Introduction to Computer Systems

Computer Security

By Nikini Amarapala
Lecture 8 | Week 09 | 21 Feb 2023

Lecture 7 Recap

- Computer Memory
- Computer Input & Output Devices

Lecture 8 Outline

- Computer Security

Computer Security

Computer security covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction and the process of applying security measures to ensure **confidentiality**, **integrity**, and **availability** of data.

Key Pillars of Cyber security are Confidentiality, Integrity and Availability.

- **Confidentiality** is about preventing the disclosure of data to unauthorized parties.
- **Integrity** refers to protecting information from being modified by unauthorized parties.
- **Availability** is making sure that authorized parties are able to access the information when needed.

CIA Explained: Confidentiality

Confidentiality is about preventing the disclosure of data to unauthorized parties.

Often confidentiality is compromised by cracking poorly encrypted data, Unauthorized access, Data Breaches or Man-in-the-middle attacks.

Data encryption, access controls, Implementing multi-factor authentication are Standard measures to establish confidentiality.

CIA Explained: Integrity

Integrity refers to protecting information from being modified by unauthorized parties.

Malware attacks, such as viruses or ransomware, can compromise data integrity by modifying or deleting files.

Hashing is a Standard measure to help ensure the integrity of data. Backing up data regularly and verifying the integrity of backups can help mitigate the impact of a malware attack.

CIA Explained: Availability

Availability is making sure that authorized parties are able to access the information when needed.

Denial of Service (DoS) attacks or system failures can cause disruptions to the availability of data.

Implementing redundancy and failover mechanisms, such as backup servers or load balancers, can help ensure availability in case of a system failure.

Vulnerability vs Threat vs Risk

- First, a **Vulnerability** exposes your organization to threats.
- A **Threat** is a malicious or negative event that takes advantage of a vulnerability.
- Finally, the **Risk** is the potential for loss and damage when the threat does occur.

A **Vulnerability** is a weakness, flaw or other shortcoming in a system (infrastructure, database or software), but it can also exist in a process, a set of controls, or simply just the way that something has been implemented or deployed. Example – Bugs in code, server misconfigurations, unpatched software, etc.

A **Threat** is a potential danger or harm that might exploit a vulnerability, which could affect the confidentiality, integrity or availability of your systems, data, people and more.

An **Attack** is a threat that is carried out (Threat action).

A **Risk** is defined as the effects of a threat exploiting a vulnerability. Example – Data Breach, Financial loss, Reputation damage, etc.

Cyber Attacks

A **cyber-attack** is an exploitation of computer device systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Some of the more common Cyber-attacks includes:

- **Ransomware**
- **Viruses**
- **Worms**
- **Trojan horse**
- **Spam**
- **distributed denial-of-service**
- **Botnet**
- **Rootkits**
- **Phishing**
- **smishing and vishing**
- **identity theft**
- **Data Breach**
- **Cyberespionage**
- **Cyberterrorism**
- **Man in the Middle Attack**

Why Cyber attacks are so Prevalent?

- **Increasing computing complexity**
- **higher computer user expectations**
- **expanding and changing systems**
- **an increase in the prevalence of bring your own device (BYOD) policies**
- **a growing reliance on software with known vulnerabilities**
- **the increasing sophistication of those who would do harm**

have caused a dramatic increase in the number, variety, and severity of security incidents are increasing dramatically.

Cyber Attacks Explained

Ransomware: Malware that stops you from using your computer or accessing your data until you meet certain demands such as paying a ransom or sending photos to the attacker

virus: A piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner

worm: A harmful program that resides in the active memory of the computer and duplicates itself

Trojan horse: A seemingly harmless program in which malicious code is hidden

spam: The use of email systems to send unsolicited email to large numbers of people.

distributed denial-of-service (DDoS) attack: An attack in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks.

Cyber Attacks Explained

botnet: A term used to describe a large group of computers, that are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners

rootkit: A set of programs that enables its user to gain administratorlevel access to a computer without the end user's consent or knowledge.

phishing: The act of fraudulently using email to try to get the recipient to reveal personal data.

smishing: Another variation of phishing that involves the use of Short Message Service (SMS) texting.

vishing: Similar to smishing except that the victims receive a voice mail message telling them to call a phone number or access a Web site.

identity theft: The theft of personal information, which is then used without the owner's permission, often to commit fraud or other crimes.

Cyber Attacks Explained

botnet: A term used to describe a large group of computers, that are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners

data breach: The unintended release of sensitive data or the access of sensitive data by unauthorized individuals

cyberespionage: The deployment of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms.

