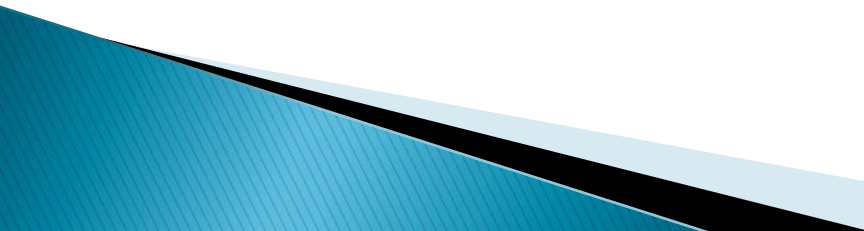


# Hardware Protection Schemes

Presented by:  
Aaron Polley

# Outline

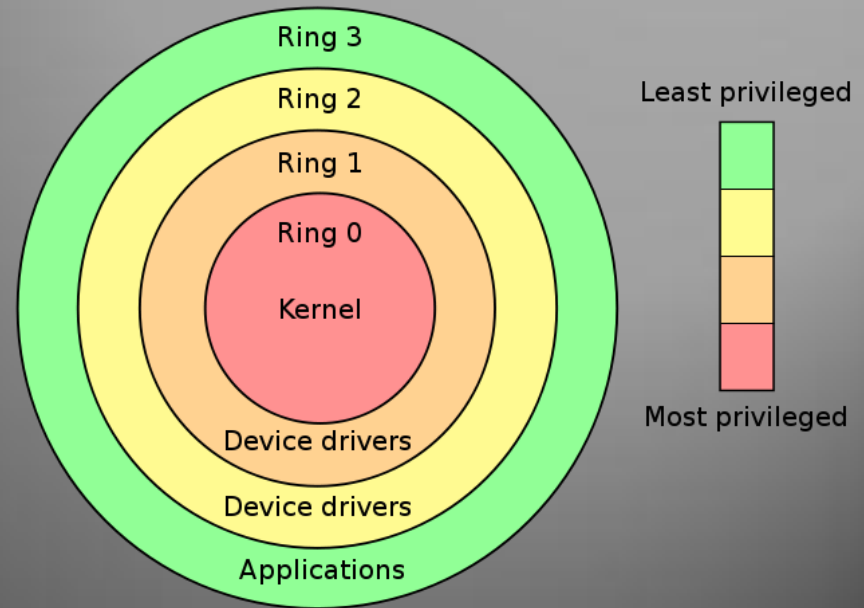
- ▶ Introduction
    - What are hardware protection schemes?
    - Why are they Important?
  - ▶ CPU Privilege Rings
    - What are they?
    - What do they do?
  - ▶ Memory management Unit (MMU)
    - What does this allow us to do?
  - ▶ Why use the MMU?
  - ▶ Conclusion
- 

# Introduction

- ▶ What are Hardware Protection Schemes?
  - They are Hardware Implemented
  - They Provide Physical protection
- ▶ Why are Hardware Protection Schemes Important?
  - Security
  - Protection
  - Communication

# CPU Privilege Rings

- ▶ What can these rings be used for?
- ▶ Commonly used
  - Ring 0
    - Full Privileges
    - Code can access everything
  - Ring 3
    - Restricted Privileges
    - Code must request the use of hardware
- ▶ Uses of:
  - Ring 0
    - Operating System Kernel
    - Drivers
  - Ring 3
    - User Applications
- ▶ Communication between Rings
  - System calls
  - Shared memory
- ▶ Why use rings?



# Memory Management Unit

- ▶ Uses of the Memory Management Unit (MMU)
  - Needed to use Privilege rings
- ▶ How does it work
  - Physical memory is mapped to a virtual table
  - These Virtual mappings
    - Tell the CPU what memory can be accessed and by who
    - Tell the CPU where the data is physically located

Physical Memory	
00x	H E L L
01x	R L D !
02x	O W O
03x	H A V E
04x	F U N
05x	L O T
06x	S O F
07x	; - )

Process A			
Page Table		Virtual Memory	
00x	00	00x	H E L L
01x	02	01x	O W O
02x	01	02x	R L D !
03x	n.a.	03x	#####
04x	n.a.	04x	#####
05x	07	05x	; - )

Process B			
Page Table		Virtual Memory	
00x	03	00x	H A V E
01x	05	01x	L O T
02x	06	02x	S O F
03x	04	03x	F U N
04x	n.a.	04x	#####
05x	07	05x	; - )

# Why use the MMU?

- ▶ Allows multiple applications to run by
  - Separating applications in memory
    - Applications are only able to access their data
  - Making the best use of the available memory
    - Data can be stored seemingly randomly in memory
  - Allows paging memory out to the Hard Drive

Physical Memory	
00x	H E L L
01x	R L D !
02x	O W O
03x	H A V E
04x	F U N
05x	L O T
06x	S O F
07x	; - )

Process A			
Page Table		Virtual Memory	
00x	00	00x	H E L L
01x	02	01x	O W O
02x	01	02x	R L D !
03x	n.a.	03x	#####
04x	n.a.	04x	#####
05x	07	05x	; - )

Process B			
Page Table		Virtual Memory	
00x	03	00x	H A V E
01x	05	01x	L O T
02x	06	02x	S O F
03x	04	03x	F U N
04x	n.a.	04x	#####
05x	07	05x	; - )

# Conclusion

- ▶ Memory and CPU work together to
  - Provide Protection for
    - Operating System Kernel
    - Drivers
    - Other application memory
- ▶ System is protected
  - From Malicious applications
- ▶ Single setup with runtime modification
  - Setup by the operating system at boot
  - Setup only once and then amended as more programs start running

# Thank You!

Contact: [webmaster@germsoft.com](mailto:webmaster@germsoft.com)