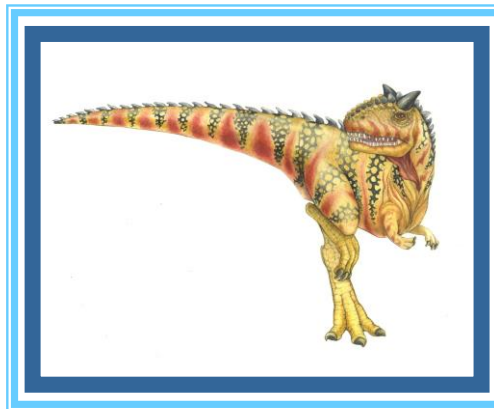
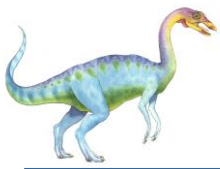


# Chapter 17: Protection

---



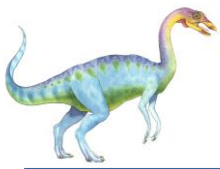


# Chapter 17: Protection

---

- Goals of Protection
- Principles of Protection
- Protection Rings
- Domain of Protection
- Access Matrix
- Implementation of Access Matrix
- Revocation of Access Rights
- Role-based Access Control
- Mandatory Access Control (MAC)
- Capability-Based Systems
- Other Protection Implementation Methods
- Language-based Protection





# Objectives

---

- Discuss the goals and principles of protection in a modern computer system
- Explain how protection domains combined with an access matrix are used to specify the resources a process may access
- Examine capability and language-based protection systems
- Describe how protection mechanisms can mitigate system attacks



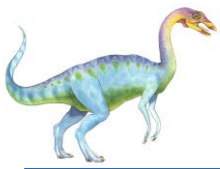


# Goals of Protection

---

- In one protection model, computer consists of a collection of objects, hardware or software
- Each object has a unique name and can be accessed through a well-defined set of operations
- Protection problem - ensure that each object is accessed correctly and only by those processes that are allowed to do so

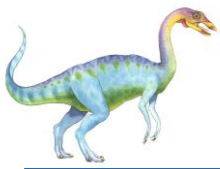




# Principles of Protection

- Guiding principle – **principle of least privilege**
  - Programs, users and systems should be given just enough **privileges** to perform their tasks
  - Properly set **permissions** can limit damage if entity has a bug, gets abused
  - Can be static (during life of system, during life of process)
  - Or dynamic (changed by process as needed) – **domain switching, privilege escalation**
  - **Compartmentalization** a derivative concept regarding access to data
    - ▶ Process of protecting each individual system component through the use of specific permissions and access restrictions





# Principles of Protection (Cont.)

---

- Must consider “grain” aspect
  - Rough-grained privilege management easier, simpler, but least privilege now done in large chunks
    - ▶ For example, traditional Unix processes either have abilities of the associated user, or of root
  - Fine-grained management more complex, more overhead, but more protective
    - ▶ File ACL lists, RBAC
- Domain can be user, process, procedure
- **Audit trail** – recording all protection-orientated activities, important to understanding what happened, why, and catching things that shouldn't
- No single principle is a panacea for security vulnerabilities – need **defense in depth**

