Security

Security services

Understanding security

- For clear thinking, it is useful to separate the following:

Threat (potential security breach)

Service (measure to deal with this threat)

Mechanism (means to provide a service)

Technology (implementation of mechanism)

Deployment (configuration)

Verification (test if it works)

Maintenance (support & keep up to date)

Understanding security

- For clear thinking, it is useful to separate the following:

Threat (e.g. leakage of private information on the Internet)

↓

Service (e.g. confidentiality)

↓

Mechanism (e.g. encryption)

↓

Technology (e.g. TLS)

↓

Deployment (e.g. configuration of version, algorithm, keys)

↓

Verification (e.g. test deployment)

↓

Maintenance (e.g. update keys, renew certificates)

Security Services

- **Authentication**
  - Correct identification of entity or source of data
- **Access control**
  - Who can access what; in what way
- **Data confidentiality**
  - Non-disclosure to external parties
- **Data integrity**
  - “Correctness” of data
- **Non-repudiation**
  - Proof that communication or transaction took place
- **Availability**
  - Ensuring system available to users when required

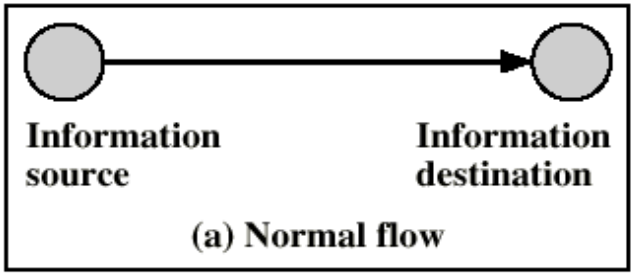
Mechanisms supporting services (examples)

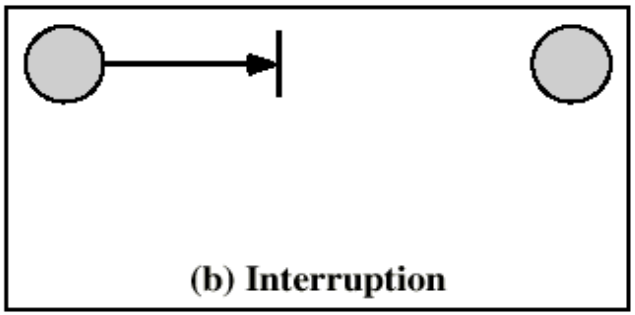
- Authentication
  - Passwords; biometrics
- Access control
  - File permissions
- Data confidentiality
  - Encryption; traffic padding
- Data integrity
  - Message digests; checksums
- Non-repudiation
  - Digital signatures
- Availability
  - Replication of data and services; Backup systems

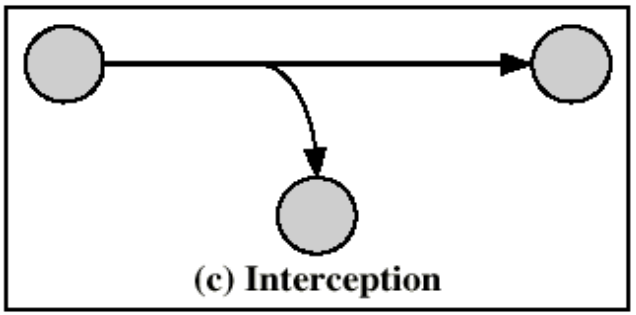
Attacks on Communications

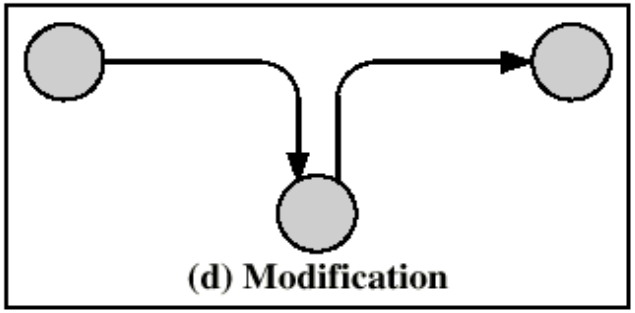
- Interruption
  - Cutting a communication line
- Interception
  - Unauthorised party gains access
- Modification
  - Unauthorised party gains access and tampers
- Fabrication
  - Unauthorised party masquerades as an authorised party

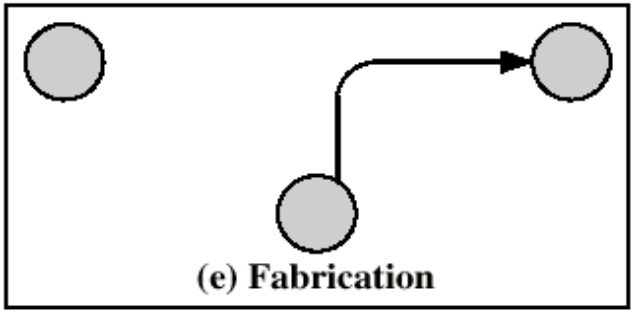
Attacks on Communications











Exercise

- Consider the 4 communications security attack types shown on the previous 2 slides (interruption, interception, modification, fabrication)
- Match each of these four attack types with a security service designed to prevent it.
- Also suggest a mechanism/technology that would realise this service