Information & System Security

Lecture 3

VIT-AP
UNIVERSITY

1.5 Topics discussed in this section:

1.5.1 Fundamental Security Design Principles

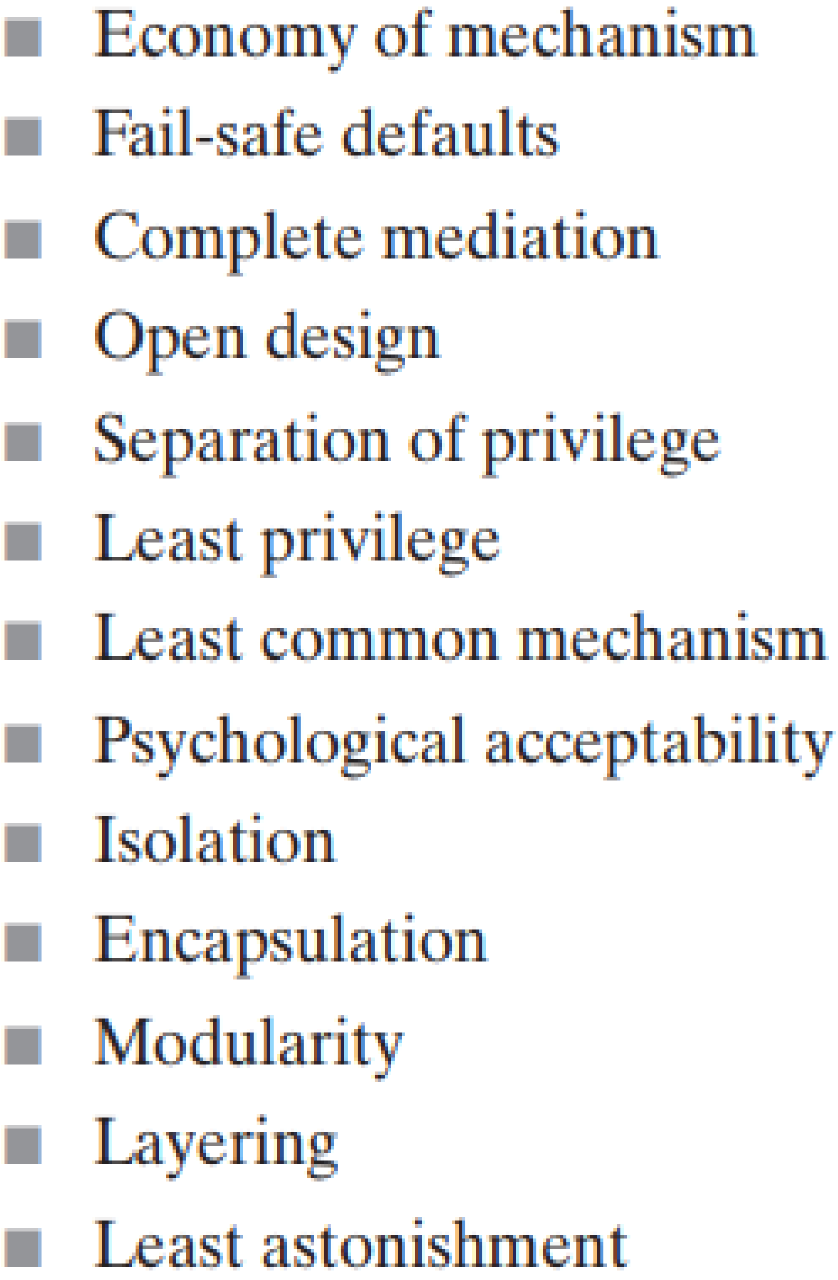
1.5.2 Information and network security policies

1.5.3 Access Control Structures

1.5.4 Model for Network Security

1.5.1 Fundamental Security Design Principles

- The National Centers of Academic Excellence in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U.S. Department of Homeland Security, list the following as fundamental security design principles.



- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

1.5.1 Fundamental Security Design Principles

- **Economy of mechanism** means that the design of security measures embodied in both hardware and software should be as simple and small as possible.

- **Fail-safe defaults** means that access decisions should be based on permission rather than exclusion. That is, the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted.

