues are as follows.
  1. Infra structure and standardization line
  2. The logical dimension
  3. The content dimension
  4. The social and developmental dimension

Challenges to Internet Governance :

- The challenges to Internet Governance are as follows :
  1. Speed and changing nature of the internet
  2. Internet as part of digitalization
  3. Concentration of digital power
  4. Digital geopolitics and the environment
  5. Shaping the digital future
  6. The future of regulation
  7. Multistakeholderism
  8. Participation in decision-making
  9. Managing critical Internet Resources
  10. Access and Diversity
  11. Security, Openness and privacy

6.13 Computer Criminals :

- Computer crime is also referred as cybercrime, e-crime, electronic crime or hi-tech crime.
- Computer criminals have access to huge amounts of hardware, software, and data.

Definition :

- Computer (Cyber) crime is defined as a crime performed by a knowledgeable computer user, sometimes referred as a hacker who illegally browses or steals a company's or individual's private data.

- Computer criminals can use a device to access a user's personal information, confidential information of business, government information, or disable a device. They can sell or explicit the above information online.

6.13.1 Causes of Cybercrimes :

- In most cases, someone commits a cyber crime to obtain goods or money.
- They target rich people or rich organizations like banks and financial firms where a large amount of money flows daily. They hack sensitive information.
- Some people commit a computer crime because they are pressured, or forced, to do so by another person.
- Some people also opt a computer crime to prove they can do it.
- It is difficult to catch such criminals.
- Hence, the numbers of cyber crime are increasing across the world.
- Computers are vulnerable, so laws are required to protect and safeguard them against cybercriminals.

6.13.2 Types of Cybercrimes :

- Following are the types of cyber-crimes :
  1. Hacking
  2. Child pornography and Abuse
  3. Piracy or Theft
  4. Identity Theft
  5. Computer Vandalism
  6. Malicious Software
  7. Fraud Calls/E-Mails
  8. Fake news sharing in social media
  9. Online illegal selling (Dark Web)

Hacking :

- In hacking, hackers send illegal instruction to any other computer or network.
- Hackers will hack a person's computer and they access his personal or sensitive information.

Child pornography and Abuse :

- The internet is used to abuse children sexually worldwide.
- In this type of cyber-crime, criminals solicit minors through chat rooms for the purpose of child pornography.

Piracy or Theft :

- When a person violates copyrights and downloads music, movies, games, and software then this crime occurs.

Identity Theft :

- In this crime, a criminal accesses person's data such as bank account, credit cards, debit card and other sensitive information to draw off money or to buy things online in the victim's name. This results in major financial losses for the victim.

Computer Vandalism :

- This crime involves destructing computers and data in various ways and disrupting businesses.
- Typical computer vandalism involves the generation of malicious programs.
- These programs are designed to perform harmful tasks such as erasing hard drive data or extracting login credentials.

Malicious Software :

- Malicious Software is Internet-based software or programs which disrupts a network.
- Such software gains access to a system, steal sensitive information and causes damage to software present in the system.

Fraud Calls / E-Mails :

- In this cyber crime, criminal contacts you through bogus messages, call or email. In bogus messages, call or email, criminal declares himself to be an employee of a bank and he has called related to your bank account or cards.
- The criminal asks for personal details like ATM card, OTP, password, etc. or asks to click on the link sent by himself.
- If you wrongly trust them and give them the details, you will lose the money in your account.

Fake news sharing in social media :

- Some cybercriminals work on social networking sites only. They spread social, religious, and political rumors.
- The people who get impressed unintentionally share the link or post shared by the unknown people in their social media. Due to this, the users have to face legal actions.
- Sharing any illegal link or post on social media is also a cybercrime.

Online Illegal Selling :

- In this type of crime, a criminal sells illegal weapons, drugs, smuggled goods, or personal information to the person.
- They sell these things on an illegal online shopping platform and the transaction is also done through crypto currency.
- It supports terrorism and black marketing.

6.14 Assets and Threat :

Assets :

- An asset is any data, device or other component of an organization's systems which is valuable.
- An asset is valuable because it contains sensitive information or can be used to access such information.
- An asset contains hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information.
- Assets should be protected from illegal access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization

Example of Asset :

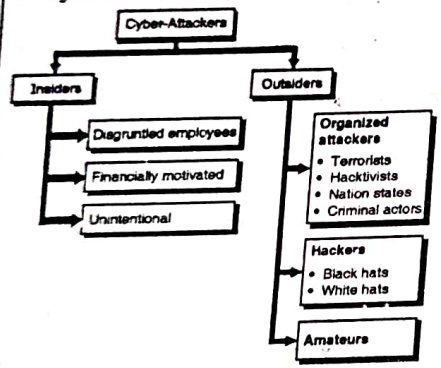
- The desktop computer, laptop or company phone of employee is considered an asset.
- Similarly, critical infrastructure such as servers and support systems are assets.
- An information asset is most common asset of organization.
- The databases and physical files are assets and they store sensitive data.
- Information is stored in an information asset container.

