
Overview of Information Security

Lecture By *Dr Richard Boateng*, UGBS, Ghana

Email: richard@pearlrichards.org

Original Slides by Elisa Bertino
CERIAS and CS & ECE Departments, Purdue University

Outline

- Information Security: basic concepts
- Privacy: basic concepts and comparison with security

Information Security: Basic Concepts

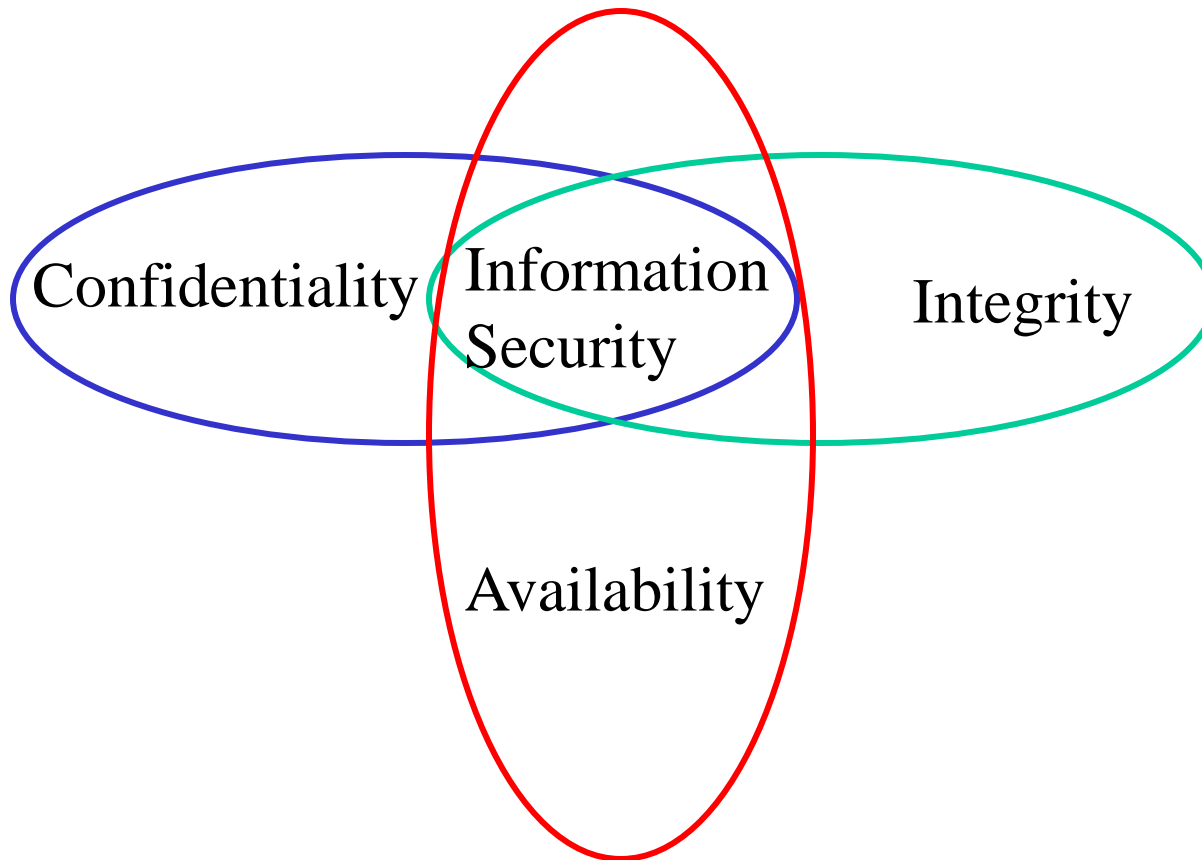
Information Security

- A state of being free from
 - unauthorized use of the system and its resources,
 - misuse of the system and its resources, and
 - disturbance of the system's operations
- The field of study about techniques for achieving and maintaining such a secure state

Information Protection - Why?

- Information are an important strategic and operational asset for any organization
- Damages and misuses of information affect not only a single user or an application; they may have disastrous consequences on the entire organization
- Additionally, the advent of the Internet as well as networking capabilities has made the access to information much easier

Information Security: Main Requirements



Information Security: Examples

- Consider a payroll database in a corporation, it must be ensured that:
 - salaries of individual employees **are not disclosed** to arbitrary users of the database
 - salaries **are modified** by only those individuals that are properly authorized
 - paychecks **are printed on time** at the end of each pay period

Information Security: Examples

- In a military environment, it is important that:
 - the target of a missile is not given to an unauthorized user
 - the target is not arbitrarily modified
 - the missile is launched when it is fired