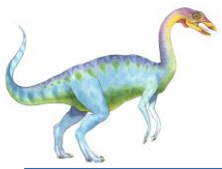




# Protection Rings

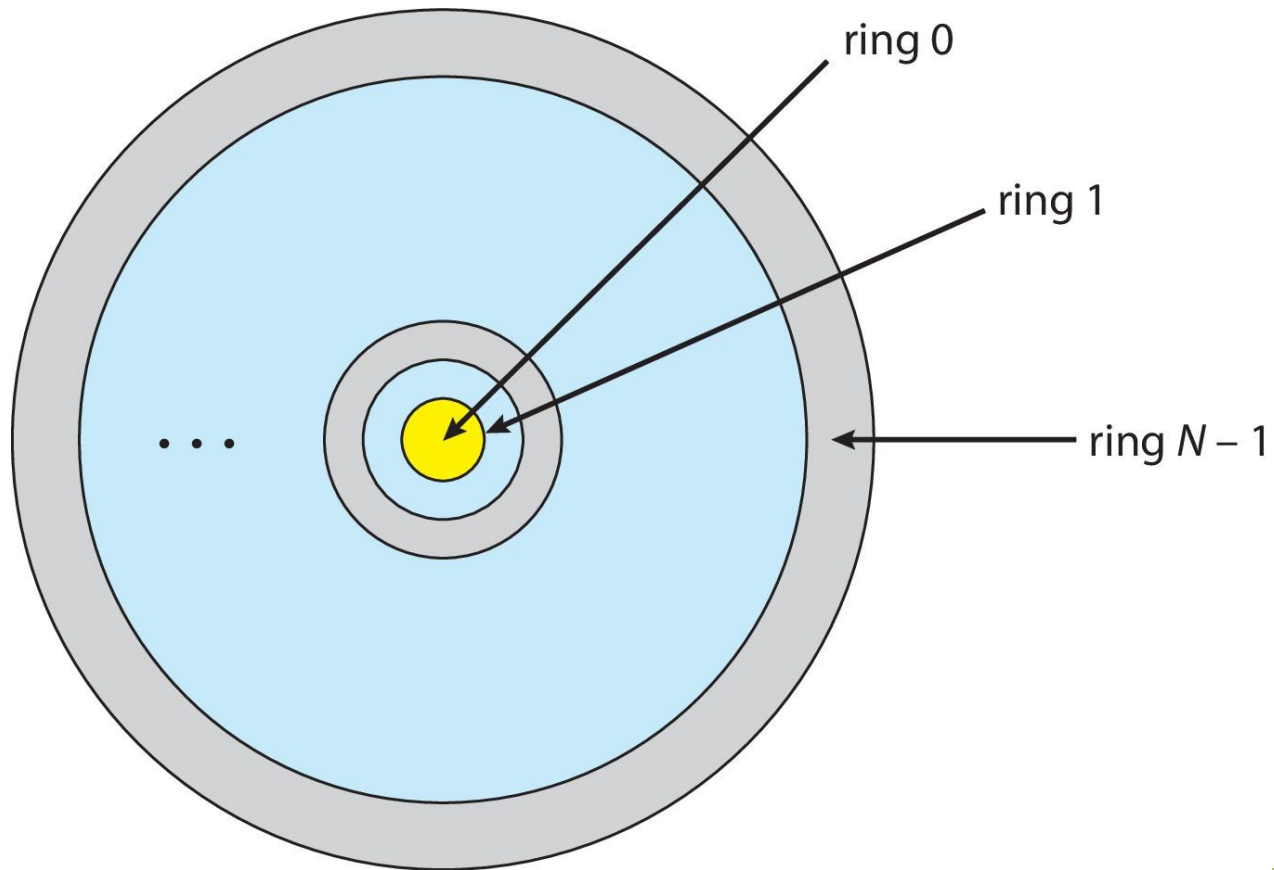
- Components ordered by amount of privilege and protected from each other
  - For example, the kernel is in one ring and user applications in another
  - This privilege separation requires hardware support
