Security Service & Security Mechanism

Erukala Suresh Babu

Digitally signed by Erukala Suresh Babu
DN: cn=Erukala Suresh Babu, o=NITW, ou=CSE, email=esbabu@nitw.ac.in, c=IN
Date: 2019.08.27 06:41:48 +05'30'

Dr. E. Suresh Babu

Assistant Professor

Department of CSE

National Institute of Technology, Warangal

Outline

- Security Service
- Security Mechanism
  - ✓ Specific Security Mechanisms
- Network Security Model
- Model for Network Access Security

Security Services

Definition of Security Services

- **Security Services** are defined from **Relevant standards**

X.800 defines a **Security service** provided by a **protocol layer** of **communicating open systems**, which ensures **adequate security** of the **systems** or of **data transfers**

Security Services Defined by X.800

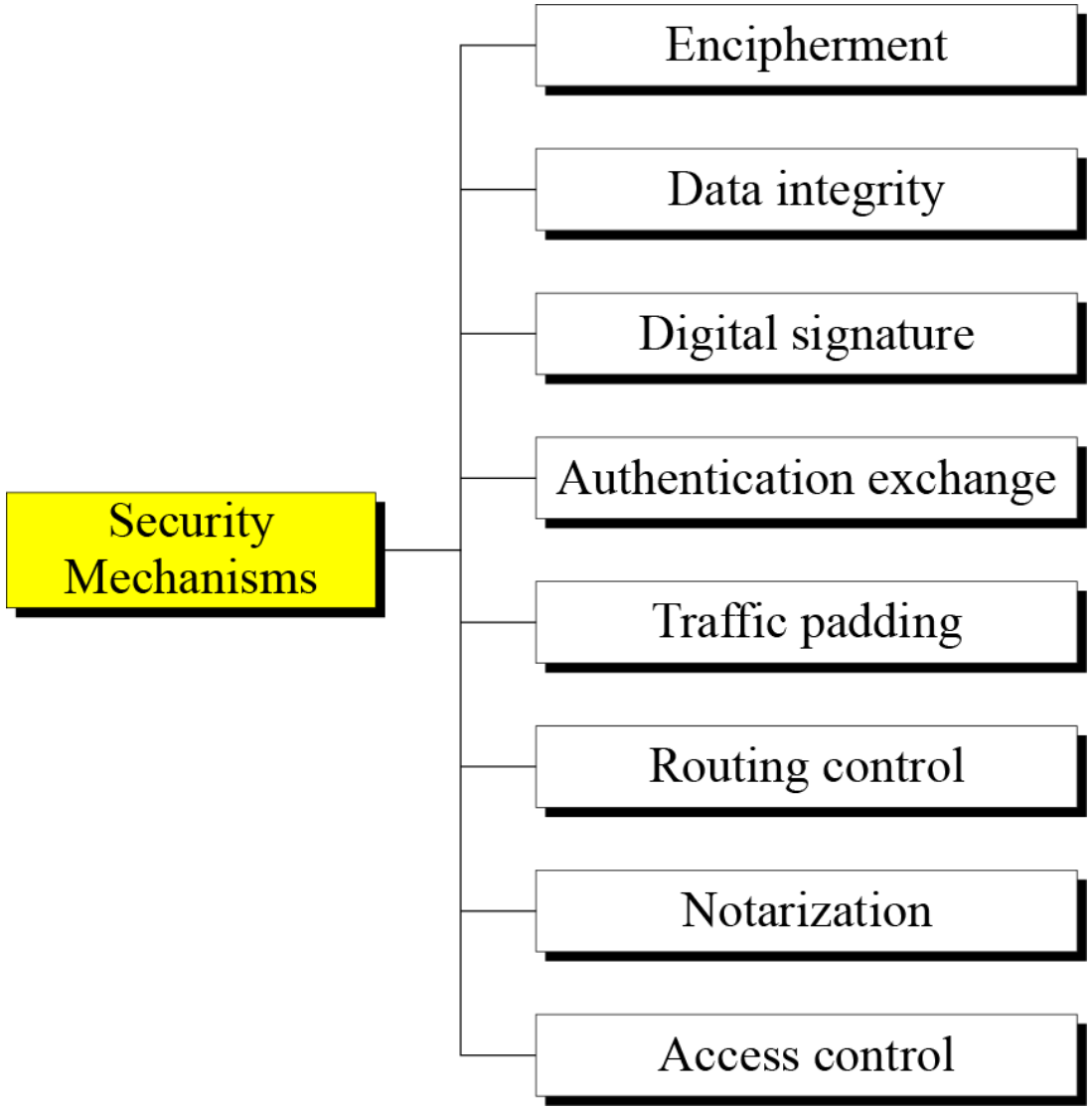
- X.800 Security Architecture for OSI defines
  - ✓ A systematic approach for security services.
- X.800 divides the security services into five categories.
  - ✓ **Authentication**
  - ✓ **Access Control**
  - ✓ **Data Confidentiality**
  - ✓ **Data Integrity**
  - ✓ **Non-Repudiation**

Security Mechanism

Security Mechanism

- A Security Mechanism is any process that is designed to detect, prevent, or recover from a security attack.
  - ✓ Examples of mechanisms are Encryption Algorithms, Digital Signatures, and Authentication Protocols.
- Security Mechanism which are the specific means of implementing one or more security services.

