Wellness Family Fitness

OPERATING SYSTEMS THEORY & CONCEPTS TRAINING

Instructed by: Liela Pressley
October 2, 2022

OBJECTIVES

- understand OS theory & implementation
- understand OS internals to design/implement architectural changes to existing OS
- describe role & basic OS functions (how interacts with hardware/software
- identify/describe basic security issues of OS
- describe and know potential security concerns of the following:
  - Privileged vs. nonprivileged states (domain switching)
  - Concurrency and synchronization
  - Application processes & threads
  - process/thread management
  - synchronization
  - inter-process communications
  - Memory management
  - virtual memory
  - real memory
  - hierarchical memory schemes
  - Uni-processor/ multi-processor interfaces/support
  - CPU scheduling
  - File systems
  - Virtualization/hypervisors
  - Access controls (models and mechanisms)
  - Creation and operation of virtualization technology
  - Domain separation
  - process isolation
  - resource encapsulation, least privilege
  - I/O issues (e.g., buffering, queuing, sharing, management)
  - Distributed OS issues
  - (client/server, message passing, remote procedure calls, clustering)

OPERATING SYSTEMS THEORY

What is the purpose of OS software?

Works behind the scenes as the bridge interface between the user and the computer hardware by managing hardware, controlling the execution of applications.

EX: When a user click on an icon for a browser, the OS will load the application machine code to the memory then send it to be processed by the CPU so it can be executed and viewed by the user.

HARDWARE — **OPERATING SYSTEMS** — **APPLICATIONS**

OPERATING SYSTEMS

How does it achieve this goal?

HARD DISK

Contains files system: all files installed including applications and their data files

MEMORY (RAM)

Knows location of machine code for ea. application and fetches it for processing

CENTRAL PROCESSING UNIT

Control Unit- opens/closes pathways through internal/external bus system to execute, process & move data

Arithmetic & Logic Unit- calculates and compares data

MAJOR FUNCTIONALITIES OF OPERATING SYSTEM

Memory Management

Code and tasks to manage memory

- how much is used and by whom
- which process needs memory space (how much)
- allocate/deallocate space

Storage/File Management

Code and tasks to manage files

- **file system-** manages storage (NIFS, CFS, CIFS, NFS)
- data stores in various tracks of Hard Disk

Process Management

Code and tasks to manage access to CPU time/access

- scheduling termination and CPU scheduling of unexecuted code

Device & Resource Management

code and tasks to provide hardware to user and connect devices

MEMORY MANAGEMENT

memory management- subdividing memory among different processes/ managing operations between main memory and disk during process execution

virtual memory- storage allocation where secondary memory can be used as if part of the main memory (amount of storage is limited to secondary memory not main

real memory- works with hardware known as memory chips (RAM), every program runs through the hardware

hierarchical memory- enhanced organization of memory to minimize access time.
Lvl 4- Magnetic Tape | Lvl 3- Magnetic Disk | Lvl 2- Main Memory | Lvl 1- Cache Memory | Lvl 0- CPU

buffer- stores data being transferred between 2 devices and an application(produced in main memory then transfers data to disk

I/O buffering- deals with speed mismatch between producers and consumers of data

I/O queuing/scheduling- used to effectively use computer resources, avoid deadlock and server all processes waiting in the queue

I/O management- *Input/Output requests are managed by device drivers w/ system programs (traffic controller, scheduler, device handler)*

STORAGE/FILE MANAGEMENT

file systems- collection of info recorded to secondary storage" divided into two parts name and extension *EX: aboutburgers.doc*

file directory- collection of files (great for efficiency, naming and grouping

PROCESS MANAGEMENT

domain separation- allows for enforcement of rules governing entry and use of domains by entities outside the domain

process isolation- isolating program running on computer to prevent tampering or interference from/by other processes

synchronization- there are 2 types: **independent process** (1. process execution doesn't affect others)and **cooperative process** (can affect or be affected by other processes)

semaphores- integer variables that are used to solve selection by using "wait and signal"- allowing for for limited resource waste

locks- synchronization technique that allows 1 thread to own it at one time, tells compiler and processor that its using shared memory

concurrency- execution of multiple instruction sequences at same time allows for applications to be run w/o waiting for another be completed- can result to deadlocks or resource starvation

