National College of Ireland

Higher Diploma in Science in Computing

Computer Architecture Operating Systems and Networks

Terminal Based Assignment Assessment

(TABA)

Friday 10th May, 09:00 am to Tuesday 14th May, 11:55 pm

Lecture: Hamilton Niculescu

Sergio Vinicio da Silva Oliveira
x23170981@student.ncirl.ie

1. IT Security

i) Confidentiality, Integrity, Availability triad

The term *Confidentiality* refers to the protection of information from unauthorized access. Preventing ransomware attacks and ensuring privacy are both important goals that can be achieved by maintaining confidentiality.

A familiar example of a corporate strategy is access control. It is possible to assign a login requirement to systems that require information created, stored and transferred control through this method, restricting only authorized persons.

Integrity refers to the data being reliable, complete, and not having been altered or modified accidentally by an unauthorized user. Data integrity can be compromised unintentionally by a system malfunction, or by operational errors such as erroneous data entry or even failure to perform procedures such as maintaining an updated backup. Moreover, the integrity of data can be compromised by malicious actors attempting to tamper with it.

To ensure data integrity, it is important to apply activities like setting up secure backup channels and sharing data only with authorized users.

In addition, services such as cloud storage, are examples of a great alliance in the prevention of data integrity. Through them, users not only store information, but also share it securely with authorized people, keeping control over who can edit specific files and folders, besides, performing automatic backups and creating version histories of files allows users to restore a file to a previous state if necessary.

Activities related to cloud services facilitate the detection of possible threats to data integrity, ensuring the security of the system and the data.

Availability refers to having access to data whenever you need it. That said, preventing attacks through the application of hardware and software measures deserves prominence to ensure the security of the system, maintaining such availability mentioned.

Implement hardware redundancy, use load balancing distributed access traffic, and configure firewalls for intrusion detection, these are examples of activities that can be implemented to ensure the availability of data even in the face of potential threats or system failures in an enterprise environment.

Washington University in St. Louis (n.d.) *Confidentiality, Integrity, and Availability: The CIA Triad*. Available at: https://informationsecurity.wustl.edu/items/confidentiality/ [Accessed 10 May 2024]

ii) In terms of security, define what is meant by a threat

According to the National Institute of Standards and Technology (NIST) (2024), a threat is defined as "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets or individuals through an information system through unauthorized access, destruction, disclosure, modification of information and/or denial of service."

NIST (2024) *COMPUTER SECURITY RESOURCE CENTER | Glossary*. Available at: https://csrc.nist.gov/glossary/term/threat [Accessed 10 May 2024]

iii) Give examples of two threats and discuss ways in which the effects of each of those threats could be minimized.

A cyber-attack is a deliberate attempt to steal, expose, alter, disable, or destroy data or applications, or other assets through unauthorized access to a network, computer system or digital device. These attacks involve resources, tools, and advanced techniques designed to aim their targets.

To prevent cyberattacks, numerous organizations employ a threat management strategy to recognize and safeguard their most crucial assets and resources. Among the main strategies, I highlight *Firewalls and Antivirus Software*, which is primarily intended to help block threat actors from entering the network, as well as regularly scanning computer systems for malicious programs and automatically eliminating the identified malware.

Another method that also deserves to be mentioned, this one related to *security awareness training*, which seeks to empower users to identify and avoid common vectors of cyber-attacks such as phishing and other social engineering attacks.

IBM (n.d.) *What is a cyberattack?* Available at: https://www.ibm.com/topics/cyber-attack [Accessed 10 May 2024]

Natural disasters are another threat that differs slightly from what was previously mentioned.

Given the events in Porto Alegre Brazil, in which several cities are completely flooded, I approach this topic as a real threat to the infrastructure of the system. Natural disasters of this magnitude can cause data loss or system downtime.

For this reason, robust disaster recovery plans must be developed to maintain system continuity. Ensuring that critical systems can be quickly restored, even after a natural disaster. Moreover, putting in place redundant systems ensures that data is accessible during and after a disaster.

Kackerone (n.d.) *Information Security: Principles, Threats, and Solutions.* Available at: https://www.hackerone.com/knowledge-center/principles-threats-and-solutions [Accessed 10 May 2024]

2. Networking and Linux Fundamentals

i) Network topology

a. -
b. Local Area Network (LAN)
c. -
d. Wide Area Network (WAN)

First I would like to introduce LAN, which means *Local Area Network*. It is a group of network devices that allow communication between multiple connected devices. The LAN belongs to private property instead of the public.

Although LAN only covers local areas, the WAN that came after the *Wide Area Network* has much wider coverage than LAN, covering entire countries and continents.

Implementation and management costs of WAN configuration networks are significantly higher than those of LAN configurations. This is due to the complexity associated with the extensive geographical coverage.

The maintenance of this network is another factor that is directly linked to cost, and at the same time presents a significant challenge. This gives to the fact that the need to operate 24/7, for this reason, deserves all the attention in its entire structure.

But not everything is disadvantageous. As mentioned, the WAN network has a wide coverage. In addition, the WAN network is characterized by having its data centralized. Through this, we can share data to all connected devices on the respective network, providing a much faster data exchange with the help of the Internet of Things (IoT) and LAN.

