# Chapter 16 -- Security

## A big deal for OSes

- Ignoring network security which is really the responsibility of the OS
- Security for the OS -- kinds of attacks
  - breach of confidentiality -- unauthorized reading of data
  - breach of integrity -- modification of data
  - breach of availability -- resource not available
  - theft of service -- unauthorized use of resources
  - denial of service -- fork bombs (minor) ...
- Attack methods
  - masquerading
  - replay attack -- replay of valid data ...
  - message modification
  - man in the middle attack
  - session hijacking
  - privilege escalation

# Security (page 2)

- Levels of security
  - physical
  - network
  - operating system
  - application
  - human

Application Level

- Malware and Trojan Horse programs
  - Major problem of "free" programs on Internet
  - not as much for open source programs
- Trap Door
- Logic Bomb
- Stack and Buffer Overflows, Code injection
  - major source of privilege escalation
  - code run on the stack
    - execvp("/bin/sh", ....)

# Security (page 3)

- Viruses
  - file
  - boot
  - macro
  - rootkit
  - source code virus
  - polymorphic -- changes signature
  - encrypted
  - stealth
  - tunneling -- interrupt handler/device drivers
  - multipartite -- various locations in the system
  - armored -- hard to figure out what it does.
  - ransomware -- encrypts data, ransom for unlock code

## System and Network Threats

- Default install of an OS
  - Many services enabled by default
  - Very few services enabled by default
- worms -- 1988 internet worm, Robert Morris
  - gets() buffer overflow, ...
  - Sobig worm, 2003, photo, target, MS windows
- Port Scanning -- find out what services are available
- Denial of Service -- various forms, network, CPU, ...
  - DDOS -- Distributed denial-of-service attachks

# Cryptography as a Security Tool (16.4)

- encryption -- a primary tool for security
  - passwords on UNIX, ...
- Symmetric Encryption:  M = D_k ( E_k (M ) )
  - DES -- data-encryption standard,  64 bit value, 56 bit key
    - Triple DES ... 3 keys:  E_k3(D_k2(E_k1(M)))
  - AES -- 2001, keys of 128, 192, or 256 bits, 128-bit blocks
  - Not good for long messages ...
- Asymmetric Encryption: RSA, public key/private key systems
- Authentication -- limiting potential senders
  - Also helps prove a message has not been modified
  - md5, SHA-1, other hash functions can be authentication
  - also digitial signatures, RSA allows anyone to verify signature
- Key Distribution
  - Symmetric encryption requires key distribution
  - reason for asymmetric encryption
    - Still can have a man-in-the-middle attack
  - Digitial certificates by a trusted, well known authority
- Implementation of Cryptography
  - Multiple layers -- networking issues here
  - Read 16.4.3 about TLS (Transport Layer Security)

# User Authentication (16.5)

## How do you know the user is allowed access?

- passwords
  - How to store passwords
  - Easy to guess passwords vs good passwords
  - User or System Generated (X-machine at LLNL)
  - One time passwords and two-factor authentication
  - Challenge / Response systems
- Biometrics
  - fingerprints
    - require both a fingerprint and a password
  - face recognition?
  - ear "print"?
  - other?

Total security policy is typically beyond the OS

- OS can provide tools
- Organization must use tools
- People must have buy-in for a security policy to work
- Must be a "living document"

# Security Defenses

## Defending from attack, both external and internal

- defense in depth -- many layers of defense are better than few
- Vulnerability Assessment:
  - Risk assessment
    - test scripts vs source code
  - Penetration testing
    - network scans
    - file system scans
    - process scans
  - US Gov ... only as secure as its most far reaching connection
- Intrusion Detection
  - honeypot -- to trap attackers
  - monitoring of system ... has some similarity to penetration testing
- Virus Protection
  - virus scanners
  - sandbox
- Read remainder of chapter (16.6.5-16.8)