CISC 3320

C30b Protection Ring

Hui Chen

Department of Computer & Information Science

CUNY Brooklyn College

Acknowledgement

- These slides are a revision of the slides provided by the authors of the textbook via the publisher of the textbook

Outline

- Concept of Protection Rings
- Examples of Protection Rings

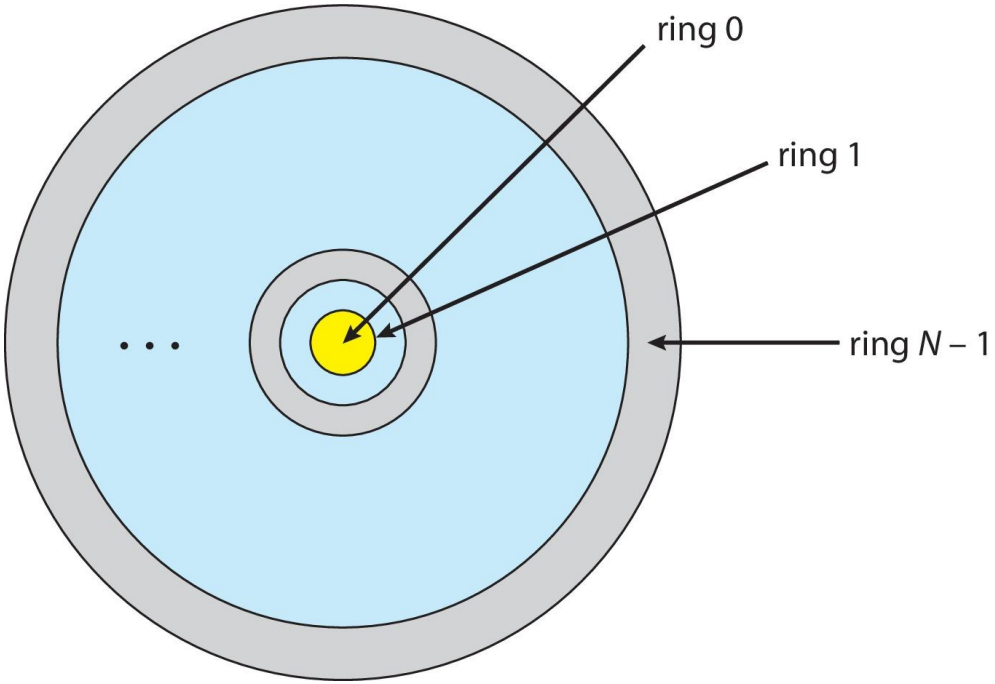
- Role-based Access Control
- Mandatory Access Control (MAC)
- Capability-Based Systems
- Other Protection Implementation Methods
- Language-based Protection

Protection Domain and Hierarchy

- Rings of protection separate functions into protection domains and order them hierarchically
- Let D_i and D_j be any two protection domains
- If $j < i \Rightarrow D_i \subseteq D_j$

Protection Rings

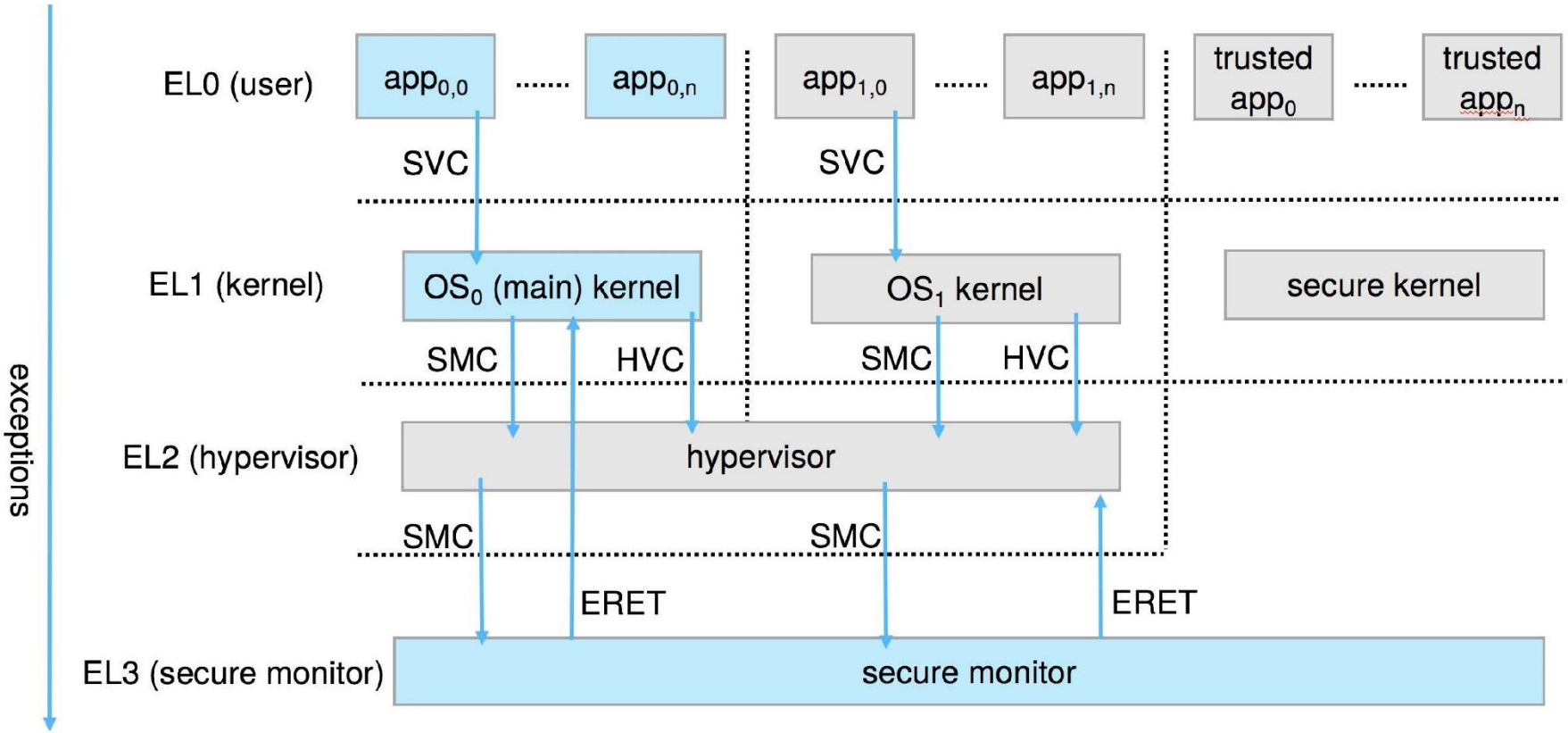
- Let D_i and D_j be any two domain rings
- If $j < i \Rightarrow D_i \subseteq D_j$



