19CS6708 – CYBER SECURITY – CLASS NOTES

Unit 1 – Introduction to Cyber System Security:

Definition of Cyber Security System

Cyber System Security as the name suggests, it protects our system from cyber attacks, malicious attacks. It is basically to advance our security of the system so that we can prevent unauthorized access of our system from attacker.

The security of computer security depends on three goals that are Confidentiality, Integrity, Authenticity. These Goals are basically threatened by attacker. There are various software to protect our information that are anti-spyware, antivirus, Firewall which helps in authorized access of information. There are other security system such as Intrusion Detection System, Cryptography, Digital Signature which will help us in protecting our system from attack.

(End of Introduction to Cyber security/Cyber Security System Topic)

Implementation and Challenges in Cyber Security:

1. Third Parties Can Unlawfully Misuse the Potential of 5G Network
2. An Increasing Rate of Mobile Malware
3. Artificial Intelligence: AI is Somewhere Controlling cybersecurity Systems
4. The Growing Popularity of IoT Devices
5. Ransomware Attacks are Targeting the Critical Business Aspects
6. No Control Over Phishing and Spear-Phishing Attacks
7. Growth of Hacktivism
8. Dronejacking is a New Wave Disturbing Cyber Experts
9. Preventive measures of social engineering
10. Office People Having Access to Data of their Organizations

(End of Implementation and Challenges in Cyber Security Topic)

Cyberspace:

Cyberspace is the non-physical domain where numerous computers are connected through computer networks to establish communication between them. With the expansion of technology, cyberspace has come within reach of every individual.

(End of Cyberspace Topic)

Cyber threats:

A cybersecurity threat is any hostile attack that attempts to gain unauthorized access to data, disrupt digital processes, or damaged data. Corporate spies, hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers, and disgruntled activists are all examples of cyber threats.

1. Ransomware - (Encrypt the file and blackmail)
2. Fileless Malware - Attack the hard disk without file storage footprint)
3. Cryptomalware – Bitcoin
4. Zero-Day Threats – Install MSoffice software first then malware.

5. Meltdown and Spectre – CPU vulnerability attacking main memory.
6. IoT Malware – Sensor malware.
7. Banking Malware
8. Stegware – Stegnogrpahy.
9. Phishing Email
10. Advanced Persistent Threats

(End of Cyber Threat topic)

Cyber Warfare

Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

An alternative view is that "cyberwarfare" is a suitable label for cyber attacks which cause physical damage to people and objects in the real world.

Clausewitz's definition of cyberwarefare:

Cyberwarfare is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived).

Taddeo offered the following definition:

The warfare grounded on certain uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy’s resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances.

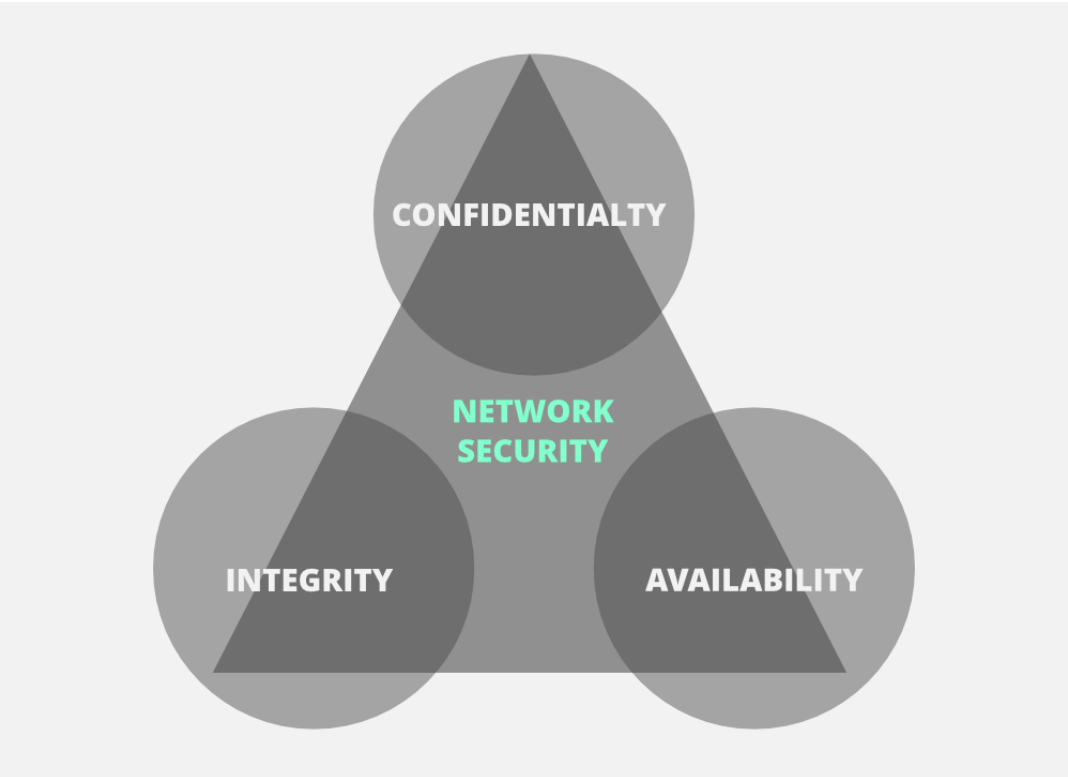
(End of cyber warefare topic)

