Operating System Security

Chapter 9

Lecturer: Pei-yih Ting

- Security risks exist for all operating systems and are not new.
- It is important to know the existing threats.
- It is also important to understand the operations and the vulnerabilities of your OS.
- Try to **harden your OS**, the morale is
  It is easier to pick the "low hanging fruit" first.

Overview

- OS Security Terms and Concepts
- Organize System Security
- Build-in Security Subsystems
- System Security Principles and Practices
- Windows Security Design
- UNIX and Linux Security Design
- System Backups
- Typical System Security Threats
- Well-Known Windows Risks
- Well-Known UNIX Risks
- System Forensics

Operating System Security Terms and Concepts

- An operating system (OS) is a layer of S/W between the hardware and user. It manages and controls access to hardware components

Resource	Example	Descriptions
Primary storage	Random Access Memory (RAM)	Physical memory that resides in the computer and is easily accessible by the processing unit. Primary storage is volatile and the contents are lost when power is removed.
Secondary storage	Disk drives, floppy disk drives, CD/DVD-ROM drives, tape drives	Nonvolatile storage for data. Includes both fixed and removable random access and sequential storage.
Processor(s)	Central processing unit (CPU)	The component(s) where instructions are executed. There may be several CPUs, as well as other special-purpose processors.
Input / Output devices	Keyboard, monitor, printer, mouse, scanner	Any device used either to collect data from the outside world or to present data to the world.
Network components	Network interface card (NIC)	Hardware device that connects the computer bus to an external network using either cables or wireless connections.

OS Security Terms and Concepts (cont'd)

- If the OS is not secure, there can be no guarantee that any resource managed by the OS is secure.
- Older OS focused on ensuring data confidentiality
  - Make sure only authorized users could see sensitive data
- Modern OS performs four basic functions
  - Positively identify a user
  - Restrict access to authorized resources
  - Record user activity
  - Ensure proper communications with other computers and devices (sending and receiving data)

to support confidentiality, integrity, and availability of data

Organizing System Security

- First steps in security are identifying and authenticating a user
  - Typically through username/password combination
- Third step is to authorize a user for specific access
  - Can be based on roles, security labels, identification, etc.
- Record accesses for later auditing
- OS security functionality is generally layered
  - At least a user layer and a kernel layer
  - The reference monitor that intercepts and authorizes requests is part of the security kernel
  - Kernel programs often have a high privilege level

Built-in Security Subsystems and Mechanisms

- To make installation and use easier, modern operating systems default to low security
  - The process of increasing the security level is called **hardening**
- As operating systems mature, more security functionalities become built in
  - For example, Kerberos ships with current Windows
  - Identification and authentication are mainly generic, the simplest one is username/password, alternatives are smart card or biometric device
  - Proper OS security implementation is more secure and efficient than security layers added on

System Security Principles and Practices

- A secure OS is a result of solid planning
- Security planning starts with understanding potential risks
  - Use risk assessment to determine and rank risks
    - Do not blindly follow "Hardening Your Computer in 10 Easy Steps"
  - Implement controls for important risks (harden the system)
    - A control is a mechanism that limits access to an object
  - Test results of hardening
    - Implemented controls work
    - All functions are operating with the implemented controls (Access is not so restrictive)
  - Train users to understand and use proper security controls

Windows Security Design

- Security model differs among Window products
  - Model described here is for MS Windows server security
- Built on the concept of Active Directory (AD)
  - AD is a directory service data structure allowing easy accessing and addressing of objects across a network
    - Objects are files, folders, shares, or printers
    - Subjects are logically grouped, users, groups, or computers
    - Each object has a discretionary access control list (DACL) that specifies which subjects can access the object
  - AD provides the framework for specifying, storing, addressing, and querying object access information

Windows Security (cont'd)

- The AD database can be physically distributed, no bottlenecks or single points of failure
- Network resources (printers, computers, users, or directory objects, etc.) are grouped in domains
  - Domains can be hierarchically grouped into trees and forests
  - Domains can form direct trust relationships with other domains
- Access rules are specified at the domain level and inherited through groups and individual objects --- easy management: An administrator
  - can apply group attributes to a set of objects
  - only has to maintain the exceptions to the generic access permissions

Windows Security (cont'd)

  - Access conflicts are resolved by giving priority to the most specific rule governing an object
    ex. If Mary is a member of the programmer group, what if Mary is granted to modify *ReadMe.doc*, but the programmer group is not granted. Mary retains her right to write, because the use is more specific than the group.
  - Access conflicts are resolved by giving priority to deny over allow
    ex. Continuing the above example, if the programmer group was specifically denied access to the *ReadMe.doc* file, Mary would not be able to access the file as long as she remains a member of the group.
- Except for the above domain security, local security is specified in local security objects.
- Both domain and local security object attributes are maintained by the Microsoft Management Console (MMC)

Windows Security (cont'd)

- MMC is the primary interface for defining and maintaining **Group Policy** objects.