  - Gates used to transfer between levels, for example the syscall Intel instruction
  - Also traps 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





# Protection Rings (MULTICS)

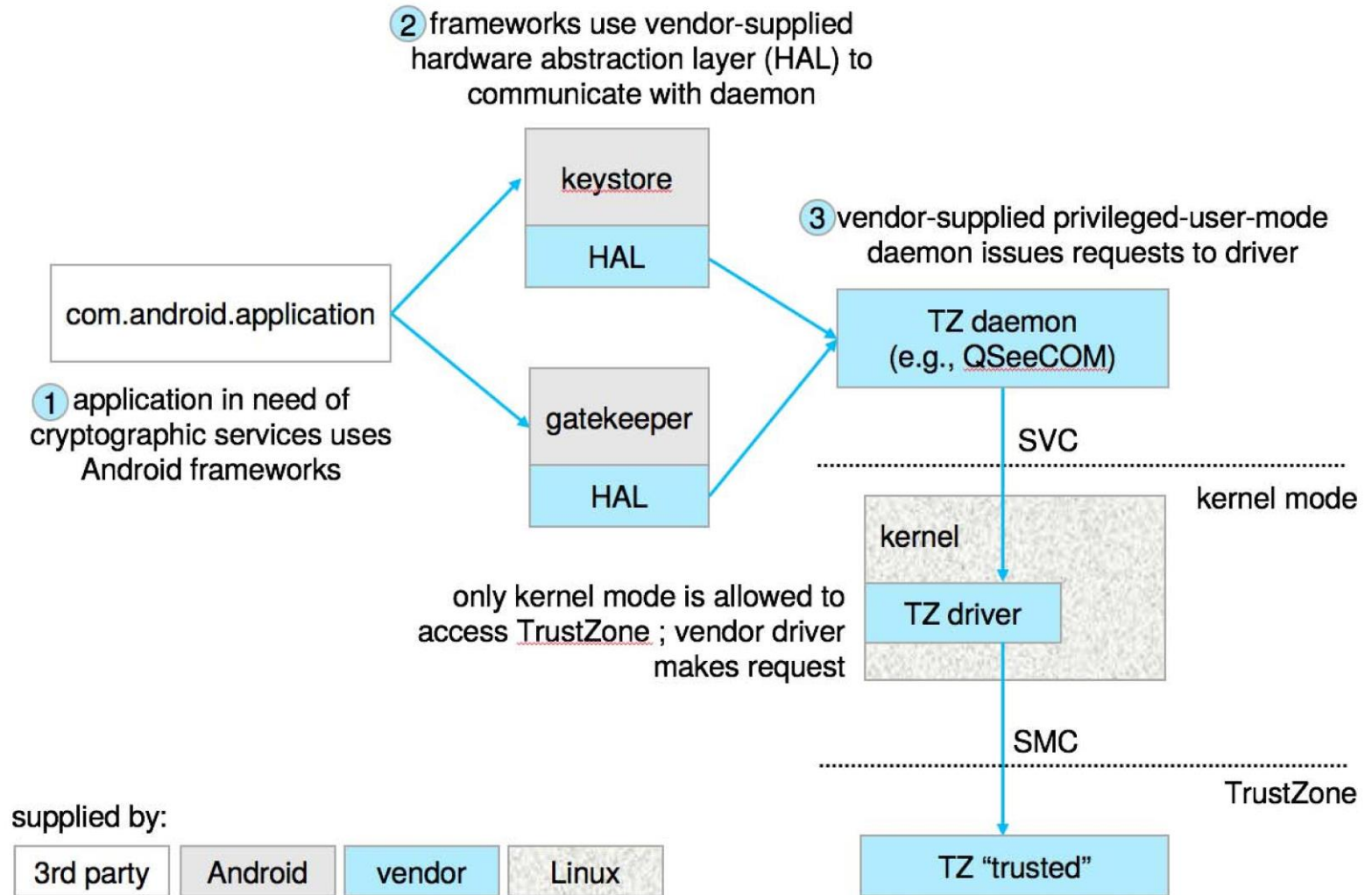
- Let  $D_i$  and  $D_j$  be any two domain rings
- If  $j < i \Rightarrow D_i \subseteq D_j$

