Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Ph.D. in Computer Science and Telecommunication
UPMC (Paris-VI), France

Objective of the course

To **introduce** common cyber security threats, vulnerabilities, and risks related to **web applications**, **networks**, **software** and mobile applications.

To **provide** basic concepts and terminology used in the information and cyber security fields

To **enable** students to differentiate between the various forms of malware and how they affect computers and networks

To **familiarize** students with basic tools and technologies used in various cyber security related tasks

Helping material

Textbook I: Computer Security Fundamentals by Chuck Easttom, 4th edition or latest

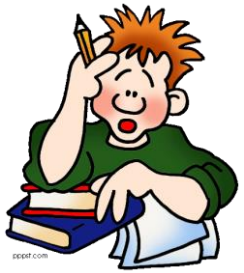
Textbook II: Computer Security: Principals and Practice, William Stallings

Presentation slides

Research Papers & Articles

Marks Distribution

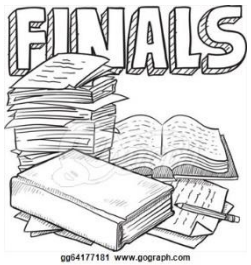
Quizzes 10%



Assignments 10%

Project & Presentation 10%

Midterm 25~30%



40~45%

Course Outline

Refer to course outline file

Course Outline

Week 1

- Introduction to the course
- Introduction to Cyber Security
- Basic security terminology
- Identifying types of threats
- security resources

Intro to
Cyber Security

Introduction to Cyber Security

Internet

- a big source of knowledge and easily accessible to all
- However, it has equal opportunities for criminals too
- **Cybercriminals** develop and use sophisticated tools and techniques (leveraging modern technologies)
  - To **perform** malicious activities aimed at distorting, disrupting and/or stealing sensitive data and information, primarily for financial gains.

Data and Information w.r.t. Cyber Security

Data

- The facts, measurements, and statistics gathered in real-time
- **associated with scientific research and examined for reasoning, discussion and decision making**.
- Initially: text, numbers or combination of both
- With **multimedia**: data incorporated images, graphics and video
- **All type of data get stored in digital form**

Data and Information w.r.t. Cyber Security

Information

- the meaning of stored data in some context for its intended receiver(s).
- In any stage, it becomes data for computers.
- When data is accurately processed in an organized manner with a specific purpose and it presents some relevant meaning to its user, then it is called **information.**
- It becomes useless if it does not lead a significant increase in end-user knowledge.

Data vs Information

Data	**Information**
used as input for computer system to generate information.	When data is processed in some organized and structured way in a particular span of time
independent in itself	needs data for its own existence
Meaningless	carries relevant meaning and becomes beneficial for end users

Data Communication, Networks, WWW, Internet

- Computers collect data from different sources, convert that data into meaningful information.
- Generated information becomes useless until it is delivered to the right person at the right time.
- equally important to transmit information quickly for the benefits of its users across the world.
- To transfer the information across the world, we use well connected **digitally networked infrastructure**

Information Security

It is concerned to protecting digital information from **destruction**, **stealing** and **unauthorized access.**

- We may like medical reports or financial records to be kept secret
- We desire privacy with our mails and social media posts.
- We do not want to disclose internet passwords, credit card numbers and banking details with anyone and fear from getting into wrong hands.
- We keep our documents, photographs and videos on online storage.
  - Due to quick and frequent requirement

Information Security

Information security is also crucial for all organizations and enterprises as they conduct business with customers and traders listed that they want to keep secret.

Areas of Information Security:

1. **Secrecy:** deals with the protection of information from unauthorized hands
2. **Integrity** ensures that received information is real and accurate as it was sent, without any modification from intruders.
3. It is concerned with the ability of users to get access of information in its **original** form at desired location and time

Information Security

4. **Authenticity** refers to the assurance that message, financial transaction or communication is from the source from where it claims. Authenticity is incomplete without identity.
5. **Trustworthiness** is concerned with ability of system to produce authentic and reliable information.
6. **Non-repudiation** refers to the ability of system to prevent the denial of authenticity from users participating in communication.

Information Security

4. **Accountability** refers the ability of system that allocates the person who uses interconnected environment for their activities on internet.
5. **Auditability** refers systematic evaluation of entire information system, measuring how well it meets the information security established criteria.

WWW Security

- World Wide Web is a system having large number of high storage capacity servers scattered across the world.
- The most important thing about the internet is its availability and utility to all
- Good people use its potential for social benefits, while
- some other use it to earn illegal profits, political and corporate benefits, distribution of restricted contents and for personal revenge as well
- People are using it as a tool to create rumours and communal violence expansion.

WWW Security

Problems posed by cyber criminals

- create malicious code to gain unauthorized access and exploit vulnerabilities.
- remotely control entire system and prevent legitimate users to make its utilization.
- Breach the confidentiality to take political, corporate and social benefits.
- Breach the secrecy and integrity of information during data transmission.

Therefore, the security of internet and WWW becomes important and essential to keep this infrastructure beyond the reach of cybercriminals

Cyber Security

- Cybersecurity is relevant to all people in the modern world, including a strong password policy to protect your emails or to businesses and other organisations needing to protect both devices and data from damages.

Cyber Crime

Cyber crimes

- are, as the name implies, crimes committed using computers, phones or the internet.

Some **types** of cyber crime include:

- Illegal interception of data.
- System interferences.
- Copyrights infringements.
- Sale of illegal items.

Cyber Security

Cyber security

- is the body of technologies, processes and practices involved in protecting individuals and organizations from cyber crime.

- designed to protect integrity of networks, computers, programs and data from attack, damage or unauthorized access.

Offensive Security

- The process of **breaking into** computer systems, exploiting software bugs, and finding loopholes in applications to gain **unauthorized access** to them.

- To beat a hacker, you need to behave like a hacker,
  - **finding** vulnerabilities and **recommending** patches before a cybercriminal does!

- **Red Teams**

Defensive Security

- The process of **protecting** an organization's network and computer systems by **analyzing** and **securing** any potential digital threats;

- **Investigating** infected computers or devices to understand
  - how it was hacked,
  - tracking down cybercriminals, or
  - monitoring infrastructure for malicious activity.
- Blue teams

Offensive vs Defensive Security?

- Which of the following better represents the process where you simulate a hacker's actions to **find vulnerabilities in a system**?

- Offensive Security OR Defensive Security

Offensive Security

Cyber Security Principles

- There are five key **principles** in cyber security:
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
  - Auditability

Cyber Security Principles

- There are five key **principles** in cyber security:

- **Confidentiality:**
  - A set of rules that limits access or place restrictions on certain type of information.
- **Integrity:**
  - Assurance that the information is trustworthy and accurate.
- **Availability:**
  - The guarantee of reliable access to the information by authorized people.

These 3 are known as common CIA traids

Cyber Security Principles

- **Accountability:**
  - Is an assurance that an individual or an organization will be evaluated on their performance or behaviour related to something for which they are responsible.

- **Auditability:**
  - A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria.