Information Assurance

Course Information

- **Credit Hours:** 3.0
- **Classes Schedule:**

  Wednesday 10:40 pm Room LTC 118, Thursday 10:40 pm Room LTC 118

  Duration : 15 Weeks
- **GCR code:**
- **Assessment:**
  - Quizzes: 10% (Announced & Unannounced)
  - Assignments/ Project : 15% (Individual & Group)
  - Viva : 5%
  - Mid Term: 25%
  - Final: 45%

Policies

- Collaboration and group work are encouraged but each student is required to submit his/her own contribution(s).
- **Cheating and plagiarism** will be strictly punished.
- **No makeup Quizzes** will be taken.
- **Late Assignments** will not be accepted.
- **Copied Assignments** will be severely dealt with.
- Quizzes and Assignments returned must be kept in safe custody; no claim of any mark corrections will be entertained without them

Reference Books

- Joseph Boyce, Daniel Jennings, “Information Assurance: Managing Organizational IT Security Risks”, Butterworth-Heinemann; 1 Edition or Latest
- Andrew Blyth, Gerald L. Kovacich, “Information Assurance: Security in the Information Environment”, Springer; 2nd Edition or Latest
- Christopher Alberts, Audrey Dorofee, “Managing Information Security Risks”, Addison-Wesley Professional; 1st Edition or Latest
- Stephen P. Robbins, Timothy A. Judge, “Essentials of Organizational Behavior", Pearson; 13rd Edition or Latest
- Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, Cengage Learning; 6 Edition or Latest

Instructor’s email

hina.batool@au.edu.pk

Please note: Other than GR or CR, you are not allowed to contact on my personal phone number.

Key Takeaways from IA

- Fundamentals of Information Assurance
- Risk Management
- Security Policies and Procedures
- Legal and Ethical Issues
- Incident Response
- Data Protection
- Compliance and Auditing
- Privacy Considerations

What is Information?

- This class is about Information Assurance; so what is “information”? How does information differ from data?

What is Information?

- “**Information** is **data** endowed with relevance and purpose. Converting data into information thus requires knowledge.
- And what characteristics should information possess to be useful?

  It should be:

  - Accurate
  - Timely
  - Complete
  - Verifiable
  - Consistent
  - Available.

Information Assurance

- If information is so valuable, what would happen if it’s lost, stolen, or altered?”→ This naturally leads to why we need Information Assurance.

What is Information Assurance (IA)?

- Information assurance defines and applies a collection of *policies*, *standards*, *methodologies*, *services*, and mechanisms to maintain ***mission integrity*** with respect to *people*, *process*, *technology*, *information*, and supporting *infrastructure*.

What is Information Assurance (IA)?

- According to the U.S. Department of Defense, IA involves:

Actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

What is Information Assurance (IA)?

According to the DoD definition, these are some aspects of information needing protection:

- **Availability**: timely, reliable access to data and information services for authorized users;
- **Integrity**: protection against unauthorized modification or destruction of information;
- **Confidentiality**: assurance that information is not disclosed to unauthorized persons;
- **Authentication**: security measures to establish the validity of a transmission, message, or originator.
- **Non-repudiation**: assurance that the sender is provided with proof of a data delivery and the recipient is provided with proof of the sender's identity.
- Is this specifically a military view? Which of these are the most important? How would you decide?

IA in History

Thought Experiment

- Suppose you visit an e-commerce website such as your bank
- Before you type in highly sensitive information, you'd like to have some assurance that your information will be protected. Do you (have such assurance)? How can you know?
- What security-relevant things do you want to happen, or not happen when you use such a website?

Thought Experiment

You might want:

- Privacy of your data
- Protection against phishing
- Integrity of your data
- Authentication
- Authorization
- Confidentiality
- Non-repudiation
- Availability
- What else?

Which of these do you think fall under Information Assurance?

Fundamental Concepts in IA

- Core Principles:
  - **Confidentiality**– ensures the disclosure of information only to those persons with authority to see it.
  - **Integrity**– ensures that information remains in its original form; information remains true to the creators intent
  - **Availability**– information or information resource is ready for use within stated operational parameters
  - **Possession**– information or information resource remains in the custody of authorized personnel
  - **Authenticity**– information or information resources conforms to reality; it is not misrepresented as something it is not.

Fundamental Concepts in IA

- Core Principles:
  - **Privacy**– ensures the protection of personal information from observation or intrusion as well as adherence to relevant privacy compliances
  - **Authorized Use**– ensures cost-incurring services are available only to authorized personnel
  - **Nonrepudiation**– ensures the originator of a message or transaction may not later deny action

IA Vs InfoSec

- Both involve people, processes, techniques, and technology (i.e., administrative, technical, and physical controls)
- **Information assurance** and information security are often used **interchangeably** (**incorrectly**)
- InfoSec is focused on the **confidentiality**, **integrity**, and **availability** of information (electronic and non-electronic)
- **IA** has **broader** connotations and explicitly includes **reliability**, **access control**, and **nonrepudiation** as well as a strong emphasis on **strategic risk management**
- ISO **information security management standards** (ISMS) are more closely aligned with **IA**