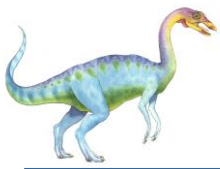




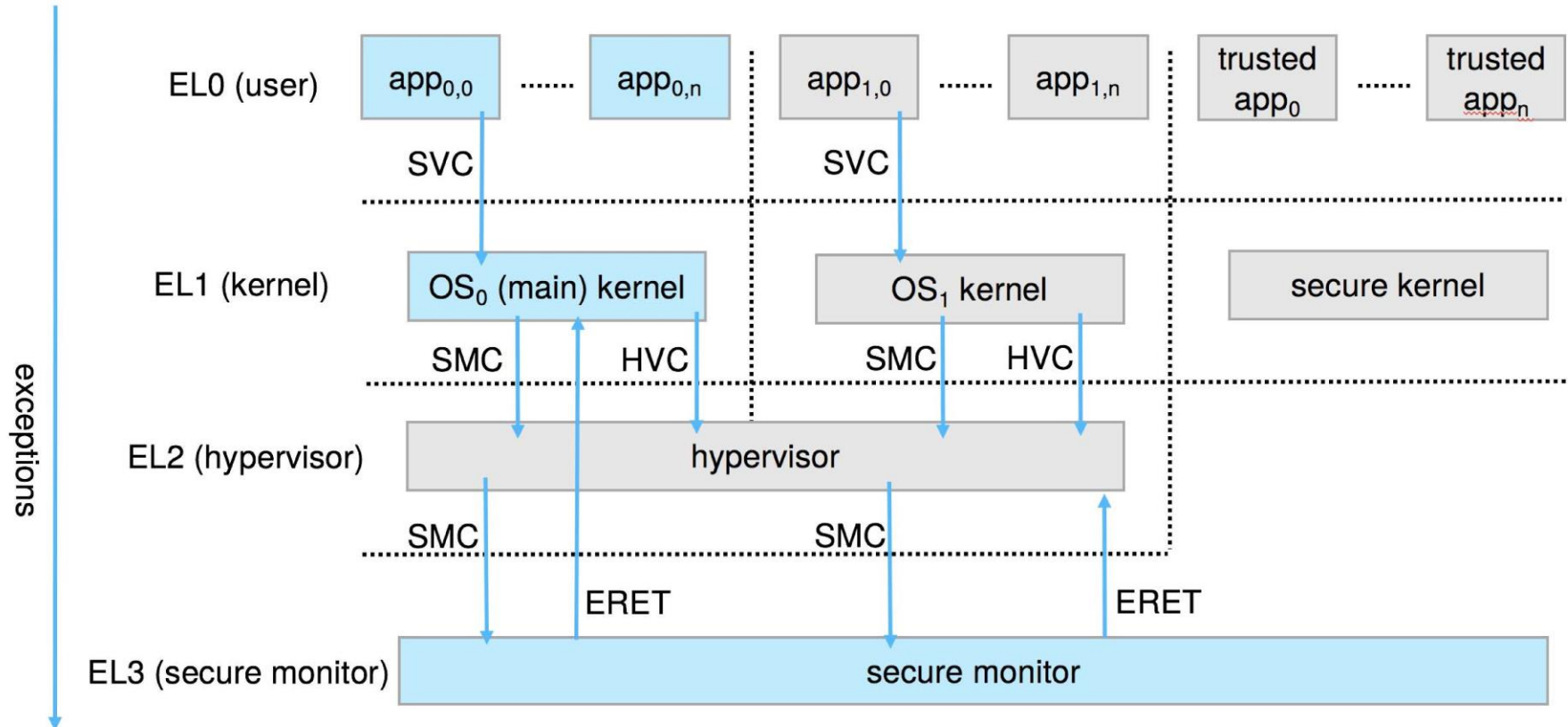


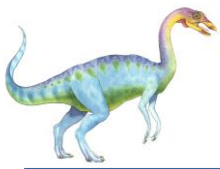
# Android use of TrustZone





# ARM CPU Architecture

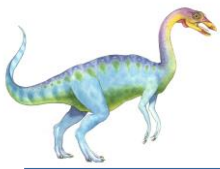




# Domain of Protection

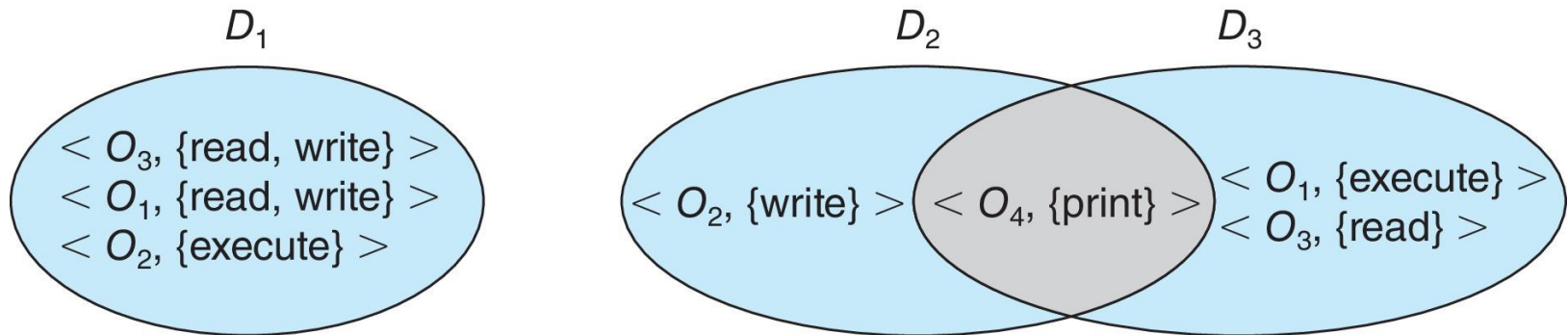
- Rings of protection separate functions into domains and order them hierarchically
- Computer can be treated as processes and objects
  - **Hardware objects** (such as devices) and **software objects** (such as files, programs, semaphores)
- Process for example should only have access to objects it currently requires to complete its task – the **need-to-know** principle
- Implementation can be via process operating in a **protection domain**
  - Specifies resources process may access
  - Each domain specifies set of objects and types of operations on them
  - Ability to execute an operation on an object is an **access right**
    - ▶ <object-name, rights-set>
  - Domains may share access rights
  - Associations can be **static** or **dynamic**
  - If dynamic, processes can **domain switch**

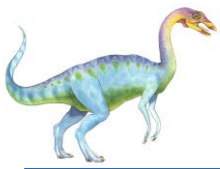




# Domain Structure

- Access-right =  $\langle \text{object-name}, \text{rights-set} \rangle$   
where *rights-set* is a subset of all valid operations that can be performed on the object
- Domain = set of access-rights





# Domain Implementation (UNIX)

- Domain = user-id
- Domain switch accomplished via file system
  - ▶ Each file has associated with it a domain bit (setuid bit)
  - ▶ When file is executed and setuid = on, then user-id is set to owner of the file being executed
  - ▶ When execution completes user-id is reset
- Domain switch accomplished via passwords
  - `su` command temporarily switches to another user's domain when other domain's password provided
- Domain switching via commands
  - `sudo` command prefix executes specified command in another domain (if original domain has privilege or password given)