Threat :

- A threat is any event that could negatively affect an asset if it's lost, knocked offline or accessed by an unauthorized party.
- Threats can be classified as conditions that compromise the confidentiality, integrity or availability of an asset and can either be intentional or accidental
- An intentional threat contains criminal hacking or a malicious insider stealing information.
- An accidental threat involves employee error, a technical malfunction or an event causing physical damage, such as a fire or natural disaster.

6.15 Categories of Cyber Attackers :

- Fig. 6.15.1 shows the categories of cyber-attackers.



(G-2988) **Fig. 6.15.1 : Categories of Cyber Attackers**

- Cyber attackers can be broadly classified into two types :
  1. Insiders
  2. Outsiders

1. Insiders :

- Insider cyber attackers act within an organization.
- The three basic categories of insiders are :
  1. Disgruntled employees
  2. Financially motivated insiders
  3. Unintentional insiders

Disgruntled employees :

- Disgruntled employees can launch disciplinary attacks or threaten the safety of internal systems.

Financially motivated insiders :

- Financially motivated insiders (Thievus) can misuse company assets or manipulate the system for personal gain.
- Some financially motivated insiders can be acting on ethical grounds or for other reasons.

Unintentional insiders :

- Unintentional insiders can unintentionally make possible outside attacks, but are not strictly primary attackers.

2. Outsiders :

- Outsider cyber attackers attempt to penetrate an organization from the outside.
- Based on organization, motives and professional level, outsider cyber attackers can be classified into the following three types :
  1. Organized attackers
  2. Hackers
  3. Amateurs

1. Organized attackers :

- An organized attacker contains organizations of terrorists, hacktivists, nation states, and criminal actors.

Terrorist :

- A terrorist search for a political statement or tries to inflict psychological and physical damage on their targets to achieve their political gain or create fear in opponents or the public.

Hacktivists :

- Hacktivists try to find a political statement, and causes damage, but the motivation is mainly to raise awareness, not encourage change through fear.

Nation states :

- A nation state attacker collects information and commits damage on the behalf of governments.
- A nation state attacker are generally highly trained, highly funded, tightly organized and are often backed by substantial scientific capabilities.
- A nation state attacks are highly sophisticated attacks and directed toward specific goals, but their specific motives can be mixed.

Criminal actors :

- Criminal actors are typically organized groups of professional criminals.
- Criminal actors can act within complex criminal ecosystems in cyberspace that are stratified and service oriented.
- The person responsible for organized crime is typically focused on control, power, and wealth.

2. Hackers :

- Hackers can be gentle explorers, malicious intruders or computer trespassers.
- A group of hackers includes individuals who break into computers mainly for the challenge and examine status achieved from getting access.
- Sometimes, hacking is not a malicious activity. A "white hat" hacker discovers weaknesses in computer systems or networks in order to improve them, often with permission or as part of a contract with the owners.
- On the contrary, "black hat" hacking is the malicious exploitation of a target system for performing illegal activities.
- The black hat hackers could be hired by or be sponsored by criminal organization or governments for financial gain or political reason.
- Thus, hacking can involve espionage, extortion, theft, vandalism etc.

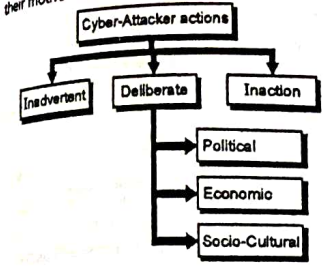
3. Amateurs :

- Amateurs are less-skilled hackers. They are also known as "script kiddies" or "noobs".
- They often use existing tools and instructions that can be found on the Internet.
- Amateurs can simply be curious or enjoy the challenge, others can be seeking to build up and demonstrate their skills to fulfill the entry criteria of a hacker group.
- An amateur makes use of very basic but powerful tools.
- They can cause a lot of damage in spite of their lower skills.

6.16 Motive of Attackers :

The categories of cyber-attackers allow us to better understand the motivation of attackers and the actions they take.

Fig. 6.16.1 shows the types of cyber-attacker actions and their motivations.



(G-2989) **Fig. 6.16.1 : Types of cyber-attacker actions and their motivations**

- The operational cyber security risks occur from three types of actions :
  1. Inadvertent actions
  2. Deliberate actions
  3. Inaction

1. Inadvertent actions :

- Inadvertent actions are generated by insiders. These actions are taken without malicious or harmful intention.