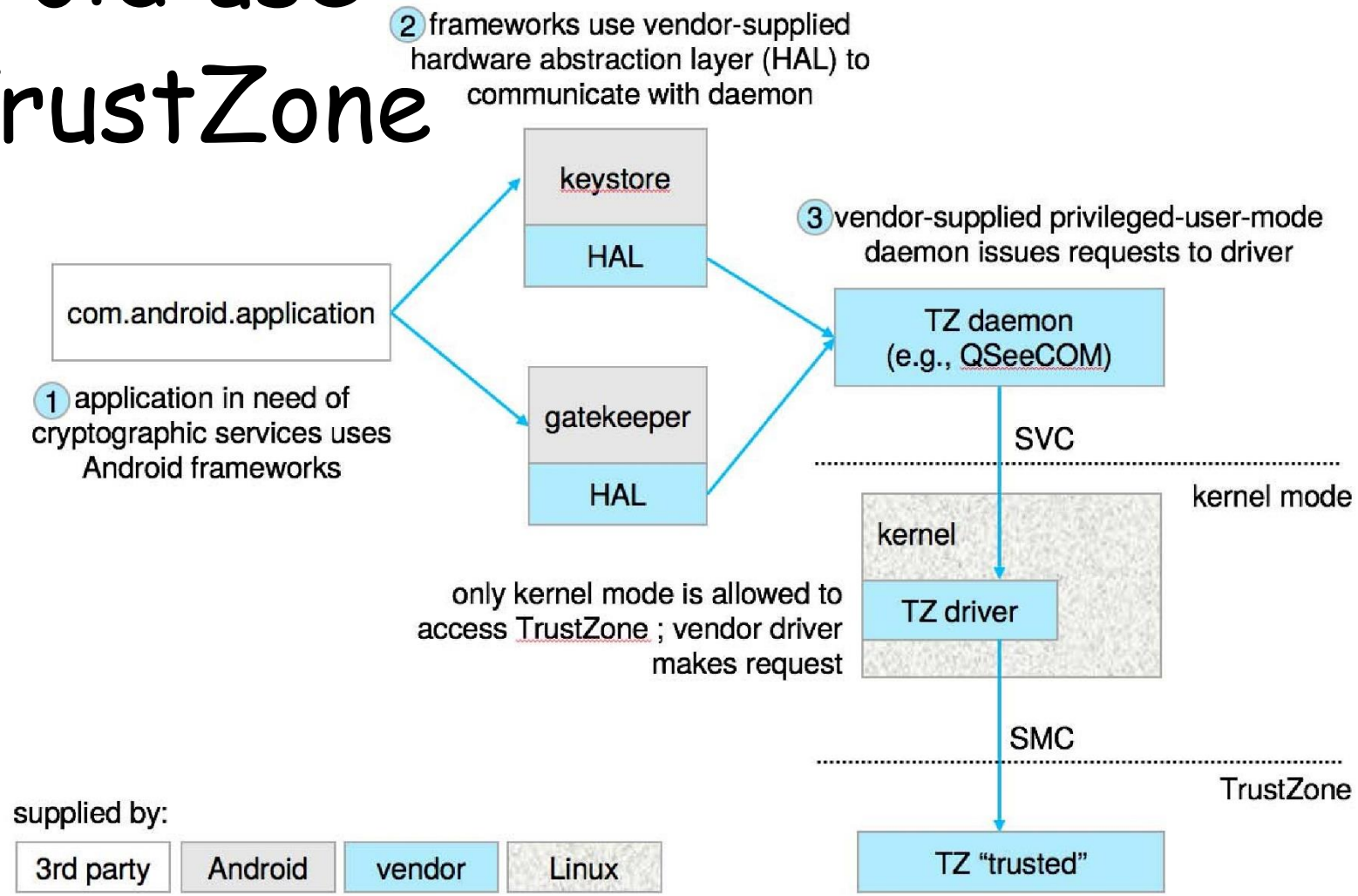
Protection Rings: Examples

- The kernel is in one ring and user applications in another
  - This privilege separation requires hardware support
  - Gates used to transfer between levels
    - e.g., the syscall Intel instruction
  - Also traps and interrupts
- **Hypervisors** introduced the need for yet another ring
- ARMv7 processors added **TrustZone**(**TZ**) ring to protect crypto functions with access via new **Secure Monitor Call** (**SMC**) instruction
  - Protecting NFC secure element and crypto keys from even the kernel

ARM CPU Architecture



Android use of TrustZone



Questions?

- Concept of protection rings
- Examples of protection rings
  - ARM and Android