- **Complete mediation** means that every access must be checked against the access control mechanism.

1.5.1 Fundamental Security Design Principles

- **Open design** means that the design of a security mechanism should be open rather than secret. For example, although encryption keys must be secret, encryption algorithms should be open to public scrutiny.

- **Separation of privilege** is a practice in which multiple privilege attributes are required to achieve access to a restricted resource. A good example of this is multifactor user authentication, which requires the use of multiple techniques, such as a password and a smart card, to authorize a user.

1.5.1 Fundamental Security Design Principles

- **Least privilege** means that every process and every user of the system should operate using the least set of privileges necessary to perform the task. A good example of the use of this principle is role-based access control.

- **Least common mechanism** means that the design should minimize the functions shared by different users, providing mutual security.

- **Psychological acceptability** implies that the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access.

1.5.1 Fundamental Security Design Principles

- **Isolation** is a principle that applies in three contexts. First, public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering.

- **Encapsulation** can be viewed as a specific form of isolation based on object-oriented functionality.

- **Modularity** in the context of security refers both to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation.

1.5.1 Fundamental Security Design Principles

- **Layering** refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected.

- **Least astonishment** means that a program or user interface should always respond in the way that is least likely to astonish the user.

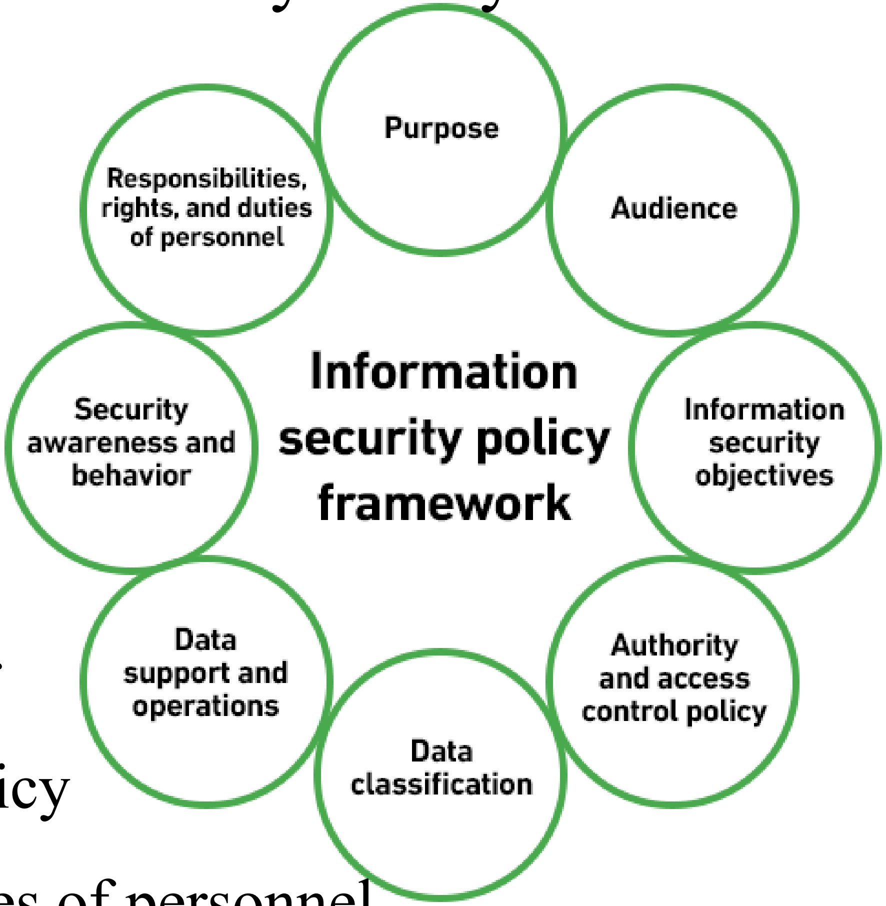
1.5.2 Information and network security policies

- An **information security policy** (ISP) is a set of rules that guide individuals who work with IT assets.
- Your company can create an information security policy to ensure your employees and other users follow security protocols and procedures.
- Creating an effective security policy and taking steps to ensure compliance is a critical step to prevent and mitigate security breaches. To make your security policy truly effective, update it in response to changes in your company, new threats, conclusions drawn from previous breaches, and other changes to your security posture.

1.5.2 Information and network security policies

- 8 Elements of an Information Security Policy

1. Purpose
2. Audience
3. Objectives-C I A
4. Data classification
5. Data support and operations
6. Security awareness and behavior
7. Authority and access control policy
8. Responsibilities, rights, and duties of personnel


Purpose
Audience
Information security objectives
Authority and access control policy
Data classification
Data support and operations
Security awareness and behavior
Responsibilities, rights, and duties of personnel
Information security policy framework

https://www.exabeam.com/information-security/information-security-policy/

1.5.2 Information and network security policies

- A **network security policy** (NSP) is a generic document that outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the company security/ network security environment.
- The security policy should define the policies that will be enforced – this is done by dictating a hierarchy of access permissions – granting users access to only what they need to do their work.

1.5.3Access Control Structures

- **Access control** is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

- There are two types of access control: **physical** and **logical**.

- **Physical** access control limits access to campuses, buildings, rooms and physical IT assets.

- **Logical** access control limits connections to computer networks, system files and data.

1.5.3Access Control Structures

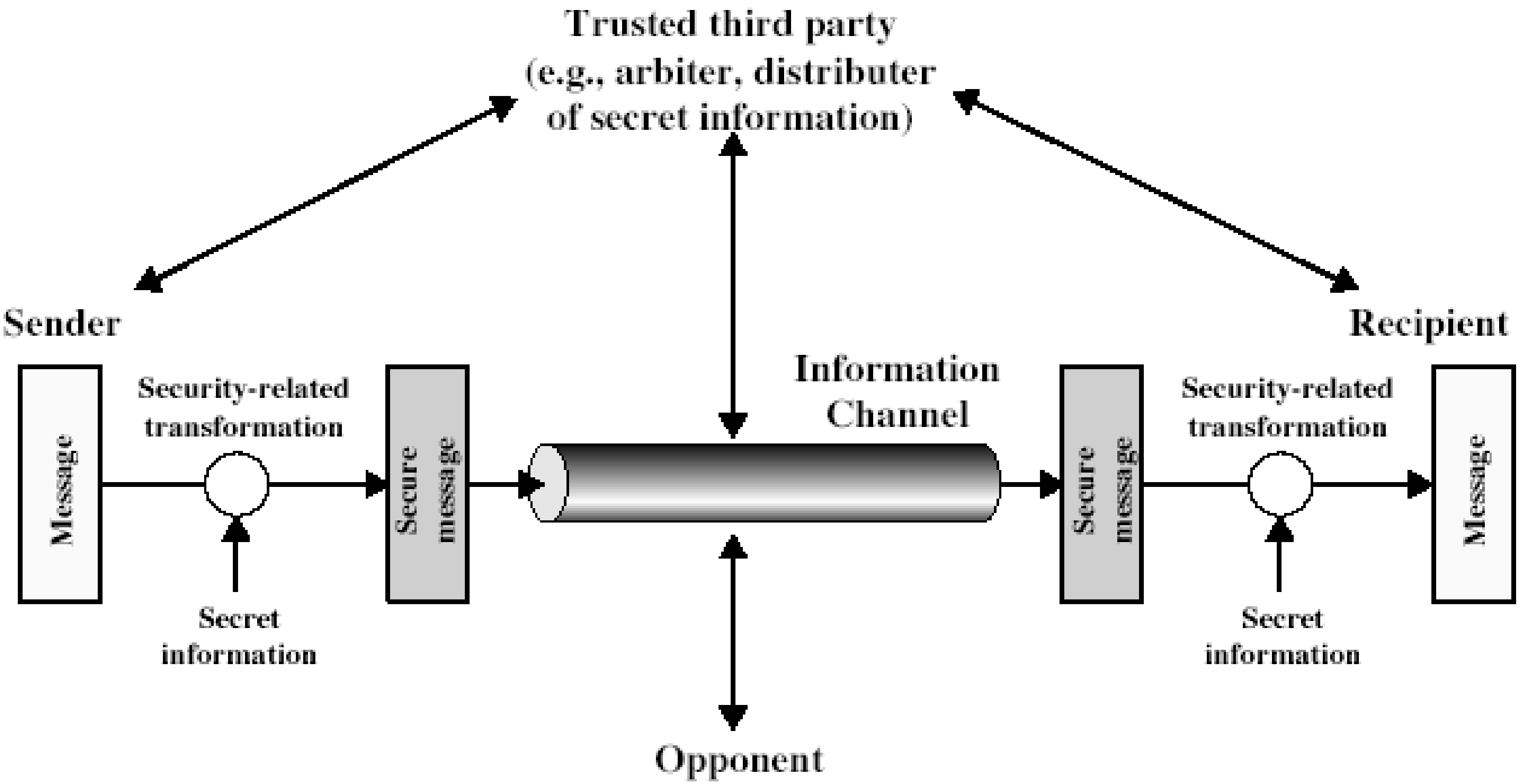
- Access control systems perform identification, authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors.
  - Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems.

1.5.3Access Control Structures

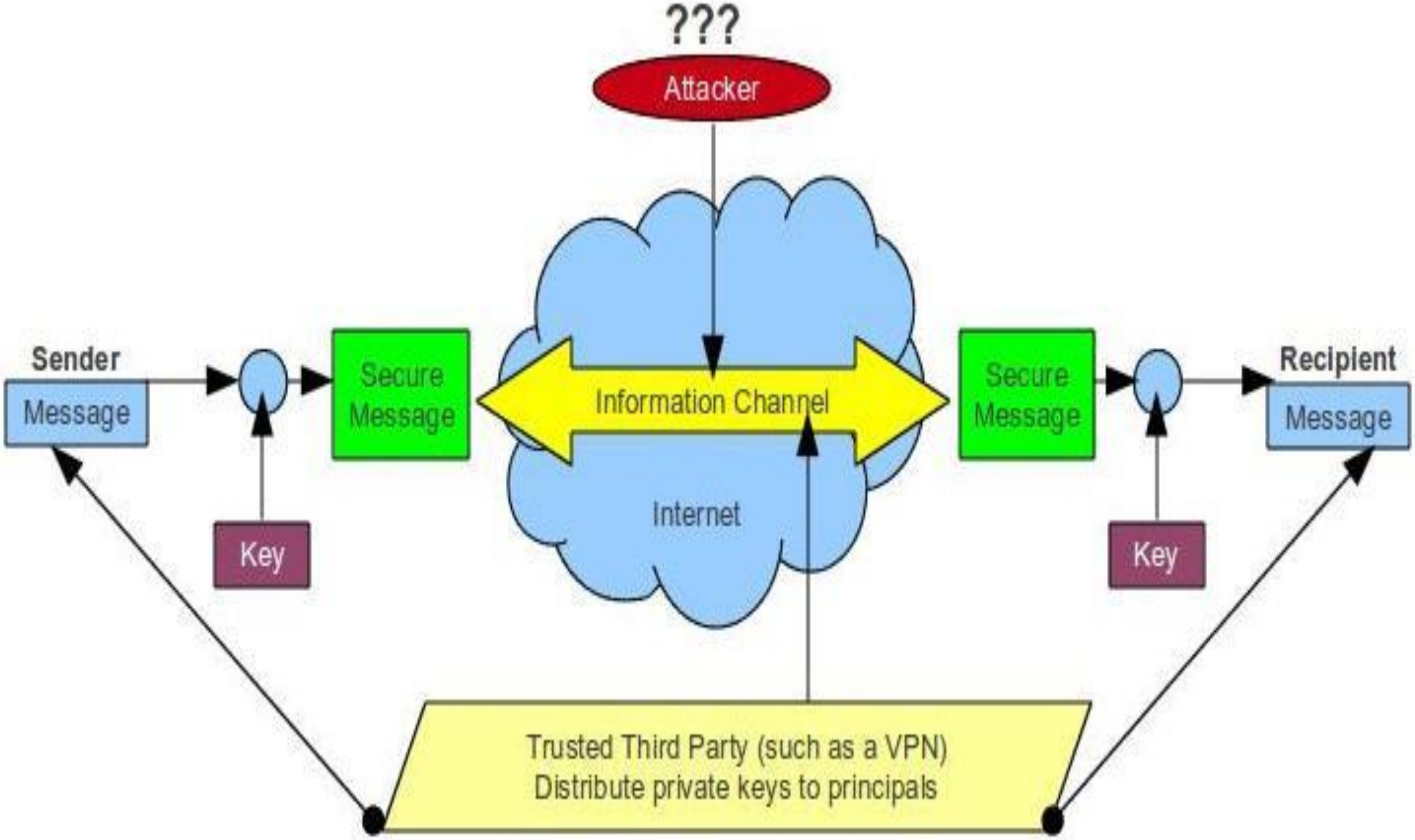
- **Types of access control**
  - The main models of access control are the following:
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
  - Role-based access control (RBAC)
  - Rule-based access control
  - Attribute-based access control (ABAC)

https://searchsecurity.techtarget.com/definition/access-control

1.5.4 Model for Network Security



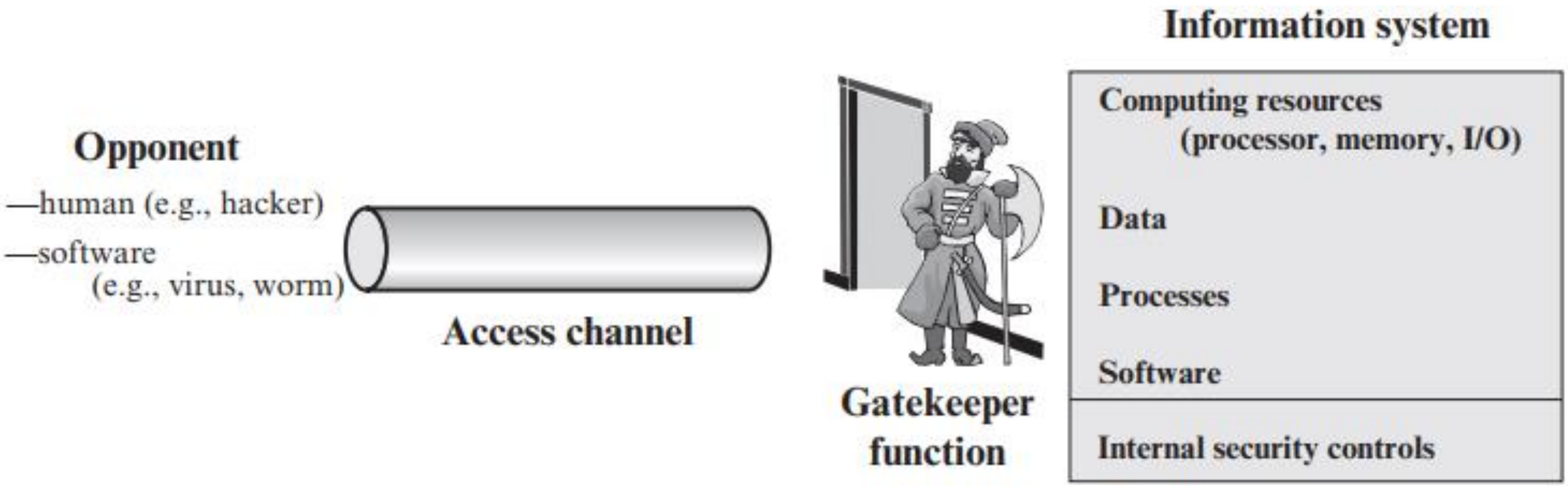
1.5.4 Model for Network Security



1.5.4 Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principles to use the transformation and secret information for a security service

1.5.4 Model for Network Security



Model for Network Access Security

1.5.3 Model for Network Security

Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems can be used to implement this model

References

- **Chapter 1 -** William Stallings, *Cryptography and Network Security Principles and Practices*, 7th Edition, Pearson Education, 2017**.**

- **Chapter 2 -** Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, *Security in Computing*, 5E, Prentice Hall, 2015.