2. Deliberate actions :

- Deliberate actions are generated by insiders or outsiders.
- These actions are taken intentionally and are intended to do harm.
- Following are three categories of motivation for deliberate actions :
  1. Political motivations
  2. Economic motivations
  3. Socio-cultural motivations

Political motivations :

- Examples of political motivations include destroying, disrupting or taking control of targets; spying and making political statements, protests or disciplinary actions.

Economic motivations :

- Examples of Economic motivations include stealing of intellectual property or economically valuable assets like funds, credit card information, blackmailing, fraud, industrial spying and damage.

Socio-cultural motivations :

- Examples of Socio-cultural motivations include attacks with philosophical, theological, political, and even humanitarian goals.
- It also includes fun, curiosity and a desire for publicity or ego satisfaction.

3. Inaction :

- Inactions are generated by insiders.
- These actions include a failure to act in a given condition because of a lack of appropriate skills, knowledge, guidance or availability of the correct person to take action.

6.17 Types of Attacks :

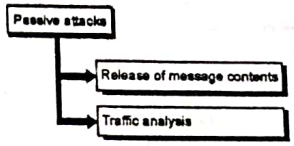
- A useful means of classifying security attacks in terms of passive attacks and active attacks.
- In computer and computer networks an attack is any attempt to alter, disable and destroy or gain unauthorized access of confidential information.
- The X.800 and RFC2828 classify security two types of attacks.
  1. Passive attacks
  2. Active attacks

6.17.1 Passive Attacks :

Definition :

- Passive attack is defined as the type of security attack where, the attacker makes attempt to collect information from the system but does not modify or alter the system data or resources.
- Examples of passive attacks are eavesdropping (extracting information) or monitoring of network traffic. The goal of attacker is to gain the information that is being transmitted.
- This is the easiest form of attack and can be performed without difficulty.

- The two types of passive attacks are shown in Fig 6.17.1.

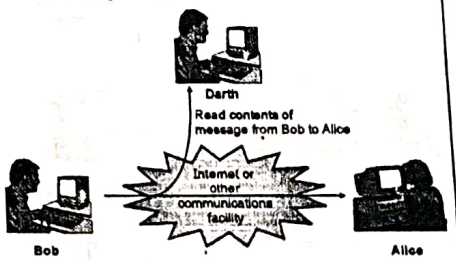


(G-2859) **Fig 6.17.1 : Types of Passive attacks**

1. Release of message contents
2. Traffic analysis

1. Release of message contents :

- We may want to prevent the attacker from learning sensitive and confidential information through transmissions that take place through telephone calls or email messages or files transferred on network.
- When we send a confidential email to our friend, we want only him to access this mail. However, if this mail is accessed by unauthorized users then contents of message are released to somewhere else. This type of attack is called release of message contents, which is shown in Fig. 6.17.2.



(G-2854) **Fig. 6.17.2 : Release of message contents**

- There are different security mechanisms available to prevent such type of attacks.

2. Traffic analysis :

- Low imagine that we mask the contents of the message using encryption.
- Now the attacker can capture the contents of the message but cannot extract any information from it
- Then he might observe a pattern of messages, to get some information like the location, or any clue regarding the origin of message.
- This type of passive attack is known as traffic analysis and is shown in Fig. 6.17.3.

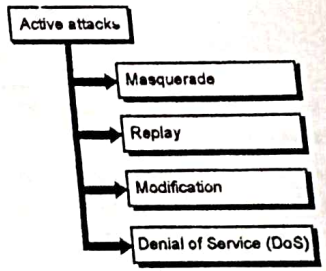
(G-2854) **Fig. 6.17.3 : Traffic analysis**

- The message is sent and received in normal manner and neither sender nor receiver is aware that someone else has read message or observed pattern of messages.
- We can prevent such attacks by means of encryption.
- While dealing with the passive attacks the emphasis is on prevention rather than detection.

6.17.2 Active Attacks :

Definition :

- An active security attack is defined as the type of attack where, the attacker is able to listen to the transmission and able to modify or obstruct it as well.
- Active attacks involve modification of a data stream or creation of a false stream of messages.
- Attacker's aim in such attack is to corrupt or destroy the data as well as network.
- Active attacks are classified into four categories as shown in Fig. 6.17.4.
- They are :
  1. Masquerade
  2. Replay attack
  3. Modification of messages
  4. Denial of service



(G-2860) **Fig 6.17.4 : Types of Active attacks**

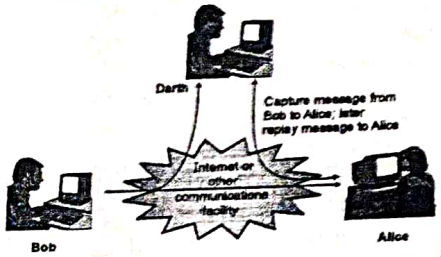
1. Masquerade :

- A masquerade takes place when an attacker pretends to be an authentic user to gain access to a system, or steal important data from system.
- An attacker generally does this by stealing login id and password of authentic user.
- Once attacker gain access, they get full access to the network and deletion or changing the data or network policies of organization as shown in Fig. 6.17.5.

