PMSCS 694

Information Security

Lecture 1

Intro. to Information Security

Md. Rafsan Jani
Associate Professor
Department of Computer Science and Engineering
Jahangirnagar University

Course Overview

- **Objective**: Students will learn the fundamentals of information security, security threats, modes of attack, cryptographic models, access control, identification, and authentication.
- **Readings**: Lecture materials and reference book.
- **Marks Distribution**(In-Class[40]+Final[60])
  - Class Tests-25%
  - Assignments-5%
  - Attendance-10%
  - Final-60%
- **Class Tests**:
  - There will be 3(Descriptive/MCQ) tests.
- **Final**: Comprehensive closed-book

Learning Objectives

- Learn to think about security when developing systems.

- Learn how computers can be attacked, how to prevent attacks and/or limit their consequences.
  - No silver bullet; man-made complex systems will have errors; errors may be exploited
  - Large number of ways to attack
  - Large collection of specific methods for specific purposes

- Learn to understand and apply security principles when designing/building/analyzing systems

Text Books

1. Information Security: Principles and Practice, 3rd Edition
   - By Mark Stamp

2. Principles of Information Security, 7th Edition
   - By Michael E. Whitman, Herbert J. Mattord

3. Foundations of Information Security
   - By Jason Andress

Google Classroom

- Google Classroom Code: **fmcvhsck**

or

- Google Classroom Invitation Link:

https://classroom.google.com/c/[illegible]ODQ4MzI0MjM0?cjc=fmcvhsck

What is Information?

- **Information** refers to *processed, structured, or organized data* that is meaningful and can be used for decision-making or understanding. It represents knowledge or insights derived from data when placed in context.
  - **Example**:
    - Raw Data: "75, 80, 90”
    - Information: "The average temperature this week is 81°F."
- **Characteristics of Information**:
  1. **Accuracy**: Information should be correct and free from errors.
  2. **Relevance**: Information should be applicable to the context or situation.
  3. **Timeliness**: Information should be available when needed.
  4. **Completeness**: Information should be comprehensive enough for decision-making.

What is an Information System?

- An **Information System (IS)** is a combination of technology, people, and processes designed to collect, process, store, and distribute information for a specific purpose. It enables organizations to manage data efficiently and supports decision-making, operations, and strategic planning.
- **Key Functions of an Information System:**
  1. **Data Collection**: Gathering raw data from various sources.
  2. **Data Processing**: Converting raw data into meaningful information.
  3. **Storage**: Safeguarding data for future use.
  4. **Analysis and Decision Support**: Analyzing data to provide insights for decision-making.
  5. **Communication**: Sharing information across stakeholders.

Information System Components

- **Components of an Information System**:
  1. **Hardware**: Physical devices like computers, servers, and networking equipment.
  2. **Software**: Programs and applications used to process data.
  3. **Data**: Raw facts that are processed into meaningful information.
  4. **People**: Users, administrators, and IT professionals who interact with the system.
  5. **Processes**: Procedures and rules for collecting, processing, and managing information.

Examples

- **Examples of Information Systems:**
  1. **Transaction Processing Systems (TPS)**: Manage day-to-day transactions (e.g., point-of-sale systems).
  2. **Management Information Systems (MIS)**: Provide summarized data for managerial decision-making.
  3. **Enterprise Systems**: Integrate processes across the organization (e.g., ERP systems).
  4. **Decision Support Systems (DSS)**: Assist in complex decision-making using data analysis and modeling.

What is Security?

- Dictionary.com says:
  - Freedom from risk or danger; safety.
  - Freedom from doubt, anxiety, or fear; confidence.
  - *Something that gives or assures safety*, as:
    - A group or department of private guards: Call building security if a visitor acts suspicious.
    - Measures adopted by a government to prevent espionage, sabotage, or attack.
    - Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault.

What is Security?

