What Does Security Mean? ... In Real Life

- No one should be able to:
  - Break into my house
  - Attack me
  - Steal my TV
  - Damage my furniture
  - Use my house to throw water balloons on people
What Does Security Mean? ... In Real Life

• No one should be able to mess with my perception of reality
  – Pretend to be my friend Bob and fool me
  – Waste my time with irrelevant things
  – Prevent me from going to my favorite restaurant
  – Destroy my road, bridge, city ..
What Does Security Mean? ... For Computers and Networks

Real World

• No one should be able to:
  – Break into my house
  – Attack me
  – Steal my TV
  – Use my house to throw water balloons on people
  – Damage my furniture

Cyber World

• No one should be able to:
  – Break into my computer
  – Attack my computer
  – Steal my information
  – Use my computer to attack others
  – Damage my computer or data
What Does Security Mean? ... For Computers and Networks

Cyber World
• No one should be able to:
  – Use my resources without my permission
  – Mess with my physical world
• I want to talk to Alice
  – Pretend to be Alice or myself or our computers
  – Prevent me from communicating with Alice

Real World
• No one should be able to:
  – Pretend to be my friend Bob and fool me
  – Waste my time with irrelevant things
  – Prevent me from going to my favorite restaurant
  – Destroy my road, bridge, city...
Computer vs. Network Security

• Does an isolated computer have security risks?
  – Computer security aims to protect a single, connected, machine

• Networking = communication at all times and in all scenarios!!!
  – Network security aims to protect the communication and all its participants

• Security = protection or fault tolerance?
  – Protection: prevent attacks
  – Fault tolerance: keep operating in spite of attacks
Security Properties

- **Confidentiality (C)**
  - Data secrecy: Keep data secret from unauthorized subjects
  - Privacy: Individuals control who can access their information

- **Integrity (I)**
  - Aka “authenticity”
  - Data integrity: Keep data from being modified
  - System integrity: Keep systems functioning as intended

- **Availability (A)**
  - Keep the system running and responsive to legitimate clients
Orthogonal Aspects

• Policy
  – Deciding what confidentiality, integrity and availability mean in a given context
    • e.g., what is CIA for student grades at a university?

• Mechanism
  – Implementing the policy
  – Various mechanisms exist: firewalls, file system access controls, authentication mechanisms, VPN, etc.
Security Goals

• Attack prevention
  – It is impossible for the attack to succeed

• Attack detection
  – Low false positives, false negatives and detection delay

A false positive is when the system detects an attack, but the attack did not occur.
A false negative is when the attack is missed by the system.

Information Sciences Institute
Security Goals

• Attack prevention
  – It is impossible for the attack to succeed

• Attack detection
  – Low false positives, false negatives and detection delay

A false positive is when the system detects an attack, but the attack did not occur.
A false negative is when the attack is missed by the system.

• Attack response
  – Retaliation, observation, recovery

• Attack recovery
  – Remedy the effects of the attack or withstand it