# Domain Implementation (Android App IDs)

---

- ❑ In Android, distinct user IDs are provided on a per-application basis
- ❑ When an application is installed, the installed daemon assigns it a distinct user ID (UID) and group ID (GID), along with a private data directory (/data/data/<appname>) whose ownership is granted to this UID/GID combination alone.
- ❑ Applications on the device enjoy the same level of protection provided by UNIX systems to separate users
- ❑ A quick and simple way to provide isolation, security, and privacy.
- ❑ The mechanism is extended by modifying the kernel to allow certain operations (such as networking sockets) only to members of a particular GID (for example, AID\_INET, 3003)
- ❑ A further enhancement by Android is to define certain UIDs as “isolated,” prevents them from initiating RPC requests to any but a bare minimum of services





# Access Matrix

- View protection as a matrix (**access matrix**)
- Rows represent domains
- Columns represent objects
- **Access** ( $i, j$ ) is the set of operations that a process executing in  $\text{Domain}_i$  can invoke on  $\text{Object}_j$

domain \ object	$F_1$	$F_2$	$F_3$	printer
$D_1$	read		read	
$D_2$				print
$D_3$		read	execute	
$D_4$	read write		read write	



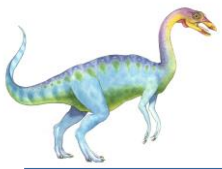


# Use of Access Matrix

- If a process in Domain  $D_i$  tries to do “op” on object  $O_j$ , then “op” must be in the access matrix
- User who creates object can define access column for that object
- Can be expanded to dynamic protection
  - Operations to add, delete access rights
  - Special access rights:
    - ▶ *owner of  $O_i$*
    - ▶ *copy op from  $O_i$  to  $O_j$  (denoted by “\*”)*
    - ▶ *control –  $D_i$  can modify  $D_j$  access rights*
    - ▶ *transfer – switch from domain  $D_i$  to  $D_j$*
  - *Copy and Owner* applicable to an object
  - *Control* applicable to domain object





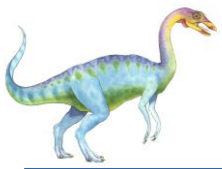


# Use of Access Matrix (Cont.)

---

- **Access matrix** design separates mechanism from policy
  - Mechanism
    - ▶ Operating system provides access-matrix + rules
    - ▶ If ensures that the matrix is only manipulated by authorized agents and that rules are strictly enforced
  - Policy
    - ▶ User dictates policy
    - ▶ Who can access what object and in what mode
- But doesn't solve the general confinement problem

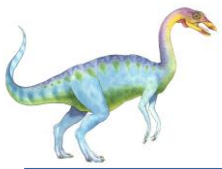




# Access Matrix of Figure A with Domains as Objects

object \ domain	$F_1$	$F_2$	$F_3$	laser printer	$D_1$	$D_2$	$D_3$	$D_4$
$D_1$	read		read			switch		
$D_2$				print			switch	switch
$D_3$		read	execute					
$D_4$	read write		read write		switch			





# Access Matrix with Copy Rights

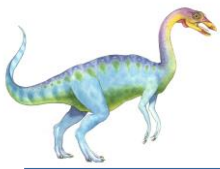
domain \ object	$F_1$	$F_2$	$F_3$
$D_1$	execute		write*
$D_2$	execute	read*	execute
$D_3$	execute		

(a)

domain \ object	$F_1$	$F_2$	$F_3$
$D_1$	execute		write*
$D_2$	execute	read*	execute
$D_3$	execute	read	

(b)





# Access Matrix With Owner Rights

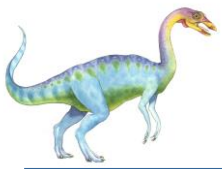
object \ domain	$F_1$	$F_2$	$F_3$
$D_1$	owner execute		write
$D_2$		read* owner	read* owner write
$D_3$	execute		

(a)

object \ domain	$F_1$	$F_2$	$F_3$
$D_1$	owner execute		write
$D_2$		owner read* write*	read* owner write
$D_3$		write	write

(b)

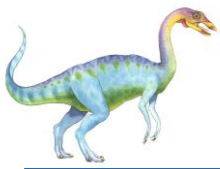




# Modified Access Matrix of Figure B

object domain	$F_1$	$F_2$	$F_3$	laser printer	$D_1$	$D_2$	$D_3$	$D_4$
$D_1$	read		read			switch		
$D_2$				print			switch	switch control
$D_3$		read	execute					
$D_4$	write		write		switch			

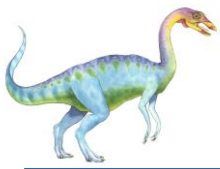




# Implementation of Access Matrix

- Generally, a sparse matrix
- Option 1 – Global table
  - Store ordered triples `<domain, object, rights-set>` in table
  - A requested operation  $M$  on object  $O_j$  within domain  $D_i$  -> search table for `<  $D_i$ ,  $O_j$ ,  $R_k$  >`
    - ▶ with  $M \in R_k$
  - But table could be large -> won't fit in main memory
  - Difficult to group objects (consider an object that all domains can read)