PROCESS MANAGEMENT

application processes- process allows machine code to be executed with necessary resources such as: virtual address space, code, security context, priority class, environment variable, process identifier, working set size & more.

application threads- entity w/in the process that can be scheduled for execution- each thread share a virtual address space and system resource

inter-process communications- **shared memory-** processes can use shared memory to find information as a record from another process
message passing- est. a comm link using (send and recieve)

uniprocessor- system that still uses only one CPU (central processing unit)

CPU scheduling- allows one process to use CPU while others are delayed (standby) because resources are unavailable (makes system more efficient, faster, fairer)

message passing- sending a message to a process (object, parallel process, function, thread etc.) can invoke another process (directly or indirectly)

remote procedure call- technique for constructing distributed client-server applications so that the called procedure won't be in same address space as calling procedure

DEVICE & RESOURCE MANAGEMENT

resource encapsulation- encapsulating resources to allow access/change to data in ways only the designer intentionally pre-defined

least privilege- minimizing the acts a user can perform on managed computer resources will limit accidental misuse and increase accountability

privileged accounts- having valid credentials to gain restrictive access to systems

virtualization- creating abstracted layer over hardware to divide resources into multiple virtual computers *(virtual machines aka VMs)* which runs individual OS and runs independently.

hypervisor- (aka virtual machine monitor) a software that creates and runs VMs, by allowing by sharing computer resources like memory and processes from the host computer

clustered systems- 2+ individual computer systems with common storage and systems so the two can work together

ACCESS CONTROL

security technique regulates who/what can view/use resources in a computing environment

goal: minimize security risk of unauthorized access to physical/logical systems

main models of AC

- *mandatory access control (MAC)-* access rights regulated by central authority based on lvls of security (ie: govt, military)
- *Discretionary access control (DAC)-* owners or admins of protected system/data/resource set policies of who is authorized
- *Role-based access control (RBAC)-* restricts access to computer resources based on individual/group w/ defined business function
- *Rule-based access control-* system admin defines conditional rules
- *Attribute-based access control- manages access rights by evaluating set of rules, policies, relationships using attributes of users, systems and environment*

OS SECURITY

OS security starts with design to ensure Confidentiality, integrity and availability

common OS security threats

- *malware-* malicious software injected into a system w/o consent to steal, destroy, corrupt data or compromise the device in use
- *Denial of Service attacks (DoS)-* clogging a system with fake requests that it will overload the system and its resources (damaging infrastructure)
- *Network Intrusion-* gaining access to system for wrong usage
  - careless insiders- neglecting security policies
  - malicious insiders- those who abuse their access
  - masqueraders- external people posing as legit users to exploit
  - clandestine user- attackers penetrating system using supervisor control
- *buffer overflow-* overwhelming buffer with data to overwrite other memory locations containing important info to inject scripts to help hijack system and crash it

REFERENCES

About Processes and Threads - Win32 apps. (2021, January 7). Microsoft Learn. Retrieved October 2, 2022, from https://learn.microsoft.com/en-us/windows/win32/procthread/about-processes-and-threads

Burns, E. (2017, March 1). Privileged Accounts Explained. Tech Monitor. Retrieved October 2, 2022, from https://techmonitor.ai/what-is/privileged-accounts-explained

Clustered Operating System - javatpoint. (n.d.). www.javatpoint.com. Retrieved October 2, 2022, from https://www.javatpoint.com/clustered-operating-system#:%7E:text=What%20is%20the%20Clustered%20Operating,for%20all%20systems%20to%20operate

Education, I. C. (2021, March 30). Virtualization. Retrieved October 2, 2022, from https://www.ibm.com/cloud/learn/virtualization-a-complete-guide

GeeksforGeeks. (2018, December 17). Memory Hierarchy Design and its Characteristics. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/memory-hierarchy-design-and-its-characteristics/?ref=gcse

GeeksforGeeks. (2020a, May 15). I/O buffering and its Various Techniques. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/i-o-buffering-and-its-various-techniques/#:%7E:text=A%20buffer%20is%20a%20memory,consumer%20of%20the%20data%20stream

