*The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.*

**—*The Art of War,* Sun Tzu**

# Information and Network Security

**USMACS503**

- Cryptography and Network Security: Principles and Practice 5th Edition, William Stallings, Pearson, 2010.
- Cryptography and Network Security, Atul Kahate, Tata McGraw-Hill, 2013.

# Unit 1

- **Introduction: Security Trends, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms**
- **Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques Steganography**
- **Block Cipher Principles, The Data Encryption Standard, The Strength of DES, AES (round details not expected), Multiple Encryption and Triple DES, Block Cipher Modes of Operation, Stream Ciphers**
- **Public-Key Cryptography and RSA: Principles of Public-Key**
- **Cryptosystems, The RSA Algorithm, Key Management: Public-Key Cryptosystems, Key Management, Diffie-Hellman Key Exchange**

# Definitions

- **Computer Security** - generic name for the  collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

# What security is about in general?

- Security is about protection of assets
  - D. Gollmann, Computer Security, Wiley
- Prevention
  - take measures that prevent your assets from being damaged (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction
  - take measures so that you can recover your assets

# Real world example

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard
- Detection
  - missing items, burglar alarms, closed circuit TV
- Reaction
  - attack on burglar (not recommended ☺), call the police, replace stolen items, make an insurance claim

# Internet shopping example

- Prevention
  - encrypt your order and card number, enforce merchants to do some extra checks, using PIN even for Internet transactions, don’t send card number via Internet
- Detection
  - an unauthorized transaction appears on your credit card statement
- Reaction
  - complain, dispute, ask for a new card number, sue (if you can find of course ☺)
  - Or, pay and forget (a glass of cold water) ☺

# Information security in past & present

- Traditional Information Security
  - keep the cabinets locked
  - put them in a secure room
  - human guards
  - electronic surveillance systems
  - in general: physical and administrative mechanisms
- Modern World
  - Data are in computers
  - Computers are interconnected

