

Network Security



Slide Set 6

Slide Set 6

What is this chapter about?

This chapter is to address

- security needs
- security services
- security mechanisms and protocols

for data stored in computers and transmitted across computer networks

2

Slide Set 6

What security is about in general?

- Security is about protection of assets
- Prevention
 - take measures to prevent assets from being tampered (or stolen)
- Detection
 - take measures so that you can detect when, how, and by whom an asset has been tampered
- Reaction
 - take measures to recover assets

3

Slide Set 6

Real-world example

- Prevention
 - locks at doors, window bars, secure the walls around the property, hire a guard, Rott...
- Detection
 - missing items, burglar alarms, CCTV, ...
- Reaction
 - attack on burglar, call the police, replace stolen items, make an insurance claim, ...

4

Slide Set 6

Internet shopping example

- Prevention
 - encrypt your order and card number, enforce merchants to do some extra checks, 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
 - Or, pay and forget

5

Slide Set 6

Information security: Past & Present

- Traditional Information Security
 - keep the cabinets locked
 - put them in a secure room
 - human guards
 - electronic surveillance systems
 - i.e. Physical and Administrative mechanisms
- Modern World
 - Data is found inside computers in digital format
 - Computers are interconnected
 - **Hence computer and network security required**

6

Some Terminologies

- Computer Security
 - automated tools and mechanisms to protect data **in** a computer, even if the computers are connected to a network e.g.
 - against hackers (intrusion)
 - against viruses
- Network Security
 - measures to prevent, detect, and correct security violations that involve the **transmission** of information in a network

Services, Mechanisms, Attacks

- 3 aspects of information security:
 - security attacks (and threats)
 - actions that compromise security
 - security services
 - services counter to attacks
 - security mechanisms
 - used by services
 - E.g. Confidentiality is a service, encryption is the mechanism

Attacks

- Attacks on computer systems
 - break-in to destroy information
 - break-in to steal information
 - blocking to operate properly
 - malicious software (malware)
 - wide spectrum of problems (more later)

Attacks

- Network Security Attacks
 - **Passive** and **Active**
- Passive attacks
 - intercept messages by *sniffing* or *snooping*.
 - What can the attacker do?
 - use information internally ("fetiche")
 - release the content ("palabre")
 - traffic analysis ("veille mouvement")
 - Hard to detect, try to prevent... How?

Attacks

- Active attacks involves interruption, modification, fabrication, deletion of messages.
 - Masquerade/Spoofing (attack on authentication)
 - pretend to be someone else to perform an illegitimate action
 - Insertion/Fabrication (attack on integrity and/or authentication)
 - create a bogus message usually via spoofing
 - Replay (attack on authentication and/or integrity and/or availability)
 - passively capture data and send later

Attacks

- Active attacks
 - Deny (attack on non-repudiation)
 - Refuse to acknowledge sending/receiving a message
 - Modification (attack on integrity)
 - change the content of a message
 - Denial-Of-Service (attack on availability)
 - prevention the normal use of servers, end users, or network itself

Security Services

- to detect and/or deter attacks
- to enhance security
- replicate functions of physical documents
 - have signatures, dates, seals, watermark
 - protection from disclosure, tampering, or destruction
 - notarize
 - record

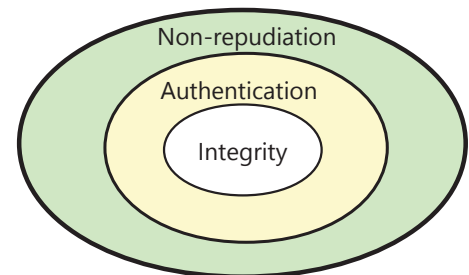
ISO 7498-2 Security Services

- Authentication
 - Assurance of the identity of the communicating entity
 - peer-entity authentication
 - mutual confidence in the identities of the parties involved in a connection
 - data-origin authentication
 - assurance about the source of the received data
- Confidentiality
 - protection of data from unauthorized disclosure

ISO 7498-2 Security Services

- Data Integrity
 - assurance that data received is exactly the same at the time sent by an authorized sender
 - i.e. no modification, insertion, deletion or replay
- Non-Repudiation
 - protection against denial by one of the parties in a communication
 - Origin non-repudiation
 - proof that the message was sent by the specified party
 - Destination non-repudiation
 - proof that the message was received by the specified party

Relationships



Security Mechanisms

- Basically cryptographic techniques/technologies
 - that serve to security services
 - to prevent/detect/recover attacks
- Encipherment (Encryption)
 - use of mathematical algorithms to transform data into a form that is not readily intelligible using ciphers
 - keys are involved

Security Mechanisms

- Message Digest
 - similar to encryption, but one-way (recovery not possible)
 - generally no keys are used
- Digital Signature & Message Authentication Code
 - Addition or Cryptographic transformation of a data unit to prove the source and the integrity of the data
- Authentication Exchange
 - ensure the identity of an entity by exchanging some information

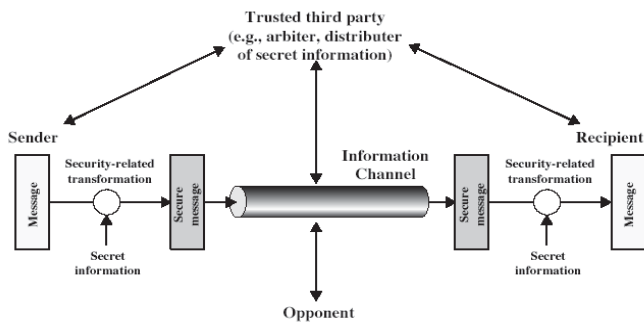
Security Mechanisms

- Notarization
 - use of a trusted third party to assure certain properties of a data exchange
- Time-stamping
 - inclusion of correct date and time within messages
- Non-cryptographic mechanisms
 - traffic padding (for traffic confidentiality)
 - Intrusion Detection Systems (more later)
 - Firewalls, Honeynet, Honeypot (more later)

Two Security references

- ITU-T X.800 Security Architecture for OSI
 - gives a systematic way of defining and providing security requirements
- RFC 2828
 - over 200 pages glossary on Internet Security

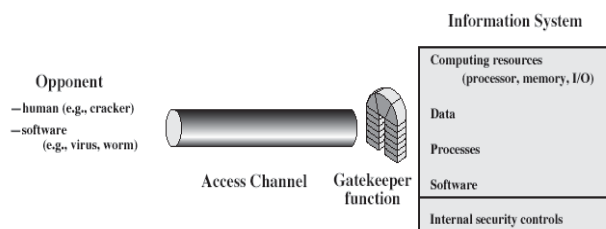
Model for Network Security



Model for Network Security

- This model requires the
 - design a suitable algorithm for the security transformation
 - generation the secret information (keys) used by the algorithm
 - Development of methods to distribute and share the secret information reliably
 - 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

- This model requires the
 - Selection of appropriate gatekeeper functions to identify users and ensure only authorized users access designated information or resources
 - e.g. what you know, what you have, who you are
 - Internal control to monitor the activity and analyze information to detect intrusion.

More on Computer System Security

- Based on security policies
 - Set of rules that specify
 - How resources are managed to satisfy the security requirements
 - Which actions are permitted, which are not
 - Ultimate aim
 - Prevent security violations such as unauthorized access, data loss, service interruptions, etc.
 - Scope
 - Organizational or Individual
 - Implementation
 - Partially automated, but mostly humans are involved

Aspects of Computer Security

- Mostly related to Operating Systems
- Similar to those discussed for Network Security
 - Confidentiality
 - Integrity
 - Availability
 - Authenticity
 - Accountability
 - Dependability

Aspects of Computer Security

- Confidentiality
 - Prevent unauthorised disclosure of information
 - Synonyms: Privacy and Secrecy
 - any differences? Let's discuss
- Integrity
 - In general, "make sure that everything is as it is supposed to be"
 - Specifically, "no unauthorized modification or deletion"
- Availability
 - services should be accessible when needed and without delay

Aspects of Computer Security

- Accountability
 - audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party
 - How can we do that?
 - Users have to be **identified** and **authenticated** to have a basis for access control decisions and to find out responsible party in case of a violation.
 - The security system keeps an **audit log (audit trail)** of security relevant events to detect and investigate intrusions.
- Dependability
 - Can we trust the system as a whole?

Fundamental Tradeoff

- Between security and ease-of-use
- Security may require clumsy and inconvenient restrictions on users and processes

"If security is an add-on that people have to do something special to get, then most of the time they will not get it"

Martin Hellman,
co-inventor of Public Key Cryptography

Designing a successful product

- User-transparent
- Do not assume potential users to be security experts
 - but provide enough set of options for security experts
- a security feature in a product is a plus, but a security product is a challenge in the market
 - people intend to pay for secure products, but not to pay security products
- Homework: Prove or disprove the last bullet by making a search in the Internet.