

University of Rochester
CSC290B
Introduction to Computer Security

Protection in
Operating Systems

January 22, 2009

Operating system functions

- Operating systems use hardware-enforced protection mechanisms to define protected objects, providing functions including:
 - Access control
 - Identity and credential management
 - Integrity protection and audit functions

Protected resources

- A robust multiprogrammed system requires controlled sharing of a number of resources:
 - Memory
 - Constantly shared devices (e.g. disks)
 - Serially shared devices (e.g. printers, tape drives)
 - Shared programs
 - Shared data (e.g. records, files, filesystems)
 - Networks

Types of separation

- Physical separation
 - E.g. separate devices user for output requiring different levels of security
- Temporal separation
- Logical separation
 - Access constrained to give impression of isolation of resources from other processes
- Cryptographic separation
 - Objects are concealed by being rendered unintelligible to outside processes

Levels of protection

- No protection
- Isolation
- Share all or share nothing
- Share via access limitation
- Share by capabilities
- Limit use of objects

Memory protection

- Roughly historical progression:
 - Relocation
 - Base & bounds registers
 - Tagged architecture
 - Memory locations include extra bits defining access rights
 - Segmentation and paging
 - Translation tables with location and protection attribute information

Privileged states

- A minimal mechanism for creation of protected objects:
 - An unprivileged state without uncontrolled access to dangerous system resources
 - A privileged state in which protected objects and dangerous system resources can be accessed
 - Enforced boundary crossings between privilege states, allowing controlled parameter checking (e.g. a “system call”)

More general access control

- Ring-based access control (e.g. Multics):
 - Data segments (data or procedure) have:
 - Access rights (e.g. read, write, execute, append)
 - Protection rings (numbered 0 to 63)
 - Procedures can cross ring boundaries
 - Lower rings are higher privilege; kernel resides in ring 0
 - Ring crossings cause faults that trap to kernel, to check arguments
 - Fault behavior depends on segments' call brackets and access brackets
 - Multics implements the same mechanism for segments on disk or segments in memory

Access control mechanisms

- Access control lists (ACLs)
- Capabilities

Access Control Lists

- List of (subject, rights) tuples
 - Subjects such as user IDs or file owners
 - Rights such as Read, Write, Execute, Modify
- Subjects could be groups
- Lists may include wildcards and have implicit processing order

Capabilities

- Capabilities are unforgeable credentials that are used to enable or control subsequent access
- Unforgeable by:
 - Hardware tagging of individual capabilities
 - State maintenance outside of user control (e.g. lists maintained by kernel and accessed by system call)
 - Unix file descriptors are a special case: local meaningless names (integers), copying them only effective with kernel assistance
 - Cryptographic means (large embedded unpredictable fields)

Introduction to Trusted Operating System Design

- Security Kernel enforcing security mechanisms
 - Reference Monitor
 - Tamperproof
 - Can't be bypassed
 - Analyzable
- Trusted Computing Base (TCB):
 - Hardware
 - Capabilities
 - Interrupt handling, clocks, timers
 - Basic Operations
 - Primitive I/O

Mandatory Access Control

- Discretionary Access Control (DAC):
 - Subjects can set security policies or treatment of individual objects
- Mandatory Access Control (MAC):
 - Policy is not under the control of subjects

Example: Palladium

- Microsoft & Trusted Computing Alliance
- Trusted Computing Platform / Trusted Platform Module (TPM)
 - Defines a standard for embedded hardware for checking authenticity of certain system components, *e.g.*:
 - Can result in a secure boot loader invulnerable to boot sector corruption attacks
 - Can provide a secure key storage facility for access to encrypted filesystems (Microsoft BitLocker)
 - Can implement Digital Rights Management (DRM) checking.