**Information and Network Security**

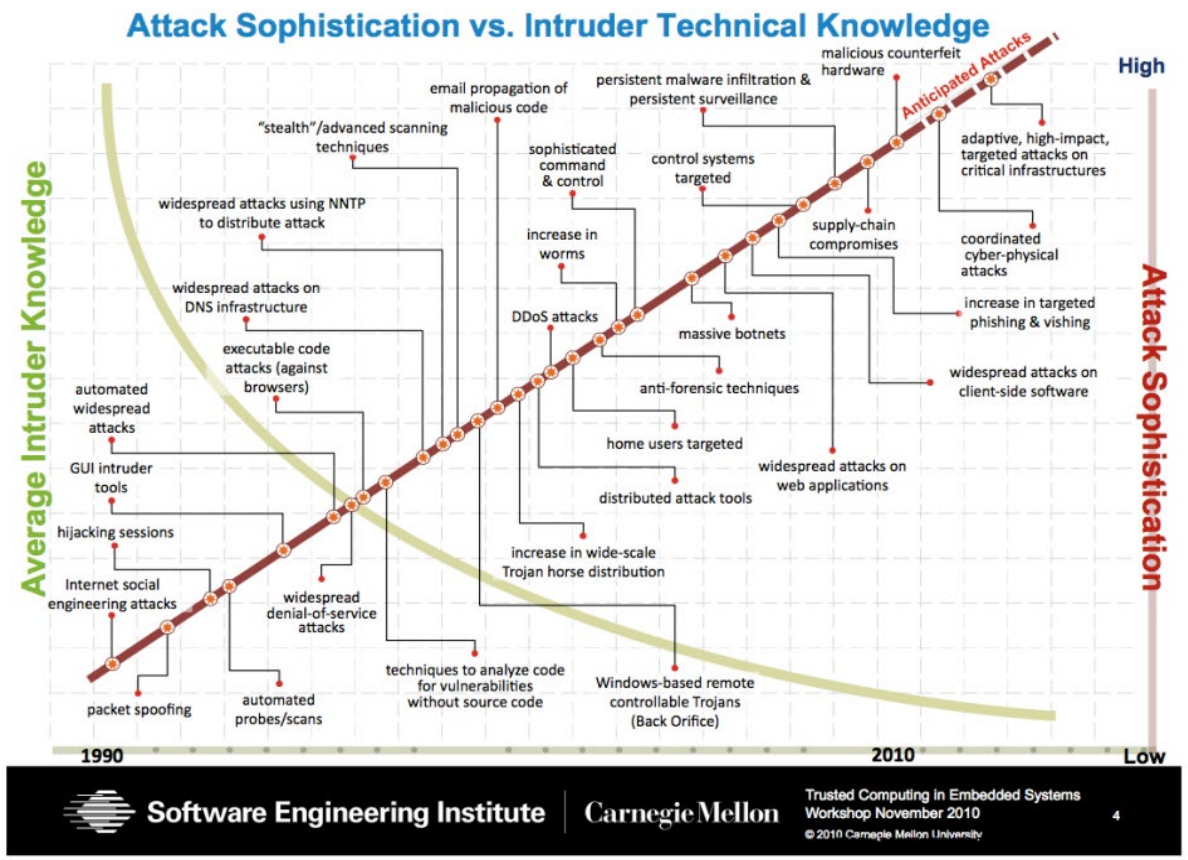
# Terminology

- Computer Security
  - 2 main focuses: Information and Computer itself
  - tools and mechanisms to protect data in a computer (actually an automated information system), even if the computers/system are connected to a network
  - tools and mechanisms to protect the information system itself (hardware, software, firmware, *ware ☺)
- Against?
  - against hackers (intrusion)
  - against viruses
  - against denial of service attacks
  - etc. (all types of malicious behavior)

# Terminology

- Network and Internet Security
  - measures to prevent, detect, and correct security violations that involve the transmission of information in a network or interconnected networks

# Security Trends




## Top Cybersecurity Trends in 2023

| Responsive Ecosystems | Restructuring Approaches | Rebalancing Practices |
