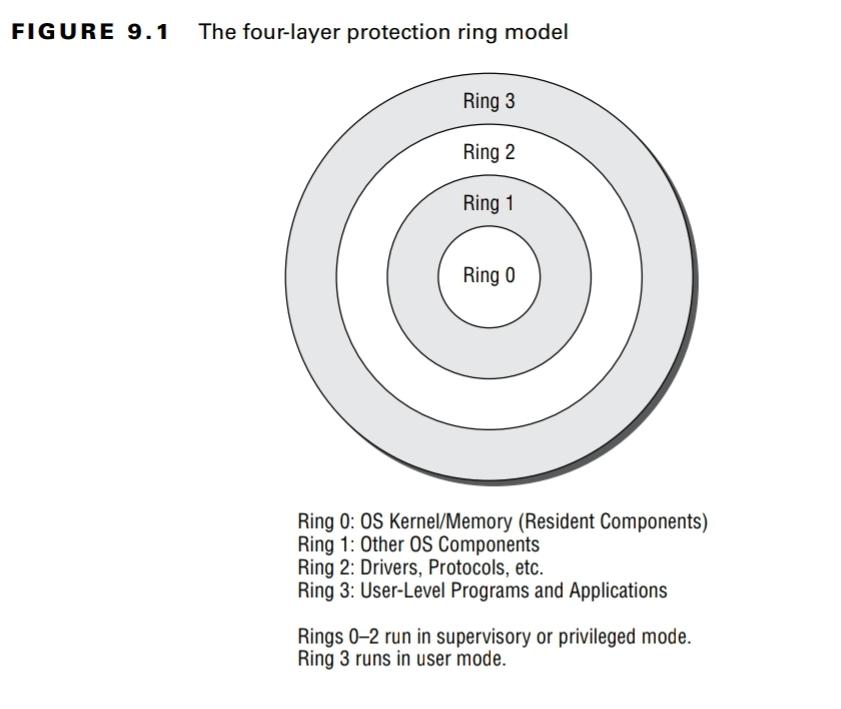
**Chapter 9: Security Vulnerabilities, Threats, and Countermeasures**

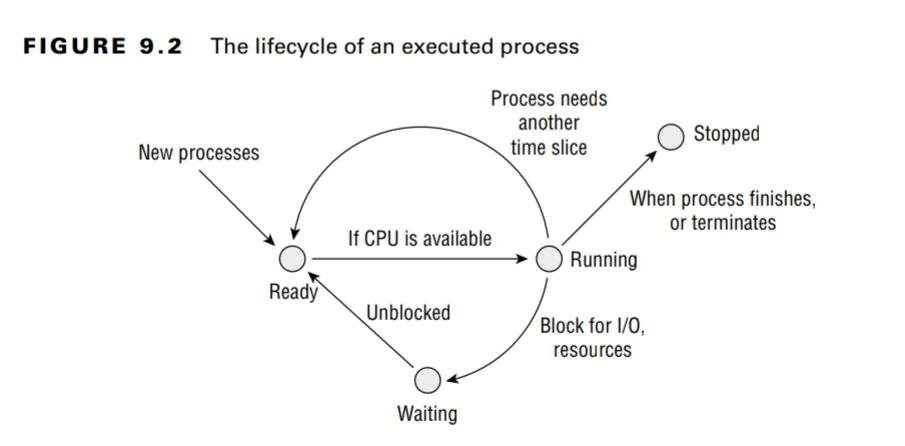
**Execution Types**

* Multitasking - Doing multiple tasks together, usually with a single processor by juggling the tasks
* Multiprogramming  Similar to multitasking. It involves the pseudo-simultaneous execution of two tasks on a single processor coordinated by the OS as a way to increase operational efficiency.
* Multi Core - Using multiple CPU cores for multi tasking
* MultiProcessor - Using multiple processor for multi tasking
* Multithreading - Application uses multiple threads under the same parent process for parallel execution

**Protection Rings**



**Process States**



There is an additional state called supervisory state(not shown in figure) in which a process requires privileges to perform privileged operations.

All user applications run only in user mode. If a process needs to perform a privileged system change, it will make a system call to the OS kernel. The kernel then evaluates it and either rejects the request or approves it and executes it using a newly created process running in privileged mode outside the control of the user.

**Read-Only Memory**

ROM - Non volatile, factory written

PROM - Can be written once

EPROM

* UVEPROM - can be erased using UV rays
* EEPROM - electronically erasable

Flash Memory - concept derived from EEPROM, non-volatile storage that can be electronically erased

**Random Access Memory**

Real/ Primary RAM - volatile and fast access memory

* Static RAM - uses J-K flip flops, costly, no need to refresh, faster
* Dynamic RAM - uses capacitors, need to refresh as capacitor loses charge over time, cheaper, slower

Cache RAM - Relatively faster, smaller and temporary RAM

Registers - The CPU includes a limited amount of onboard memory, known as registers.

**Memory Addressing**

* Register Addressing - CPU fetches data from registers
* Immediate Addressing  - Data is provided as part of the instruction
* Direct Addressing - direct memory address of data is provided
* Indirect Addressing - address of pointer is provided
* Base+Offset Addressing - Base address and offset is provided, CPU computes the data address

Virtual memory is a special type of secondary memory that is used to expand the addressable space of real memory. The most common type of virtual memory is the pagefile or swapfile.

Distributed control systems (DCS) focuses on processes and is state driven, whereas SCADA focuses on data gathering and is event driven. DCS is more suited to operating on a limited scale, whereas SCADA is suitable for managing systems over large geographic areas. PLC units are effectively single-purpose or focused-purpose digital computers.

Type 1 hypervisor is a bare metal machine hypervisor in which there is no host OS. Type 2 hypervisors have a host OS managing the guest OS.

Process Isolation focuses on providing separate memory spaces for each process’s instructions and data. It prevents unauthorized data access and protects the integrity of processes.

A rootkit is malware that embeds itself deep within an OS.

Some forms of attack occur in slow, gradual increments rather than through obvious or recognizable attempts to compromise system security or integrity. These are called incremental attacks. Two such forms of it are data diddling and the salami attack.

Arduino is an open source hardware and software organization that creates single-board 8-bit microcontrollers without including an OS that can execute C++ programs specifically written to its limited instruction set.

Real Time Operating system (RTOS) minimizes latency and delay, and optimizes for mission-critical operations.