- Security means protecting our assets, whether from attackers invading your networks, natural disasters, vandalism, loss, or misuse.
- Generally, two types of assets
  - **Physical assets:** those that are tangible objects or materials such as gold, or those that have value to your business, such as computing hardware, etc.
  - **Logical assets:** assets that exist as data or intellectual property(software, source code, or data, etc.).

What is Information Security?

- **Information security**, often referred to as ***InfoSec***, is the practice of *protecting information and information systems* from unauthorized access, use, disclosure, disruption, modification, or destruction.
- In other words, you want to protect your data and systems from those who seek to misuse them, intentionally or unintentionally, or those who should not have access to them at all.
- It encompasses a wide range of strategies, technologies, and processes to safeguard the confidentiality, integrity, and availability of data.

Information Security Domains

- Information security covers various domains and employs multiple controls and measures, including:
  - **Physical Security:** Protecting physical assets, such as servers and data centers, from physical threats like theft, vandalism, natural disasters, and unauthorized access.
  - **Network Security:** Securing the confidentiality, integrity, and availability of network and data transmissions.
    - This includes firewalls, intrusion detection/prevention systems (IDS/IPS), virtual private networks (VPNs), and secure protocols.
  - **Application Security:** Ensuring that software applications are designed and maintained to be secure against threats.
    - This involves secure coding practices, regular updates and patches, and application testing.

Information Security Domains

- Information security covers …
  - **Endpoint Security**: Protecting end-user devices such as computers, smartphones, and tablets from threats.
    - This includes antivirus software, endpoint detection and response (EDR) solutions, and mobile device management (MDM).
  - **Identity and Access Management (IAM)**: Managing and controlling user identities and access privileges.
    - This includes authentication (verifying identity) and authorization (granting access rights), often implemented through multi-factor authentication (MFA) and role-based access control (RBAC).
  - **Incident Response**: Developing and implementing procedures to detect, respond to, and recover from security incidents.
    - This includes having an incident response plan, conducting regular drills, and post-incident analysis.

Information Security Domains

- Information security covers …
  - **Risk Management:** Identifying, assessing, and prioritizing risks to information assets, and implementing measures to mitigate those risks.
    - This involves conducting risk assessments, vulnerability assessments, and applying appropriate controls.
  - **Compliance and Governance:** Ensuring adherence to laws, regulations, and standards relevant to information security.
    - This includes compliance with frameworks like ISO/IEC 27001, GDPR, HIPAA, and others.

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Why do we need Security?

- Protect vital information while still allowing access to those who need it
  - – Ex: Trade secrets, medical records, etc.
- Provide authentication and access control for resources
  - – Ex: AFS(Available-for-sale)
- Guarantee availability of resources
  - – Ex: 5 9's (99.999% reliability)

When Are You Secure?

- Eugene Spafford once said, “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then, I have my doubts.”
- A system in such a state might be secure, but it’s not usable or productive.
- As you increase the level of security, you usually decrease the level of productivity
- When securing an asset, system, or environment, you must consider how the level of security relates to the value of the item being secured.
- The cost of the security you put in place should never outstrip the value of what it’s protecting.

When Are You Secure?

- Defining the exact point at which you can be considered secure presents a bit of a challenge.
  - Are you secure if your systems are properly patched?
  - Are you secure if you use strong passwords?
  - Are you secure if you're disconnected from the internet entirely?
- The answer to all these questions is no.
- No single activity or action will make us secure in every situation.

Examples of Threats

- **Malware**: Viruses, ransomware, or spyware designed to disrupt, steal, or damage data.
- **Phishing**: Fraudulent attempts to steal sensitive information via email or other communication.
- **Unauthorized Access**: Gaining access to systems or data without proper authorization.

Importance of Information Security

- Protects sensitive personal, financial, and organizational data.
- Maintains trust with stakeholders and customers.
- Complies with legal and regulatory requirements (e.g., GDPR, HIPAA).
- Safeguards against financial losses and reputational damage due to breaches.

Survey-First Day

- Please fill-out this form:

https://forms.gle/WJnxPQTKrcsHMCeS7

My email: rafsan@juniv.edu