

# Security Architecture & Models

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: security\_architecture\_models.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

## ❖ CPU

- **The CPU Contains a control unit ALU**
- **The control unit control the timing of the execution**
- **The control unit is an Arithmetic Logic Unit ALU**
- **The ALU performs mathematical functions and logical operations**
- **The CPU contain Primary Storage which is a type of memory**
- **The primary storage is where data is temporarily held before being processed by the CPU**
- **The data being processed enter the CPU in blocks at a time.**
- **If the software do not properly set the Boundaries for how much data can come in as block extra data can slip in and be executed. This is how buffer overflow work**
- **A CPU's time and processing has to be shared between many tasks. Software and system INTERRUPTS are used to handle that.**
- **CPU Modes & Protection**
  - **Protection rings - provide strict boundaries and definitions on what the processes that work within each ring can access and what commands they can execute**
  - **The operating system has several protection mechanisms to ensure that processes do not negatively affect each other or the critical components of the system itself**
  - **One protection mechanism is Memory Segment**
  - **Another type of protection is protection RINGS**
  - **The rings provide strict boundaries and definitions on what the processes can access and what command they can execute**
  - **Their are 4 Rings.**
    - **RING 0**
      - ♦ It has the most privilege
      - ♦ Operating system Kernel
    - **RING 1**
      - ♦ Remaining parts of the Operating system
    - **RING 2**
      - ♦ Operating system Utilities, File system Drivers I/O drivers & utilities
    - **RING 3**
      - ♦ Applications e.g web browser, word processor, database, Email client, etc...
  - **The process that work in the inner rings "EXIST IN PRIVILEGE MODE" or System mode**
  - **The processes that work in the outer Rings "EXIST in a USER MODE"**
  - **These rings provide an intermediate layer between subjects and objects**
  - **A subject in ring 3 cannot directly access an object in ring 1 or ring 0**
  - **A subject in ring 1 cann access an object in Ring 3**

- Operating system processes are executed in SYSTEM MODE and applications are executed in USER MODE

## ❖ Memory

### ➤ Primary Storage

- Main Memory directly accessed by the CPU
- Used for the storage of instructions and data for an executing program
- It is not a permanent storage area

### ➤ Secondary Storage

- Nonvolatile storage such as disks, CDs, etc

### ➤ Real storage

- Memory allocation for a program
- As instructions and data are processed, they are moved back to the system's memory spaces called Real storage
- Applications are given a segment of memory called Real Storage to hold data and instructions

### ➤ Virtual Storage

- When RAM and secondary (disk) storage are used together they form virtual storage
- The system use the hard disk space to extend the RAM memory
- When a program requests access to data it is brought from the had disk back into memory this process is called PAGING
- Paging - the process of recalling information that is written to disk when volatile storage is used up
- When an application runs it thinks it is the only program running this is can be possible by using virtual memory and virtual machines

### ➤ Memory Types

- **RAM**
  - Read Access Memory
  - Type of temporary storage
  - It is used for read/write activities
  - It is a volatile memory
  - The most well know type of RAM are Static & Dynamic
  - Static RAM does not need continual refresh
  - Dynamic RAM need continual refresh
- **ROM**
  - Read Only Memory
  - It is a NONVOLATILE storage facility
  - For most part data inserted into a ROM cannot be altered.
  - The software that is stored within the ROM is called FIRMWARE
- **EPROM**
  - Erasable and Programmable read-only Memory
  - Can be modified, deleted, or upgraded Elctrically

### ➤ Cache memory

- Part of the RAM that is used for high-speed writing and reading
- It holds instructions and data from primary storage

### ➤ Memory Mapping

- Access to the memory needs to be controlled to ensure that data does not get

- corrupted. This type of control happen using Memory MAPPING and addressing
- The CPU can access the memory directly using PHYSICAL addresses instead of pointers to memory segments
- When a computer runs software, it does not want to expose itself to software written by good and bad programmers so computer enable software to use the memory indirectly using INDEX TABLES and pointers
- This type of memory architecture provides protection and efficiency
- Mapped memory enables different programs to access the data and perform their own functions on it.

## ❖ Operating States

- Ready State
  - An application is ready to resume processing
- Supervisory State
  - The system is executing a system or privileged routine
- Problem State
  - The system is busy executing an application. Mean the system is working on a problem
- Wait State
  - An application is waiting for an event to complete. e.g. user input, wait for a print job to finish

## ❖ Multithreading Multitasking

- The operating system provide time slicing and interrupts to ensure that processes are provided with adequate access to the CPU
- Process - a program in execution that works in its own address space and can only communicate with other processes in a controlled manner by the OS
- A thread represents a piece of code that is executed within a process
- Multithreading - when a system can process more than one request at a time
- Multitasking - when the CPU can process more than one process at a time
- Multiprocessing - using more than one CPU at the same time in parallel
- Deadlock - when a computer uses all available resources and does not release them

## ❖ Input/Output Device

- A deadlock situation occurs when two processes are trying to access the same resource at the same time
- The deadlock will happen when a process use a resource and does not release it