|---|---|---|
| • Threat Exposure Management<br>• Identity Fabric Immunity<br>• Cybersecurity Validation | • Cybersecurity Platform Consolidation<br>• Security Operating Model Transformation<br>• Composable Security | • Human-Centric Security Design<br>• Enhancing People Management<br>• Increasing Board Oversight |

Sustainable Balanced Cybersecurity Programs

Source: Gartner


Gartner

# Security objectives

## Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

## Integrity

- Data integrity
  - Assures that information changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

## Availability

- Assures that systems work promptly and service is not denied to authorized users

# OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements

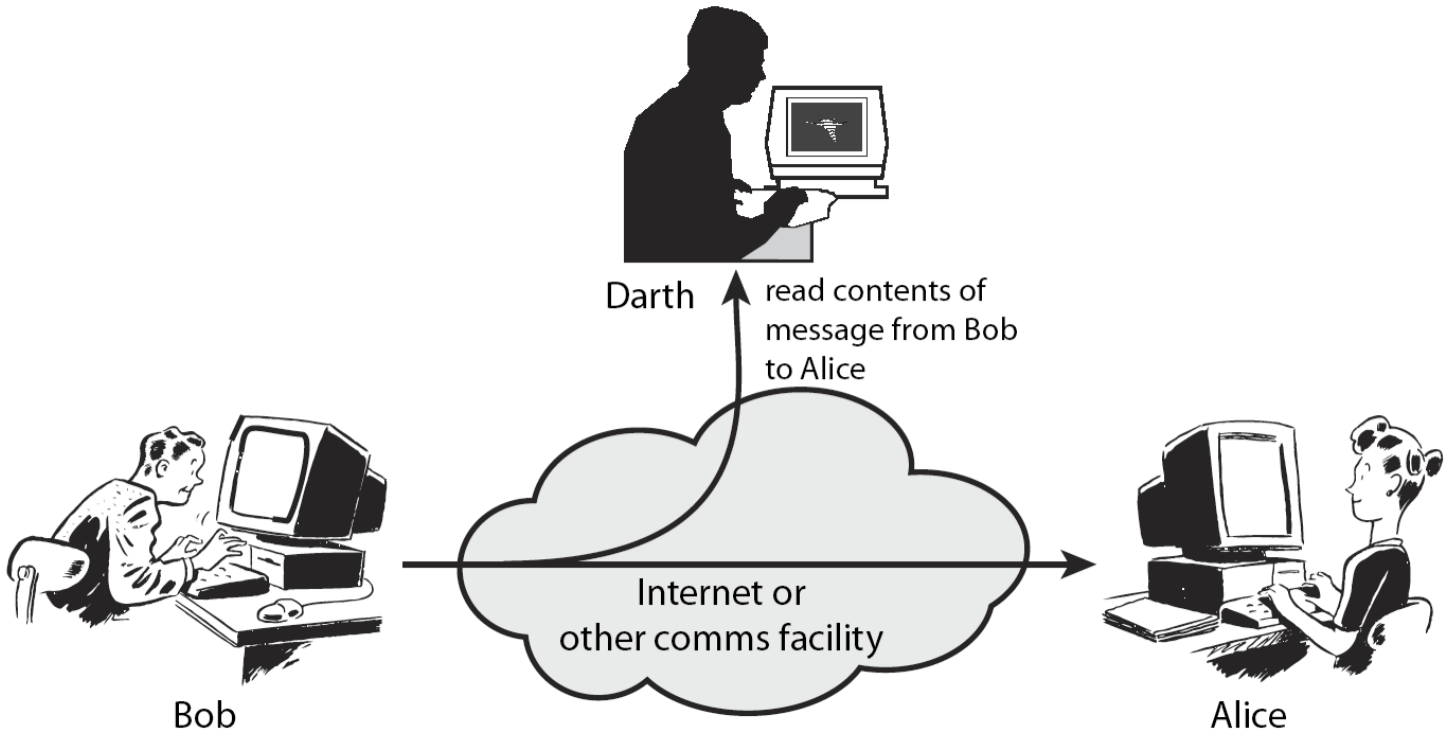
# Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**