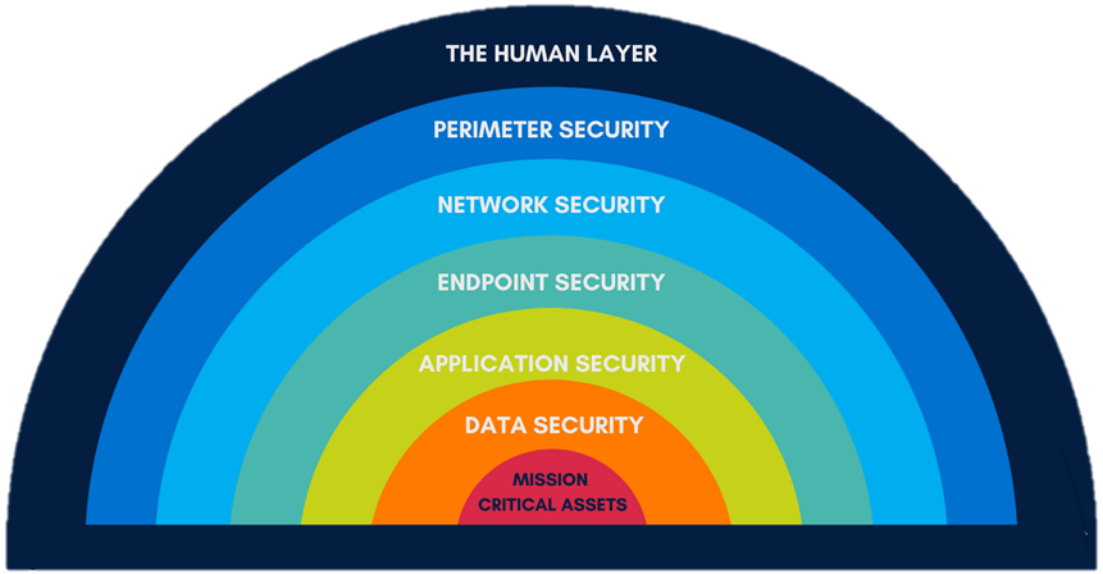
cyberterrorism: The intimidation of government or civilian population by using information technology to disable critical national infrastructure (e.g., energy, transportation, financial, law enforcement, emergency response) to achieve political, religious, or ideological goals.

Man in the middle attacks: It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

Perpetrators of Computer Crime

Type of Perpetrator	Description
Black hat hacker	Someone who violates computer or Internet security maliciously or for illegal personal gain (in contrast to a white hat hacker who is someone who has been hired by an organization to test the security of its information systems)
Cracker	An individual who causes problems, steals data, and corrupts systems
Malicious insider	An employee or contractor who attempts to gain financially and/or disrupt a company's information systems and business operations
Industrial spy	An individual who captures trade secrets and attempts to gain an unfair competitive advantage
Cybercriminal	Someone who attacks a computer system or network for financial gain
Hacktivist	An individual who hacks computers or Web sites in an attempt to promote a political ideology
Cyberterrorist	Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations, utilities, and emergency response units

The Layers of Cyber Security



- **Mission Critical Assets** – This is the data you need to protect
- **Data Security** – Data security controls protect the storage and transfer of data.
- **Application Security** – Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.
- **Endpoint Security** – Endpoint security controls protect the connection between devices and the network.
- **Network Security** – Network security controls protect an organization's network and prevent unauthorized access of the network.
- **Perimeter Security** – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.
- **The Human Layer –** Humans are the weakest link in any cyber security posture. Human security 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.

Examples of Cyber Security Measures

- **Data Security** – Data Classification, Encryption, data loss prevention (DLP), and backup and recovery systems.
- **Application Security** – Secure coding practices, vulnerability scanning, and penetration testing.
- **Endpoint Security** – Antivirus and anti-malware software, host-based intrusion detection and prevention systems, and endpoint detection and response (EDR) solutions.
- **Network Security** – Network segmentation, virtual private networks (VPNs), and network access controls.
- **Perimeter Security** – Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
- **The Human Layer –** Security training for employees, phishing awareness programs, incident response plans, and security policies.

Lecture 8 Post Lecture Activities

- Who are the perpetrators of Computer Crime?
- Explain CIA in Cybersecurity & How to ensure CIA?
- What are the Layers of Cyber Security? Explain each and give example cybersecurity measures for each layer.

Lecture 9 Next Week

- Computer Networks

Thank you