

CSE 409/509

Rob Johnson

OH: Wed 10-12

2313D CS

<http://www.cs.sunysb.edu/~rob/teaching/cse509-s09/>

### Security

- People breaking into systems
- Crypto
- Privilege
- Privacy
- Trust
- Authentication
- Denial of Service

### Confidentiality

- People breaking into systems
- Crypto
- Privacy
- Eavesdropper cant' read mail
- Man-in-the-middle attacks
  - Truck company hijacked website of real truck company, criminals would make a deal to ship stuff, then they would pass it off to the real trucking company for a lower price, or sometimes they just took the money and ran.
- Message recipient secrecy/anonymity
- Timing information

### Integrity

- People breaking into systems
- Crypto
- Client Information
- Pricing Info
  - Lower price of amazon.com's Ipad to \$1.
- Contents of RAM, Cookies
- Password
- User Database
  - Remote attacker's possible first target to gain some local access to machine

### Availability

- Denial of Service
- Website availability
- I/O

- Fill disk
- Swapstorm
- Crash programs
  - “Ping of Death”
  - Reboots
- Performance degradation

Integrity and Confidentiality are generally intertwined.

If someone can change a key the Confidentiality is gone.

If someone can recover a secret key, Integrity is gone.

If you lose Confidentiality you might lose Integrity.

Availability is a weaker goal because you generally don't lose confidentiality or Integrity when you lose availability.

### Security

Adversary/Enemy

Threat Models- describe capabilities and Limitations of the Adversary.

$2^{23}$  seconds per year

Adversary has limited CPU time

$2^{32}$  instructions per second

$2^{20}$  computers

Gives the hacker  $2^{75}$  instructions per year

### Local Vs Remote

- Generally initial set of privileges
  - Remote: can sent packets to victim system
  - Local: login
    - Run unprivileged arbitrary code
    - Can act as remote if desired for some reason

### Bandwidth

- 56 KB/s in the old days
- botnet of 100k machines(at 56 KB/s)
  - 5.6 GB/s

Time limits: Ex: message “attack at dawn” if message is received by enemy after dawn it is useless.

Physics: Ex:

Quantum Crypto.

Devices that could verify that other device it was talking to is near by. This could be done by determining how long it takes for a message to travel between points (Round Trip Time)

## Propagation Delay/Limits

### Scale of adversary's investment vs Value of system

If secret is worth \$1million, you wont spend more than that to protect it, and they wont spend more than that to get it (if they know the value beforehand).

### Knowledge

- Generally underestimated
- Should assume knowledge of:
  - Hardware Configuration
  - OS Configuration
  - Source code
  - Password length
  - Open ports
  - Etc
- Should assume unknown:
  - Password
  - Secret keys
  - Random numbers

(Talking about publishing a paper about vulnerabilities in locks)

### Benefits of publishing vulnerabilities (Full Disclosure)

- Manufacturers build better locks
- Fix bugs
- User can mitigate risks
- Users can buy different locks
- No back doors
- May deter attackers because knowledge is known (probably not)

### Benefits of non-disclosure

- Give the manufacturers time to fix the problem before it is known
- Prevent exploitation of the bug
- Prevent script kiddies
- Preserve image of manufacturers
- "Ignorance is Bliss" - the users feel safer

### Trust

- Trust == Dependence
- If we trust X and X fails, then attacker wins
- Example: Apache webserver on a linux machine
- Must Trust:
  - Disk (htaccess files)
    - developers
  - Keyboard

- developers
  - Apache binary
    - Apache developers
  - Cables
  - Trust OS to not let apache do things it shouldn't
    - OS developers
  - Users?
  - Certificate Authority (CA)
  - Cryptography
    - Cryptographers
  - CPU
  - RAM
  - Compiler
  - Admin
  - ISP
- Transitive trust, if you trust Admin and Admin trusts Apache then you trust apache, and apache trusts X then you trust X etc.
- Mitigate disk trust by using check summing, mirroring (put data on 2 drives, to make sure that one company isn't modifying the data).
- Trusted Computing Base (TCB)
- 

We import a lot of parts, and trust them with no real “reason” to.