# Implementation of Access Matrix (Cont.)

---

- Option 2 – Access lists for objects
  - Each column implemented as an access list for one object
  - Resulting per-object list consists of ordered pairs **<domain, rights-set>** defining all domains with non-empty set of access rights for the object
  - Easily extended to contain default set -> If  $M \in$  default set, also allow access





# Implementation of Access Matrix (Cont.)

- Each column = Access-control list for one object  
Defines who can perform what operation

Domain 1 = Read, Write  
Domain 2 = Read  
Domain 3 = Read

- Each Row = Capability List (like a key)  
For each domain, what operations allowed on what objects  
Object F1 – Read  
Object F4 – Read, Write, Execute  
Object F5 – Read, Write, Delete, Copy



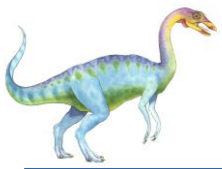




# Implementation of Access Matrix (Cont.)

- Option 3 – Capability list for domains
  - Instead of object-based, list is domain based
  - **Capability list** for domain is list of objects together with operations allows on them
  - Object represented by its name or address, called a **capability**
  - Execute operation  $M$  on object  $O_j$ , process requests operation and specifies capability as parameter
    - ▶ Possession of capability means access is allowed
  - Capability list associated with domain but never directly accessible by domain
    - ▶ Rather, protected object, maintained by OS and accessed indirectly
    - ▶ Like a “secure pointer”
    - ▶ Idea can be extended up to applications



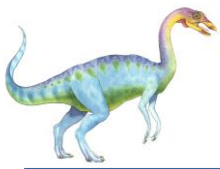


# Implementation of Access Matrix (Cont.)

---

- Option 4 – Lock-key
  - Compromise between access lists and capability lists
  - Each object has list of unique bit patterns, called **locks**
  - Each domain as list of unique bit patterns called **keys**
  - Process in a domain can only access object if domain has key that matches one of the locks

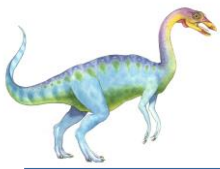




# Comparison of Implementations

- Many trade-offs to consider
  - Global table is simple, but can be large
  - Access lists correspond to needs of users
    - ▶ Determining set of access rights for domain non-localized so difficult
    - ▶ Every access to an object must be checked
      - Many objects and access rights -> slow
  - Capability lists useful for localizing information for a given process
    - ▶ But revocation capabilities can be inefficient
  - Lock-key effective and flexible, keys can be passed freely from domain to domain, easy revocation



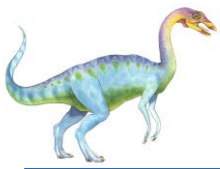


# Comparison of Implementations (Cont.)

---

- Most systems use combination of access lists and capabilities
  - First access to an object -> access list searched
    - ▶ If allowed, capability created and attached to process
      - Additional accesses need not be checked
    - ▶ After last access, capability destroyed
    - ▶ Consider file system with ACLs per file



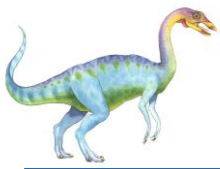


# Revocation of Access Rights

---

- Various options to remove the access right of a domain to an object
  - **Immediate vs. delayed**
  - **Selective vs. general**
  - **Partial vs. total**
  - **Temporary vs. permanent**
- **Access List** – Delete access rights from access list
  - **Simple** – search access list and remove entry
  - **Immediate, general or selective, total or partial, permanent or temporary**