(G-2855) **Fig. 6.17.5 : Masquerade attack**

2. Replay attack :

- A replay attack is also known as playback attack where attacker repeatedly transmits the valid data to make the network congested or delayed the transmission of data.
- Replay attack involves passive capturing of data and retransmission of subsequent information to create an undesirable effect as shown in Fig. 6.17.6.



(G-2856) **Fig. 6.17.6 : Replay attack**

3. Modification of messages :

- In modification, the original data sent by the authentic user is disrupted or modified by the attacker to make it non meaningful for the receiver. Usually the content sequence in the message is changed.
- Thus in modification of message as shown in Fig. 6.17.7, the attacker modifies the contents of message after sender sends it but before it reaches to indented recipients.

(G-2857) **Fig. 6.17.7 : Modification of messages**

4. Denial of service :

- In the denial of service attack, an attacker makes the network unavailable for the user to communicate securely, as shown in Fig. 6.17.8.

(G-2858) **Fig. 6.17.8 : Denial of service**

- It is generally done by interrupting in the network connection between the users or making some services unavailable for user or disrupts the entire network by overloading it with unwanted messages.
- This slows down the network and becomes unavailable for users.
- The active attacks can be detected easily as compared to passive attacks. Once attacker got entire access to the network or server he can do the following things :
  1. Flood the entire network or server with traffic until shutdown occurs due to overloading.
  2. Block ongoing traffic to deny the access to network resources even to the authorized users.

- Different security policies like firewall, intrusion detection system helps to protect such type of attacks.

6.17.3 Comparison of Active and Passive Attacks :

Table 6.17.1 : Comparison of Active and Passive Attacks

Sr. No.	Parameter	Active Attack	Passive Attack
1.	Physical control of the network	Needed	Not needed
2.	Ease of detection	Easy	Difficult
3.	Affects the system?	Yes	No
4.	Modification of data?	Yes	No
5.	Types	Masquerade, session replay, denial of service	Release of message, traffic analysis.
6.	Checking of loopholes	No	Yes
7.	Prevention	Difficult	Easy

6.18 Software Attacks :

Definition :

- The software designed to gain access of computer or installed into the computer without the permission of the user is known as software attack.
- The meaning of the term malware is malicious software.
- Malicious code (sometimes called as malware) is a type of software attack.
- Malware is a file or code delivered over a network which infects, explores, steals or conducts almost any behaviour of host computer.
- Malware is designed to gain access of computer or installed into the computer without the permission of the user.
- Malware software monitors the user's actions and keystrokes silently and gathers all confidential information of user.
- The unwanted tasks are performed in the host computer for the benefit of a third party. Malwares degrades the performance of the host computer.

Types of Malware (Software attacks) :

- The software attacks are as follows :
  1. Virus
  2. Worm
  3. Trojan horse
  4. Adware
  5. Spyware
  6. Browser hijacking software
  7. Scareware

Virus :

- A virus is a self-replicating program code.
- A virus can damage or harm the host computer by deleting or adding files.
- It spreads throughout the computer files without user's knowledge.
- During the time of execution, the replicated copy of virus is self inserted into the other computer programs.
- A virus can be spread though email attachment, pen drives, digital images, audio or video clips, etc.
- It can occupy memory space of the computer by replicating the copy of the code. It slows down the performance of the computer or formats the host machine.

Worm :

- Worms are very similar to viruses which can replicate themselves.
- It is a replicating code that comes via emails which appear legitimate.
- Worms do not need human interference to travel over the entire network and they can spread from the infected machine to the whole network.
- Worms can spread through a network by using the loopholes in the operating system or through email.
- Due to the replication and spreading, worms consume the network resources such as space and bandwidth and can force the network to choke.

Trojan horse :

- It is a malicious code installed in the host machine by pretending to be useful software.
- Due to this, the user clicks on the link or download the file that pretends to be a useful file or software from a legal source.
- It damages the host computer by manipulating the data. It also generates a backdoor in the host computer that could be controlled by a remote computer.

Adware :

- Adware is a special type of malware used for forced advertising.
- Adware malware redirects the page to some advertising page or pop-up an additional page that promotes some product or event.

Spyware :

- Spyware is installed in the target computer with or without the user consent.
- It is designed to steal sensitive and confidential data from the target computer.
- Spyware collects the browsing habits of the user and sends it to the remote server.

Browser hijacking software :

- This is a malicious software downloaded along with the free software offered over the Internet and it is installed in the host computer without the knowledge of the user.
- Browser hijacking software modifies the setting of browser and redirect links to other unintentional sites.