Security Mechanism



Security Mechanisms (X.800)

Specific Security Mechanisms

Encipherment

- The use of **mathematical algorithms** to **transform data** into a form that is not readily intelligible.
- The **transformation and subsequent recovery** of the data depend on an algorithm and **zero or more encryption keys.**

Digital Signature

- Data appended to a **cryptographic transformation** of, a data unit that allows a recipient of the data unit to prove the source and **integrity of the data unit** and **protect against forgery** (e.g., by the recipient).

Authentication Exchange

- A mechanism intended to **ensure the identity of an entity** by means of information exchange..

Traffic Padding

- The **insertion of bits into gaps** in a **data stream** to **frustrate traffic analysis attempts.**

Routing Control

- Enables selection of particular physically **secure routes for certain data** and **allows routing changes**, especially when a breach of security is suspected.

Notarization

- The use of a trusted third party to assure certain properties of a data exchange.

Relationship Between Security Services And Mechanisms

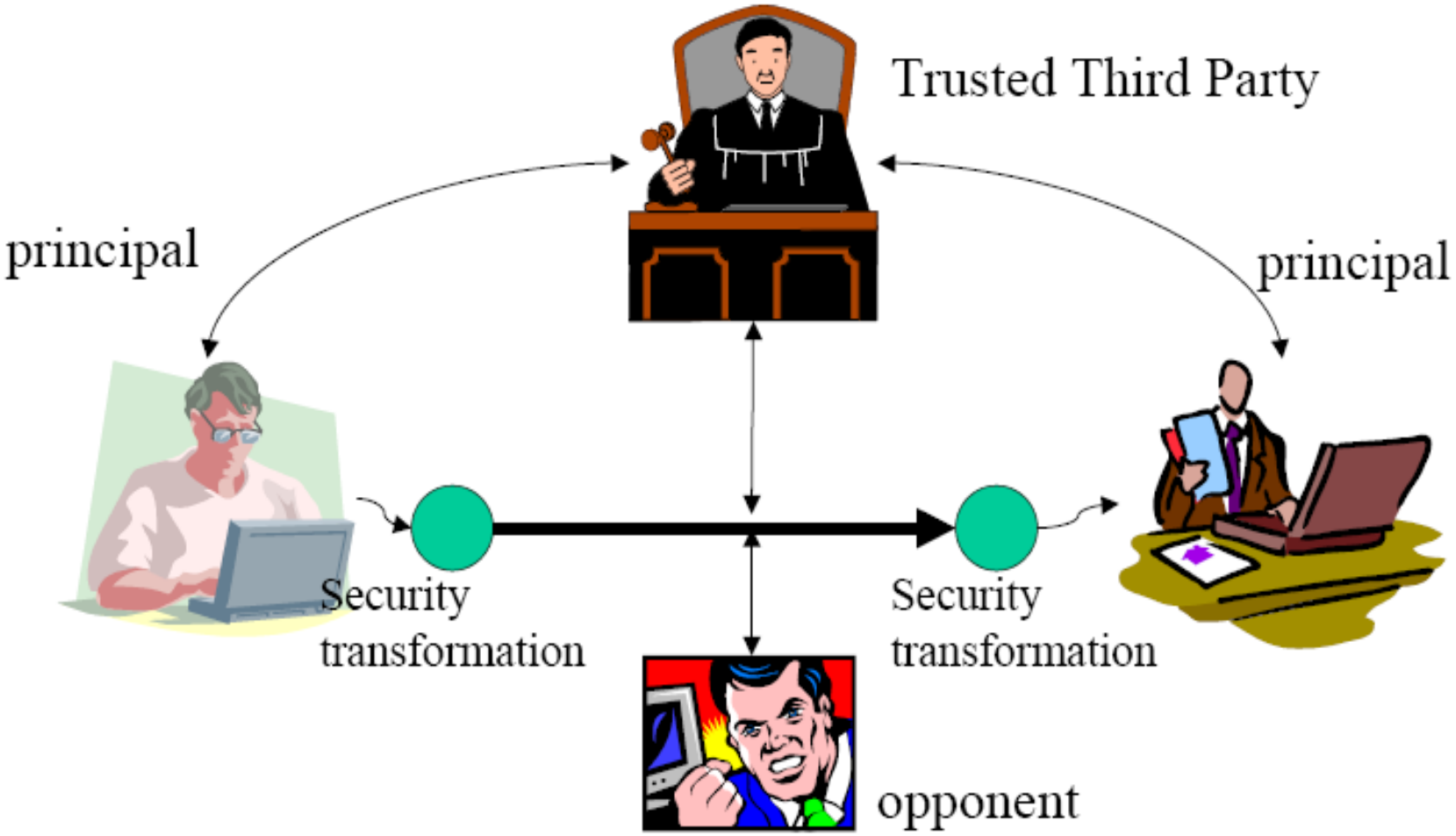
Security Service	Supporting Security Mechanisms
Authentication	Encipherment, Digital Signature, Authentication Exchange
Access Control	Access Control
Confidentiality	Encipherment, Routing Control
Data Integrity	Encipherment, Digital Signature, Data Integrity
Nonrepudiation	Digital Signature, Data Integrity, Notarization
Availability	Data Integrity, Authentication Exchange

Observation

- No single mechanism that will support all services required
- One particular element underlies many of the security mechanisms in use
  - ✓ **CRYPTOGRAPHIC TECHNIQUES**

Network Security Model

Network Security Model

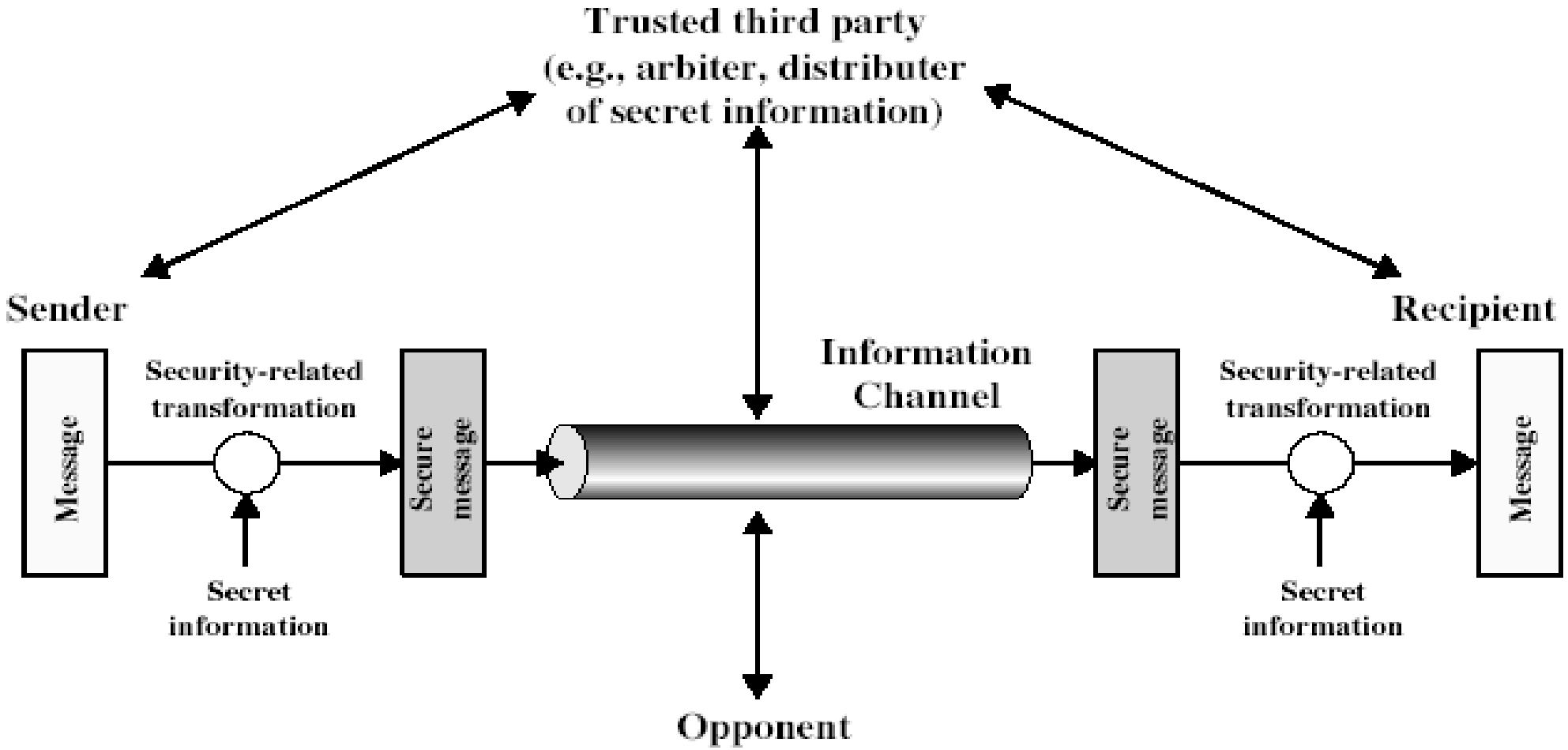


Network Security Model

- There are four basic tasks in designing a particular security service:

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

Network Security Model



Cryptography Basics

Thank U