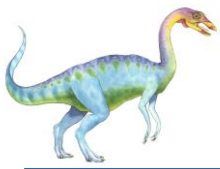




# Revocation of Access Rights (Cont.)

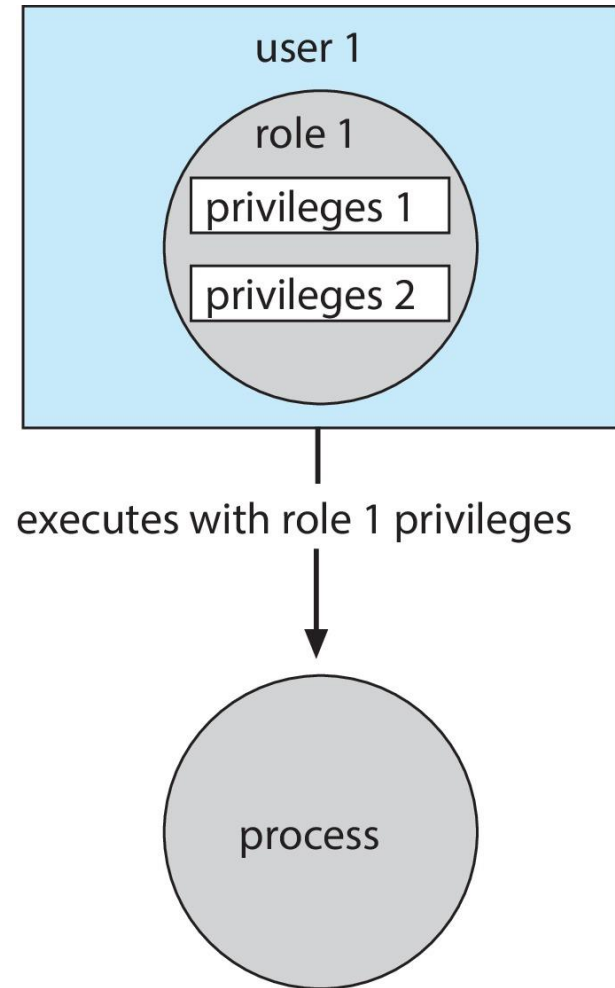
- **Capability List** – Scheme required to locate capability in the system before capability can be revoked
  - **Reacquisition** – periodic delete, with require and denial if revoked
  - **Back-pointers** – set of pointers from each object to all capabilities of that object (Multics)
  - **Indirection** – capability points to global table entry which points to object – delete entry from global table, not selective (CAL)
  - **Keys** – unique bits associated with capability, generated when capability created
    - ▶ Master key associated with object, key matches master key for access
    - ▶ Revocation – create new master key
    - ▶ Policy decision of who can create and modify keys – object owner or others?





# Role-based Access Control

- Protection can be applied to non-file resources
- Oracle Solaris 10 provides **role-based access control (RBAC)** to implement least privilege
  - **Privilege** is right to execute system call or use an option within a system call
  - Can be assigned to processes
  - Users assigned **roles** granting access to privileges and programs
    - ▶ Enable role via password to gain its privileges
  - Similar to access matrix





# Mandatory Access Control (MAC)

- Operating systems traditionally had discretionary access control (DAC) to limit access to files and other objects (for example UNIX file permissions and Windows access control lists (ACLs))
  - Discretionary is a weakness – users / admins need to do something to increase protection
- Stronger form is mandatory access control, which even root user can't circumvent
  - Makes resources inaccessible except to their intended owners
  - Modern systems implement both MAC and DAC, with MAC usually a more secure, optional configuration (Trusted Solaris, TrustedBSD (used in macOS), SELinux), Windows Vista MAC)
- At its heart, labels assigned to objects and subjects (including processes)
  - When a subject requests access to an object, policy checked to determine whether or not a given label-holding subject is allowed to perform the action on the object



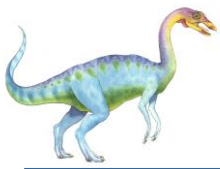




# Capability-Based Systems

- ❑ Hydra and CAP were first capability-based systems
- ❑ Now included in Linux, Android and others, based on POSIX.1e (that never became a standard)
  - ❑ Essentially slices up root powers into distinct areas, each represented by a bitmap bit
  - ❑ Fine grain control over privileged operations can be achieved by setting or masking the bitmap
  - ❑ Three sets of bitmaps – permitted, effective, and inheritable
    - ▶ Can apply per process or per thread
    - ▶ Once revoked, cannot be reacquired
    - ▶ Process or thread starts with all privs, voluntarily decreases set during execution
    - ▶ Essentially a direct implementation of the principle of least privilege
- ❑ An improvement over root having all privileges but inflexible (adding new privilege difficult, etc)



