LECTURE # 1

Introduction to Information Security

LEARNING OBJECTIVE

Upon completion of this material, you should be able to:

- Understand the definition of information security
- Understand the key terms and critical concepts of information security
- Comprehend the history of computer security and how it evolved into information security

Administrative Matters

Textbook

Principles of Information Security, 6th edition by M. Whitman and H. Mattord, 2017.

References Material:

- Computer Security: Principles and Practice, 4th edition by William Stallings, 2017.
- Computer Security, 3rd edition by Dieter Gollmann, 2011.
- Computer Security Fundamentals, 3rd edition by William Easttom, 2016.

GRADING SYSTEM AND WEIGHTAGES OF ASSESSMENTS

Relative grading system will be followed to award grades. Weightages are as under:

Theory Based Courses	
Assignments	= 8 %
Quizzes	= 8 %
Presentations	= 4 %
Mid Semester Examination	= 30 %
End Semester Examination	= 50 %

OTHER RULES

- Discussion is encouraged in class but cross talking is not allowed.
- Leave/ absent will be considered as “ABSENT” in class, for which no retake of Assignments, Quiz etc will be considered.
- Submit solutions to all assessments honestly, copied / plagiarized solutions will be given reduced / zero marks.
- Phone should be on silent mode.
- Assignments, quizzes and exams should be neat.

WHAT IS SECURITY

- The state of being or feeling secure;
  - freedom from fear
  - anxiety
  - danger
  - Doubt
- State or sense of safety or certainty
- Something that gives or assures safety, tranquility, certainty, etc.; protection; safeguard

What is an Information System?

- Information System (IS): an entire set of
  - Software
  - Hardware
  - Data
  - People
  - Procedures, and
  - Networks

  necessary to use information within an organization

Introduction to Information Security

- Information Security involves protecting data and information systems from
  - Unauthorized access
  - Use
  - Disclosure
  - Disruption
  - Modification
  - Destruction
- Information security is about ensuring that data is safe from attacks, leaks, and unauthorized access.
- The increasing dependence on information technology means increased risks – there is a clear increase in incidents such as data breaches, fraud, and the spread of malicious code.

Introduction to Information Security

Challenges in the Current Environment:

- Cyber threats have increased due to the widespread use of the internet, mobile devices, and cloud computing.
- The complexity of modern IT infrastructure makes it more vulnerable to security risks.

Key Terminologies:

- **Asset**: What is being protected (e.g., data, networks).
- **Vulnerability**: Weakness that can be exploited.
- **Threat**: Potential cause of an unwanted incident.

SECURITY PRINCIPLES

Security Goals

- **Detective**: Identify security incidents or vulnerabilities, methods to detect security breaches (e.g., IDS, SIEM).
- **Preventive**: Stop threats from impacting systems (e.g., firewalls, encryption).
- **Corrective**: React to incidents and recover, actions to fix security breaches (e.g., backup, patch management).
- **Layered Security**: The idea that multiple layers of defense (people, processes, and technology) protect data and systems. Firewalls + Antivirus + User training.

SECURITY PRINCIPLES

Authentication:

- The process of verifying the identity of a user or system.
- Common methods: passwords, biometrics, multi-factor authentication (MFA).
- Importance of strong password policies and MFA.

Authorization:

- Determines what an authenticated user is allowed to do.
- **Access control models**
  - ✔ **Discretionary Access Control (DAC)**: Owners control access to resources.
  - ✔ **Role-Based Access Control (RBAC)**: Access is based on user roles.
  - ✔ **Mandatory Access Control (MAC)**: Access based on security clearances.

SECURITY PRINCIPLES

Accountability:

- Ensures that actions can be traced back to the responsible party.
- Logging and auditing: Keeping records of activities.
- Importance in compliance (GDPR, HIPAA).

Non-repudiation:

- The ability to prove that someone performed an action (e.g., sent a message, completed a transaction).
  - **Digital signatures**: Provide proof that a message was sent by a specific person
  - **Hashing**: Generates a unique identifier for data to ensure it hasn't been altered.

SECURITY PRINCIPLES

Risk Management:

- Identifying, assessing and mitigating security risks.
- Steps:
  - Risk identification: Identify vulnerabilities
  - Risk assessment: Evaluate the likelihood and impact of threats
  - Risk control: Implement measures to mitigate or manage risks (e.g., encryption, access controls).
- Methods:
  - Accept
  - Avoid
  - Transfer
  - Mitigate risks

CIA TRIAD

The **CIA Triad** is the foundation of information security. It represents three key principles:

