CSE487: Cyber Security, Law, and Ethics

Introduction to Cyber Security

Instructor: Dr. Md. Hasanul Ferdaus

PhD (Monash University), MS (KIT, Germany & Polito, Italy), BSc (CSE BUET)

Assistant Professor

Department of CSE, East West University

Former Faculty Member, Monash University and CQ University, Australia

Former Researcher, Melbourne University, Australia

Former Researcher, KIT and FZI, Germany

Cyber Security

- In present-day society, our daily lives are increasingly reliant on the use of technology.
- This dependence brings numerous advantages, including quick access to online information and the convenience offered by smart home automation and concepts like the Internet of Things (IoT).
- Despite the generally optimistic view of technological progress, cyber security threats posed by modern technology are indeed a tangible danger.
- **Cyber Security** is a way to protect electronic devices and services connected to the internet from potential threats.

What is Cyber Security ?

- Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals.
- Cybersecurity involves shielding against fraudulent tactics, such as phishing, unauthorized data access, identity theft, and malicious ransomware attacks.
- Broadly the term "Cyber Security" is used to describe protection against various forms of cybercrimes, including identity theft and international digital warfare.
- Definition by Cisco Systems Inc.: "***The practice of protecting systems, networks, and programs from digital attacks. These cyberattacks typically aim to gain unauthorized access, manipulate or destroy sensitive information, extort money from users, or disrupt normal business operations.***"

Why is Cybersecurity Important ?

- An instance of security breach can result in the exposure of personal data belonging to numerous individuals.
- Such breaches not only carry significant financial implications for companies but also causes a great loss of trust of their customers.
- Therefore, it is crucial to prioritize cybersecurity in order to safeguard businesses and individuals against the threats posed by spammers and cybercriminals.

Scale of Cyber Security Threats

- It is projected that cybercrime will result in an annual cost of 10.5 trillion USD worldwide by 2025, accordingly to Cybercrime Magazine.
  https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
- The global expenses associated with cybercrime are anticipated to increase by approximately 15 percent each year over the next four years.
  https://www.thenationalnews.com/business/technology/2021/12/29/top-10-cyber-crime-trends-to-watch-out-for-in-2022/
- Various factors, including the pandemic, the prevalence of cryptocurrency, and the growing trend of remote work, are converging to create a fertile ground for criminals to exploit.

Scope of Cyber Security

- Cybersecurity involves the utilization of technologies, procedures, and approaches to safeguard computer systems, data, and networks against malicious attacks.

Application Security

- Implementation of various protective measures within an organization's software and services to counter a wide range of threats.
- Development of secure code, design of secure application structures, establishment of rigorous data input validation, and other tasks aimed at reducing the risk of unauthorized access or alteration of application resources.

Scope of Cyber Security

Identity Management and Data Security

- Actions, frameworks, and procedures that facilitate the verification and validation of legitimate individuals accessing an organization's information systems.
- Implementation of robust data storage mechanisms to safeguard information, whether it is in transit or stored on servers or computers.
- Utilization of state-of-the-art authentication protocols, such as two-factor or multi-factor authentication, to enhance security.

Scope of Cyber Security

Network Security

- Hardware and software components employed to safeguard the network and infrastructure against disruptions, unauthorized entry, and various forms of misuse.
- By implementing robust network security measures, organizations can effectively shield their assets from a diverse range of threats, whether originating from within the organization or outside of it.

Scope of Cyber Security

Mobile Security

- This particular field focuses on safeguarding both personal and organizational data stored on devices such as tablets, cell phones, and laptops from various risks, including unauthorized entry, device misplacement or theft, malware, viruses, and more.
- Furthermore, mobile security utilizes authentication and educational measures to enhance overall security.

Cloud Security

- The establishment of secure cloud architectures and applications for organizations that utilize cloud service providers such as Amazon Web Services, Google Cloud, Microsoft Azure, Rackspace, and others.

Scope of Cyber Security

Disaster Recovery and Business Continuity Planning

- The Disaster Recovery (DR) and Business Continuity (BC) subdomain encompasses procedures, notifications, monitoring, and strategies devised to assist organizations in preparing for the continuity of their business-critical systems during and after various incidents, such as extensive power outages, fires, or natural disasters.
- It aims to facilitate the resumption and recovery of operations and systems that may have been compromised or disrupted as a result of the incident.

Scope of Cyber Security

User Education

- Information is a valuable asset and the knowledge of cyber threats among staff plays a crucial role in the overall cybersecurity framework.
- Providing comprehensive training to business personnel on the fundamentals of computer security is vital for promoting awareness about industry best practices, organizational procedures and policies, as well as recognizing, monitoring, and reporting suspicious or malicious activities.
- This subdomain encompasses cyber security-oriented courses, programs, and certifications aimed at enhancing staff expertise in this field.