Scareware :

- Suddenly a pop-up alert appears on the screen while surfing the Internet and it warns about the presence of dangerous virus, spywares, etc. in the user's computer.
- As a remedy, the message suggests download the full version of the software.
- When the user proceeds to download, a scareware is downloaded into the host computer.
- It holds the host computer until ransome money is paid.
- The scareware can neither be uninstalled from computer nor can it be used till the money is paid.

6.19 Hardware Attacks :

Definition :

- The attacks which directly exploit interaction with a system's electronic components are known as hardware attacks.

Hardware attacks :

- The following are the common hardware attacks :
  1. Backdoors
  2. Spying
  3. Inducing faults
  4. Hardware modification
  5. Fake product assets

Backdoors :

- The backdoors are manufactured for malware or other penetrative purposes. They aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory
- The creation of backdoor includes the presence of hidden methods for bypassing normal computer authentication systems.

Spying :

- Spying gains access to protected memory without opening other hardware.

Inducing faults :

- If faults includes in ay hardware interrupts the normal behaviour of system.

Hardware modification :

- The modification in hardware tampers invasive operation of hardware or software.

Fake product assets :

- A fake product asset creates extraordinary operations, and those operations gains malicious access to the systems.

6.19.1 Devices Affected by Hardware Attacks :

- Hardware attack affects the following devices :
  1. Access control systems like authentication tokens
  2. Network appliances
  3. Industrial control systems
  4. Surveillance systems
  5. Components of communication infrastructure

6.19.2 Motive of Hardware Attacks :

- The main motivations of hardware attacks are:
  1. To clone the hardware.
  2. To break the services and obtaining them with piracy.
  3. To imitate user authentication for system access.
  4. To leak the data.
  5. To unlock devices in order to gain access to an internal shell or to increase control of a system.
  6. To unlock hidden features.

6.20 Cyber Threats :

- A cyber threat is a malicious and purposeful attack by an individual or organization in order to gain unauthorized access to another individual's or organization's network to damage, disturb, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.
- In this section we will the following cyber threats :
  1. Cyber Warfare
  2. Cyber Crime
  3. Cyber Stalking
  4. Cyber Terrorism
  5. Cyber Espionage

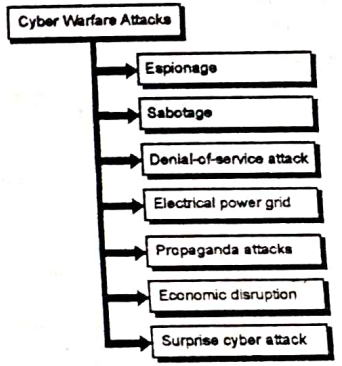
6.21 Cyber Warfare :

Definition :

- Cyber Warfare is a set of actions by a nation or organization to attack on countries or institutions computer network systems with the purpose of disrupting, damaging or destroying infrastructure by viruses or denial-of-service attacks.
- Cyber warfare tries to attack on financial infrastructure, public infrastructure like dams or electrical systems, on safety infrastructure like traffic signals or early warning systems, attacks against military resources or organizations etc.

6.21.1 Types of Cyber Warfare Attacks :

- Fig. 6.21.1 shows of the main types of Cyber Warfare Attacks.



(G-2991)**Fig. 6.21.1 : Types of Cyber Warfare Attacks**

1. **Espionage :**
   - Espionage means spying other countries to steal secrets.
   - Espionage may involve using a botnet or spear-fishing attack in order to gain a foothold in a computer before extracting sensitive information.
2. **Sabotage :**
   - Government organizations should determine sensitive information and the risks if data is compromised.
   - Hostile governments or terrorists can steal data, destroy it, or influence insider threats.
   - Insider threats can be careless employees or government employees with relationship to the attacking country.
3. **Denial-of-Service Attack :**
   - With flooding of fake requests and forcing the website to handle these requests, DoS attacks prevent legal users from accessing a website.

- This type of attack disturbs critical operations and systems and block access to sensitive websites by civilians, military and security personnel, or research bodies.

4. **Electrical Power Grid :**

- Attack on the power grid allows attackers to immobilize critical systems, disturb infrastructure, which results in the physical harm.
- An attack on the power grid disturbs communications and render services like text messages and broken communications.

5. **Propaganda Attacks :**

- This attack tries to control the minds and thoughts of people living in or fighting for a target country.
- Propaganda attack can be used to expose embarrassing truths, spread lies to make people lose trust in their country, or side with their enemies.

6. **Economic Disruption :**

- Mostly economic systems operate using computers.
- Attackers target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

7. **Surprise Cyber attack :**

- This attack takes place when the enemy is not expecting attack and it weaken their defences.
- Surprise cyber attack can be used to weaken the enemy in preparation for a physical attack as a form of hybrid warfare.

