



Module 19: Security

- The Security Problem
- Authentication
- Program Threats
- System Threats
- Securing Systems
- Intrusion Detection
- Encryption
- Windows NT



Operating System Concepts 19.1 Silberschatz, Galvin and Gagne ©2002



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.



Operating System Concepts 19.2 Silberschatz, Galvin and Gagne ©2002



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.
- Passwords may also either be encrypted or allowed to be used only once.



Operating System Concepts 19.3 Silberschatz, Galvin and Gagne ©2002



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.
- Stack and Buffer Overflow
 - ◆ Exploits a bug in a program (overflow either the stack or memory buffers.)



Operating System Concepts 19.4 Silberschatz, Galvin and Gagne ©2002

System Threats

- Worms – use spawn mechanism; standalone program
- Internet worm
 - ✦ Exploited UNIX networking features (remote access) and bugs in *finger* and *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.
 - ✦ *Safe computing*.
- Denial of Service
 - ✦ Overload the targeted computer preventing it from doing any sueful work.

Operating System Concepts 19.5 Silberschatz, Galvin and Gagne ©2002

The Morris Internet Worm

The diagram illustrates the Morris Internet Worm attack mechanism. It shows two systems: a **target system** and an **infected system**.

- The **infected system** sends three types of attacks to the **target system**:
 - rsh attack
 - finger attack
 - sendmail attack
- These attacks cause a **grappling hook** to be installed on the **target system**.
- The **grappling hook** on the target system sends a **request for worm** to the **infected system**.
- The **infected system** responds by sending the **worm** back to the **target system**.

Operating System Concepts 19.6 Silberschatz, Galvin and Gagne ©2002



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.)

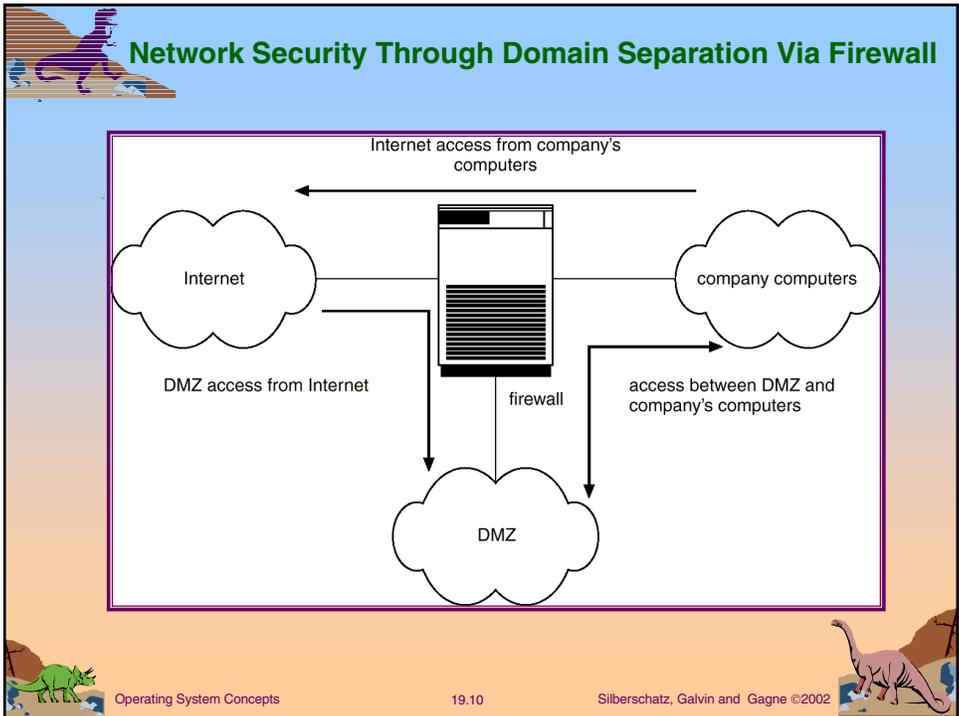
- Check for:
 - ◆ Short or easy-to-guess passwords
 - ◆ Unauthorized set-uid programs
 - ◆ Unauthorized programs in system directories
 - ◆ Unexpected long-running processes
 - ◆ Improper directory protections
 - ◆ Improper protections on system data files
 - ◆ Dangerous entries in the program search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



FireWall

- A firewall is placed between trusted and untrusted hosts.
- The firewall limits network access between these two security domains.

Operating System Concepts 19.9 Silberschatz, Galvin and Gagne ©2002





Intrusion Detection

- Detect attempts to intrude into computer systems.
- Detection methods:
 - ◆ Auditing and logging.
 - ◆ Tripwire (UNIX software that checks if certain files and directories have been altered – I.e. password files)
- System call monitoring



Data Structure Derived From System-Call Sequence

system call	distance = 1	distance = 2	distance = 3
open	read getrlimit	mmap	mmap close
read	mmap	mmap	open
mmap	mmap open close	open getrlimit	getrlimit mmap
getrlimit	mmap	close	
close			





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.



Operating System Concepts 19.13 Silberschatz, Galvin and Gagne ©2002



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.



Operating System Concepts 19.14 Silberschatz, Galvin and Gagne ©2002



Encryption Example - SSL

- SSL – Secure Socket Layer
- Cryptographic protocol that limits two computers to only exchange messages with each other.
- Used between web servers and browsers for secure communication (credit card numbers)
- The server is verified with a **certificate**.
- Communication between each computers uses symmetric key cryptography.



Computer Security Classifications

- U.S. Department of Defense outlines four divisions of computer security: **A**, **B**, **C**, and **D**.
- **D** – Minimal security.
- **C** – Provides discretionary protection through auditing. Divided into **C1** and **C2**. **C1** identifies cooperating users with the same level of protection. **C2** allows user-level access control.
- **B** – All the properties of **C**, however each object may have unique sensitivity labels. Divided into **B1**, **B2**, and **B3**.
- **A** – Uses formal design and verification techniques to ensure security.





Windows NT Example

- Configurable security allows policies ranging from D to C2.
- Security is based on user accounts where each user has a security ID.
- Uses a subject model to ensure access security. A subject tracks and manages permissions for each program that a user runs.
- Each object in Windows NT has a security attribute defined by a security descriptor. For example, a file has a security descriptor that indicates the access permissions for all users.

