Lecture notes for 1.5 “Defenses”

Reminder: HW 1 due
Reminder: Office Hours now Mondays at 3:00

- Responses to attacks
  - Prevention: block the attack, close the vulnerability
  - Detection: realize attack is happening or has happened
    - online or after-the-fact
  - Recovery: resume original use
  - Deterrence: complicate the attack
  - Deflection: make someone else look more appealing
    - run faster than your friend, not the bear

- Defense-in-depth / layered security
  - Encryption
    - [draw picture]
      - plaintext + key --> [encipher] --> ciphertext
      - ciphertext + key --> [decipher] --> plaintext
    - Basis of numerous security protocols
    - Provides data confidentiality & integrity (how?)
    - Does it provide availability?
  - Software controls
    - Access controls in DBMS & OS
    - Program design & QA
    - Attack detection: virus scanners, IDS
    - Vulnerability patching
  - Hardware controls
    - Smart cards / multi-factor authentication
    - Cable locks [example: after breaking in, attackers walk out with entire VCR recording surveillance cameras]
    - Attack prevention: firewalls, IPS
  - Physical access control
    - Guards
  - Principle of weakest link: Security can be no stronger than its weakest link

- Principle of easiest penetration: Intruders will use any available means of penetration

Effective defenses

- Correctly respond to attacks (e.g. actually detect an attacker)
- Do not false alarm
- What false alarm rate would you accept?
- Scale: high-security sites may accept higher false alarms for higher detection rates
- [draw picture] ROC curve