

Computer Systems Security

Dr. Ayman Abdel-Hamid

College of Computing and Information Technology

Arab Academy for Science & Technology and
Maritime Transport

Chapter 1

Introduction

Outline

- Attacks, services and mechanisms
- Security attacks
- Security services
- Security mechanisms
- A model for network security, and network access security

Background

- Information Security requirements have changed in recent times
- traditionally provided by *physical* and *administrative* mechanisms
- computer use requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission

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

Possible Security Violations

- A transmits a file to B. C (not authorized to read the file) monitors transmissions and captures a copy
- D transmits a message to computer E, instructing E to update an authorization file. User F intercepts the message, alters its contents to add or delete entries and forward to E which accepts the message as being from D
- User F constructs its own message and transmits to E as if coming from D
- Denying sending a message

Services, Mechanisms, Attacks

- Need systematic way to define security requirements
- Consider three aspects of information security:
 - *security attack*
 - action that compromises the security of information owned by an organization
 - *security mechanism*
 - Designed to detect, prevent, or recover from a security attack
 - *security service*
 - Enhances the security of data processing systems and information transfers of an organization
- Consider in reverse order

Security Service

- enhances the security of the data processing systems and the information transfers of an organization
- intended to counter *security attacks*
- make use of one or more *security mechanisms* to provide the service
- replicate functions normally associated with physical documents
 - e.g., have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed (problems with electronic documents)

Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: *cryptographic techniques*

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
- have a wide range of attacks
- can focus of generic types of attacks
- note: often *threat & attack* mean same

OSI Security Architecture

- ITU-T (International Telecommunication Union, Telecommunication Standardization Sector) **X.800** *Security Architecture for OSI*
- defines a systematic way of defining and providing security requirements

Security Service

- **X.800 defines it as:** *a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers*
- **RFC 2828 defines it as:** *a processing or communication service provided by a system to give a specific kind of protection to system resources*
- X.800 defines it in 5 major categories

Security Services (X.800) ^{1/7}

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received are exactly as sent by an authorized entity
- **Nonrepudiation** - protection against denial by one of the parties in a communication
- What about **Availability**?

Security Services (X.800) ^{2/7}

- **Authentication** - *assurance that the communicating entity is the one claimed*
 - Peer Entity Authentication
 - ✓ Confidence in the identities of entities connected (corroboration of identity of peer entity in an association)
 - ✓ Used at establishment of connection, and during data transfer phase
 - Data-Origin Authentication
 - ✓ Source of received data is as claimed

Security Services (X.800) ^{3/7}

- **Access Control** - *prevention of the unauthorized use of a resource*
 - Who can have access to a resource?
 - Under what conditions?
 - If you are granted access, what are you allowed to do?

Security Services (X.800) ^{4/7}

- **Data Confidentiality** –*protection of data from unauthorized disclosure*
 - Connection Confidentiality
 - ✓ All user data is protected
 - Connectionless Confidentiality
 - ✓ All user data in a single data block is protected
 - Selective-Field Confidentiality
 - Specific fields are protected
 - Traffic-flow Confidentiality
 - ✓ Protecting traffic flow from analysis

Security Services (X.800) 5/7

- **Data Integrity** - *assurance that data received are exactly as sent by an authorized entity (no modification, insertion, deletion, or replay)*
 - Connection Integrity with Recovery
 - Connection Integrity without Recovery
 - Selective-field Connection Integrity
 - Connectionless Integrity
 - Selective-Field Connectionless Integrity

Security Services (X.800) 6/7

- **Nonrepudiation** - *protection against denial by one of the parties in a communication*
 - Nonrepudiation, Origin
 - Nonrepudiation, Receiver

