Introduction

19CSE311 Computer Security

Jevitha KP

Department of CSE

Introduction

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

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

Definitions

- Cryptography
  - Cryptography, a word with Greek origins, means “secret writing.”
  - Refer to the science and art of transforming messages to make them secure and immune to attacks.
  - Cryptography referred only to the encryption and decryption of messages using secret keys,
  - Categories :
    - symmetric-key encipherment,
    - asymmetric-key encipherment and
    - hashing.

Definitions

- Steganography
  - Origin in Greek, means “covered writing,” in contrast with cryptography, which means “secret writing.”
  - Cryptography means concealing the contents of a message by enciphering;
  - Steganography means concealing the message itself by covering it with something else

Definitions

- Cryptanalysis
  - **Study of methods for obtaining the meaning of encrypted information, without access to the secret information that is typically required to do so**.
  - Involves knowing how the system works and finding a secret key.
  - Cryptanalysis is also referred to as codebreaking or cracking the code

Services, Mechanisms, Attacks

- need systematic way to define requirements
- consider three aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- consider in reverse order

Security Service

- is something that 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
  - eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

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**
- hence our focus on this area

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 X.800 Security Architecture for OSI
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Security Services

- 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)

- **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 is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

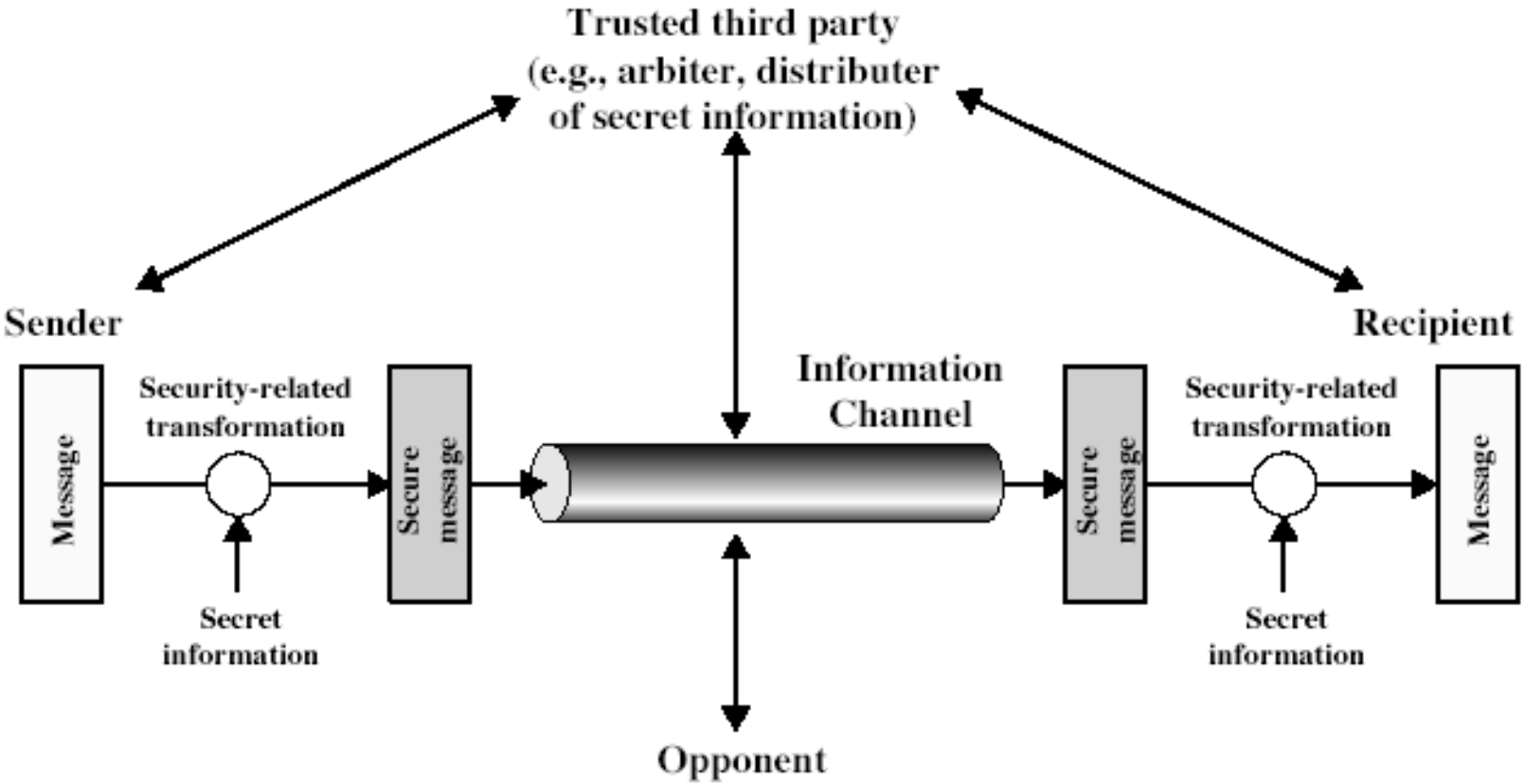
Security Mechanisms (X.800)

- 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

Classify Security Attacks as

- **passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

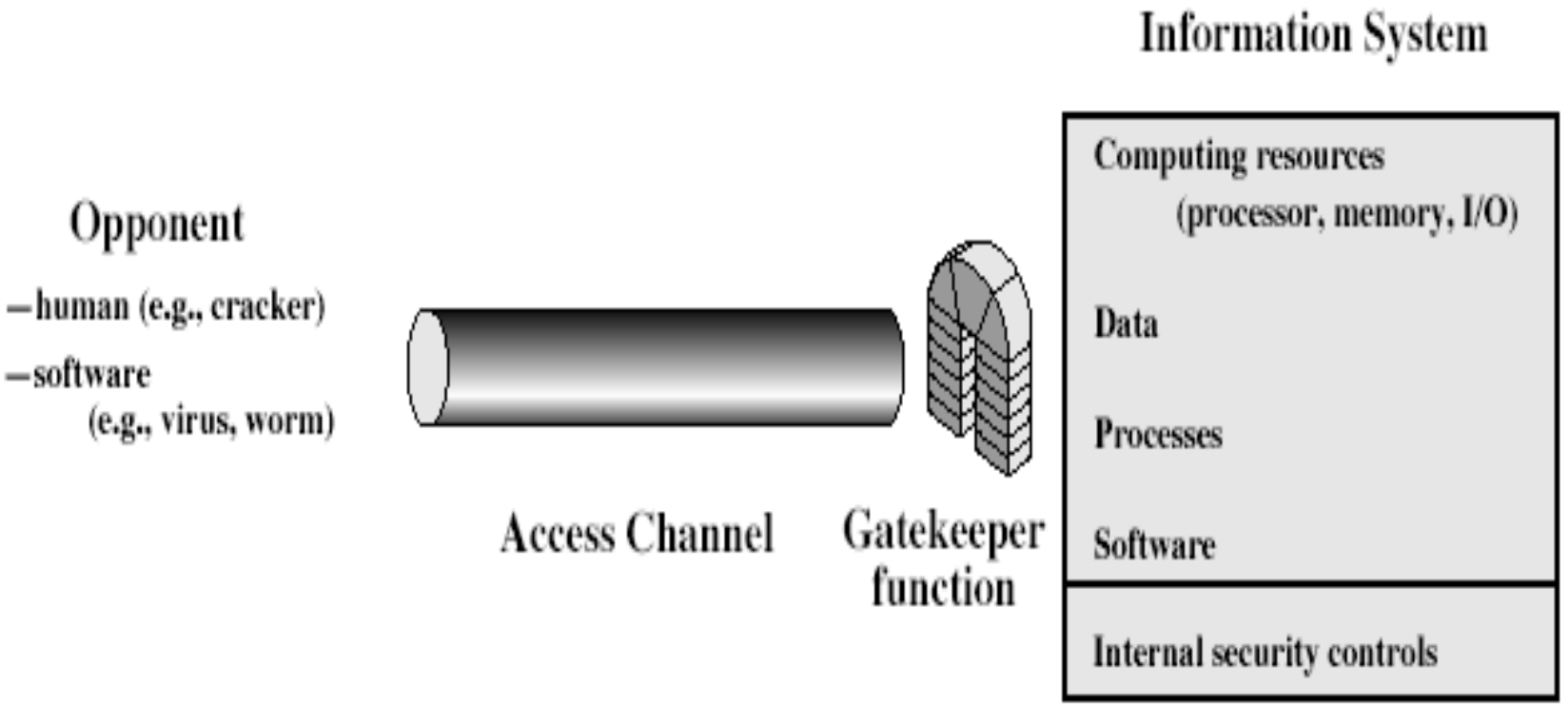
Model for Network Security



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

Model for Network Access 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

Summary

- have considered:
  - computer, network, internet security def's
  - security services, mechanisms, attacks
  - X.800 standard
  - models for network (access) security