6.22 Cyber Crime :

Definition :

- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Cybercriminals or a hacker commits cybercrime to make money.
- Cybercrime is carried out by individuals or organizations.
- Some cybercriminals are prepared and they use advanced techniques and are highly technically skilled. Others are trainee hackers.
- Cybercrime is an illegal action against any individual using a computer, its systems, and its on ine or offline applications.
- Various types of Cyber crime attack modes are Hacking, Denial of Service Attack, Software Piracy, Phishing, and Spoofing.

Examples of Cybercrime :

- Following are some most commonly occurring Cybercrimes :
  1. The fraud by manipulating computer network
  2. Unauthorized access to or modification of data or application.
  3. Intellectual property theft which includes software piracy.
  4. Industrial spying and access to or theft of computer materials.
  5. Writing or spreading computer viruses or malware.
  6. Digitally distributing child pornography

6.23 Cyber Stalking :

Definition :

- It is an act of constant and unwanted contact from someone online.
- Cyber stalkers make use of internet, cell phone, and/or any other electronic communication device to stalk another person.
- It may involve false claims, threats, identity theft, damage to data or equipment, solicitation of minors for sexual purposes, and any other form of repeated offensive behaviour.
- It may include creeping where a person obtains the personal information about another through the internet, typically social networking sites.
- Cyber stalking can occur anywhere, including at home, work, schools, in chat rooms, message boards, discussion forums, emails, text messages, and on social networking sites.

Typical Cyberstalkers :

- Most of the time the cyberstalker is someone the victim knows.

- Some cyber stalkers search their victims by using a search engine and become obsessed with finding information about the victim.
- Typical Cyber stalkers can be :
  1. Co-workers
  2. Former spouses
  3. Friends
  4. Boyfriends
  5. Girlfriends
  6. Ex-partner
  7. Online associates

Examples of Cyber Stalking :

- Cyberstalkers use a variety of strategies and techniques to humiliate, harass, control and threaten their victims.
- Many cyberstalkers are technically knowledgeable as well as creative in their ways.
- Following are some examples of how Cyberstalking might take place :
  1. Sending threatening, vulgar or offensive emails or messages to the victim
  2. Releasing the victim's confidential information online.
  3. Tracking of online actions of the victim through tracking devices.
  4. Posting offensive, suggestive, or rude comments online.
  5. Joining the same groups and forums as the victim.
  6. Posting or distributing real or fake photos of the victim.
  7. Sending explicit photos of themselves to the victim
  8. Using technology for blackmailing or threatening the victim.
  9. Making fake posts intended to shame the victim.
  10. Repeatedly messaging the victim.
  11. Hacking of the victim's online accounts.
  12. Attempting to extract explicit photos of the victim.
  13. Sending unwanted gifts or items to the victim.
  14. Tagging the victim in irrelevant posts.
  15. Creating fake profiles on social media to follow the victim.
  16. Continuing harassment even after being asked to stop.
  17. Using hacking tools to get into the victim's laptop or smart phone camera and secretly record them.

6.23.2 Types of Cyber Stalking :

- The following are the types of Cyber Stalking :
  1. Catfishing
  2. Monitoring check-ins on social media
  3. Spying via Google Maps and Google Street View
  4. Hijacking webcam
  5. Installing Stalkerware
  6. Tracking location with geotags

1. **Catfishing :**

- Catfishing includes the formation of fake profiles or copying of existing ones on social media to approach victims.

Monitoring check-ins on social media :

- Observing the activities of a victim on social media to precisely estimate their behaviour pattern.

Spying via Google Maps and Google Street View :

- To spy on a victim and find their location from posts or photos on social media by using the street View.

Hijacking webcam :

- Webcams can be hijacked by launching malware-infected files into the victim's computer.

Installing Stalkerware :

- Stalkerware records the location, allows access to texts and browsing history, makes audio recordings, etc., without the victim's knowledge.

Tracking location with geotags :

- Digital pictures are geotagged with the time and location of the picture.
- If it is in the metadata format, it becomes easier for stalkers to access that information by using special apps.

6.23.3 Protective Measures for Cyber Stalking :

- The Protective Measures for Cyber Stalking are as follows :
  1. Build up the routine of logging out of the PC when not in use.
  2. Set strong and unique passwords for your online accounts.
  3. Cyber Stalkers can use the low security of public Wi-Fi networks to spy on your online activity. So, avoid sending personal emails or sharing your sensitive information when connected to an unsecured public Wi-Fi.
  4. Make use of the privacy settings provided by the social networking sites and keep all information restricted to the nearest friends only.

