UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione

Security Introduction

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Course of Network Security, Spring 2014

http://www.tlc.unipr.it/veltri

Network Security

- Networked scenario:
  - **Network are composed of interconnected nodes**
  - **Nodes provide services and store information**
  - **Users access services and exchange/store information**
- In such a distributed scenario it is important to assure communication and application security in terms of:
  - **privacy/confidentially**
  - **Integrity/consistency**
  - **availability**
  - **etc.**

Security Service

- Is something that enhances the security of the systems and the information transfer
  - **intended to counter security attacks**
- Make use of one or more security mechanisms to provide the service
- Replicate functions normally associated with physical objects/documents
  - **e.g. signatures, dates, proof of reception, notarization, recording, etc.**

Security Services (X.800 and RFC 2828)

- ITU-T Recommendation X.800 (Security Architecture for OSI)
  - **defines a systematic way of defining and providing security requirements**
  - **a useful abstract overview of security concepts**
- X.800 defines *Security Service* as
  - **a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers**
- IETF RFC 2828 (Internet Security Glossary) defines *Security Service* as
  - **a processing or communication service provided by a system to give a specific kind of protection to system resources**
  - **security services implement security policies, and are implemented by security mechanisms**

Security Services (X.800)

X.800 defines 5 major categories

- **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 Services (RFC 2828)

- Access control
- Audit
- Data origin authentication
- Peer entity authentication
- Data integrity
- Data confidentiality
- Availability
- System integrity
- Non-repudiation

Security Services (RFC 2828) (cont.)

- Access control service
  - **a security service that protects a system against an entity using a system resource in a way not authorized by the system's security policy**
    - in short, protection of system resources against unauthorized access
- Audit service
  - **a security service that records information needed to establish accountability for system events and for the actions of system entities that cause them**
- Authentication service
  - **a security service that verifies an identity claimed by or for an entity**
  - **in a network, there are two general forms of authentication service: i) peer entity authentication service**
  - **ii) data origin authentication service**

Security Services (RFC 2828) (cont.)

- Peer entity authentication service
  - **a security service that verifies an identity claimed by or for a system entity in an association**
  - **this service is used to confirm the identity of one entity to another, thus protecting against a masquerade by the first entity**
  - **unlike data origin authentication service, this service requires an association to exist between the two entities**
- Data origin authentication service
  - **a security service that verifies the identity of a system entity that is claimed to be the original source of received data**
  - **this service is provided to any system entity that receives or holds the data**
  - **this service is usually bundled with connectionless data integrity service (and does not previously requires a peer entity authentication service)**
  - **(See: data integrity service)**

Security Services (RFC 2828) (cont.)

- Data integrity service
  - **data integrity is the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner**
  - **data integrity service protects against unauthorized changes to data, including both intentional change or destruction and accidental change or loss, by ensuring that changes to data are detectable**
  - **a data integrity service can only detect a change and report it to an appropriate system entity; changes cannot be prevented unless the system is perfect (error-free) and no malicious user has access**
  - **however, a system that offers data integrity service might also attempt to correct and recover from changes**
  - **although data integrity service is defined separately from data origin authentication service and peer entity authentication service, it is closely related to them**

Security Services (RFC 2828) (cont.)

- Data confidentiality service
  - **data confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity)**
    - in short, data confidentiality service protects data against unauthorized disclosure
- System integrity service
  - **the system integrity is the quality that a system has when it can perform its intended function**
  - **system integrity service protects system resources in a verifiable manner against unauthorized or accidental change, loss, or destruction**
- Availability service
  - **a security service that protects a system to ensure its availability**
  - **this service addresses the security concerns raised by denial-of-service (DoS) attacks**

Security Services (RFC 2828) (cont.)

- Non-repudiation service
  - **a security service that provide protection against false denial of involvement in a communication**
  - **there are two basic kinds of non-repudiation service:**
    - i) ”non-repudiation with proof of origin" - this service can be viewed as a stronger version of a data origin authentication service, in that it proves authenticity to a third party
    - ii) ”non-repudiation with proof of receipt" - protects the originator against an attempt by the recipient to falsely deny receiving the data
  - **does not prevent an entity from repudiation; it provides evidence that can be stored and later presented to a third party**

Security Mechanisms (X.800)

- Security services are provided by means of different security functions/ mechanisms
  - **they can be included in appropriate communication layer**
- Examples of security mechanisms are
  - **enciphering**
  - **authentication exchange**
  - **data integrity check**
  - **digital signature**
  - **notarization (third-party authentication)**
  - **access control**
  - **traffic padding**
  - **routing control**
  - **etc.**

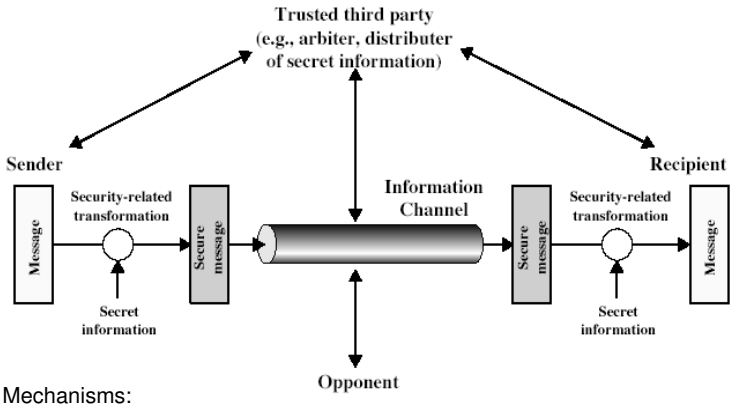
Relationship Between Security Services and Mechanisms

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Classification of Security Attacks

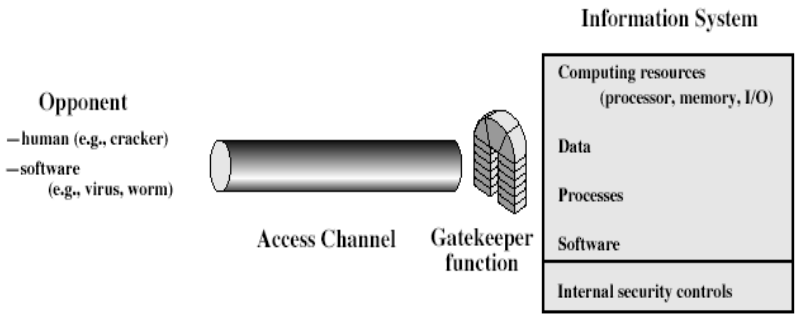
- **passive attacks** (eavesdropping on, or monitoring of transmissions):
  - **Interception (snooping)**
    - obtain message contents (attacks confidentiality)
  - **Traffic analysis**
    - monitor traffic flows (attacks confidentiality)
- **active attacks** (modification of data stream):
  - **Spoofing**
    - fabrication of messages with a fake source entity (attacks authenticity)
  - **Tampering**
    - modify of message content (insert, cancel, modify data) (attacks integrity)
  - **Replay/Reflection**
    - replay previous messages to/from the same of different entity (attacks authenticity)
  - **Repudiation**
    - deny having sent or received a message (attacks Non-reputation)
  - **Denial of Service (DOS)**
    - Interruption of a network or application service (attacks availability)

Model for Communication Security



- Mechanisms:
  - **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



- 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**