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

# Security Introduction

Luca Veltri

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

Corso di Sicurezza nelle reti di telecomunicazioni, a.a. 2008/2009

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



## Network Security

- Network are composed of interconnected hosts
- Hosts provide services and store information
- Users access services and exchange/store information
- In a distributed scenario it is important to assure:
  - **privacy/confidentially**
  - **Integrity/consistency**
  - **availability**
  - **etc.**





## Security Service

- Is something that enhances the security of the data processing systems and the information transfers of an entity or organization
  - **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
  - **eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed**





## 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
- availability
- data confidentiality
- data integrity
- system integrity
- non-repudiation





# Security Services (RFC 2828) (cont.)

- access control service
  - **a security service that protects against a system 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**
  - **deals with constancy of and confidence in data values, not with the information that the values represent**
  - **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)**
  - **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**
  - **does not prevent an entity from repudiation; it provides evidence that can be stored and later presented to a third party**
  - **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





# 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
  - **encipherment**
  - **digital signatures**
  - **access controls**
  - **data integrity check**
  - **authentication exchange**
  - **traffic padding**
  - **routing control**
  - **notarization (third-party authentication)**
  - **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 | | | |





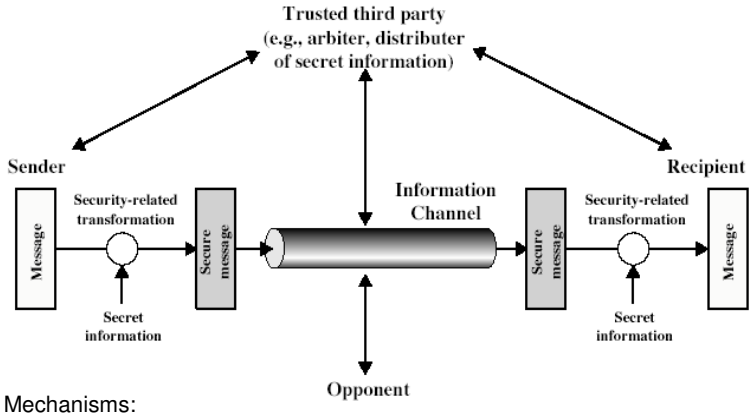
# Classify Security Attacks as

- **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):
  - **Fabrication (spoofing)**
    - masquerade of one entity as some other (attacks authenticity)
  - **Replay**
    - replay previous messages (attacks authenticity)
  - **Modification (tampering)**
    - modify messages in transit (attacks integrity)
  - **Interruption**
    - denial of service (DoS) (attacks availability)





# Model for Communication Security

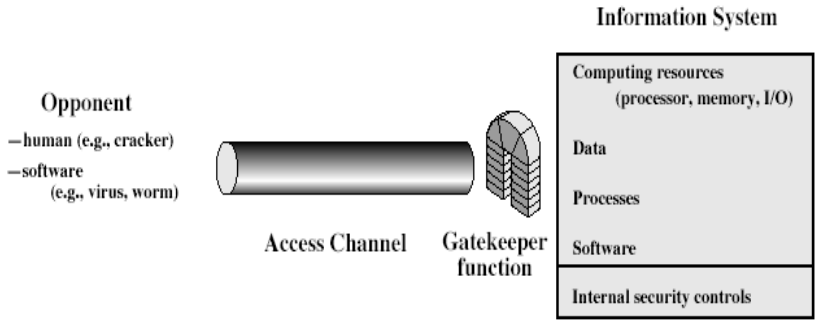



- Mechanisms:
  - **design a suitable algorithm for the security transformation**
  - **generate the secret information (keys) used by the algorithm**
  - **develop methods to distribute and share the secret information**
  - **specify a protocol enabling the principals to use the transformation and 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**

# Network security: The ideal world

- Strong authentication of both services and users
- Reliable authorization/access control, and effective abuse control
- Flawless protocols, operating systems, and applications
- Perfect policy, perfect policy enforcement
- Every user is a secure expert





# The real world

- Effective security protection are not deployed
- Sites do not install vendor patches
- Sites do not use sufficient AAA for remote access
- Sites do not monitor restrict access to their internal hosts
- Sites do not dedicate staff or sufficient resources to improve and maintain security
- Sites do not implement policies
- ...





# Sicurezza: vari aspetti..

- ✓ matematica (teoria dei numeri, crittografia)
- ✓ protocolli (protocolli di rete, autenticazione, etc)
- ✓ architetture di rete e relative funzioni (nodi, gateways, etc)
- ✓ servizi
- ✓ software (algoritmi, OSs, middleware, bachi)
- ✓ hardware, elettronica, elettromagnetismo, ottica, biomedica, etc
- ✓ aspetti sociali (comportamentali e stimoli esterni)
- ✓ legislazione
- ✓ politica
- ✓ etc.