IA Relationship to Computer Security

IA includes considerations for non-security threats to information systems, such as acts of nature and the process of recovery from incidents. IA emphasizes management, process, and human involvement, and not merely technology. IA deployments may involve multiple disciplines of security:

- COMPUSEC (Computer security)
- COMSEC (Communications security),
- SIGSEC (Signals security) and TRANSEC (transmission security)
- EMSEC (Emanations security) denying access to information from unintended emanations such as radio and electrical signals
- OPSEC (Operations security) the processes involved in protecting information

Four Security Domains

IA has four major categories:

- Physical security
- Personnel security
- IT security
- Operational security

Four Security Domains

- **Physical security** refers to the protection of hardware, software, and data against physical threats to reduce or prevent disruptions to operations and services and loss of assets.
- **Personnel security** focuses on making sure that people (employees, staff) don't accidentally or intentionally harm the system, whether it's by making changes or causing important data to become unavailable.
- **IT security** collectively contributes to an IT infrastructure achieving and sustaining confidentiality, integrity, availability, accountability, authenticity, and reliability.
- **Operational security** involves the implementation of standard operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources

Four Security Domains

Into which of these would you put the following?

- Enforcing hard-to-guess passwords
- Encrypting your hard drive
- Locking sensitive documents in a safe
- Stationing a marine guard outside an embassy
- Assigning security clearances to staffers
- Using SSL for data transfers
- Having off-site backup of documents

Four Security Domains

- **Enforcing hard-to-guess passwords**

  IT Security: Relates to authentication, confidentiality, and integrity of systems.

- **Encrypting your hard drive**

  IT Security: Protects confidentiality and integrity of stored data.

- **Locking sensitive documents in a safe**

  Physical Security: Prevents unauthorized physical access to paper-based or digital records.

- **Stationing a marine guard outside an embassy**

  Physical Security: Direct protection against physical intrusions or attacks.

Four Security Domains

- **Assigning security clearances to staffers**

Personnel Security: Controls who can access sensitive information based on trust level.

- **Using SSL for data transfers**

IT Security: Protects confidentiality and integrity of data in transit.

- **Having off-site backup of documents**

Operational Security: A standard procedure ensuring availability and resilience in case of disaster

Levels of IA

According to Blyth and Kovacich, IA can be thought of as protecting information at three distinct levels:

- Physical
- Perceptual
- Infrastructure

IA Levels: Physical

The lowest level focus of IA is the physical level: computers, physical networks, telecommunications and supporting systems such as power, facilities and environmental controls. Also at this level are the people who manage the systems.

- **Desired Effects**: what we want
- **Attacker's Operations**: what bad actors try to do
- **Defender's Operations**: what we do to stop or fix it

IA Levels: Physical

The lowest level focus of IA is the physical level: computers, physical networks, telecommunications and supporting systems such as power, facilities and environmental controls. Also at this level are the people who manage the systems.

- **Desired Effects**: controlled access, operational continuity
- **Attacker's Operations**: sabotage, unauthorized access
- **Defender's Operations**: regular inspections and maintenance, incident response,

IA Levels: Infrastructure

The second level focus of IA is the information structure level. This covers information and data manipulation ability maintained in cyberspace, including data structures, processes and programs, protocols, data content and databases.

- **Desired Effects**: data integrity, confidentiality, availability
- **Attacker's Operations**: data breaches, denial of service
- **Defender's Operations**: data encryption, access control

IA Levels: Perceptual

The third level focus of IA is the perceptual level, also called social engineering. This is abstract and concerned with the management of perceptions of the target, particularly those persons making security decisions.

- **Desired Effects**: informed decision-making, trust in security measures
- **Attacker's Operations**: phishing, manipulation, impersonation
- **Defender's Operations**: Training, clear communication

Factors Adversely Affecting IA

- **Interruption:**

  An information asset of the system becomes unstable, unavailable or lost.

  Examples: The physical theft/destruction of a computer system. The removal of information from an information system. This is an attack on availability

- **Interception:**

  Unauthorized party has gained access to an information asset. The party can be a program, computer system or person.

  Example: Recording a telephone conversation or monitoring a computer network. This is an attack on confidentiality

Factors Adversely Affecting IA

- **Modification:**

  Unauthorized party tampers with the asset.

  Example: The unauthorized installation of monitoring software or hardware. The unauthorized insertion, manipulation or deletion of information. This is an attack on integrity

- **Fabrication:**

  Counterfeiting (imitate fraudulent of an asset)

  Example: An intruder may insert fake transactions into a computer network. This is an attack on integrity.

