

OPERATING SYSTEMS

Timothy Hnat

Department of Computer Science
University of Virginia

Sept 17, 2007



PROTECTION

- What are the goals of protection?



PROTECTION

- What are the goals of protection?
 - Prevent mischievous, intentional violation of an access restriction
 - Each program component uses system resources according to the stated policies



PROTECTION

- What is the difference between a Policy and a Mechanism?



PROTECTION

- What is the difference between a Policy and a Mechanism?
 - Policy: Determine what will be done (These will change with time)
 - Mechanism: Determine how something will be done



PROTECTION

- What is the principle of least privilege?



PROTECTION

- What is the principle of least privilege?
 - Dictates that programs, users, and even system be given just enough privileges to perform their tasks.



PROTECTION

- What is an access matrix? How does it work?



PROTECTION

- What is an access matrix? How does it work?
 - Its rows represent domains and the columns represent objects.
 - Each cell contains access rights.



PROTECTION

- What is the confinement problem and how do we solve it?



PROTECTION

- What is the confinement problem and how do we solve it?
 - The confinement problem is a guarantee that no information initially held in an object can migrate outside of its execution environment.
 - In general, it is unsolvable



PROTECTION

- What are the ways to implement an access matrix?



PROTECTION

- What are the ways to implement an access matrix?
 - Global Table
 - Access Lists for Objects
 - Capability Lists for Domains
 - Lock-Key Scheme - Objects have bit patterns called locks and domains have bit patterns called keys. Only if the key matches the lock is access granted.



PROTECTION

- What are some of the problems with revocation of access rights



PROTECTION

- What are some of the problems with revocation of access rights
 - Immediate versus delayed
 - Selective versus general (All the users of an object or just a subset?)
 - Partial versus total
 - Temporary versus permanent



PROTECTION

- Revocation of capabilities



PROTECTION

- Revocation of capabilities
 - Reacquisition
 - Back-pointers (Must follow all pointers to access rights)
 - Indirection (Contains pointers)
 - Keys



LANGUAGE BASED PROTECTION

- How can we do language based protection?



LANGUAGE BASED PROTECTION

- How can we do language based protection?
 - Compiler enforcement
 - Protection is simply declared
 - Requirement can be stated independently
 - Enforcement need not be provided by the designer of a subsystem
 - Declarative notion is natural



LANGUAGE BASED PROTECTION

- What are the relative merits of enforcement based solely on a kernel as opposed to enforcement provided largely by a compiler?



LANGUAGE BASED PROTECTION

- What are the relative merits of enforcement based solely on a kernel as opposed to enforcement provided largely by a compiler?
 - Security (Compiler is responsible. What about a new compil?)
 - Flexibility (The kernel limits the user-defined policy)
 - Efficiency (Best when provided by the hardware. Language based states can be verified offline)



REAL-TIME SYSTEMS

- Define real-time systems



REAL-TIME SYSTEMS

- Define real-time systems
 - Hard real-time systems provide guarantees that a process will complete before its deadline
 - Soft real-time systems provide best effort and ensure that real-time tasks receive priority.



REAL-TIME SYSTEMS

- What types of memory systems are in real-time systems?



REAL-TIME SYSTEMS

- What types of memory systems are in real-time systems?
 - Typically: real-addressing modes only (Hard real-time)



MULTIMEDIA SYSTEMS

- Real-time streaming
- Progressive download
- On-demand streaming
- File systems may require many terabytes of storage



MULTIMEDIA SYSTEMS ISSUES

- Compression and decoding
- Multimedia tasks must have scheduling priorities
- File systems must meet the rate requirements of continuous media
- Network protocols must support bandwidth requirements while minimizing delay and jitter

