Information Assurance and Security

LECTURE 1 : INTRODUCTION TO INFORMATION SECURITY

Resource Personnel

Kavinga Yapa Abeywardena (Lecturer in Charge)
Senior Lecturer
Department of Computer Systems Engineering
Email: kavinga.y@sliit.lk

Ms. Chethana Liyanapathirana (Co-Lecturer)
Senior Lecturer
Department of Computer Systems Engineering
Email: chethana.l@sliit.lk

Mr. Kanishka Yapa (Co-Lecturer)
Lecturer
Department of Computer Systems Engineering
Email: kanishka.y@sliit.lk

Dr. Harinda Fernando (Co-Lecturer)
Assistant Professor
Department of Computer Systems Engineering
Email: harinda.f@sliit.lk

Mr. V.A.M. Ragunathan Sinthujan (Co-Lecturer)
Lecturer – SLIIT Northern UNI
Department of Information Technology
Email: sinthujan.r@sliit.lk

Lecture Delivery

Lectures (Face-to-face)	**2**	**Hours/Week**
Tutorials	**1**	**Hours/Week**
Labs	**2**	**Hours/Week**

Assessment Criteria

Continuous Assessments			
● Midterm Examination	20	%	L01-LO3
● Assignment	30	%	LO2-LO4
End Semester Assessment			
● Final Examination	50	%	LO1-LO5
TOTAL	100	%	

Introduction to Information Security

Objective:

- Describe the formal definition of Computer Security and Information Security
- Describe Confidentiality, Integrity, and Availability as the key security requirements
- Describe the security threats and attacks types

Recommended Texts

W. Stallings and L. Brown, “Computer Security, Principles and Practice, 2nd edition, Pearson, 2012, Chapter 1.

Supplementary text

Charles P. Pfleeger and Shari L. Pfleeger, Security in Computing (3rd edition). Prentice-Hall. 2003. ISBN: 0-13-035548-8.

Computer Security

Definition (NIST Computer Security Handbook)

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Key objectives of Computer Security:

- Confidentiality
- Integrity
- Availability

Information Security (InfoSec)

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

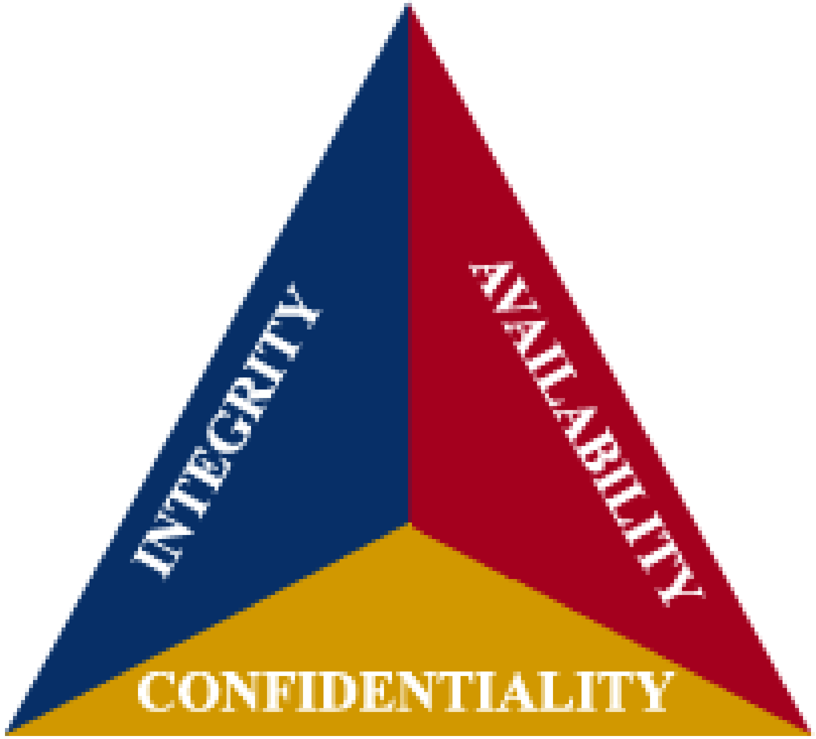
(Source : NIST Glossary of Key Information Security Terms)

Information Assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

(Source : NIST Glossary of Key Information Security Terms)

CIA Triad



Confidentiality (C)

This term covers two related concepts.