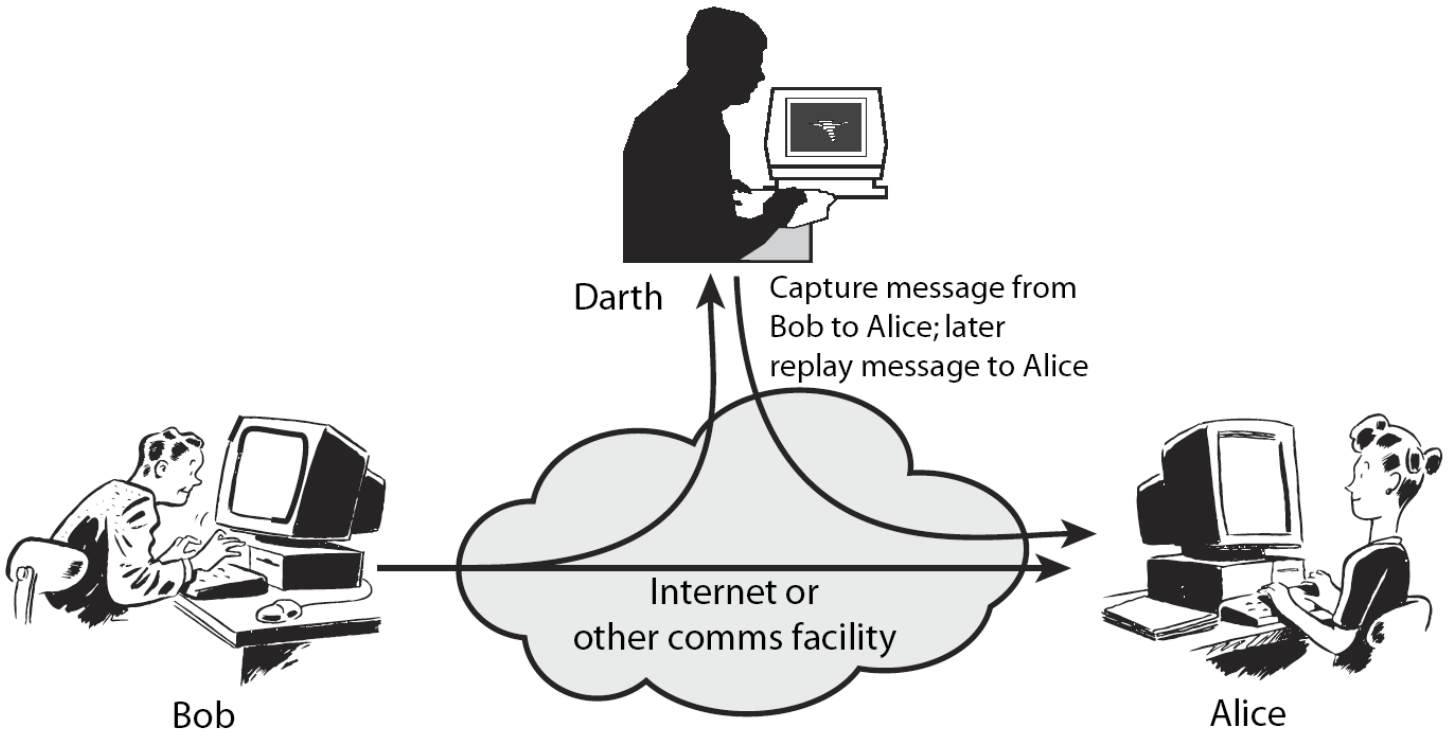
# Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on  information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- can focus of generic types of attacks
  - passive
  - active

