CSE 509 - System Security Rob Johnson

http://www.cs.sunysb.edu/~rtjohnso/teaching/cse509-sp07

office hours: 2313D 11:20 - 12:20

What is security?

- restriction from unauthorized access
  - manipulate/use
  - safety/non-malicious
  - integrity (can't change data)
  - availability (for authorized users)
    - denial of service
  - confidentiality (can't read data)

security goals

- **Confidentiality**
  - attacker can't read password/credit card over network
  - theives can't read data from a stolen laptop
  - hide process time/CPU usage/mem usage
  - hide the fact that you communicated at all
  - anonymity/privacy

- **Integrity**
  - only authorized users can modify file/database
  - only authorized users can modify process memory
  - only authorized users can detect DB violation constraints
  - execute/file access permissions
  - attacker can't modify messages in transit
  - only accept unmodified messages from Bob

- **Availability**
  - attacker can't deny users access to amazon.com
  - attacker can't use my CPU time, disk, printer, RAM, etc.
  - attacker can't use/drain power

Security (Adversary) vs. Reliability

- adversary: faults can occur in worst possible combination
- reliability: faults are random/independent

Threat Model: defines the capabilities, limitations, and possible goals of an attacker

- computation

  1 pentium ——— 2^{32} cycles/second

  super computer ——— 2^{16} CPUs

  $= 2^{48}$ cycles/sec

  one year ——— 2^{25} seconds/year

  $= 2^{73}$ cycles/year

  100 years ——— 2^{7} years

  (with no increase in computational power)

  $= 2^{80}$ cycles/100-years

  AES: 128-bit key

  $Pr[\text{success}] = 2^{-48}$

- bandwidth

  DOS amazon.com

  Assume the attacker has
  - one dialup connection
  - one million other users' desktops with DSL

On today's internet, attacker can have mucho bandwidth

- time "attack at dawn"

- money if a message is worth $1m, the attacker will only spend < $1m to break it

- expertise e.g. script kiddies

- knowledge
  - hardware configuration
  - OS version
  - application versions
  - configuration info
  - don't know
    - password
    - random number generator output

- Local vs. Remote

  local: attacker has account on system

  remote: attack over network

- Active vs. Passive

  active: may send, modify, or supress messages

  passive: listens to messages (harder to catch)

Defender — Goals

Attacker — Capabilities "Threat model"

email ½ page paper reviews (plain text in body)

rtjohnso+509r@cs