Module 20: Security

- The Security Problem
- Authentication
- Program Threats
- System Threats
- Threat Monitoring
- Encryption
The Security Problem

- Security must consider external environment of the system, and protect it from:
  - unauthorized access.
  - malicious modification or destruction
  - accidental introduction of inconsistency.
- Easier to protect against accidental than malicious misuse.
Authentication

- User identity most often established through passwords, can be considered a special case of either keys or capabilities.

- Passwords must be kept secret.
  - Frequent change of passwords.
  - Use of “non-guessable” passwords.
  - Log all invalid access attempts.
Program Threats

- **Trojan Horse**
  - Code segment that misuses its environment.
  - Exploits mechanisms for allowing programs written by users to be executed by other users.

- **Trap Door**
  - Specific user identifier or password that circumvents normal security procedures.
  - Could be included in a compiler.
System Threats

- Worms – use spawn mechanism; standalone program
- Internet worm
  - Exploited UNIX networking features (remote access) and bugs in \textit{finger} and \textit{sendmail} programs.
  - Grappling hook program uploaded main worm program.
- Viruses – fragment of code embedded in a legitimate program.
  - Mainly effect microcomputer systems.
  - Downloading viral programs from public bulletin boards or exchanging floppy disks containing an infection.
  - \textit{Safe computing}. 
The Morris Internet Worm

- Grappling hook
- Finger attack
- Sendmail attack
- Request for worm
- Worm sent

Target system

Infected system
 Threat Monitoring

• Check for suspicious patterns of activity – i.e., several incorrect password attempts may signal password guessing.

• Audit log – records the time, user, and type of all accesses to an object; useful for recovery from a violation and developing better security measures.

• Scan the system periodically for security holes; done when the computer is relatively unused.
Threat Monitoring (Cont.)

- Check for:
  - Short or easy-to-guess passwords
  - Unauthorized set-uid programs
  - Unauthorized programs in system directories
  - Unexpected long-running processes
  - Improper directory protections
  - Improper protections on system data files
  - Dangerous entries in the program search path (Trojan horse)
  - Changes to system programs: monitor checksum values
Network Security Through Domain Separation Via Firewall

- Internet access from company's computers
- DMZ access from Internet
- Firewall
- Access between DMZ and company's computers

Diagram shows the flow of data between the Internet, DMZ, and company computers, with a firewall in the middle to control the access.
Encryption

- Encrypt clear text into cipher text.
- Properties of good encryption technique:
  - Relatively simple for authorized users to encrypt and decrypt data.
  - Encryption scheme depends not on the secrecy of the algorithm but on a parameter of the algorithm called the encryption key.
  - Extremely difficult for an intruder to determine the encryption key.
- Data Encryption Standard substitutes characters and rearranges their order on the basis of an encryption key provided to authorized users via a secure mechanism. Scheme only as secure as the mechanism.
Encryption (Cont.)

- Public-key encryption based on each user having two keys:
  - public key – published key used to encrypt data.
  - private key – key known only to individual user used to decrypt data.

- Must be an encryption scheme that can be made public without making it easy to figure out the decryption scheme.
  - Efficient algorithm for testing whether or not a number is prime.
  - No efficient algorithm is known for finding the prime factors of a number.