6.24 Cyber Terrorism :

Definition :

- Cyber terrorism is a deliberate attack against a computer system, computer data, programs and other information with the only aim of violence against secret agents and subnational groups.
- Cyber terrorism is also known as information wars.
- It can be defined as an act of Internet terrorism that includes deliberate and large-scale attacks and disruptions of computer networks using computer viruses, or physical attacks using malware, to attack individuals, governments and organizations.
- The main goal of cyber terrorism is to cause harm and destruction.
- Individuals and groups are misusing the secrecy with the use of the internet.
- They threaten individuals, certain groups, religions, ethnicities or beliefs.

6.24.1 Categories of Cyber Terrorism :

- Cyber terrorism can be broadly categorized under three major categories :
  1. Simple
  2. Advanced
  3. Complex

Simple :

- Simple cyber terrorism consists of basic attacks including the hacking of an individual system.

Advanced :

- Advanced cyber terrorism is more sophisticated attacks and can involve hacking many systems and/or networks.

Complex :

- Complex cyber terrorism is coordinated attacks that can have a large-scale impact and make use of sophisticated tools.

6.24.1 Examples of Cyber Terrorism :

- Cyber terrorism can happen over the public internet, over private computer servers, or even through secured government networks.
- There are many ways in which a criminal could use electronic means to incite fear and violence.
- It less expensive to buy a computer than to access guns or bombs, making this approach attractive for many potential criminals worldwide.
- It can be unidentified and conducted at a great distance away from the target.
- Following are few examples of cyber terrorism :
  1. Foreign governments can use hackers to spy on U.S. intelligence communications in order to learn about location of our troop or otherwise gain a planned advantage at war.
  2. Domestic terrorists can break into the private servers of a corporation to learn trade secrets, steal banking data or the private data of their employees.
  3. Global terror networks can disturb a major website to generate a public nuisance or inconvenience, or even more seriously, try to stop traffic to a website publishing content with which they disagree.
  4. International terrorists try to access and disable the signal which flies drones or otherwise controls military technology.

6.25 Cyber Espionage :

Definition :

- Cyber espionage or cyber spying is a attack in which an unauthorized user tries to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

- Cyber espionage is mainly used to collect sensitive or classified information, trade secrets or other types of IP that can be used by the attacker to create a competitive advantage or sold for financial gain.
- In some cases, the breach is simply cause reputational harm to the victim by exposing private information or questionable business practices.
- Cyber espionage attacks are motivated by financial gain; they can also be installed in combination with military operations or as an act of cyber terrorism or cyber warfare.
- Cyber espionage can lead to interruption of public services and infrastructure, as well as loss of life when it is part of a broader military or political campaign.
- The most common targets of cyber espionage contains large corporations, government agencies, academic institutions or other organizations that possess valuable IP and technical data.
- Cyber spies most commonly attempt to access the following assets :
  1. Military intelligence.
  2. Intellectual property such as product formulas or blueprints.
  3. Business goals, strategic and marketing plans.
  4. Research and Development data and activity.
  5. Academic research data.
  6. Political strategies, affiliations and communications.
  7. Salaries, bonus structures and other sensitive information regarding organizational finances and expenditures.
  8. Client or customer lists and payment structures.

6.25.1 Cyber Espionage Tactics :

- Cyber espionage tactics are varied. They include, but are not limited to :
  1. Cyber Espionage exploits vulnerabilities in websites or browsers.
  2. Cyber Espionage makes supply chain attacks that target the primary target's partners.
  3. Malware, Trojans and worms.
  4. Spear phishing emails intended to escalate the attacker's network rights.
  5. Infecting updates for commonly used third-party software applications.

6.25.2 Preventive Measures for Cyber Espionage :

- In order to protect data and prevent cyber espionage, an organization can take following precautions :
  1. Observe systems for unexpected behaviors. The security monitoring tools can help to pick up on or prevent any suspicious activity from happening.
  2. Make sure about protection and updating of critical infrastructure.
  3. Identifying the techniques used in cyber espionage attacks can give an organization a good baseline in what to protect.
  4. Data policies should be intact, including who has access to what information. This will help ensure only those who need access to critical information can gain access.
  5. Make a cyber security policy that addresses security procedures and risks.
  6. If an attack is detected an organization should be able to quickly respond to minimize damage.
  7. Ensure that there are no vulnerabilities in a system and any used third-party software systems are secured and well protected against cyber attacks.
  8. Educate employees about security policies. Introduce them, how to avoid opening suspicious-looking emails with links or document attachments.
  9. Check what data can be stored on individual's mobile devices for organizations that make use of bring your own device (BYOD).
  10. The passwords should be changed periodically.

6.26 Comprehensive Cyber Security Policy :

Definition :

- Cyber security policies are a set of rules of how companies or organizations should practice responsible security.

