Lecture 1

Introduction to Network Security
Lecture 1—Contents

Class introduction

Security terminology
- Goals
- Attacks and threats
- Services
- Mechanisms

Positioning of security services in networks
Lecture 1— Contents

Class introduction

Security terminology
  Goals
  Attacks and threats
  Services
  Mechanisms

Positioning of security services in networks
A theory for information security

- Information Theory
  - fundamental limits

- Complexity Theory
  - feasible solutions

Security Theory?

- optimal strategies

Game Theory
Relationship with other areas of information security

- cloud computing security
- network security
- social network security
- computer security
cryptography
- physical security
digital forensics
- database security

Nicola Laurenti
Network Security
spring 2015
Class summary

1. Introduction to notions of information security
2. Unconditional vs computational security
3. Cryptographic and non cryptographic security mechanisms
4. Network security protocols at different layers
5. Further issues on security of wireless, mobile and ad hoc networks
Class features

With respect to other classes in Network Security, this class is characterized by the following features, inherited from the research activity at our Department:

**wrt the subject matter**

Beside the customary topics in network security we will also focus on:

- Wireless communications and networks
- Physical and data link layer security
- Unconditional security

**wrt the treatment**

We aim to provide an engineering view of the discipline, by using:

- Quantitative analysis
- Mathematical modeling and notation
- Probabilistic approach
Lecture 1—Contents

Class introduction

Security terminology
  Goals
  Attacks and threats
  Services
  Mechanisms

Positioning of security services in networks
Security goals

Desirable features of communication and networks

**Confidentiality**  information is available to the intended receiver only

**Integrity**  information is received exactly as sent

**Availability**  service is always available even if someone intends to disrupt the network (see difference vs. reliability and safety)

**Accountability**  it is always possible to identify who is responsible for any information event

**Privacy**  information is (used but) not disclosed to anyone (see conflict with accountability)

...
General attacks and threats

Attacks can threaten security goals

Eavesdropping learning confidential information

Modification modifying a message in transit

Denial of service make the service unavailable (e.g., by keeping it busy)

Forging building a fake message, pretending it was sent by someone else

Masquerade posing as someone else in a single message transmission or interactive protocol

Repudiation denying having sent or received some message

Profiling gathering information about a single user

Fingerprinting identifying the user associated with some message

Traffic analysis learning origin, destination, length, times, of communications (not the content)
Security services

Security services should protect communications and network protocols from attacks

**Secrecy** makes message unintelligible for eavesdroppers

**Data integrity** makes it possible to detect whether a message was intercepted and modified

**Access control** can protect from denial of service

**Message authentication** allows to detect forged messages

**Entity authentication** protects from masquerades

**Notarization** prevents repudiation by source and/or destination

**Anonymization** prevents consistent association between message and user

...
Security services

A security mechanism are a way to implement some security service

Encryption
Digital signature
Intrusion detection
Message authentication codes
Distribution of cryptographic keys
Randomization

...
Lecture 1— Contents

Class introduction

Security terminology
  Goals
  Attacks and threats
  Services
  Mechanisms

Positioning of security services in networks
What security services do we need and where?
Your real-world example