Lecture 10: Access Control in General-Purpose OSs

Summary

We provide an overview of memory and general object protection in general-purpose OSs. This lecture follows P&P, Sections 4.3 and 4.4.

Memory and Address Protection

Reference: P&P, Section 4.2

Goals of memory protection

Techniques

Fences

Base/Bounds Registers

Tagging

Segmentation

Paging

Paging with Segmentation

Case Study: Intel IA-32 real-address mode (*Intel 64 and IA-32 Architectures: Software Developer's Manual*, Volume 3B, Chapter 20)

Protection of General Objects

Reference: P&P, Section 4.4

Access Control Matrix

Directory

Access Control List (Example: ACLs in the Andrew File System)

Role-Based Access Control (RBAC; Example: ANSI RBAC Model)

Capability (Example: Kerberos)

Exercises

P&P, Chapter 4, Exercises 1 - 21.

Describe the memory models and protection schemes available for the Intel 64 and IA-32 “protected mode.” See *Intel 64 and IA-32 Architectures: Software Developer’s Manual*, Volume 3A, Chapters 3 - 5.

When running Linux on an Intel architecture, which memory model and protection schemes does it use?