Factors Adversely Affecting IA

- **Repudiation of origin**

  A false denial that an entity sent or created something

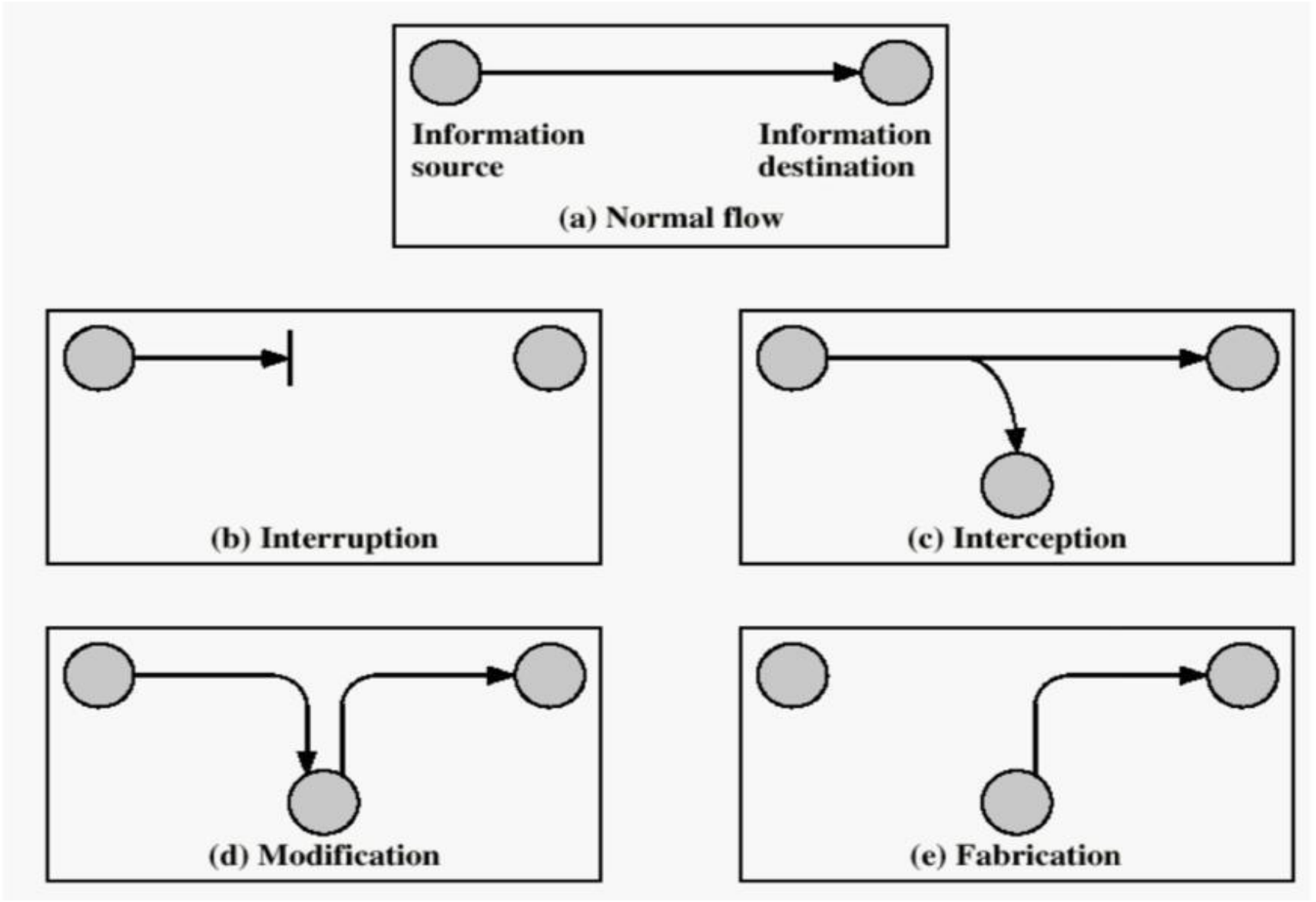
- **Denial of Receipt**

  A false denial that an entity received some information or message. Example, I didn’t receive the shipment.

- **Denial of Service**

  long term inhibition of information/service. Attack on availability.

Factors Adversely Affecting IA



IA Functional Components

Note that IA is both proactive and reactive involving: protection, detection, capability restoration, and response.

- **IA environment protection pillars:** ensure the availability, integrity, authenticity, confidentiality, and non-repudiation of information.
- **Attack detection:** timely attack detection and reporting is key to initiating the restoration and response processes.

IA Functional Components

- **Capability restoration:** relies on established procedures and mechanisms for prioritizing restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer. A post-attack analysis should be conducted to determine the command vulnerabilities and recommended security improvements.

- **Attack response:** involves determining actors and their motives, establishing cause and complicity, and may involve appropriate action against perpetrators.

Some Basic IA Terms

An asset is the resource being protected, including:

- **physical assets**: devices, computers, people
- **logical assets**: information, data (in transmission, storage, or processing), and intellectual property.
- **system assets**: any software, hardware, data, administrative, physical, communications, or personnel resource within an information system.

Some Basic IA Terms

Often a security solution/policy is phrased in terms of the following three categories:

- **Objects:** the items being protected by the system (documents, files, directories, databases, transactions, etc.)
- **Subjects:** entities (users, processes, etc.) that execute activities and request access to objects.
- **Actions:** operations, primitive or complex, that can operate on objects and must be controlled.
- For example, in the Unix operating system, processes (subjects) may have permission to perform read, write or execute (actions) on files (objects). In addition, processes can create other processes, create and delete files, etc.

Thanks a lot