95-753

Lecture 2

Vulnerability Survey
Security Policies

Richard J. Orgass
Heinz School
Carnegie Mellon University

Vulnerabilities and Attacks

- Technical
  - Trojan Horses
  - Back Doors
  - Password Cracking
  - File Permissions and path settings
  - SUID Scripts and Programs
  - Trusted Hosts (rhosts)
  - Buffer Overflows
  - Scanning and Sniffing
  - Spoofing
  - TCP/IP Attacks
  - Session Hijacking
  - Denial of Service
  - Many others

Vulnerabilities and Attacks -- 2 --

- Social
  - Shoulder Surfing
  - Manipulation
    - social engineering to obtain sensitive information
      - pretending to be a system administrator or high level official
      - asking for sensitive info to help break into systems
      - "The Watchman" has lots of examples
- Physical
  - System Access
    - Passwords in LILO doesn't help a lot
    - Networking Issues
      - copper wire vs fiber optics
    - false fire alarms
    - looting as a result of natural disaster
    - etc, etc, etc.

Security Overview

- Higher speed
  - computers
  - networks
- Many more users
- Easier to use cracking tools
- 1999 CSI/FBI survey
  - 31% of respondents experienced system penetration by outsiders
  - 97% of respondents reported abuse of access by insiders
  - 55% of respondents reported unauthorized access by outsiders
  - 86% of respondents reported that likely source of attack was from disgruntled employees
  - 53% of respondents reported attacks from domestic competitors
  - **It's far worse now!!!**

What is computer/network security?

- Elements of a Computing Environment
  - Functional requirements
    - reliability
    - integrity
    - confidentiality
- Risk Analysis
  - Vulnerability Analysis
    - identify what could happen
    - threat analysis
    - cost of degrading system performance
- Security Policy
  - Risk analysis plus
    - procedures for managing a computing environment
      - account management
      - system installation procedures
      - communications procedures
      - use of security tools ...

Computer/Network Security -- 2--

- Security Policy
  - Result of following
    - consistent and predictable environments
    - easier to detect break-ins or unauthorized access
  - **Single most important security document**
    - must be well done
    - must be properly used

Securing Computers and Networks

- Simple slogans that help a lot
  - You are not invulnerable!
  - People are the weakest link
  - That which is not expressly permitted is forbidden
  - Always assume the bad-guy knows more than you do,
  - Practice vigilance and perseverance.
  - Always thoroughly investigate any publicly available software you decide to use.
  - With few exceptions, the implementation of any security measure will reduce either system and network performance or user convenience or both.
  - Plan for change.

User Privacy and Administrator Ethics

- User privacy must be guaranteed.
- Like Cesar's wife, the system administrators must be beyond reproach with respect to user privacy.
- Even monitoring for breakins must be done carefully!!

Remember

- Crackers break into computer systems
  - thieves
  - belong in jail
- Hackers are excellent but unconventional programmers
  - highly creative
  - create high quality maintainable code
  - earn their high salaries and more