Points of vulnerability

- Hardware
  - Accidental misuse (soda, corn chips, fire)
    - (story of water into laptop keyboard at conference)
  - Deliberate misuse (fire extinguisher into system, theft)
  - What kind of attacks are these?
    - Note that theft may lead to data loss, so confidentiality attack
- Software
  - Bugs in network server programs
  - Modification (remove license checks)
  - Backdoors, trojans, worms, viruses, spyware, rootkits
  - Intentional errors inserted by malicious programmers (Linux kernel code example)
- Data
  - Confidentiality & integrity primary concerns
  - In 2007, the UK government lost 37 million items of personal data
- Networks
  - Allows outside world to access your systems
  - Wireless networks for laptops often allow insiders to bypass firewalls
- People
  - Social engg
  - The best technical security solutions fail when users are naïve

Def: Vulnerability

- A weakness in the security system that might be exploited to cause harm
- Ex: in procedures, policy, design, or implementation
- OpenBSD philosophy: software bugs are vulnerabilities that attackers aren't yet smart enough to break

Def: Threat

- A set of circumstances that has the potential to cause loss or harm
- Vulnerabilities can occur without threats: access to buggy software is blocked by a firewall
- Threats can occur without vulnerabilities: fire can destroy a data center

Def: Attack
- An active attempt to exploit a vulnerability

Types of attack
- Eavesdropping
  - Monitor email, spyware
  - MITM attack against web commerce, SSL supposed to prevent
- Interruption
  - Denial of service, block traffic, consume resources
- Alteration
  - SQL injection attack that drops main customer table
- Fabrication
  - Spoof email address
  - Replay previously observed credential

Def: Confidentiality
- Objects read only by authorized subjects
- How: OS access controls (rwx bits), crypto over networks
- Failures are eavesdropping violations

Def: Integrity
- Objects altered only by authorized subjects
- How: OS access controls (rwx bits), crypto hashes
- Failures are alteration violations and fabrication violations

Def: Availability
- Objects accessible to authorized subjects
- How: ensure unauthorized subjects cannot consume all access requests
  - SYN cookies
- Failures are interruption violations, DoS attacks

Def: Authenticity
- Subjects appear only with their own identity
- How: passwords, authentication

- Failures prevent appropriate enforcement of confidentiality, integrity, & availability

Def: Threat Model
- Attacker's expected level of skill, equipment, & determination
- Amateurs to nation-states
- In the middle: organized crime, terrorists

Economics of protection
- Resources spent on protection should not exceed value of protected objects
- Level of protection should reflect danger to objects given realistic threat model
- The “bear rule”
  - If you and your friend run into a bear in the woods, you don't have to outrun the bear; you only need to outrun your friend.
  - Protections do not need to be perfect, just enough to make you a less interesting target
  - Useful for generic attacks
  - Not that useful for targeted attacks against a specific object in your protection