- **Data confidentiality :** Assures that confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy :** Assures that the owners have control on:
    - ➢ What information related to them may be collected and stored,
    - ➢ By whom and to whom that information may be disclosed.

NIST's Requirement: Preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Loss of confidentiality means unauthorized disclosure of information.

Integrity (I)

This term covers two related concepts.

- **Data integrity:** Information and programs are changed only in a specified and authorized manner.
- **System integrity:** A system performs its intended function in an unimpaired manner, and free from deliberate or inadvertent unauthorized manipulation of the system.

Requirement: Guard against improper information modification or destruction, including ensuring information nonrepudiation authenticity.

Loss of Integrity means unauthorized modification or destruction of information.

Availability (A)

Systems work promptly and service is not denied to authorized users.

NIST's requirement: Ensuring timely and reliable access and use of information.

Loss of Availability means disruption to the authorized users in accessing or use of information.

Additional Objectives

Authenticity: Able to verify that

- the users are who they claim they are, and
- the system receives data from a trusted source.

NIST includes authenticity as part of Integrity

Accountability: Able to trace back the actions performed by an entity to that entity.

Accountability supports: nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery and legal action.

Read the examples of C-I-A in the textbook (Stallings & Brown)

Computer Security Model (RFC 2828)

1) **System Resource** or asset that needs to be protected

- Hardware: e.g., Computer System, data storage, communication devices.
- Software: e.g., operating systems, program utilities and applications.
- Data: e.g., data and password files, databases.
- Communication facilities and networks: e.g., LAN, WAN, routers, etc.

2) **Vulnerabilities** of system resources

Definition: A flaw or weaknesses in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

When the resource is corrupted → violate Integrity

When the resource is leaky → violate Confidentiality

When the resource is unavailable → violate Availability

Computer Security Model (cont.)

3) **Threat** is a possible danger that might exploit a vulnerability.

It represents a potential harm to the system resource.

4) **Attack** is a threat that is carried out (threat action)

Two attack types:

- Active attack: An act that has negative effects on system resources
- Passive attack: An act to make use of system information but it does not affect the system

The origin of an attack:

- Inside attack is carried out by an entity inside the security perimeter.
- Outside attack is performed by an unauthorized users.

Computer Security Model (cont.)

5) **Adversary** is an entity that carried out an attack

- A threat agent or an attacker.

6) **Countermeasure** is any means taken to address an attack,

- to prevent an attack from being successful,
- to detect the attack if the attack is successful, and
- to recover from the damage due to the attack.

7) **Risk** is the expected loss due to a particular attack.

- Examples?

Exploits

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack.

- *Used as a verb, exploit refers to the act of successfully making such an attack (make use of a vulnerability).*

Vulnerability Assessment

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in Information systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

Penetration Testing

Penetration testing (also called pen testing or ethical hacking) is the practice of testing a Information system, network or web application to find security vulnerabilities that an attacker could exploit. The process involves gathering information about the target before the test, identifying possible entry points, attempting to break in either virtually or for real and reporting back the findings.

Penetration testing can be automated with software applications or performed manually.

Goal of Penetration Testing

- Identify weak spots in an organization's security posture
- Measure the compliance of its security policy
- Test the staff's awareness of security issues
- Determine whether and how the organization would be subject to security disasters.

Passive Attacks

Passive attack is performed by eavesdropping or monitoring data transmission

- The attacker only learns or makes use of information without affecting system resources
- Passive attack is hard to detect because data is not altered
- Use attack prevention (not detection) to handle it

Two types of passive attacks.

- Release of message contents (confidentiality) – Ex: Eavesdropping on Communication Channels
- Traffic analysis, if the data is encrypted.

Active Attacks

Active attacks alters system resources or affecting their operations. Active attack is difficult to prevent but easy to detect

Four categories of active attack:

- Replay. Capture and retransmit data unit to produce an unauthorized effect
- Masquerade. One entity pretends to be another entity
- It usually includes other form of attack, e.g., replay
- Data modification. Alter some portion of legitimate data, delay the data, or reorder the data to produce an unauthorized effect
- Denial of Service. Prevent or disallow the legitimate use of facilities

Inside attacks

Attack vectors can also originate from inside the network. An internal user, such as an employee, can accidently or intentionally:

- Steal and copy confidential data to removable media, email, messaging software, and other media.
- Compromise internal servers or network infrastructure devices.
- Disconnect a critical network connection and cause a network outage.
- Connect an infected USB drive into a corporate computer system.