CIA Triad:

The **CIA** triad is one of the most important models which is designed to guide policies for information security within an organization.

CIA stands for :

1. Confidentiality
2. Integrity
3. Availability



These are the objectives that should be kept in mind while securing a network.

Confidentiality :

Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent

over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it. Encryption standards include **AES**(Advanced Encryption Standard) and **DES** (Data Encryption Standard). Another way to protect your data is through a VPN tunnel. VPN stands for Virtual Private Network and helps the data to move securely over the network.

Integrity: :

The next thing to talk about is integrity. Well, the idea here is to make sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.

We have two common types: SHA (Secure Hash Algorithm) and MD5(Message Direct 5).

Availability :

This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network get exhausted.

(End of CIA Triad Topic)

Cyber Terrorism:

Cyber Terrorism:

- Cyber Terrorism basically involves damaging large-scale computer networks to achieve a loss of data and even loss of life. Hackers make use of computer viruses, spyware, malware, ransomware, phishing, programming language scripts, and other malicious software to achieve their purposes.
- Also, these types of cyber-attacks which often lead to criminal offenses are referred to as Cyber Terrorism. These cyber-attacks create panic and physical damage to a large number of people.

- Cyber Terrorism deals with creating damage to the people and their data using computer networks intentionally in order to achieve their meaningful purpose.
- Government Agencies like the FBI (Federal Bureau of Investigations) and the CIA (Central Intelligence Agency) in the past have detected multiple cyber attacks and cyber crimes through terrorist organizations.
- The main purpose behind carrying out Cyber terrorism is to carry out some cyberattack that makes a threat.
- According to the FBI, a Cyber Terrorism attack is defined as a cybercrime that may be used intentionally to cause harm to people on large scale using computer programs and spyware.
- In most cases, the criminals target the banking industry, military power, nuclear power plants, air traffic control, and water control sectors for making a cyber terrorism attack for creating fear, critical infrastructure failure, or for political advantage.

Working

The cyber terrorism attacks work in the following ways:

- They use computer viruses, worms, spyware, and trojans to target web servers and IT service stations. They want to attack

military utilities, air force stations, power supply stations to disrupt all the services.

- They use a Denial of Service attack where the original verified user cannot access the services for which he is authorized. This creates a sense of fear among the people for important essential services like medical emergencies.
- These attacks help cyber criminals to get unauthorized access to the user's computer using hacking and then stealing that information to fulfill their wrong purposes.
- Ransomware helps them to hold data and information by asking for some ransom money from the victim and they even leak the private data of the users if they don't get the desired amount.
- They mostly use phishing-based techniques to target users using infected spam emails to steal the user's information and reveal that identity to everyone.
- The most popular attack used in cyber terrorism is the APT (Advanced persistent threat). They use complex penetrating network models to hack into large-scale computer networks like in an organization. They make themselves undetected in that organization network and then they continuously steal

information related to military equipment, national defense information, etc.

Attacks:

The cyber terrorism attacks are usually carried out as follows:

- **Unauthorized access:** Attackers aim to disrupt and damage all the means of access to the service. Instead, the hacker gains unauthorized access to the important resources.
- **Disruption:** These attacks focus on disrupting public websites and critical infrastructure resources to create fear within the society of massive fatalities and commotion.
- **Cyberespionage:** The government usually carry out some spyware operations on other government of other country related to military equipment to gain an advantage over rival nations in terms of military intelligence.
- **Economic failure:** Cybercriminals want all the technical system failures to cause a large-scale economic failure like crashing the electricity or water systems for multiple days to create a panic of these services within the society.

(End of Cyber Terrorism topic)

Cyber Security of Critical Infrastructure

Cybersecurity: