Network Security

Attila Özgit

METU, Department of Computer Engineering

ozgit@metu.edu.tr

Based on:

Henric Johnson's (Blekinge Institute of Technology,Sweden) course slides

William Stallings' "Network Security Essentials" book.

Outline

- Introduction
  - Information Security
  - Network Security vs. Computer Security
- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defense
- A model for Internetwork Security

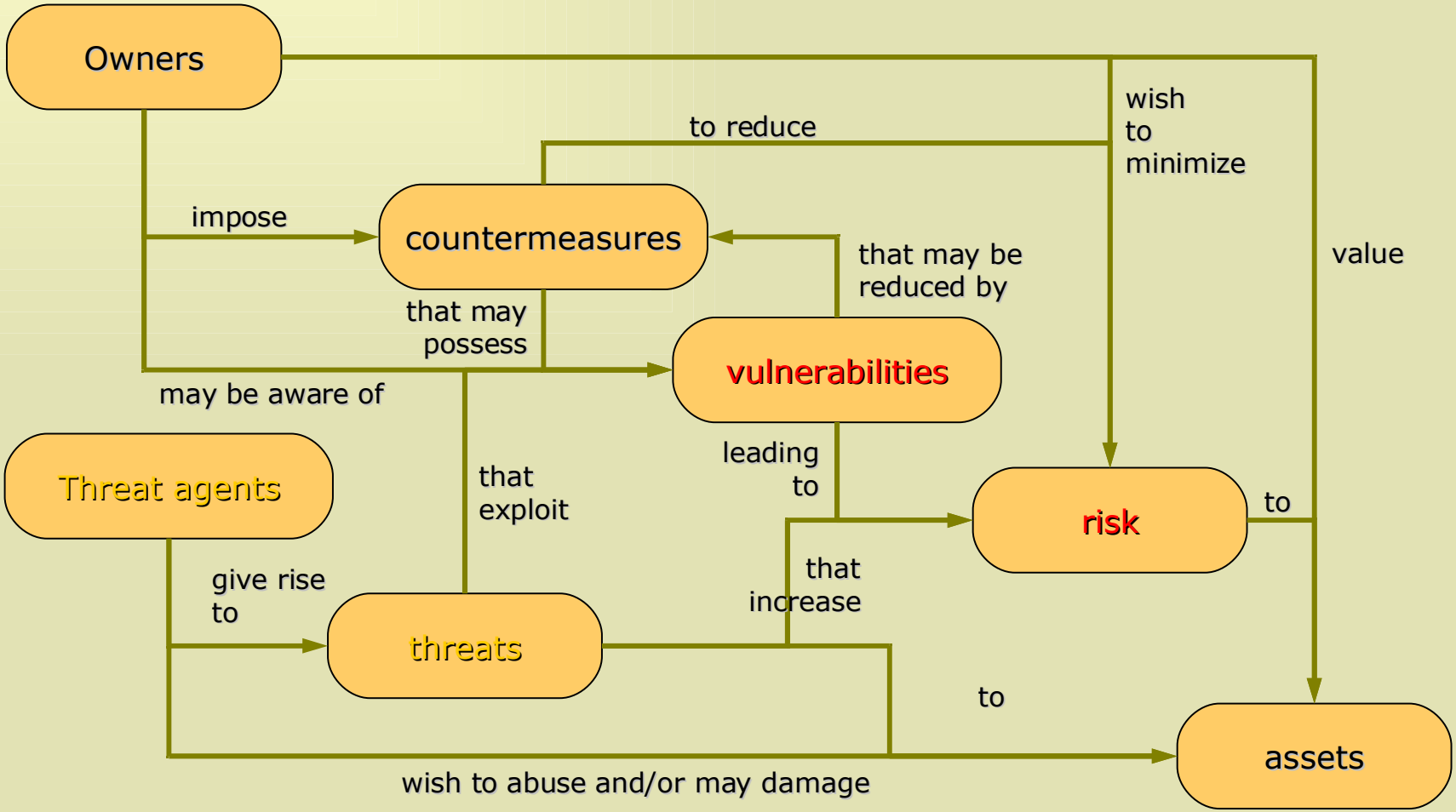
A Definition

- *Security* is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable.

Vulnerability, Threat and Attack

- A vulnerability is a known or unknown *weakness* of an (somehow) accessible service - software.
- A threat is a *potential* violation of security.
  - Flaws in design, implementation, and operation.
- An attack is any *action* that violates security.
  - Active *adversary*.

Owners / Risks / Assets



Attacks, Services and Mechanisms

- **Security Attack:** Any action that compromises the security of information.
- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.
  - Intended to counter security attacks

Policy & Mechanisms

- *Policy*: collection of high-level statements of what is, and is not allowed.
- *Mechanism*: a procedure, tool, or method of enforcing a policy.
  - Security mechanisms implement functions that help *prevent, detect, and respond to recovery from* security attacks.
  - Security functions are typically made available to users as a set of *security services* through APIs or integrated interfaces.
  - Cryptography underlies many security mechanisms.

Security Services

- *Authentication*: assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from
- *Non-repudiation*: offer of evidence that a party indeed is the sender or a receiver of certain information
- *Access control*: facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections
- *Monitor & response*: facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

Security Services

- *Security management*: facilities for coordinating users' service requirements and mechanism implementations throughout the enterprise network and across the Internet
  - Trust model
  - Trust communication protocol
  - Trust management infrastructure

Impacts of Attacks

- Theft of confidential information
- Unauthorized use of
  - Network bandwidth
  - Computing resource
- Spread of false information
- Disruption of legitimate services

All attacks can be related and are dangerous!

Security Attacks

- **Interruption:** (an attack on availability)
  - An asset of the system is destroyed or becomes unavailable or unusable – by an unauthorized party
- **Interception:** (an attack on confidentiality)
  - An unauthorized party gains access to an asset by observing the communication
- **Modification:** (an attack on integrity)
  - An unauthorized party not only gains access to but tampers with an asset – "Man in the middle"
- **Fabrication:** (an attack on authenticity)
  - An unauthorized party inserts counterfeit objects into the system

Security Attacks

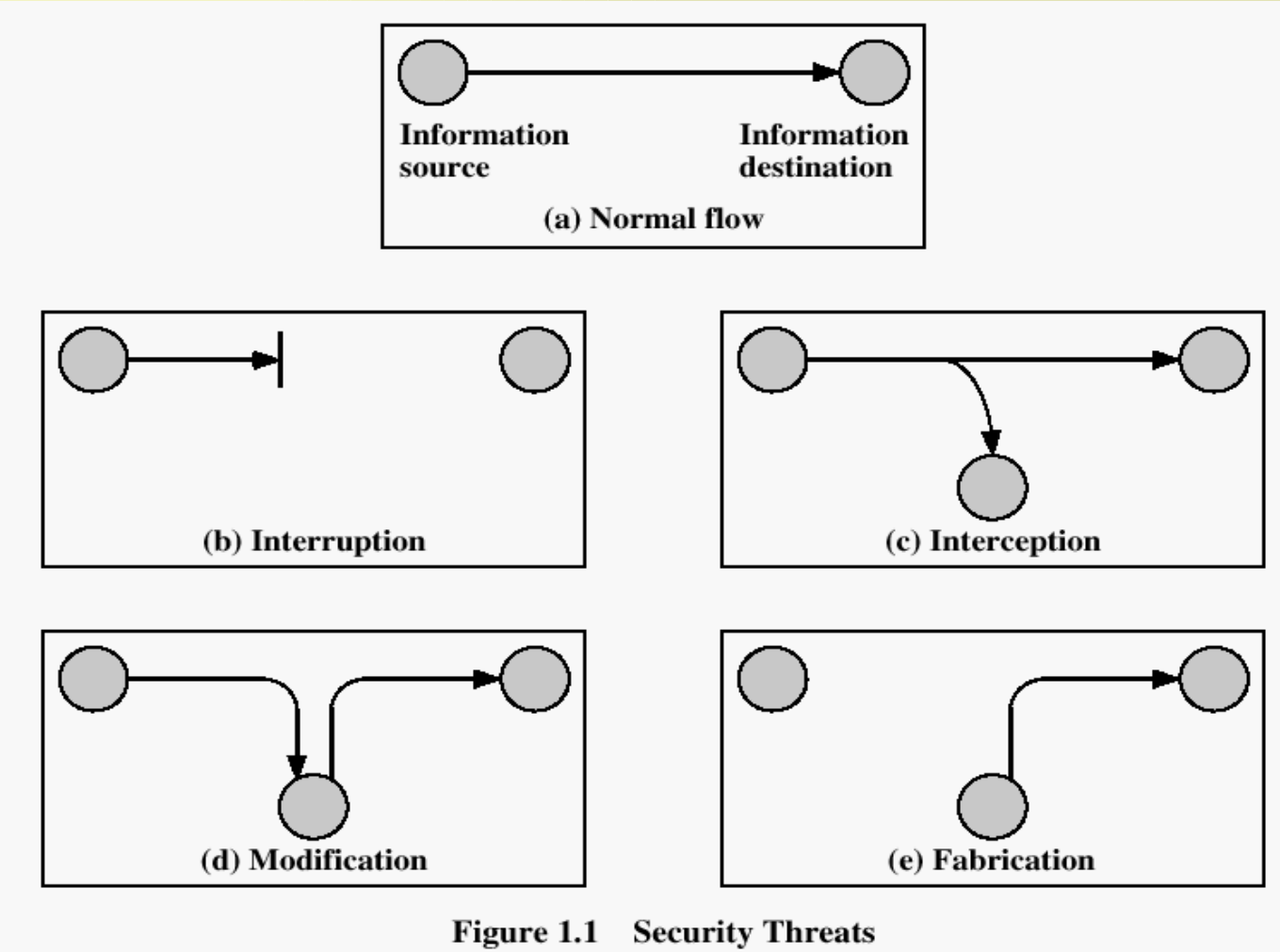
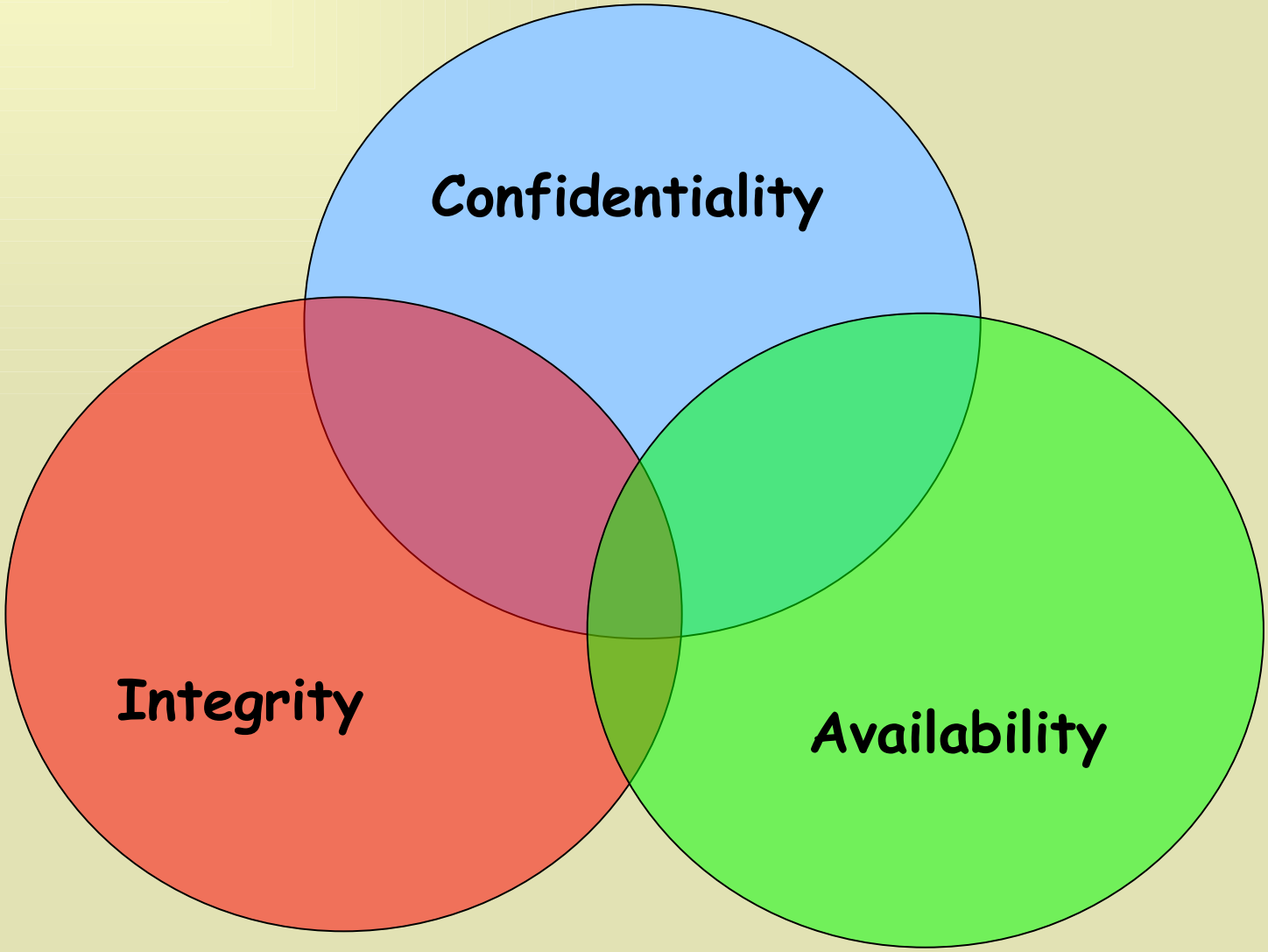


