MCA 205B: Cyber Security

Unit-I

History of cyber security

The origin of cyber security began with a research project. It only came into existence because of the development of viruses.

- Cyber security proper began in 1972 with a research project on ARPANET (The Advanced Research Projects Agency Network), a precursor to the internet.
- The history of cyber security began with a research project. A man named Bob Thomas realized that it was possible for a computer program to move across a network, leaving a small trail wherever it went.
- ARPANET developed protocols for remote computer networking. He named the program Creeper, and designed it to travel between Tenex terminals on the early ARPANET, printing the message "I'M THE CREEPER: CATCH ME IF YOU CAN."
- Reaper was the very first example of antivirus software and the first self-replicating programme, making it the first-ever computer worm.
- Creeper was the first computer worm, while Reaper was the first antivirus software, designed to eliminate Creeper.

What is cyber security?

Cyber Security is the practice of Protecting computers, mobile devices, Servers, electronic Systems, networks, and data from malicious attacks.

- It is also known as Information Security (**INFOSEC**) or Information Assurance (**IA**), System Security.
- The first cyber malware virus developed was pure of innocent mistakes. But cyber security has evolved rapidly because of the impeccable increase in the cyber crime law field on the Web.
- We can divide cyber security into two parts one is cyber, and the other is security.

1. Cyber refers to the technology that includes systems, networks, programs, and data.

2. Security is concerned with the protection of systems, networks, applications, and information.

Types of Cyber security

There are 5 types

1. Application security
2. Cloud security
3. Information security
4. Mobile security
5. Network security

What is cyber attck?

define a cyber attack as:

> *An attack, via cyberspace, targets an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.*

- A **cyberattack** is any offensive maneuver that targets computer information systems, computer networks, infrastructures, personal computer devices, or smartphones.
- Depending on the context, cyberattacks can be part of cyber warfare or cyberterrorism.
- A cyberattack can be employed by sovereign states, individuals, groups, societies or organizations and it may originate from an anonymous source. A product that facilitates a cyberattack is sometimes called a cyber weapon.
- A well-known example of a cyber attack is a distributed denial of service attack (DDoS). Cyberattacks have become increasingly sophisticated and dangerous.

Cyber security tool?

Cyber security refers to protecting hardware, software, and data from attackers.

- It protects against cyberattacks like accessing, changing, or destroying sensitive information.
- There are many cyber security tools that can conduct a privacy audit for all software, find and remove the latest threats.
- These cyber security tools help you to manage file access control and perform forensic analysis.

Types of security tools:

Solar winds security event manager :

- It provides a network and host intrusion detection system that reports security threats in real time and allow for monitoring and responding.
- It's a cloud based solution that also offers indexed log search capabilities.

Key features:

- Continuous updates on threat intelligence
- Security information and an event manager
- A full set of integrated reporting tool

Sasyxsence:

- This is a clear for small business organizations and a set annual fee for use with up to 10 devices.
- This tool provides patch management , security scanning and remediation for cloud based systems to prevent data breaches.

Key features:

- Insight form a security scanner to identify authorization issues antivirus status and security implementation.
- Patching support for all major operating systems.
- Communication blocks between the internet and an infected device to isolate the endpoint and destroy malicious process before they spread.

Intruder:

- It's a popular cloud based scanner that help identify network weakness to avoid data breaches.
- This software also offers a nonstop solution for an organizations cyber security requirements.

Key features:

- Unlimited scans and user accounts
- Checks for web application flow , including cross site scripting and sql injection.
- Notifications for emerging threats.
- PCI ASV scans.

Net sparker:

- Net sparker is a recommended choice for any size business, offering a range of pricing plans, including a quote to establish a customized deal.
- Its an application solution that addresses automated security testing through automation accuracy ,scalability and security.

Key feaures:

- A comprehensive and interactive scanning system that can quickly defect vulnerabilities.
- Support for developers to improve code to protect data and systems.
- A complete overview of an organizations applications security.
- on boarding training and assistance for new users.
- Behaviour based testing.

Vipre:

- Vipre offers protection against a range of evolving online threats and is available in 3 different pricing plans. It can help you protect against identify theft, ransomware and computer viruses.
- Its business protection offers comprehensive email and endpoint security and privacy, along with real-time threat intelligence.

Key feataures:

- Simplified solution to help protect a business from online threats.
- Scalable pricing options in addition to all inclusive packages.
- AI technology to provide advanced protection.
- Full integration with existing systems that's easy to develop and manage.
- E mail encryption.

Security Threats

- Security Threat is defined as a risk that which can potentially harm computer systems and organization.
- The cause could be physical such as someone stealing a computer that contains vital data.
- The cause could also be non-physical such as a virus attack.
- In these tutorial series, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

What are Physical Threats?

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

The following list classifies the physical threats into three (3) main categories;

Internal: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.

External: These threats include Lightning, floods, earthquakes, etc.

Human: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

What are Non-physical threats?

