Information Assurance and Security (CSC 303)

Lecture objectives:

- We seek basic understanding of information assurance and security

Information, Security

- Information is data (raw fact(s)) with meaning.
- Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.

Information Security

- Information Security, sometimes shortened to **InfoSec,** is simply the process of keeping information secure (i.e. defending information, whether electronic or physical from unauthorized access, use, disclosure, modification,…, or destruction).

Information Security Cont.:

InfoSec, therefore involves protecting an information's:

- Availability
- Integrity and
- Privacy/Confidenciality/Secrecy

Information Security Cont.:

- Information Security involves a Tradeoff between Security and Usability:
- There is no such thing as a totally secure system – except perhaps one that is entirely unusable by anyone!
- Corporate Information Security's goal is to provide an appropriate level of security, based on the value of an organization's information and its business needs.

Information Assurance (IA):

- IA is the act of ensuring that data is not lost when critical issues such as natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost arise. It is strongly related to the field of information security, and also with business continuity.

IA Cont.:

- IA is the act of ensuring that data is not lost when critical issues such as natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost arise. It is strongly related to the field of information security, and also with business continuity.

IA Cont.:

- Therefore in addition to defending against malicious hackers and code (e.g., viruses), IA practitioners consider corporate governance issues such as privacy, regulatory and standards compliance, auditing, business continuity, and criminology, in addition to computer science.

System Vulnerability, Security System and Threat:

- The term **threat** refers to any potentially harmful circumstance or event.
- Threats to computerized information systems include hardware and software failure; user errors; physical disasters such as fire or power failure; theft of data, hacking, unauthorized use of data,...,and telecommunications disruptions

System Vulnerability, Security System and Threat:

- **Security systems** are created for the purpose of protecting assets against threats. If our computer is threatened by viruses, then our security system may include such things as antivirus software, network firewalls and file protection mechanisms to guard against this threat.

System Vulnerability, Security System and Threat Cont.:

- **vulnerability** is a weakness within a security system intended to protect an asset.
- When data are stored in digital form, they are more vulnerable than when they exist in manual form.
- On-line systems and telecommunications are especially vulnerable because data and files can be immediately and directly accessed through computer terminals or at points in the telecommunications network.

System Vulnerability, Security System and Threat Cont.:

- No system is ever completely secure, because every system has vulnerabilities.
- However, damage does not occur unless there is an **attack** (a deliberate attempt to exploit a vulnerability).
- Any mechanism that is designed to guard against a vulnerability is called a **mitigation.**

Contemporary security challenges and vulnerabilities: