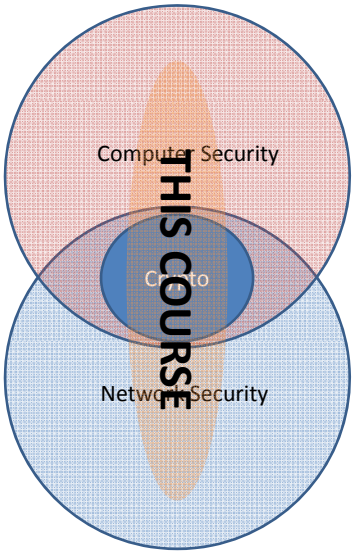
Computer and Network Security

Lecture 1

Introduction to Security

Acknowledgements:
Slides material taken from G. Tsudik, P. Krzyzanowski, D. Boneh, etc.

Bird's eye view



Outline

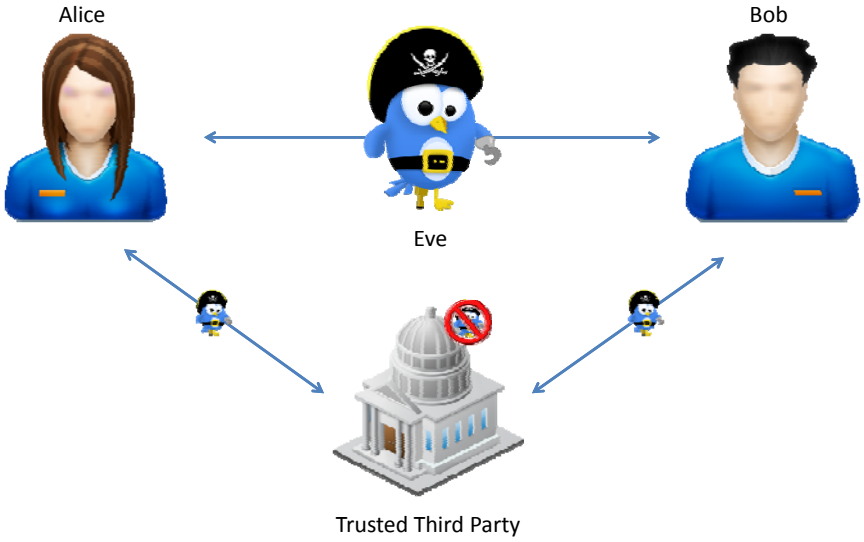
- The players
- Terminology
- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defense

The players – Computer Security

Attacker or adversary

Your PC

The players – Network Security



Terminology - Security

- Access Control & Authorization
- Accountability
- Privacy
- Intrusion Detection
- Tamper-resistance
- Certification and Revocation

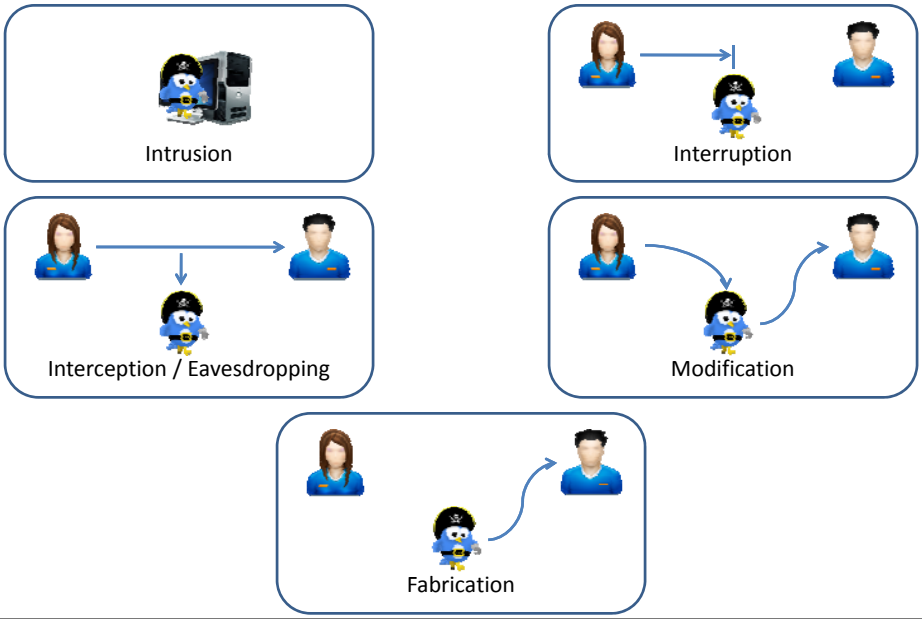
Terminology – Crypto

- Cryptography, Cryptanalysis, Cryptology
- Cipher, Cryptosystem
- Encryption/Decryption
- Confidentiality
- Authentication
- Identification
- Integrity
- Non-repudiation
- Freshness
- Intruder, Eavesdropper, Adversary,
- Anonymity, Unlinkability/Untraceability

Attacks, Services and Mechanisms

- Security Attack:
  - Any action that aims to compromise the security of a system
- Security Mechanism:
  - A measure designed to detect, prevent, or recover from, a security attack
- Security Service:
  - Something that enhances the security of a system
  - A *security service* makes use of one or more *security mechanisms*
- Example:
  - Attack: Eavesdropping (interception)
  - Mechanism: Encryption
  - Service: Confidentiality

Some classes of attacks



Some security services

- Confidentiality:
  - to assure privacy
- Authentication:
  - to assert who created or sent data
- Integrity:
  - to show that data has not been altered
- Access control:
  - to prevent misuse of resources
- Availability:
  - to offer permanence, non-erasure

Some methods of defense

- Cryptography → confidentiality, authentication, identification, integrity, etc.
- Software Controls → intrusion
- Hardware Controls → user authentication (holders)
- Policies → prevent insider attacks / flaws
- Physical Controls → access control