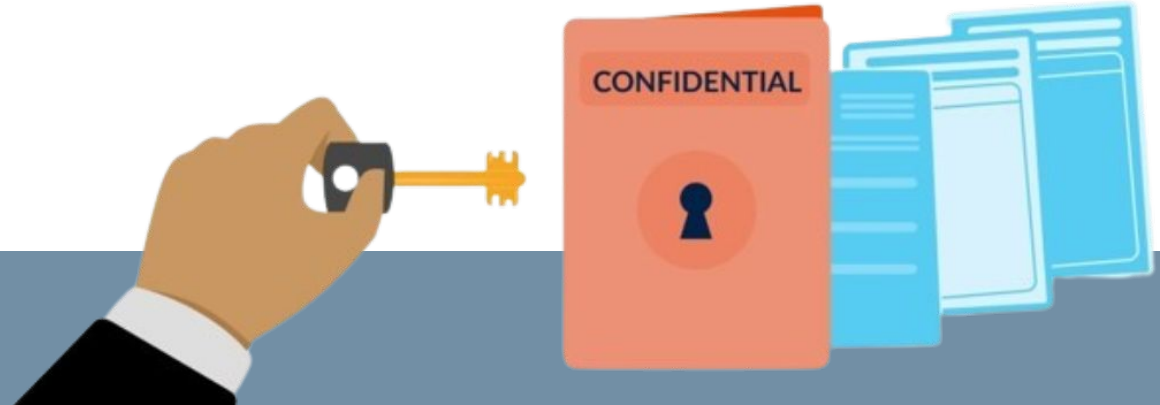
- **Confidentiality**
- **Integrity**
- **Availability**

CONFIDENTIALITY

Definition: Ensuring that sensitive information is only accessible to those authorized to access it.

Methods to Maintain Confidentiality:

- **Encryption**: Transforming data into an unreadable format for unauthorized users.
- **Access Controls**: Limiting access through authentication and authorization methods.
- **Data Classification**: Identifying sensitive data and applying appropriate protection.



CONFIDENTIALITY

Confidentiality Threats:

- **Data breaches**: Unlawful access to personal or confidential information.
- **Social engineering**: Manipulating people into disclosing sensitive information (e.g., phishing attacks)
- **Phishing**: Attackers trick users into revealing sensitive information

Mitigation:

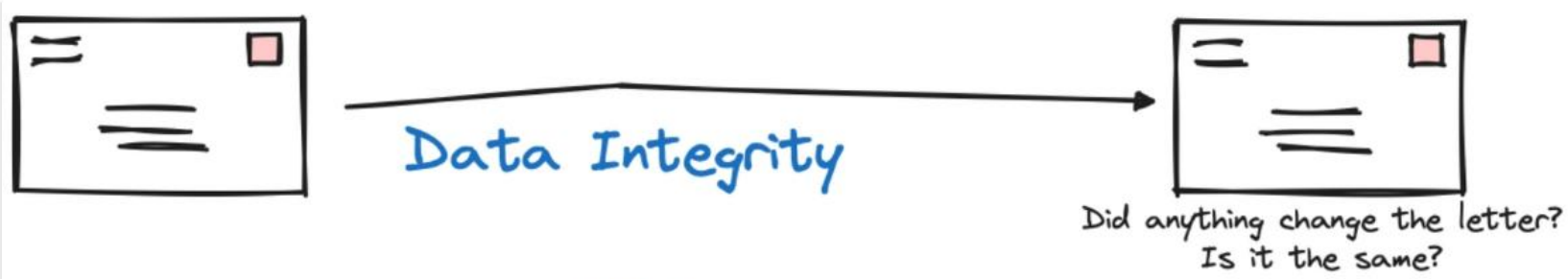
- Strong access controls, encryption, MFA, data masking.
- Training employees on recognizing phishing attacks and other social engineering techniques.

INTEGRITY

Definition: Ensuring the accuracy, consistency, and trustworthiness of data over its lifecycle.

Methods to Maintain Integrity

- **Hashing**: Using algorithms to generate a unique value for data. Any change in the data alters the hash
- **Checksums and Hashes**: Used to detect data corruption during transmission
- **Digital Signatures**: Verifies the authenticity of a document or message



INTEGRITY

Integrity Threats:

- **Data Tampering**: Unauthorized alteration of data (e.g., man-in-the-middle attacks)
- **Malware**: Ransomware and viruses that modify data
- **Man-in-the-Middle Attacks**: Intercept and alter communications between two parties.

Mitigation:

