OS Security I: Principles

Chengyu Song

Slides modified from John Mitch and Dawn Song
• Lab2
  • Make sure your exploit is robust, we will test to see if it works on our machine
• Midterm quick review
Overview of OS security

• Problems
  • An application may be a malware
  • A benign software can be compromised and becomes malicious

• Goal: how can we still protect the system?

• Approach: security system architecture that follows a set of basic design principles
Principles of secure design

• Compartmentation
  • Isolation
  • Principle of least privilege

• Access control
  • Complete mediation, tamper proof, correctness

• Defense in depth

• Keep it simple
First idea: compartmentation

http://staff.imsa.edu/~esmith/treasurefleets/treasurefleets/watertight_compartments.htm
Compartmentation you have seen

- In ships
- In buildings
- At home

What was the first concept you learn in the OS class?
Isolation

- Mechanisms to enforce the separation
  - Reference monitor
- Hardware reference monitors
  - Examples?
- Software reference monitors
  - Examples?
Principle of least privilege

- Privilege
  - Ability to access or modify a resource
- Principle of **Least Privilege**
  - A system module should only have the *minimal* privileges needed for intended purposes
Monolithic design

System

Network
User input
File system

Network
User device
File system
Problem of monolithic design
Problem of monolithic design
Software compartmentation

- Identify components of the program
- Identify privileges required by each component
- Group components based on privileges
- Separate and isolate
- Enforce least privilege
Examples

• Web Browsers
• Microkernels
Secure browser with compartmentation
Microkernel

Monolithic Kernel based Operating System

- Application
- VFS
- IPC, File System
- Scheduler, Virtual Memory
- Device Drivers, Dispatcher, ...

Hardware

Microkernel based Operating System

- Application IPC
- UNIX Server
- Device Driver
- File Server

Basic IPC, Virtual Memory, Scheduling

Hardware

https://en.wikipedia.org/wiki/Microkernel
Caveats

• Performance degradation
  • Why?

• Inter-component interface design
  • Why we need Inter-component communication?
  • What can go wrong?
For next class ...

• OS Security II: Access Control