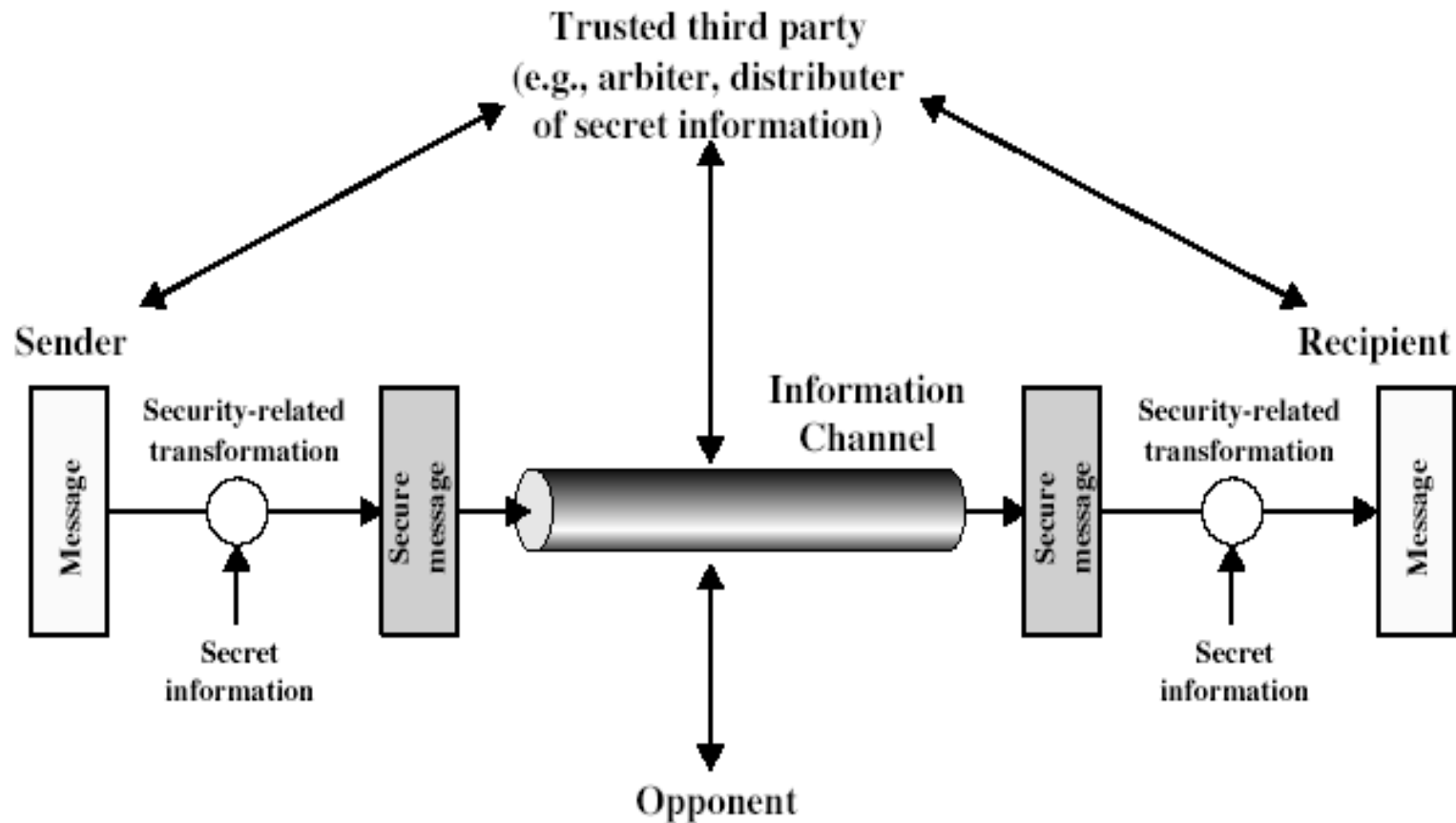
Security Mechanisms (X.800) ^{7/7}

- specific security mechanisms:
 - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
 - trusted functionality, security labels, event detection, security audit trails, security recovery
- Others not included here?