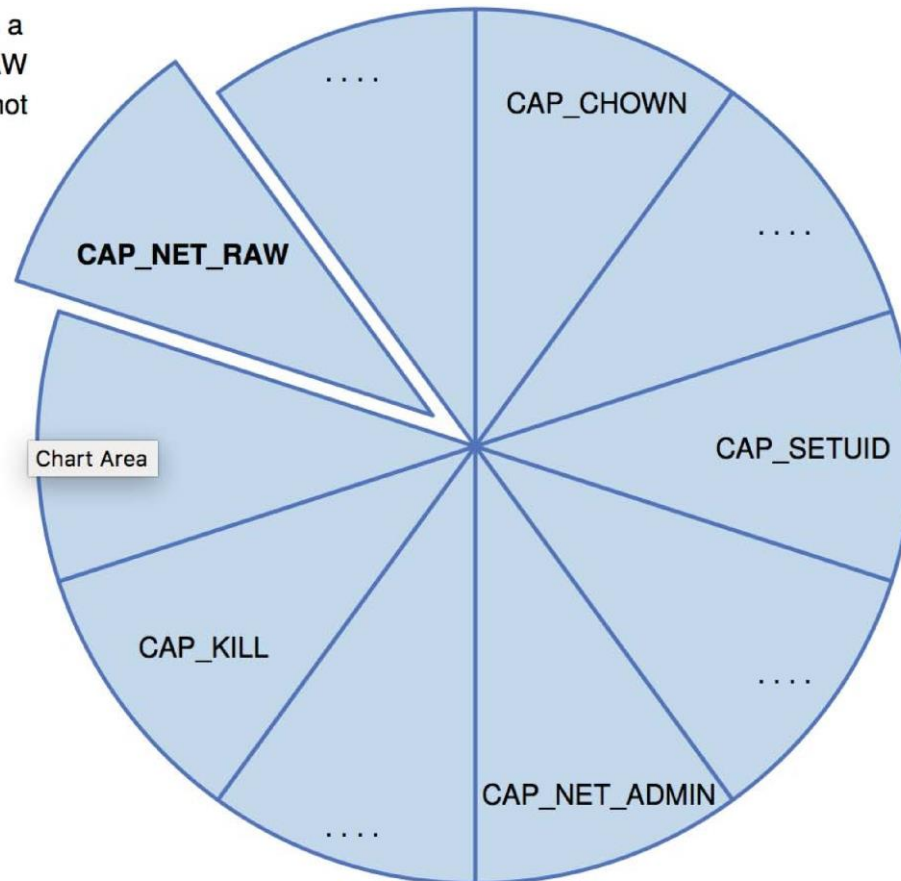


# Capabilities in POSIX.1e

In the old model, even a simple `ping` utility would have required root privileges, because it opens a raw (ICMP) network socket

Capabilities can be thought of as "slicing up the powers of root" so that individual applications can "cut and choose" only those privileges they actually require

With capabilities, `ping` can run as a normal user, with `CAP_NET_RAW` set, allowing it to use ICMP but not other extra privileges





# Other Protection Improvement Methods

---

- System integrity protection (SIP)
  - Introduced by Apple in macOS 10.11
  - Restricts access to system files and resources, even by root
  - Uses extended file attribs to mark a binary to restrict changes, disable debugging and scrutinizing
  - Also, only code-signed kernel extensions allowed and configurably only code-signed apps
- System-call filtering
  - Like a firewall, for system calls
  - Can also be deeper –inspecting all system call arguments
  - Linux implements via SECCOMP-BPF (Berkeley packet filtering)





## Other Protection Improvement Methods (cont.)

---

- Sandboxing
  - Running process in limited environment
  - Impose set of irremovable restrictions early in startup of process (before `main()`)
  - Process then unable to access any resources beyond its allowed set
  - Java and .net implement at a virtual machine level
  - Other systems use MAC to implement
  - Apple was an early adopter, from macOS 10.5's “seatbelt” feature
    - ▶ Dynamic profiles written in the Scheme language, managing system calls even at the argument level
    - ▶ Apple now does SIP, a system-wide platform profile



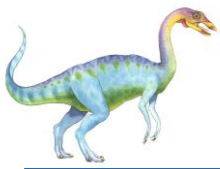


## Other Protection Improvement Methods (cont.)

---

- Code signing allows a system to trust a program or script by using crypto hash to have the developer sign the executable
  - So code as it was compiled by the author
  - If the code is changed, signature invalid and (some) systems disable execution
  - Can also be used to disable old programs by the operating system vendor (such as Apple) cosigning apps, and then invalidating those signatures so the code will no longer run



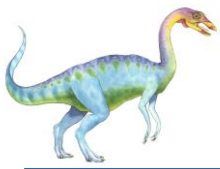


# Language-Based Protection

---

- Specification of protection in a programming language allows the high-level description of policies for the allocation and use of resources
- Language implementation can provide software for protection enforcement when automatic hardware-supported checking is unavailable
- Interpret protection specifications to generate calls on whatever protection system is provided by the hardware and the operating system





# Protection in Java 2

- Protection is handled by the Java Virtual Machine (JVM)
- A **class** is assigned a protection domain when it is loaded by the JVM
- The protection domain indicates what operations the class can (and cannot) perform
- If a library **method** is invoked that performs a privileged operation, the stack is **inspected** to ensure the operation can be performed by the library
- Generally, Java's load-time and run-time checks enforce **type safety**
- Classes effectively **encapsulate** and protect data and methods from other classes





# Stack Inspection

protection domain:	untrusted applet	URL loader	networking
socket permission:	none	*.lucent.com:80, connect	any
class:	gui: ... get(url); open(addr); ...	get(URL u): ... doPrivileged { open('proxy.lucent.com:80'); } <request u from proxy> ...	open(Addr a): ... checkPermission (a, connect); connect (a); ...





# End of Chapter 17

---