- A non-physical threat is a potential cause of an incident that may result in;
- Loss or corruption of system data
- Disrupt business operations that rely on computer systems
- Loss of sensitive information
- Illegal monitoring of activities on computer systems

- ❖ Cyber Security Breaches
- ❖ Others

The non-physical threats are also known as logical threats. The following list is the common types of non-physical threats;

- ✓ Virus
- ✓ Trojans
- ✓ Worms
- ✓ Spyware
- ✓ Key loggers
- ✓ Adware
- ✓ Denial of Service Attacks
- ✓ Distributed Denial of Service Attacks
- ✓ Unauthorized access to computer systems resources such as data
- ✓ Phishing

Other Computer Security Risks

- To protect computer systems from the above-mentioned threats, an organization must have logical security measures in place.
- The following list shows some of the possible measures that can be taken to protect cyber security threats

• To protect against viruses, Trojans, worms, etc. an organization can use anti virus software. In additional to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user's computer.

- Unauthorized access to computer system resources can be prevented by the use of authentication methods. The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc.
- Intrusion-detection/prevention systems can be used to protect against denial of service attacks.

• There are other measures too that can be put in place to avoid denial of service attacks.

What is vulnerability assessment

- A vulnerability assessment is a systematic review of security weaknesses in an information system.
- It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.
- Examples of threats that can be prevented by vulnerability assessment include:

1. SQL injection, XSS and other code injection attacks.
2. Escalation of privileges due to faulty authentication mechanisms.
3. Insecure defaults – software that ships with insecure settings, such as a guessable admin passwords

There are several types of vulnerability assessments. These include:

Host assessment –

• The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.

Network and wireless assessment –

• The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.

Database assessment –

• The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.

Application scans –

• The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code

Vulnerability assessment: Security scanning process

The security scanning process consists of four steps: testing, analysis, assessment and remediation.

1. Vulnerability identification (testing)

- The objective of this step is to draft a comprehensive list of an application's vulnerabilities.
- Security analysts test the security health of applications, servers or other systems by scanning them with automated tools, or testing and evaluating them manually.
- Analysts also rely on vulnerability databases, vendor vulnerability announcements, asset management systems and threat intelligence feeds to identify security weaknesses.

2. Vulnerability analysis

- The objective of this step is to identify the source and root cause of the vulnerabilities identified in step one.
- It involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability.

- For example, the root cause of a vulnerability could be an old version of an open source library. This provides a clear path for remediation – upgrading the library.

3. Risk assessment

- The objective of this step is the prioritizing of vulnerabilities.
- It involves security analysts assigning a rank or severity score to each vulnerability, based on such factors as:

✓ Which systems are affected.

✓ What data is at risk.

✓ Which business functions are at risk.

✓ Ease of attack or compromise.

✓ Severity of an attack.

✓ Potential damage as a result of the vulnerability.

4. Remediation

- The objective of this step is the closing of security gaps.
- It's typically a joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability.

Roles in Security

- The role of the government is to make regulations to force companies and organizations to protect their systems, infrastructure and information from any cyberattacks, but also to protect its own national infrastructure such as the national power-grid.
- The government's regulatory role in cyberspace is complicated. For some, cyberspace was seen as a virtual space that was to remain free of government intervention, as can be seen in many of today's libertarian block chain and bitcoin discussions.
- Many government officials and experts think that the government should do more and that there is a crucial need for improved regulation, mainly

due to the failure of the private sector to solve efficiently the cyber security problem.

- R. Clarke said during a panel discussion at the RSA Security Conference in San Francisco, he believes that the "industry only responds when you threaten regulation. If the industry doesn't respond (to the threat), you have to follow through.
- On the other hand, executives from the private sector agree that improvements are necessary, but think that government intervention would affect their ability to innovate efficiently.
- Daniel R. McCarthy analysed this public-private partnership in cyber security and reflected on the role of cyber security in the broader constitution of political order.
- On 22 May 2020, the UN Security Council held its second ever informal meeting on cyber security to focus on cyber challenges to international peace.
- According to UN Secretary-General António Guterres, new technologies are too often used to violate rights.

Critical Thinking in Cyber Security

Strong thinking skills are required to outsmart malicious attacks

Vigilant and effective cyber security specialists have the critical thinking skills and mindset that enable them to anticipate and defend against internal and external threats. The challenges of working in these rapidly changing and complex fields require the ability to reason well in highly precise contexts as well as ambiguous and uncertain contexts, to ability to analyze problems and to evaluate alternatives, and the ability to explain clearly what needs to be done and why. Applying these skills in a speedy, effective, logical and

organized manner requires focus, resourcefulness, foresight, and responsiveness.

Strong Critical Thinking Enables Cyber Security Specialists

- To apply quantitative and algorithmic skills
- To make high stakes decisions about data security
- To assess and manage technology risks
- To plan, evaluate, and implement cyber security measures
- To respond to security breaches/threats