Information Security - main requirements

- *Confidentiality* - it refers to information protection from unauthorized read operations
 - the term *privacy* is often used when data to be protected refer to individuals
- *Integrity* - it refers to information protection from modifications; it involves several goals:
 - Assuring the integrity of information with respect to the original information (relevant especially in web environment) – often referred to as *authenticity*
 - Protecting information from unauthorized modifications
 - Protecting information from incorrect modifications – referred to as *semantic integrity*
- *Availability* - it ensures that access to information is not denied to authorized subjects

Information Security – additional requirements

- *Information Quality* – it is not considered traditionally as part of information security but it is very relevant
- *Completeness* – it refers to ensure that subjects receive all information they are entitled to access, according to the stated security policies

Possible Targets of Security Threats

- ***Information:*** Unauthorized Access to the Information Stored in the System
- ***Control:*** Executing Unauthorized Control of the System or Its Component(s)
- ***Functionality / Performance / Availability:*** Disabling or Degrading the functionality, Performance or Availability of the System

Classes of Threats

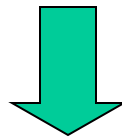
- **Disclosure**
 - Snooping, Trojan Horses
- **Deception and Social Engineering**
 - Modification, spoofing, repudiation of origin, denial of receipt
- **Disruption**
 - Modification
- **Usurpation**
 - Modification, spoofing, delay, denial of service

Possible Source(s) of Threats

- Inside the System
- Outside the System
- Interface to the System (including communication channels)

Information Security: A Complete Solution

- It consists of:
 - first defining a *security policy*
 - then choosing some *mechanism* to enforce the policy
 - finally providing *assurance* that both the mechanism and the policy are **sound**



SECURITY LIFE-CYCLE

Policies and Mechanisms

- Policy says what is, and is not, allowed
 - This defines “security” for the information
- Mechanisms enforce policies
- Composition of policies
 - If policies conflict, discrepancies may create security vulnerabilities

Approaches to Information Security

1. Prevention of Threats → Policies

- Attempt to design a system so that it's perfectly secure

2. Exclusion of Unknown Entities → Identification and Authentication

- Attempt to distinguish well-known entities from suspicious entities

3. Hiding Important Information → Cryptography

- Attempt to make critical information incomprehensible
Theoretically, except one-time pad, there is no encryption scheme perfectly secure.

4. Detection of Potential Threats → Monitoring, Auditing, Detection, and Confinement

- Attempt to identify violation of security policies or possible trials of intrusion to a system

Encryption

- In cryptography, **encryption** is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special information, usually referred to as a *key*.
- The result of the process is **encrypted** information (in cryptography, referred to as ciphertext).

Information Security – Mechanisms

- Confidentiality is enforced by the **access control mechanism**
- Integrity is enforced by the **access control mechanism** and by **the semantic integrity constraints**
- Availability is enforced by the **recovery mechanism** and by detection techniques for DoS attacks – an example of which is query flood

Information Security – How?

Additional mechanisms

- *User authentication* - to verify the identity of subjects wishing to access the information
- *Information authentication* - to ensure information authenticity - it is supported by **signature** mechanisms
- *Encryption* - to protect information when being transmitted across systems and when being stored on secondary storage
- *Intrusion detection* – to protect against impersonation of legitimate users and also against insider threats

Information Security – How?

- Information must be protected at various levels:
 - The operating system
 - The network
 - The data management system
 - Physical protection is also important

Data vs Information – which is important?

- Computer security is about controlling access to information and resources
- Controlling access to information can sometimes be quite elusive and it is often replaced by the more straightforward goal of controlling access to data
- The distinction between data and information is subtle but it is also the root of some of the more difficult problems in computer security
- *Data* represents information. *Information* is the (subjective) interpretation of data

Inference - Example

Name	Sex	Programme	Units	Grade Ave
Alma	F	MBA	8	63
Bill	M	CS	15	58
Carol	F	CS	16	70
Don	M	MIS	22	75
Errol	M	CS	8	66
Flora	F	MIS	16	81
Gala	F	MBA	23	68
Homer	M	CS	7	50
Igor	M	MIS	21	70

Assurance

Assurance is a measure of how well the system meets its requirements; more informally, how much you can trust the system to do what it is supposed to do. It does not say what the system is to do; rather, it only covers how well the system does it.

- Specification
 - Requirements analysis
 - Statement of desired functionality
- Design
 - How system will meet specification
- Implementation
 - Programs/systems that carry out design

Case Studies

Management and Legal Issues

- Cost-Benefit Analysis
 - Is it more cost-effective to prevent or recover?
- Risk Analysis
 - Should we protect some information?
 - How much should we protect this information?
- Laws and Customs
 - Are desired security measures illegal?
 - Will people adopt them?

Human Factor Issues

- Organizational Problems
 - Power and responsibility
 - Financial benefits
- People problems
 - Outsiders and insiders
 - Social engineering

Key Points

- Policies define security, and mechanisms enforce security
 - Confidentiality
 - Integrity
 - Availability
- Importance of assurance
- The human factor