Figure 1.1 Security Threats

Security Goals



Threats

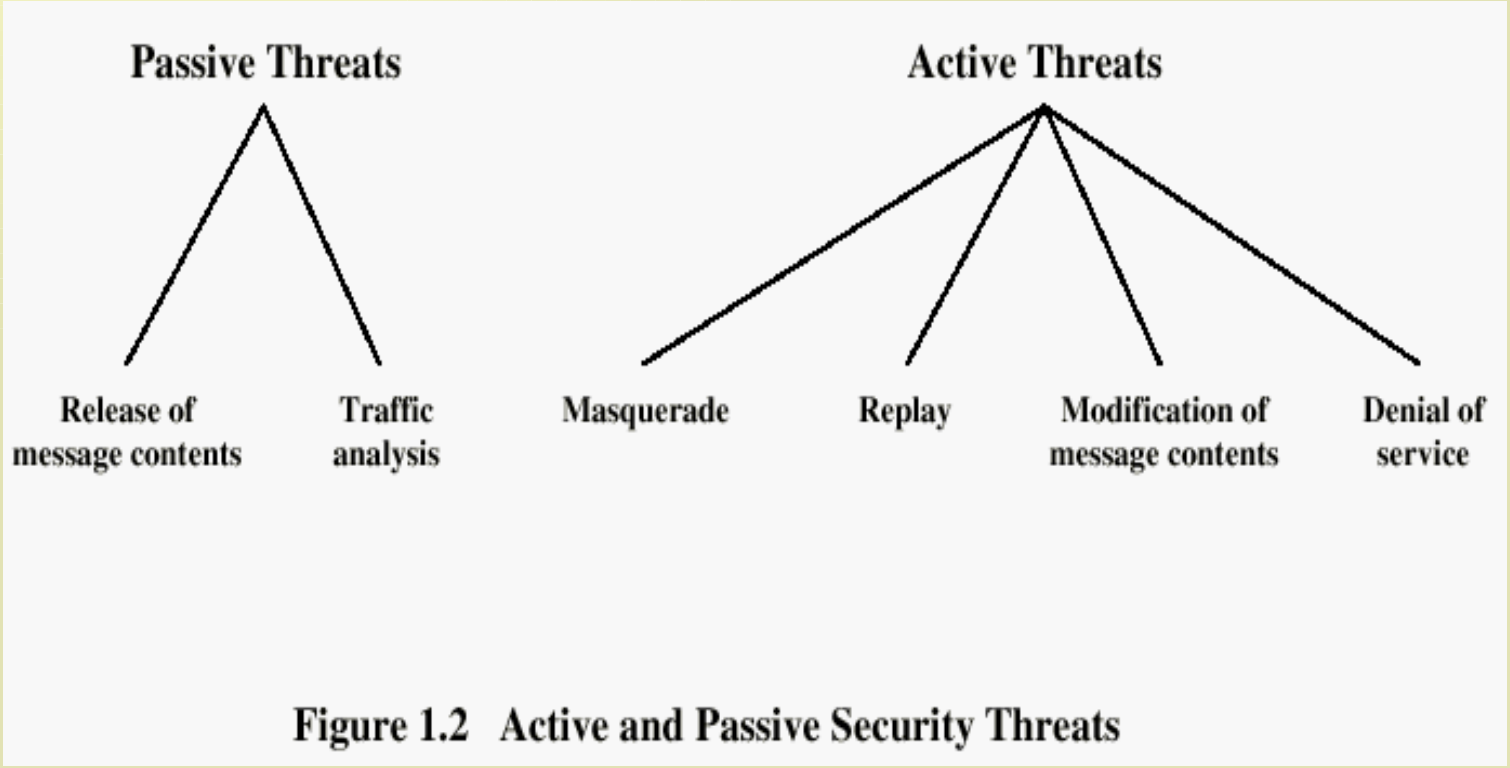


Figure 1.2 Active and Passive Security Threats

Passive Attacks

- Release of message contents
  - e.g. a telephone conversation, an e-mail message
    - Subject to interception
- Traffic Analysis
  - e.g. opponent could observe the frequency and length of messages being exchanged (even though the messages are encrypted)
    - can guess the nature of communication
- Very difficult to detect
- Emphasis is on prevention rather than detection

Active Attacks

- Masquerade
  - One entity pretending to be a different entity
    - Usually includes one of the other forms of attacks
- Replay
  - Passive capture of a data unit and its subsequent retransmission
- Modification of messages
  - Some portion of a legitimate message is altered, or that messages are delayed or reordered
- Denial of service
  - Prevents or inhibits the normal use or management of computing/communications facilities
- Difficult to prevent
- Emphasis is on detection and recovery rather than prevention

Security Services

- Confidentiality (privacy)
  - Protection of transmitted data from passive attacks
    - All user data or selected messages or selected portions of messages
  - Protection of traffic flow from analysis
- Authentication (who created or sent the data)
  - Assuring that a communication is authentic
    - Two entities are authentic
    - Connection is not interfered (no masquerading party)
- Non-repudiation (the order is final)
  - Receiver can prove that the message was in fact sent by the alleged sender
    - Vice-versa

Security Services (Cont'd)

- Access control (prevent misuse of resources)
  - By identification or authentication
    - So that access rights can be tailored to the individual
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

A Model for Network Security

- Two parties (principals)
  - Exchanging messages through a logical information channel
  - By doing a security-related transformation
  - Using a piece of secret information
- A Trusted Third Party
  - To help secure transmission
- Opponent
  - Trying to listen to or break the communication