# Passive Attacks

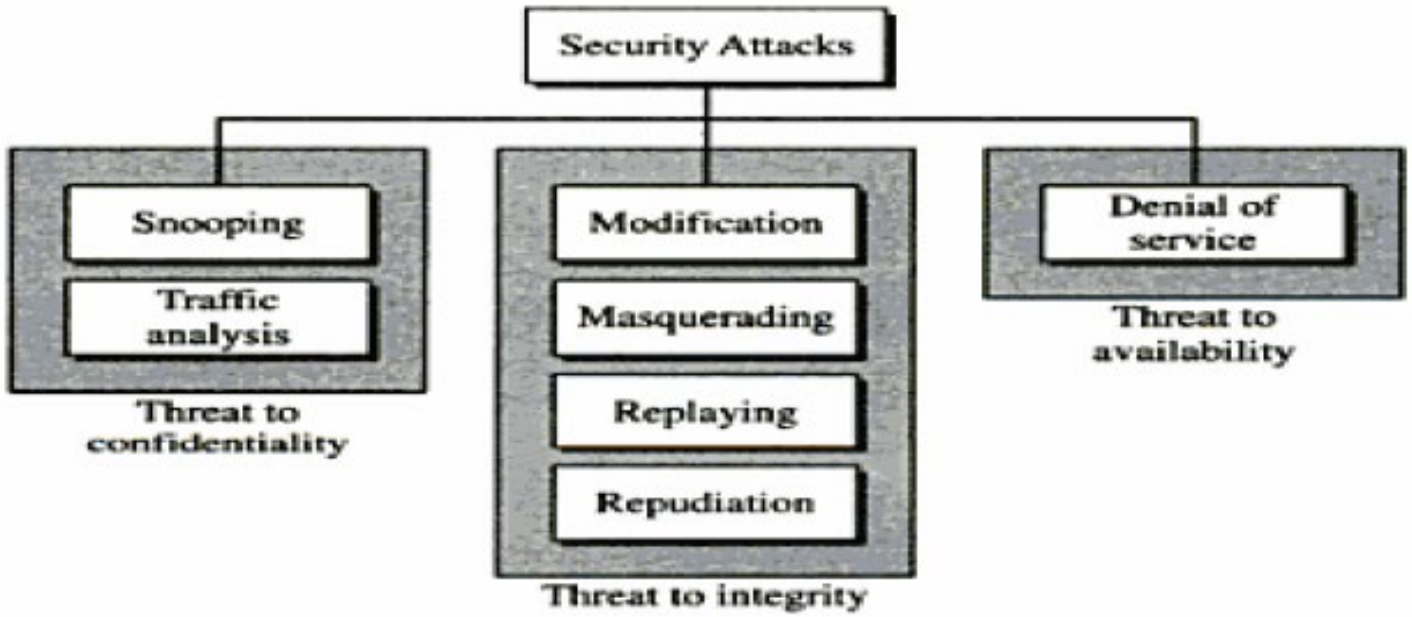


# Active Attacks



# ATTACKS

*Taxonomy of attacks with relation to security goals*



# ATTACKS

## Attacks threatening Confidentiality

- **Snooping:**

  unauthorized access/interception of data

  for prevention data is made non intelligent by using encipherment techniques

- **Traffic Analysis:**

  by monitoring online traffic and guessing imps

## Attacks threatening Integrity

- **Modification**

  modifies the information for benefit/ delete/delays

- **Masquedrading(spoofing)**

  attacker impersonates somebody else

- **Replaying**

  obtains a copy of a message sent by a user and later tries to replay it

- **Repudiation**

  performed by one of the two parties in communication

# ATTACKS

## Attacks threatening Availablity

- **Denial of service:**

  may slow down or totally interrupt the service

  bogus requests for crashing the server/ delete server's response/intercepting the client's request for overloading the server

- **Traffic Analysis:**

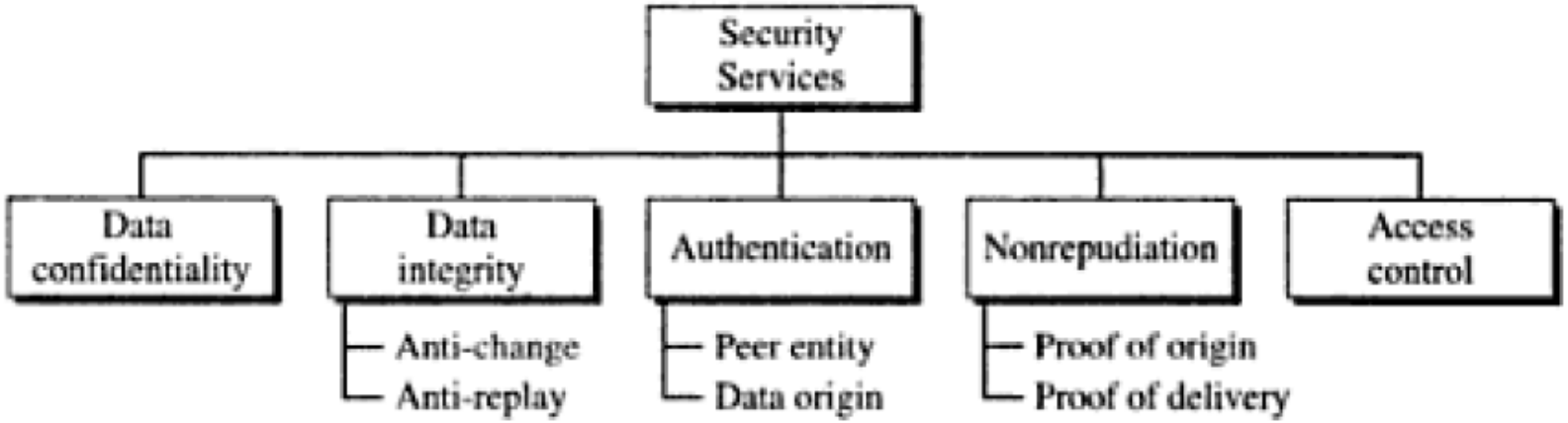
  by monitoring online traffic and guessing imps

**Table 1.1** *Categorization of passive and active attacks*

| *Attacks* | *Passive/Active* | *Threatening* |
|---|---|---|
| Snooping<br>Traffic analysis | Passive | Confidentiality |
| Modification<br>Masquerading<br>Replaying<br>Repudiation | Active | Integrity |
| Denial of service | Active | Availability |

# Security services

**Figure 3.3** *Security services*



# Security mechanisms

# Security mechanisms

- **Encipherment**

  hiding/covering data,cryptography & stegnagraphy

- **Data Integrity**

  appends to data a short checkvalue

- **Digital Signature**

  electronically signs and verified

- **Authentication exchanged**

  exchange messages to prove identity

- **Traffic padding**

  inserting bogus data to divert traffic analysis

# Security mechanisms

- **Routing Control**

  selecting and continuously changing routes

- **Notarization**

  selecting a third party to control the communication (to repudiation)

