

Security

Access privileges for users

- Users are given a base-level of access with their accounts
- Both UNIX and Windows NT allow additional privileges to the users by using the concept of groups
 - Groups are created for users who require similar access to a resource
- Access privileges in UNIX
 - Generally provided by flat files – `/etc/passwd` and `/etc/group` to maintain user and group information on individual computers
 - Multiple UNIX computers can be managed with a distributed network database such as NIS/YP or NIS+
 - Computers can be organized into domains to manage the NIS services
 - Users can go from one host to another because of host equivalence, implemented by the file `/etc/hosts.equiv`
- Access privileges in Windows NT
 - User and group information is stored in the registry
 - Network security database is provided by Windows NT Netlogon Service
 - Computers can be organized into domains or administrative groupings
 - Relationships can be created among domains so that users from one domain have access to resources in another without requiring the user to have an account in every domain, with this relationship referred to as *trust* in the Windows NT domain system (same as host equivalence in UNIX)
 - A domain is limited to 40,000 users
 - * If a single domain exceed 40,000 users, or the organization requires multiple administrative units, then multiple domains can be used
 - * At least one computer running Windows NT server is required for each domain

System security

- Protecting the system against break-ins
 - Attempt by an unauthorized person to gain access to the system
 - Attempt may be motivated by maliciousness or mere mischievousness
- Security deals with both guarding against external threats as well as authorized users as potential intruders
- Three well-known Unix security problems
 - The `sendmail` program
 - * In older implementations, `sendmail` used to have a debug mode designed to sort out delivery problems
 - * System administrator could type out raw commands and observe the effects
 - * Since `sendmail` runs as SUID root, a nefarious user could use `sendmail` to execute other commands as root
 - The `finger` program
 - * In older systems, the `finger` program did not check whether `.plan` file is readable by the user and displayed its contents
 - * Any user could create a link to any file as `.plan` and `finger` himself to view the contents of that file
 - The `passwd -f` program
 - * Used to change the GECOS information in the `/etc/passwd` file

- * Could be used to make additional entries in the password file
- Other bugs in the system still exist, for example, the problems with Java
- Security in UNIX
 - Traditionally, UNIX comes with all the lights turned on
 - Even the most minimal UNIX includes network services that may not be required; they become the focus of security attacks on UNIX systems
 - To secure a UNIX computer, you have to find out the network services offered by it, and turning them off one by one if they are not needed
- Security in Windows NT
 - Traditionally, Windows NT comes with all the lights turned off
 - You need to install the network services that are needed

Threats to Computer Systems

- Historical perspective
 - Older machines – less users, more open
 - New machines – multiple users, more potential for problems
- Threats, vulnerabilities and attacks

Threat. Any potential occurrence, malicious or otherwise, that can have an undesirable effect on the assets and resources associated with a computer system

Vulnerability. Some characteristic of a computer that makes it possible for a threat to potentially occur

Attack. An action taken by a malicious intruder that involves the exploitation of certain vulnerabilities in order to cause an existing threat to occur; the definition of attack in terms of malicious intruders removes innocent errors from the purview of computer security

Exemplified by a house where threat is that a burglar may steal some valuables and the vulnerability is a flimsy screen door
- Types of threats
 - Disclosure threat
 - * Giving information to someone who should not have it
 - * In computers, the information may be compromised while it is stored on the machine or while it is being transmitted over the network
 - Integrity threat
 - * Unauthorized change to information stored on a computer system or in transit over the network
 - * Changes in patient records in a hospital
 - Denial of service threat
 - * Access to some computer resource is intentionally blocked due to a malicious action taken by another user
 - * Commonly seen as long print jobs on printers so that other users cannot use the printers
- Attacker intent
 - How can you determine the intent of a person classified as an attacker?
 - Loss of Viking Probe due to erroneous DO statement in Fortran
 - Errors in C where = is placed and == intended

- Security and usability
 - Higher the security paranoia, lesser the usability of the machine
 - A goal in the design and development of security solutions for computer systems is to reduce the degree in which increases in security affect the usability of the system
- Other impediments to security
 - Retrofitting security into existing systems

Thinking about security

- Questions to ask
 - What are you trying to protect?
 - What valuable assets might be lost?
- Hypothetical case – Theft of the system
 - Loss of equipment
 - * Monetary cost
 - * Loss of computer as a physical object
 - Loss of data
 - * Company secrets
 - * Information about individuals
 - Loss of use
 - * Requirement of the computer to manufacturing or providing customer service
 - * Business or educational role of the computer
 - Physical vandalism
 - * Broken or damaged equipment
 - * Someone pouring a cup of coffee on operator console
 - * Also includes natural disasters that make the system unusable, flood, earthquake, fire
 - Electronic vandalism
 - * Corrupted or removed files
 - * Creating garbage processes on the system to make it unusable
 - * Introducing a virus into the system

Security auditing

- A mechanism to record the events on the system as they happen
- Most common logging facility on UNIX is `syslog`
 - Level of logging and location for logging information is normally customized using a configuration file `/etc/syslog.conf`
 - Logged message includes a message header and a message body
 - Message header consists of a facility indicator, a severity level indicator, a timestamp, a tag string, and optionally the process ID
- Security logging on Windows NT
 - By default, security logging is turned off

- Security logging is turned on by running `User Manager for Domains` to enable auditing and determine the events to be tracked
- Events are stored in a non-textual format and can be viewed through the `Event Viewer` program
- Security log contains both valid and invalid logon attempts as well as events related to resource use, including creating, opening, or deleting files or other objects
 - * Multiple logon failures can be taken to be an indication that someone is trying to break into the system

Logon security

- UNIX logon security is based on authenticating the system user, with subsequent access to system resources determined by file permissions
- Windows NT security is based on the concept of *access to objects*; when a user is authenticated, an *access token* is generated and compared to access control lists on objects

Login process in UNIX

1. User types in a username and password
2. Password is encrypted using the Data Encryption Standard (DES)
3. Encrypted password is compared to the password field in the password file (`/etc/passwd` or `/etc/shadow`), possibly by the Network Information Service (NIS)
4. If they match, logon proceeds
5. A shell starts that runs with a `uid` and `gid` from `/etc/passwd`

Login process in Windows NT

1. WinLogon requests a username and password, and sends them to Local Security Authority (LSA) in the security subsystem
2. LSA queries the Security Accounts Manager (SAM) to determine if the username and password are authorized
3. SAM checks the username and password against information contained in the directory database
4. If access is approved, LSA creates an access token with the granted access rights, and then passes the access token back to the WinLogon process
5. WinLogon calls for a new process for the user, usually `explorer.exe`, to which the user's token is attached