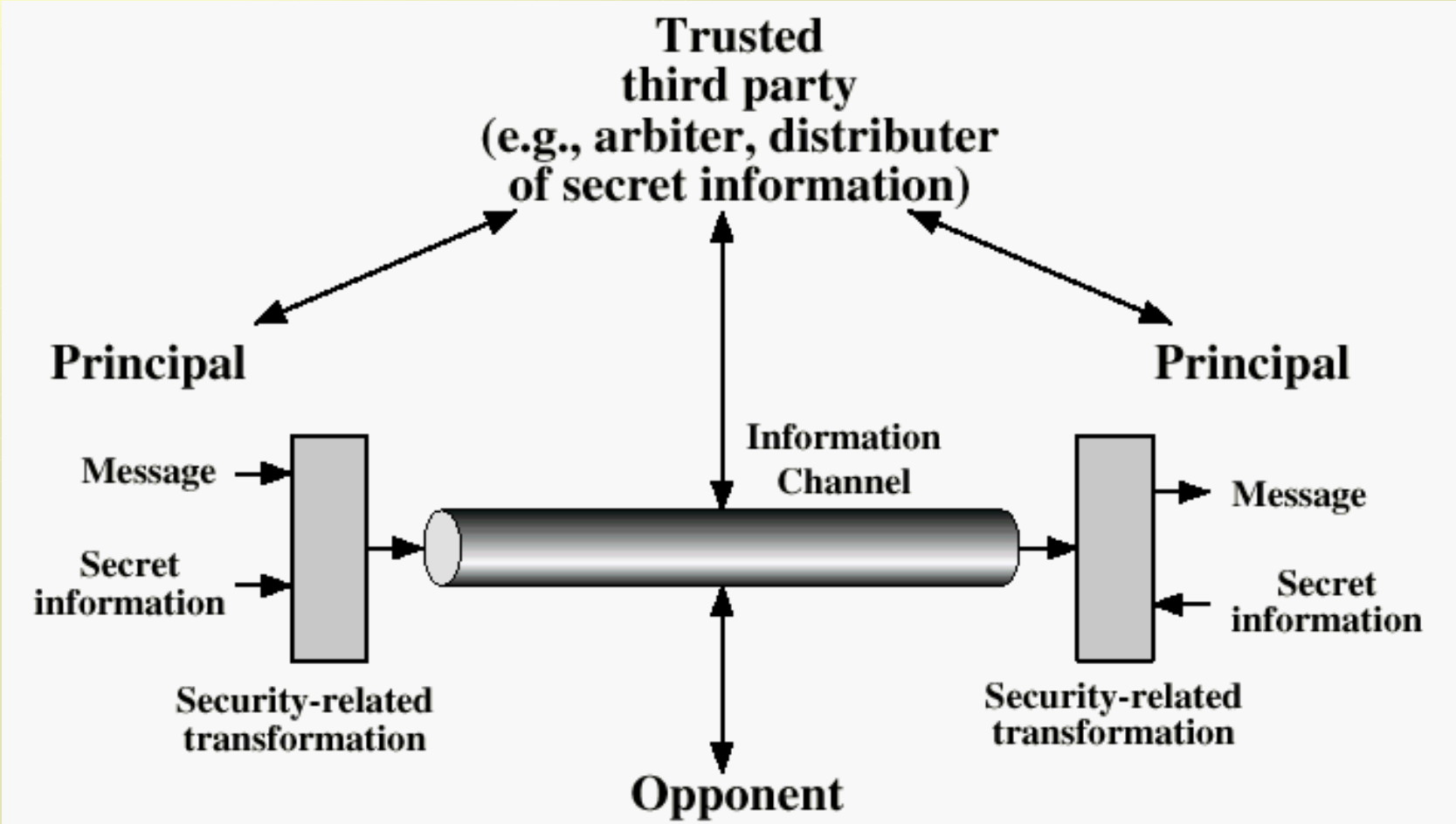


Figure 1.3 Model for Network Security

Security Services

- Four Tasks:
  - Design an algorithm for performing the security-related transformation
  - Generate the secret information
  - Develop methods for the distribution and sharing of the secret information
  - Specify a protocol to be used by the two principals

Network Access Security Model

- Protecting an information system from unwanted access
  - Hackers, intruders, criminals
  - Software/Hardware logic exploiting vulnerabilities
  - Two kinds of threats (software):
    - Information access threats
    - Service threats
      - e.g. Viruses, worms, Trojans
- Security mechanisms:
  - A gatekeeper function
  - Variety of internal controls
    - Monitor activity, analyze stored information

