What is Security?

Confidentiality – sensitive data remains secret

Integrity – unauthorized modification cannot occur

Availability – data accessible

Much of Security is reliability

↳ keep your personal data confidential

↳ Allow only authorized access or modification

↳ correct and meaningful results when you need them

What is Privacy?

- control of information about yourself

Ex:

Credit Card Info, List of Names

Loss of privacy may or may not be loss of confidentiality

Privacy ≠ Security

Consequences: SPAM, fraud, identity theft

Balance between Security and Privacy

Ex:

CCTV - Photographs of everyone

Airports - full body scans

Organizations generally favour security over privacy

Adversaries

Murphie's law: random, non-malicious events - everything that can go wrong

Who are the bad guys?

↳ amauters
↳ "script-kiddies" (use other people's exploits)

↳ crackers
↳ organized crime

↳ governments
↳ terrorists

- Most serious threat: organized crime (economic)

How secure should we make it?

Principle of Easiest Penetration
- weakest point
- think like an attacker
- human - bribe, social engineering

Principle of Adequate Protection
- the economics of security
- don't spend too much

Assets: things we want to protect:
↳ hardware ↳ software ↳ data

Threats: loss or harm that might befall a system

Vulnerability:

Interception: uncauthorized access

Interuption: loss of availability

Fabricatrion

Modification

Attack: the action the adversary does to exploit the vulnerabilityto execute the threat

Control: removing or reducing vulnerability.

Defence:
Prevent, Deteranee, Deflect, detect, recover
Deterance C Deflection

Defence in depth: different seaurity