GeeksforGeeks. (2020b, August 28). I/O scheduling in Operating Systems. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/i-o-scheduling-in-operating-systems/

GeeksforGeeks. (2021a, April 1). Inter Process Communication (IPC). Retrieved October 2, 2022, from https://www.geeksforgeeks.org/inter-process-communication-ipc/

GeeksforGeeks. (2021b, November 2). File Systems in Operating System. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/file-systems-in-operating-system/

GeeksforGeeks. (2021c, November 22). Memory Management in Operating System. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/memory-management-in-operating-system/

GeeksforGeeks. (2021d, November 26). Concurrency in Operating System. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/concurrency-in-operating-system/

GeeksforGeeks. (2022a, June 16). Introduction of Operating System - Set 1. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/introduction-of-operating-system-set-1/

GeeksforGeeks. (2022b, June 16). Introduction of Process Synchronization. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/introduction-of-process-synchronization/

GeeksforGeeks. (2022c, June 22). Difference between Process and Thread. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/difference-between-process-and-thread/

GeeksforGeeks. (2022d, July 5). CPU Scheduling in Operating Systems. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/cpu-scheduling-in-operating-systems/#:%7E:text=CPU%20Scheduling%20is%20a%20process,efficient%2C%20faster%2C%20and%20fairer.

GeeksforGeeks. (2022e, July 14). Virtual Memory in Operating System. Retrieved October 2, 2022, from https://www.geeksforgeeks.org/virtual-memory-in-operating-system/?ref=gcse

An Introduction to Operating Systems Theory. (2014, April 18). [Video]. YouTube. Retrieved October 2, 2022, from https://www.youtube.com/watch?v=xc_co-RcJwg&feature=youtu.be

Lutkevich, B. (2022, July 7). access control. SearchSecurity. Retrieved October 2, 2022, from https://www.techtarget.com/searchsecurity/definition/access-control

PCMag. (n.d.). Definition of uniprocessor. PCMAG. Retrieved October 2, 2022, from https://www.pcmag.com/encyclopedia/term/uniprocessor

Product Documentation | ServiceNow. (n.d.). Retrieved October 2, 2022, from https://docs.servicenow.com/bundle/quebec-servicenow-platform/page/administer/company-and-domain-separation/concept/c_DomainSeparation.html

Reading 23: Locks and Synchronization. (n.d.). Retrieved October 2, 2022, from https://web.mit.edu/6.005/www/fa15/classes/23-locks/

Real Memory - 2131 Words | 123 Help Me. (n.d.). Retrieved October 2, 2022, from https://www.123helpme.com/essay/Real-Memory-481015#:%7E:text=Real%20memory%20deals%20with%20the,hardware%20which%20is%20physical%20memory.

Rosencrance, L., & Matturro, B. (2021, October 21). Remote Procedure Call (RPC). SearchAppArchitecture. Retrieved October 2, 2022, from https://www.techtarget.com/searchapparchitecture/definition/Remote-Procedure-Call-RPC#:%7E:text=Remote%20Procedure%20Call%20is%20a,systems%20like%20a%20local%20system

Semaphores in Operating System. (n.d.). Retrieved October 2, 2022, from https://www.tutorialspoint.com/semaphores-in-operating-system

Techopedia. (n.d.). Message Passing. Retrieved October 2, 2022, from https://www.techopedia.com/definition/3230/message-passing#:~:text=Message%20passing%2C%20in%20computer%20terms,another%20process%2C%20directly%20or%20indirectly.

Understanding OS Security: Threats and Security Controls. (2022, April 12). Hysolate. Retrieved October 2, 2022, from https://www.hysolate.com/learn/sandboxing/understanding-os-security-threats-and-security-controls/

Understanding virtualization. (n.d.). Retrieved October 2, 2022, from https://www.redhat.com/en/topics/virtualization

vmware. (n.d.). What is a hypervisor? Vmware. Retrieved October 2, 2022, from https://www.vmware.com/topics/glossary/content/hypervisor.html#:~:text=A%20hypervisor%2C%20also%20known%20as,such%20as%20memory%20and%20processing.

What Is Process Isolation? (2022, September 18). EasyTechJunkie. Retrieved October 2, 2022, from https://www.easytechjunkie.com/what-is-process-isolation.htm