Network Access Security Model

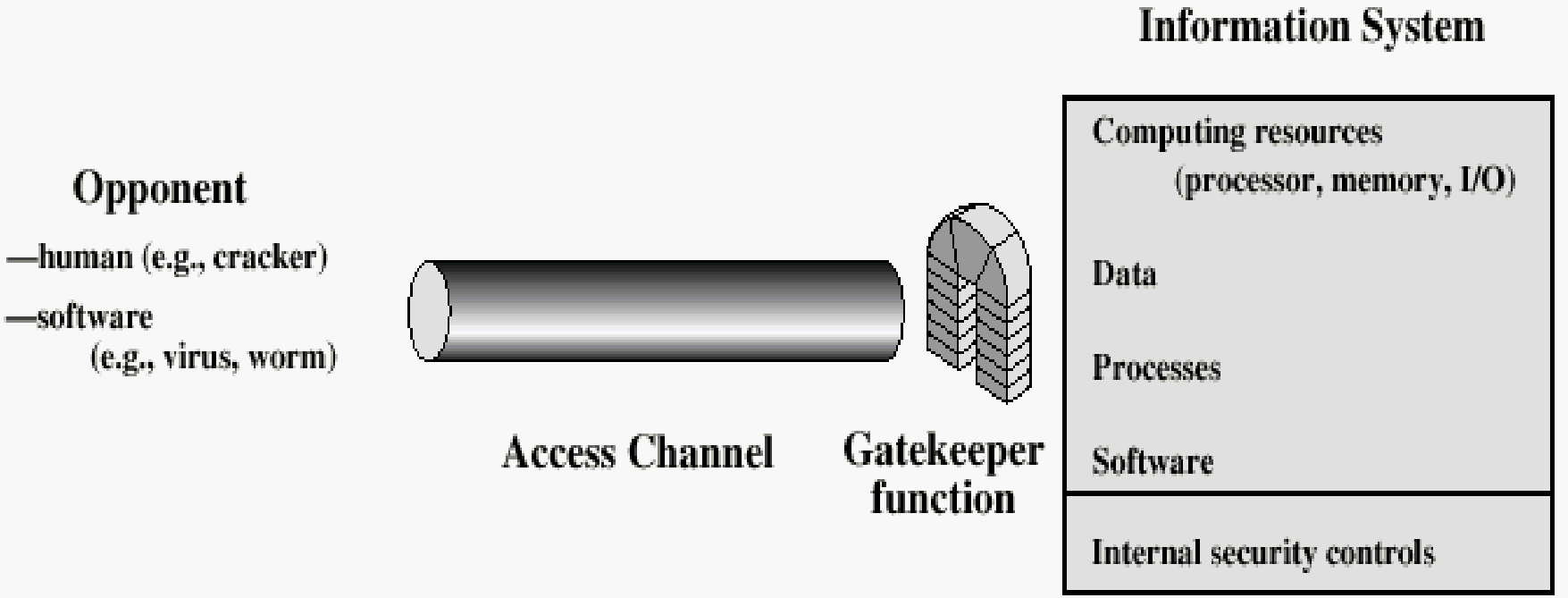


Figure 1.4 Network Access Security Model

Methods of Defense

- Encryption (secure channels)
- Software Controls (access limitations in a data base, in operating system protect each user from other users)
- Hardware Controls (smartcard)
- Policies & Procedures (frequent changes of passwords)
- Physical Controls

The Art of War - Stratagem

- Some Rules of War
  - Know when to fight and when not to fight. (1)
  - Know how to handle both superior and inferior forces. (2)
  - Animate your army by the same spirit throughout all its ranks. (3)
  - *Prepare yourself and wait to take the enemy unprepared. (4)*
  - Create military capacity that is not interfered with by the sovereign. (5)
- Hence the saying:
  - If you know the enemy and know yourself, you need not fear the result of a hundred battles.
  - If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
  - *If you know neither the enemy nor yourself, you will succumb in every battle.*

Challenging Questions

Commander's Attack Triage Questions

- Am I under attack ?
- What is the nature of the attack ?
  - Class, Mechanism, From where ?
- What is mission impact ?
  - Urgency, Damage assessment & control, Initial response
- When did attack start ?
  - Follow-on damage assessment, What have I done wrong ?
- Who is attacking
  - What are they trying to do, What is their next step ?
- What can I do about it ?
  - Course of action analysis, Collateral damage risk, Reversibility of action
- Long term solution

Currently, we are relatively ***Blind*** and ***Powerless*** ...

Intelligence - knowing the enemy… and yourself

Kinetic (Conventional)

- Know adversary position in land, sea and air
- Know adversary capabilities - weapons, forces, projection
- Keep element of surprise - stealth, deception
- Know your own troops position and status
- Know warning signs of really bad events (nuke launch)
- Be able to measure effect of your actions - photos

Cyberspace

- Know where malicious code is and adversary entry points
- Know adversary capabilities - toolkits, effects on our systems
- Occlude adversary on intrusion detection, policy, recovery
- Know the configuration of own defenses & dependencies
- Know the symptoms of a large-scale cyber-attack
- Be able to measure effect of policy & configuration changes