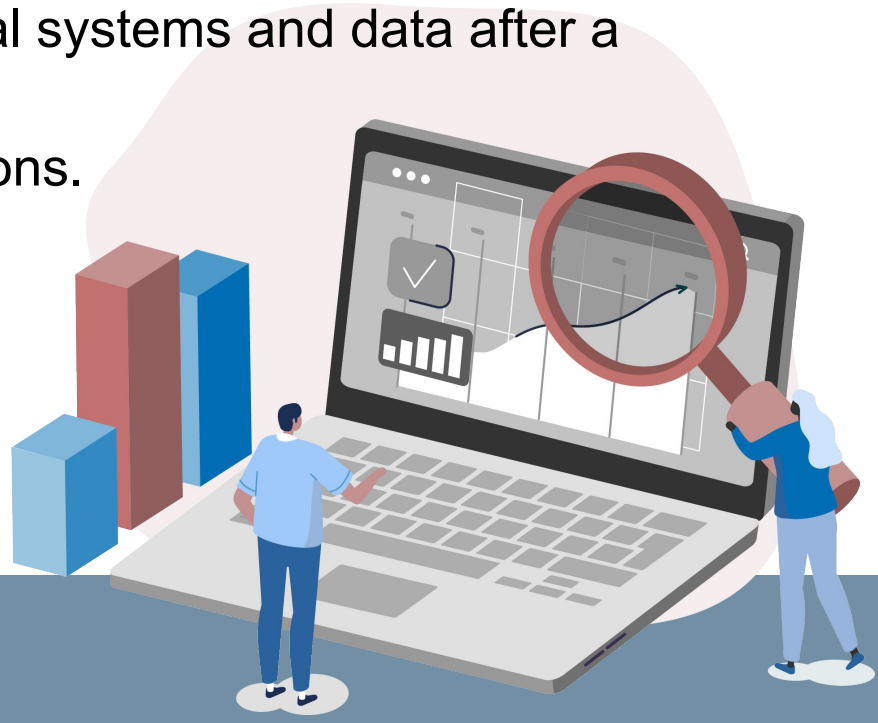
- Regular data backups
- Use of cryptographic checksums (e.g., MD5, SHA) to ensure data integrity
- Intrusion detection systems (IDS) and file integrity monitoring

AVAILABILITY

Definition: Ensuring that authorized users have reliable access to information and resources when needed.

Methods to Maintain Availability

- **Data Backups**: Regularly backing up data to ensure recovery in case of failure.
- **Disaster Recovery Plans**: Outlining how to restore critical systems and data after a disaster.
- **Redundancy**: Having backup systems and failover solutions.



AVAILABILITY

Availability Threats:

- **Denial of Service (DoS) Attacks**: Overloading systems to make them unavailable to legitimate users.
- **Hardware/Software Failures**: Natural disasters, human error, or technical failures leading to outages.

Mitigation:

- Load balancing and failover systems.
- Data centers and cloud solutions with high uptime guarantees (99.9%+).
- Implementing regular maintenance schedules and system monitoring.

RELATIONSHIP BETWEEN THE CIA TRIAD

Interconnection: Each principle supports the others. For example, ensuring data integrity and confidentiality contributes to data availability.

Balancing Security: You may need to trade off one principle against another (e.g., too much security may reduce availability, and excessive availability may compromise confidentiality)

CASE STUDIES

Case Study 1: Equifax Data Breach (Confidentiality)

- **Incident**: In 2017, the personal information of 147 million people was exposed due to a vulnerability in a web application.
- **Failure**: Confidentiality was breached because attackers exploited a known vulnerability that Equifax had failed to patch.
- **Lessons**: The importance of regular patch management and encryption.

CASE STUDIES

Case Study 2: WannaCry Ransomware Attack (Availability)

- **Incident**: In 2017, the WannaCry ransomware attack infected over 230,000 computers, encrypting files and demanding ransom.
- **Failure**: Availability was compromised because victims could no longer access critical files.
- **Lessons**: The importance of data backups, patching systems, and using antivirus software to prevent ransomware.

CASE STUDIES

Case Study 3: Target Data Breach (Integrity)

- **Incident**: In 2013, attackers breached Target's systems and installed malware on point-of-sale systems, compromising 40 million credit and debit card accounts.
- **Failure**: Integrity was breached because attackers were able to steal customer financial data.
- **Lessons**: The need for stronger encryption and better monitoring of third-party vendors

SUMMARY AND CONCLUSION

Before we wrap up, let’s take a moment to revisit the key points we’ve covered today.

- We began by exploring the fundamental **security principles** that drive information security. Remember, these principles—**authentication, authorization, and accountability**—form the backbone of a secure environment.
  - ✔ Authentication verifies who you are
  - ✔ Authorization determines what you can access
  - ✔ Accountability ensures that actions can be traced back to their source.
- Together, these principles guide us in building systems that are protected from unauthorized access and misuse.

SUMMARY AND CONCLUSION

- Then, we moved into the heart of today's discussion—the **CIA Triad**. We talked about:
  - ✔ **Confidentiality**, which ensures that sensitive information stays private and is only accessible to those who are authorized
  - ✔ **Integrity** ensures that the data we rely on is accurate, consistent, and unaltered
  - ✔ **Availability** ensures that systems and data are accessible to authorized users when they need them
- These three pillars are interconnected, and they must be balanced carefully. Without one, the others suffer.

SUMMARY AND CONCLUSION

- As we've seen, information security is not just an IT issue, it's a **business issue**, a **legal issue**, and in some cases, even a **human rights issue**. We live in an era where the **threat landscape** is more complex and widespread than ever. Cybercriminals are becoming more sophisticated, and the attacks we face are more targeted.
- In today's world, **every organization, big or small,** needs to be vigilant. It's not just about protecting **company assets**—it's about protecting **customer trust**. A single breach can lead to devastating financial losses, legal liabilities, and damage to reputation that's difficult to recover from."

THANK YOU