- It starts with general security expectations, roles, and responsibilities inside the company.
- There are a set of patterns that platforms offer to make a well efficient cyber policy.
- Cyber security policy also considered as "living document" which means the document is never finished, but it is continuously updated with change in the requirements of the technology and employees.
- The security policies are used to manage our network security. Some security policies are automatically created during the installation. We can modify policies to suit our particular environment.
- The larger organizations have more clauses as they have more stakeholders inside and outside.
- While the smaller organizations follow basic safety measures to ensure safety at the operational level.
- C-level Business Executives, Legal Department, Human Resources Department, Procurement Department, Board Members, External Personnel etc. can write the cyber security policies

Importance / Need of Security policies :

- The security policies are required because of the following reasons :
  1. It can make or break a business deal.
  2. It upholds discipline and accountability.
  3. It increases efficiency.
  4. It helps to educate employees on security literacy.

Updating Cyber Security Policies :

- Cyber security policies should be changed with time.
- It should be changed after every 12 months so that companies can stay up to date.
- The stakeholders should review all this policies before processing in order to avoid negligence.
- Avoiding policies can lead to threats as well as fines and lawsuits.

6.26.1 Cyber Security Policies :

- Some of the common cyber security policies that organizations follow are as follows :

Virus and Spyware Protection policy :

- This security policy makes sure the detection and removal of viruses by reducing security risk.
- The digital signatures are used to authenticate signals and detect suspicious behavior.

Intrusion Prevention policy :

- Intrusion Prevention policy has an automatic feature to detect network or browser attacks.
- It protects applications from vulnerabilities and uses legal ways for content checking. This contains data packages and malware as well.

Application and Device Control :

- This policy is made for the protection of the system's resources from different parts of the system.
- The device control policy is applicable for Apple and Windows while the application control policy is applicable only for Windows.

Information Security Policy :

- Information Security Policy is made for employees to keep the company's rules and guidelines in mind and follow them in terms of security.

Business Continuity Plan :

- Business continuity plan uses the recovery plan to restore everything necessary for the company's work. It defines how an organization should act during an emergency.

E-Commerce Policy :

- This policy ensures the management and operations of services according to the policy guidelines.

E-Mail Policy :

- This policy regulates the rules for handling emails inside an organization. This can be from sender or receiver.

Firewall Policy :

- The firewall is present in the network of all companies. This policy monitors its traffic.
- It ensures that internet traffic coming is secure and does not cause any threat to the organization.

Information Technology Purchasing Policy :

- This policy is required when the company uses its funds to buy any technical asset or service.

- It has a set of standards, procedures, and restrictions that they need to abide while making a purchase decision. IT department must be in the loop while this process.

Internet Policy :

- This policy is contains the regulations about using company's internet. This is for employees, clients, and even other stakeholders.

Password Policy :

- Password Policy restricts companies from using easy to guess passwords.
- They should generate strong passwords and change them frequently to avoid security breaches.

Server Security Policy :

- This policy defines internal server base configuration standards and restrictions and this is applicable for servers owned by the company as well as outsourced by them.

Social Media Acceptable Use Policy :

- This policy takes care of things related to social media to maintain security inside the organization.

Website Operation Policy :

- This policy defines guidelines about information protection, standard confidentiality and ethical transactions on the website.

Wireless Connectivity Policy :

- This policy defines guidelines that organizations need to follow while using free and unsecured Wi-Fi, to keep the data safe.

Review Questions

Q. 1 What are the various security principles or goals ?

Q. 2 Which are the security attacks ?

Q. 3 What are active and passive attacks ?

Q. 4 Discuss the types of attacks.

Q. 5 Classify the different types of attacks and explain them with examples.

Q. 6 State and explain the three security goals.

Q. 7 Define the following terms in relation with a message :
(a) Confidentiality
(b) Integrity
(c) Availability

Q. 8 Explain different types of attacks on the message integrity.

Q. 9 Write a short note on : SQL injection.

Q. 10 Write a short note on : Man in the middle attack.

Q. 11 Write a short note on : Phishing and password cracking.

Q. 12 List the types cyber attacks.

Q. 13 Define cyber security.

Q. 14 Write a short note on : Importance of cyber security.

Q. 15 Why do cyber attacks happen ?

Q. 16 What are the challenges in cyber security ? Explain in brief.

Q. 17 Write a short note on : Blockchain Revolution.

Q. 18 Differentiate between treat and vulnerability.

Q. 19 Give the classification of security attacks.

Q. 20 What are the different types of cyber attacks ?

Q. 21 Write a short note on : Challenges to Internet Governance.

Q. 22 State and explain : Cyber espionage.

Q. 23 Write a short note on : Types of cyber warfare attacks.

Q. 24 State and explain : Cyber security policies.

Q. 25 State cyber terrorism and explain it with an example.

□□□