- **Access Control**

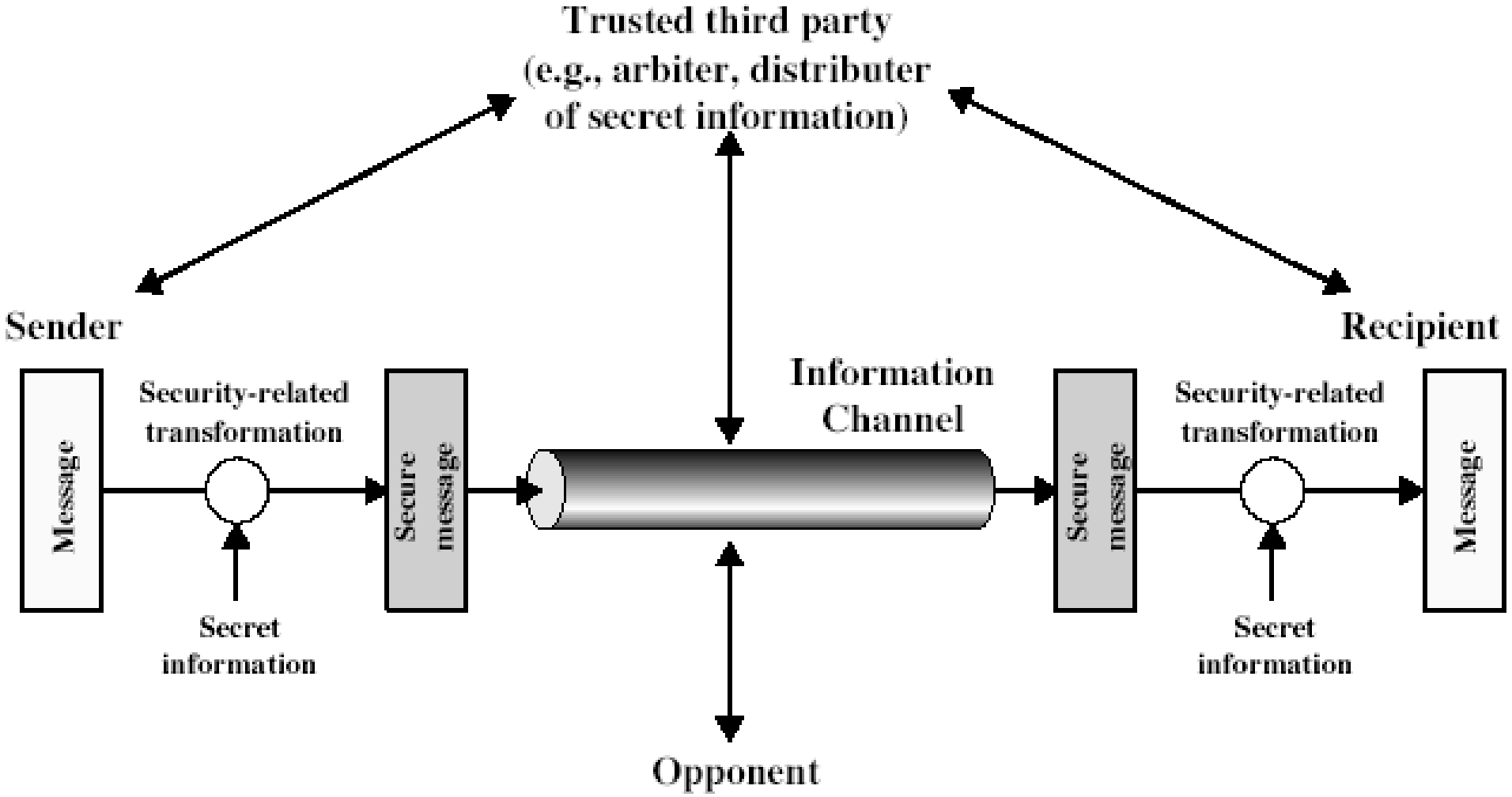
  uses methods to prove that a user has access right to the data

# Services vs Mechanism

**Table 1.2** *Relation between security services and security mechanisms*

| *Security Service* | *Security Mechanism* |
|---|---|
| Data confidentiality | Encipherment and routing control |
| Data integrity | Encipherment, digital signature, data integrity |
| Authentication | Encipherment, digital signature, authentication exchanges |
| Nonrepudiation | Digital signature, data integrity, and notarization |
| Access control | Access control mechanism |

# Model for Network Security



# Model for Network Security

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

# Model for Network Access Security