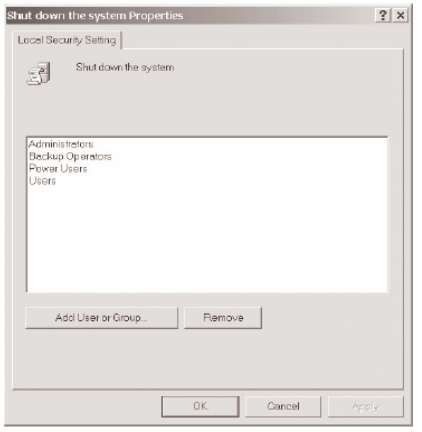
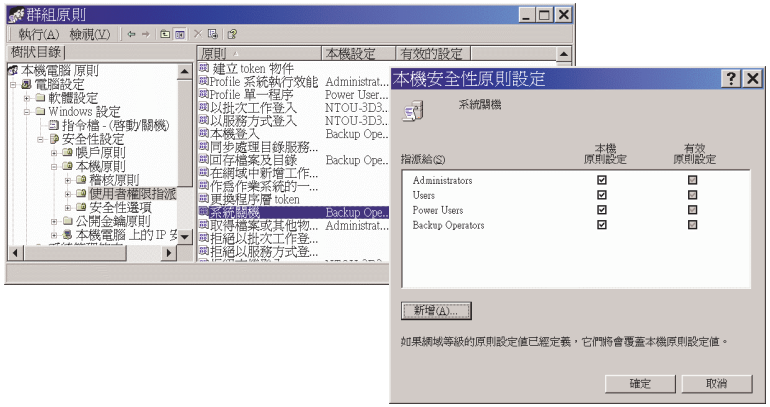


Figure 9.1
Windows XP Local Security Policy setting

Windows Security (cont'd)

- Using gpedit.msc to change group policy directly under windows 2000



UNIX and Linux Security Design

- Basic security is constructed around files
  - Everything is presented as a file (files, directories, devices, processes)
- Understanding file permissions is crucial
- Each file has a mode field
  - 10 character field that specifies type of file and permissions for the owner, group, and world
  - Permission types are read, write, and execute
  - View the mode field using the *ls –l filename* command

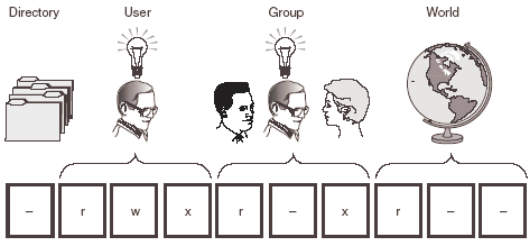


Figure 9.2
UNIX file permissions

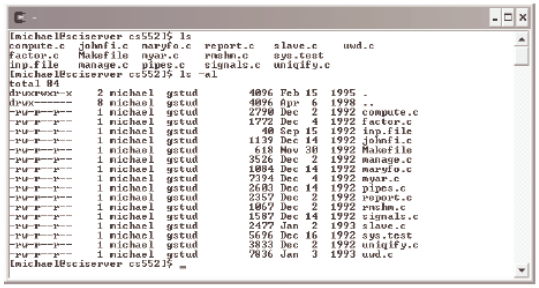


Figure 9.3
UNIX file listing with mode fields

TABLE 9.2 UNIX File Mode Field Components

Position	Values	Description
1	- --Regular file	
	d--Directory	
	l--Symbolic link	
	b--Block special file	
	c--Character special file	The first character of the file mode field indicates the type of the file. These are just some of the various valid file types. There are a few other advanced types. The file type can affect how the permissions are implemented.
2 to 4	r--Read permission	
	w--Write permission	
	x--Execute permission	
	- --No permission	Access permissions for the file's owner. Permissions can be combined; for example, rwx indicates the file's owner can read, write, and execute the file. The permission r-- would allow the user only to read the file.
5 to 7	r--Read permission	
	w--Write permission	
	x--Execute permission	
	- --No permission	Access permissions for users that belong to the group the file is assigned to.
8 to 10	r--Read permission	
	w--Write permission	
	x--Execute permission	
	- --No permission	Access permissions for users who are neither owners of the file nor members of the file's group.