Internal threats also have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees also have knowledge of the corporate network, its resources, and its confidential data.

Outside attacks

Many attack vectors originate from outside the corporate network. Outside attacks are performed by an unauthorized users.

- For example, attackers may target a network, through the Internet, in an attempt to disrupt network operations and create a denial of service (DoS) attack.

Computer Security Model

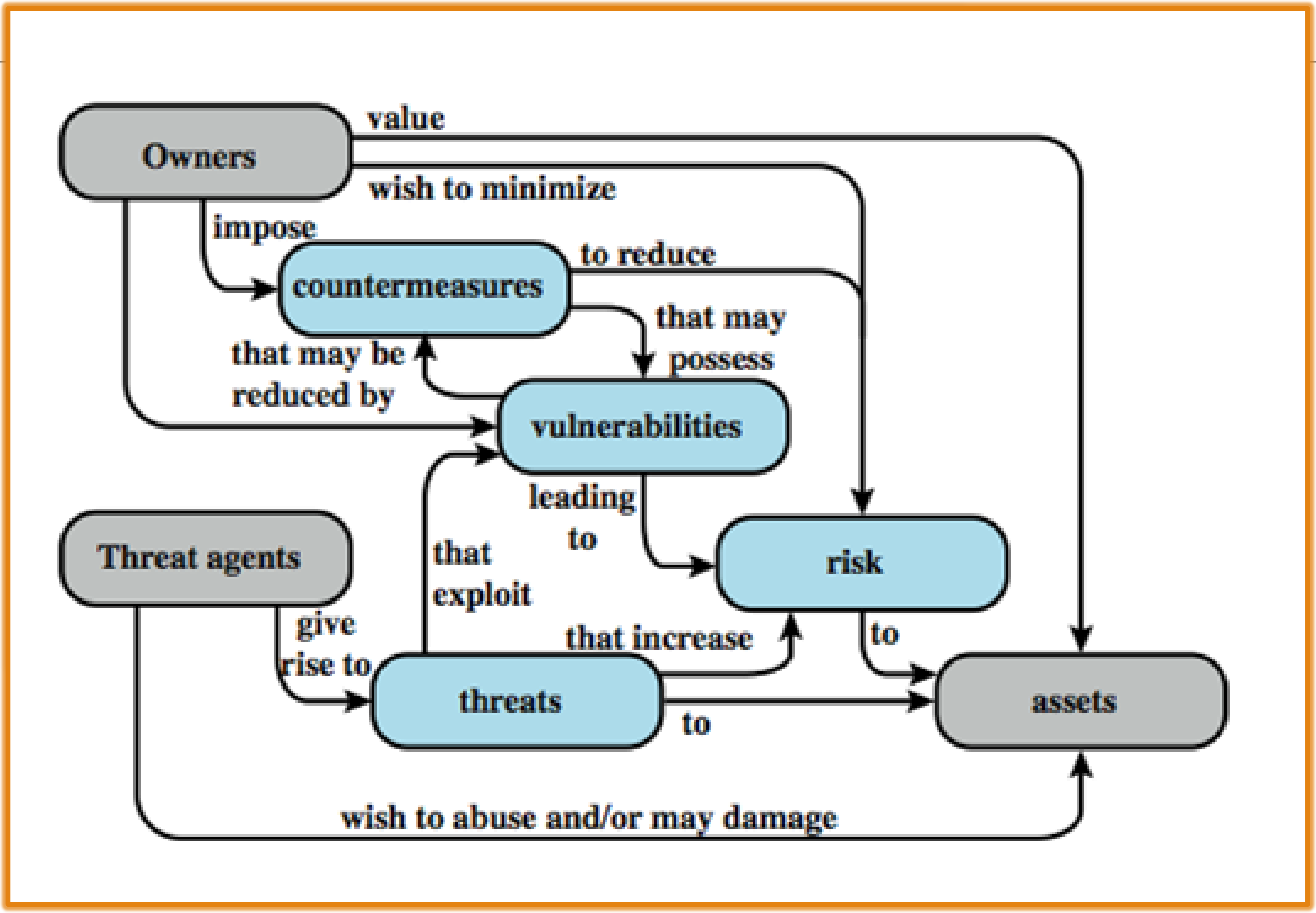


Figure from Stallings & Brown textbook