TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science Institute for System Architecture, Operating Systems Group

Protection and the Control of Information Sharing in Multics

Paper Reading Group
Presentation by Stefan Kalkowski

Dresden, 2006-12-06

MULTICS - an ambitious project

- Multiplexed Information and Computing Service (1964-2000)
- Goals: 100% reliability and scalability, multi-purpose system
- Power plant notion
- PL/1 instead of machine language
- Virtual memory (segmentation and paging)
- Dynamic linking

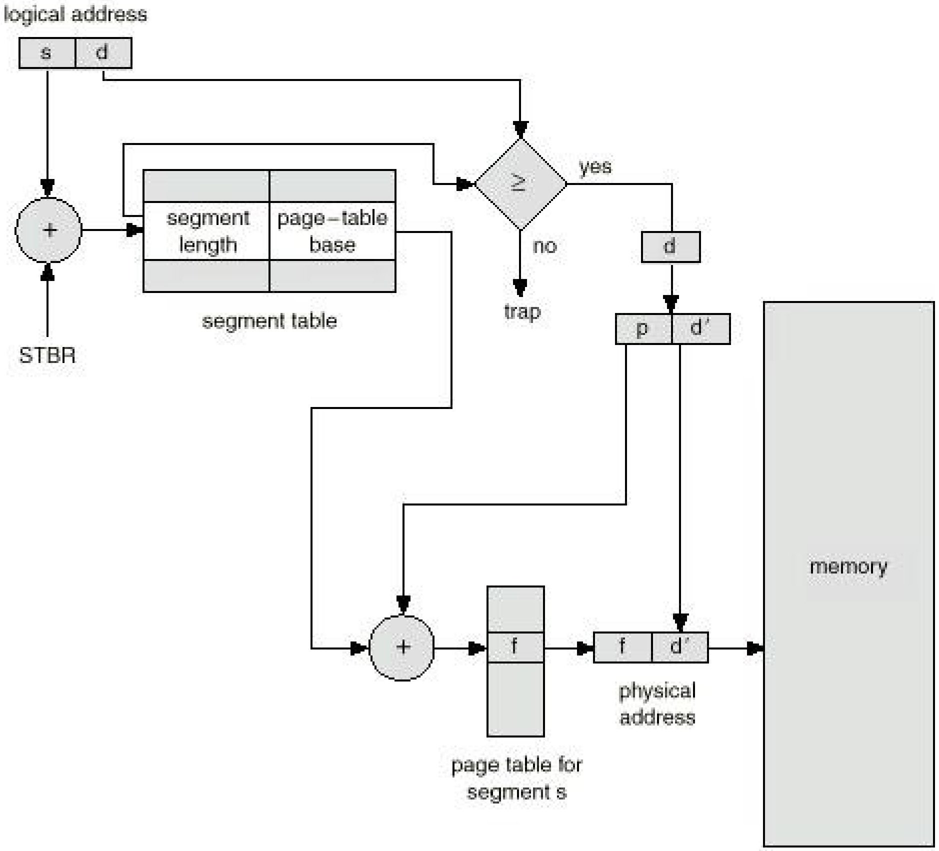
Security design principles

- Permission vs. exclusion
- Check every access to every object
- Open design
- Principle of least privilege
- Usability of protection mechanisms
- *Decentralization of protection specifications*
- *Support of protected subsystems*

Storage system

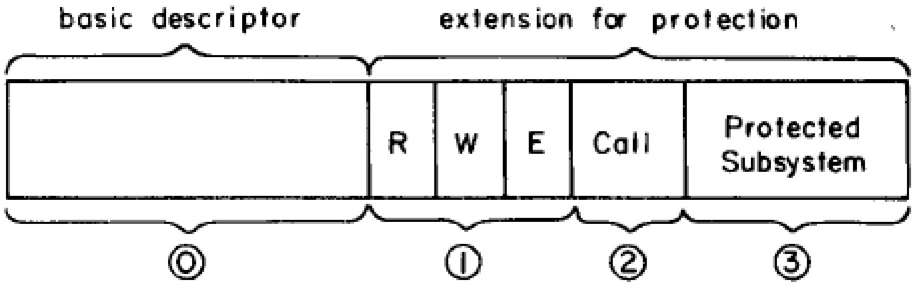
- Hierarchical structured
- “Everything is a segment”
- Open-ended ACLs per segment
- Access mode: *r, rw, re, rew, none*
- ID: *principal#project#compartment*
- Initial ACLs per directory
- Trap extension for flexible access control

Memory Model



Primary memory protection

- Hardware segmentation and rings of protection
- A segment descriptor (SD) contains: read, write and execute flags
- Every SD has an own ring number
- For “ring downgrading” a gate extension and gate list resides in a SD



Further notes

- For sandboxes use protected subsystems
- Immediate revocation through back-pointers
- Supervisor uses descriptor segments itself
- All authentication happens interactively

Weaknesses (out of the paper)

- “Complex TCB”, ~ 300 modules (~6000 LOC) *(partially results from ring software emulation)*
- Proposal: argument-range checking hardware
- Complexity of the user interface (price of high flexibility)
- Overprivileged system administrator in the actual implementation
- IDS and Honeypots are missing

Questions

- Science fiction useful?
- Supervisor really to complex?
- Immediate revocation, is it practical?
- Segmentation and clean virtual memory