System Backups

- A backup is a complete or partial copy of the system
  - Typically stored on removable media
  - Typically scheduled on a regular basis
- Used to recover from system problems, attacks, disasters, etc.
- Can be a major vulnerability
  - A portable copy of your system is easier to gain access to
  - Usually the access control does not extend to the backup
  - Must be very careful to protect your backups
- Verify the media on which you copy your system
  - Backups on an old or poor quality media may not be restorable

Typical System Security Threats

- Threats come in two forms
  - A subject is given more authorization to access or modify resources than he or she should have
  - Authorized subjects are denied access to resources they should be able to use
- Software bugs are a common security threat
  - Caused by sloppy programming
  - Provide opportunities to attackers by leaving system in an unexpected state, sometimes with high privilege levels
  - Best defense is to have well trained programmers and follow established software development methods
  - There are also some runtime protection environments

System Security Threats (cont'd)

- Back Doors
  - An entry point into a program that bypasses the normal security mechanisms
  - Software developers often include these for easier development and testing
  - Can be used by developer for malicious purposes or discovered by an attacker
  - Formal testing of software should find most back doors.

System Security Threats (cont'd)

- Impersonation or Identity Theft
  - Compromising a password gives an attacker a way to impersonate or hijack a user's identity
  - Users often do not protect their passwords appropriately
  - Insidious because audit logs can't distinguish between the real user and the attacker
  - Defense is to teach users the importance of password security

Keystroke Logging

- A set of methods used to intercept the keystrokes a user enters
- Types of tools
  - Software tools require privilege to install
  - Hardware tools plug into the keyboard
  - A video camera can be focused on the keyboard
- Keystroke logging is used for multiple purposes
  - Testing and quality assurance (replay keystrokes for repetitive tests)
  - Evidence collection when inappropriate activity is suspected
  - Malicious attacks when an attacker is able to compromise security

Well-Known OS Risks

- Attackers are well aware of the security vulnerabilities in every operating system
- The SANS/FBI Twenty Most Critical Internet Security Vulnerabilities is an up-to-date list of known vulnerabilities for Windows and UNIX operating systems
- Current lists along with detailed descriptions of the vulnerabilities are available at http://www.sans.org/top20/

Well-Known Windows Risks

- The top three Windows vulnerabilities are:
  - Internet Information Services (IIS), Microsoft's Web server
    - Vulnerable to unexpected requests and buffer overflows
    - Sample users and applications are often unprotected after installation
  - Microsoft Data Access Components (MDAC) – Remote Data Services
    - Older versions only allow attackers to run commands locally with administrator privilege
  - Microsoft SQL Server
    - Attackers can access database contents because of issues with open ports and insecure default users and sample applications

Well-Known UNIX Risks

- The top three UNIX vulnerabilities
  - Remote Procedure Calls (RPCs)
    - Allow an attacker to get access to root privilege on a remote computer
  - Apache Web Server
    - Generally considered more secure than IIS, but still has possible vulnerabilities if not configured carefully
  - Secure Shell (SSH)
    - SSH is considered much more secure than alternatives, but still requires careful configuration and does contain some software vulnerabilities

System Forensics: Scanning and Footprinting

- Security administrators should regularly assess the current status of a computer by locating and analyzing stored status data
- Computer forensics is the process of searching for evidence of a specific activity by searching log files and file systems
- System footprinting (or baselining) is a "snapshot" of the computer at a particular point in time for comparison purposes
  - Often first done immediately after a computer is brought online

The Security Auditor's Role

- The security auditor and the security administrator should be different people
- The security auditor's job is
  - To validate the effectiveness of controls being used to mitigate threats
  - To ensure compliance with the controls
  - To ensure that legal requirements are satisfied
- The existence of formal auditing can be important in any legal proceedings related to computer security

Assessing Security Risks

- Risk assessment is the process of identifying potential risks and ranking them
- To assess risks
  - Start with a list of the assets that must be protected
  - Rank the importance of the assets
  - Create a list of events that could cause data loss, whether from natural, man-made, or malicious causes
    - Make sure to include management in this process
  - Determine which threats can be reasonably addressed
  - Determine risk priorities using quantitative and qualitative risk analysis techniques

Summary

- Modern operating systems perform four basic security functions: identify users, restrict access to authorized resources, record user activity, and ensure proper communications
- Security functionality is located in the security kernel
  - Kernel programs often run with high levels of privilege
- Hardening is the process of increasing an O.S. security level
- Windows server security is built on the Active Directory concept

Summary (cont'd)

- UNIX and Linux systems use the concept of files and file permissions for security
  - Each resource has a mode field specifing permissions
- System backups provide insurance against data loss but are physically highly vulnerable to theft and loss
- Three common types of security threats are software bugs, back doors, and impersonation or identity theft
- OS vulnerabilities are well documented for both attackers and security administrators

Summary (cont'd)

- Baselining or system footprinting is a technique for creating a system "snapshot" for comparison purposes
- Computer forensics is the process of searching for evidence of a specific activity
- A security auditor should regularly review the security controls and compliance of an organization
- Risk assessment is the process of identifying the specific security threats that must be addressed within an organization

Assignments

- Reading: Chapter 9
- Practice 9.17 Challenge Questions

- Turn in Challenge Exercise 9.1 next week