Operating Systems Security

Information Security Principles

tgeng@email.sc.edu

September 22, 2021

Security in Operating System

- The operating system is the fundamental controller of all system resources, which makes it a primary target of attack, as well.
- Protection levels:
  - Physical
  - Human, social engineering
  - Operating system
  - Programs
  - Network

Operating System Structure

An operating system is an executive or supervisor for a piece of computing machinery. The operating systems are not just for conventional computers:

- a dedicated device
- an automobile, an airplane
- a smartphone, tablet
- a network appliance

A Bit of History

- Single User
- Multiprogramming and Shared Use
- Time Slicing
- Priority
- Multiple Cores

Protected Objects

- memory
- sharable I/O devices
- serially reusable I/O devcies
- sharable programs and subprocedures
- networks
- sharable data

Tools to Implement Security Functions

- Access Control
- Audit
- Virtualization
- Sandbox
- Separation and Sharing
- Hardware Protection of Memory
- Virtual Memory

Virtualization

Virtualization can present a user the appearance of a system with only the resources the user is entitled to use.

- Hardware Virtualization
- Software Virtualization
- Storage Virtualization
- Network Virtualization
- Desktop Virtualization

Virtual Machine

The virtual machine runs as a process in an application window, similar to any other applications, on the operating system of the physical machine.

- Process VM: allows a single process to run as an application on a host machine, providing platform-independent programming environment by masking the information of the underlying hardware or operating system.
- System VM: it is fully virtualized for a physical machine, runs like another individual physical machine.

Advantages and Disadvantages of VM

Advantages:

- VMs can run multiple operating system environments on a single physical computer, saving physical space, time and management costs.
- Virtual machines support legacy applications, reducing the cost of migrating to a new operating system.
- VMs can also provide integrated disaster recovery and application provisioning options.

Disadvantages:

- Running multiple virtual machines on one physical machine can result in unstable performance if infrastructure requirements are not met.
- Virtual machines are less efficient and run slower than a full physical computer.

Hypervisor

A hypervisor is also called virtual machine monitor, is the software that implements a virtual machine. It receives all user access requests, directly passes along those that apply to real resources the user is allowed to access, and redirects other requests to the virtualized resources.

Sandbox

- A sandbox is an environment from which a process can have only limited controlled impact on outside resources. As its name implies, the sandbox is a protect environment in which a program can run and not endanger anything else on the system.
- While virtual machines virtualize the hardware to create a “computer”, sandbox only packs up just a single app along with its dependencies. Since it doesn’t need the installation of multiple guest operating system, so it’s more lightweight.

Honeypot

- Honeypot's most important feature is faux and intention to lure an attacker.
- There is no definition that how the honeypot should be build, we can use virtual machine to build one honeypot, we can even use one separate server to build one.
- Attackers can be monitored and controlled.

Separation and Sharing

The basis of protection is separation, it means keeping one user's objects separate from other users.

- Physical separation, by which different processes use different physical objects
- Temporal separation, by which processes having different security requirements are executed at different times
- Logical separation, by which users operate under the illusion that no other processes exist
- Cryptographic separation, by which processes conceal their data and computations in such as way that they are intelligible to outside processes

Hardware Protection of Memory

- Memory can be used to share data
- Protection
  - protect the memory spaces of different guest machines in one host machine
  - protect the memory of different users in one operating system
  - even in a single user operating system, the memory spaces of different processes need to be protected from the interfere of each other

Fence

The simplest form of memory protection was introduced in single-user operating system, to prevent the faulty user program from destroying part of the resident portion of the operating system.

Fence Register

Fence register indicates the end address of the memory used by operating system.

Fence

Disadvantages:

- It cannot handle the multiple user operating system
- If one program occupies all the available memory by exploring where is the fence register, then the operating system could not declare new memory space anymore

Base/Bounds Registers

Lower bound is called base register and the upper bound is called bounds register. The memory space between the base register and the bounds register are the memory space for the user's program.

Base/Bounds Registers Problem

Base/Bounds registers imposes one problem that is the memory space of one user's program and data are contiguous. The permission control is not flexible.

Tagged Architecture

Every word of machine memory has one or more extra bits to identify the access rights to that word.

Virtual Memory

- Segmentation
- Paging

Segmentation

Segmentation allows hardware-supported controlled access to different memory sections in different access modes. In other words, a program will be divided into several pieces having different access rights.

`<MAIN, 0x1334>`, name and offset

A Segment Translation Table which contains all these names and offsets is maintained by the operating system.

Advantages of Segmentation

- The OS can place any segment at any location and move any segment to any location, even after the program starts to run
- A segment can be removed from main memory if it is not bing used currently and placed in the hard disk temporarily
- Every address reference should pass through the OS, this central management gives OS opportunity to check the protection or extra processing

Paging

- Paging is similar to segmentation, but all pages are of the same fixed size
- Paging is helpful on fixing the problem of fragmentation

Linux Security Model

- Linux File System Security
- Linux Security Module

Linux File System

- In Linux, almost everything is a file
- I/O device is accessed via a “special” file
  - `/dev/cdrom` points to optical driver, and `/dev/sda`, `/dev/nvme0` point to the hard drives
- Have other special files like named pipes, a conduit between processes or programs
- Since everything is a file, so security is very important.

Users and Groups

- Users and Groups are not files
- users
  - someone or something capable of using files
  - can be human or process
  - `lpd` (Linux Printer Daemon) runs as user lp
- groups
  - list of user accounts
  - user's main group membership specified in `/etc/passwd`
  - user can be added to additional group by editing `/etc/group`
  - command line: `useradd`, `usermod`, `userdel`

Understanding `/etc/passwd`

`andy:x:1021:1020:CSCE stud:/home/andy:/bin/bash`

- `andy`: username. Used when user logs in, it should be between 1 and 32 characters in length
- `x`: password. An `x` character indicates that encrypted password is stored in `/etc/shadow` file.
- `1021`: user ID (UID). Each user must be assigned a user ID.
  - UID 0 is reserved for root
  - UID 1-99 are reserved for other predefined accounts such as `lp`, `svn`, `sshd`, and `mysql`
  - UID 100-999 are reserved by system for administrative and system accounts
- `1020`: group ID (GID). The primary group ID, which is stored in `/etc/group` file
- `CSCE stud`: user ID info. The comment field. Allows you to add extra information about the users such as user's full name, phone number.
- `/home/andy`: home directory. The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes `/`.
- `/bin/bash`: which shell is used. The absolute path of a shell. Sometimes, it can be a command instead of a shell when the user doesn't have to login.

Snapshot of `/etc/group`

`CSCE522:x:1020:andy,peter`

- `CSCE522`: name of the group
- `x`: generally password not used, hence it is empty or blank. It can store encrypted password, useful to implement privileged groups
- `1020`: group ID (GID). Group ID must be assigned to every user.
- `andy,peter`. List of user names of users who are members of the group. The user names must be separated by commas.

File Permission

- Every file or folder in Linux has three types of access permissions
  - read (R), write (W), execute (X)
- permission defined by three types of users
  - owner of file, group that owner belongs to, others

```
-rw-rw-r-- 1 root root 118 Mar 25 01:38 config.yml
```

The file permission can be modified by `chmod`,

- `chmod u+x .config`
- `chmod g=x .config`
- `chmod o-x .config`
- `chmod a+x,g-w .config`
- `chmod 777 .config`

Directory Permission

```
drw-rw-r-- 1 root root 353 Mar 25 01:38 .config
```

Security Module

DAC is used in original Unix

- AppArmor
- SELinux
- Smack
- TOMOYO Linux
- Yama