Classify Security Attacks as

- **passive attacks** - *eavesdropping on, or monitoring of, transmissions to:*
 - obtain message contents, or
 - monitor traffic flows
 - Difficult to detect since no alteration of data
- **active attacks** – *modification of data stream, or creation of a false stream*
 - masquerade of one entity as some other
 - replay previous messages
 - modify messages in transit
 - denial of service

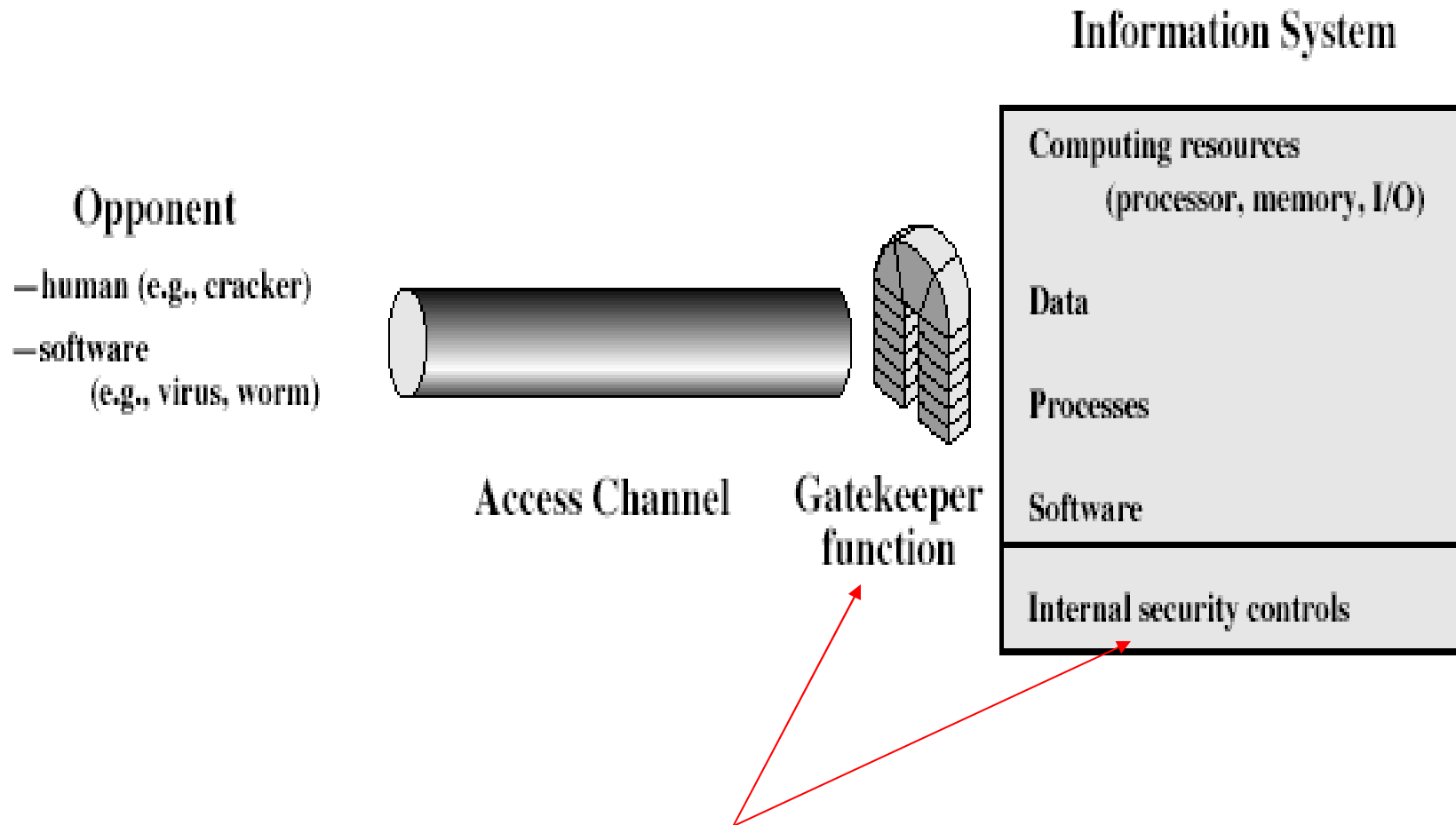
Model for Network Security ^{1/2}



Model for Network Security ^{2/2}

- 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 principals to use the transformation and secret information for a security service

Network Access Security Model ^{1/2}



Network Access Security Model ^{2/2}

- 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

Further Reading

- RFC 2828 (Informational), *Internet Security Glossary*, available at <http://www.ietf.org>