The LAN network on the other hand, proves to have a simple and reasonable cost. Due to the main objective being a local network, the complexity of implementation, configuration and cost, are relatively low. Moreover, the installed ethernet cabling allows for a much faster communication, often surpassing the speed of 100Mbps.

However, even being a low cost network compared to the WAN network, it's important to consider the cost of maintenance and management. It is expensive to establish a LAN, due to the need for specialized software for installing servers. Communication hardware such as hubs, switches, routers and cables should also be considered in this cost.

Additionally, LANs require regular maintenance and management to ensure optimal performance. This can be time-consuming and expensive.

Geeks for Geeks (2023) *Advantages and Disadvantages of LAN, MAN and WAN.* Available at: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-lan-man-and-wan/ [Accessed 11 May 2024]

ii) *Linux Fundamentals*

The purpose and benefits of running commands in sequence or a pipeline are determined by the specific task at hand.

Pipeline

Why: Because, enables data processing to be more efficient. Pipeline execution involves feeding the output of one program directly into another program, without any need for intermediate storage.

When: It is necessary to complete multiple tasks simultaneously.

Where: Pipelines are frequently utilized in command-line environments to handle word processing, data manipulation, and system administration tasks.

Who: System administrators, developers, and anyone who works extensively at the command line and needs to efficiently process large amounts of data.

To exemplify this approach, consider a scenario in which the user has a log file in which it is necessary to find all occurrences of a given error, count how many times it occurs and classify the results by frequency. In this case, the user can use the *grep* command to find the error lines, send that output to *wc -l* to count them, and then send that output to *sort* the results by frequency.

Geeks for Geeks (2023) *Piping in Unix or Linux*. Available at: https://www.geeksforgeeks.org/piping-in-unix-or-linux/ [Accessed 11 May 2024]

Sequential Execution

Why: Because there are cases where we need to complete one program before starting another.

When: Each program in the sequence is responsible for performing a different task and relies on the output of the previous one.

Where: In different scenarios, such as data processing pipelines, sequential execution can be employed to handle data in specific ways at each step.

Who: It can be performed by those who need to perform a series of tasks in a specific order without performing multiple tasks simultaneously.

A practical example for applying this approach would be in a scenario in which the user has the need to perform a series of activities, such as resize, compress and upload images to a server. In this case, the user would execute a command to resize all the images, then another command to compress them and finally a command to load them on the server.

Comparing the two approaches, we have the sequential execution, being direct, following a linear process in which a task is completed before moving on to the next. Again, used in cases where the tasks in which each step depends on the previous one.

On the other hand, pipeline execution allows parallel processing of tasks, making it more efficient to handle large data sets or repetitive tasks. Stand out in cases where intermediate data storage is not required.

Medium (2024) *Introduction to Linux*. Available at: https://medium.com/@aserdargun/introduction-to-linux-f20e68de3e59 [Accessed 11 May 2024]

3. Cloud Computing

i) Virtualisation

Virtualization involves the creation of a simulated or virtual computing environment instead of a physical one. Virtualization frequently involves the creation of computer-generated versions of hardware, operating systems, storage devices, and others. This makes it possible for organizations to divide a single physical computer or server into multiple virtual machines. Each virtual machine has the ability to interact independently and run various operating systems or applications, while sharing the resources of one host machine.

VMware (n.d.) *What is virtual infrastructure?* Available at: **https://www.vmware.com/topics/glossary/content/virtual-infrastructure.html** [Accessed 11 May 2024]

Server, desktop, network, and storage are the four main elements that define virtualization.

Server Virtualization involves dividing a single server into multiple small, isolated virtual servers. The process does not necessitate the installation of new or additional servers; rather, the virtualization software or hardware takes an existing server and divides it into multiple isolated virtual servers. All of these servers are capable of operating on their own.

Desktop Virtualization is the process of replacing traditional physical desktop computing environments with virtual ones. It enables the creation and storage of multiple desktop environments for users on one host that can be stored in the cloud or in a data centre.

Network Virtualization is a technology that enables the separation of the logical network from the physical network infrastructure. It enables multiple virtual networks to coexist on a physical network, each functioning independently and isolated from one another.

The concept of *Storage Virtualization* involves abstracting and separating the logical view of storage from its physical implementation. It enables the management of multiple storage devices (like hard drives, solid state drives, or storage arrays) from various vendors together as a single unified storage resource.

Medium (2023) *A Comprehensive Guide to Types of Virtualization.* Available at: **https://medium.com/@sandzlvu/a-comprehensive-guide-to-types-of-virtualization-d34af8c04cf1** [Accessed 11 May 2024]

ii) Type 1 and Type 2

Type 1 and type 2 hypervisors are software that can be used to run a single physical machine and multiple virtual machines (VMs).

The Type 1 hypervisor sits on top of the metal server and has direct access to hardware resources.

The type 1 hypervisor has a very efficient architecture. Multiple virtual machines can be managed and allocated resources directly without the host operating system being involved. The risk of instability is reduced by the absence of a host operating system, making these hypervisors safer.

Type 2 hypervisors are programs that are installed on a host operating system. Hosted hypervisors, like other software applications, are limited in their ability to control computer resources. The system administrator instead allocates resources to the hosted hypervisor and distributes them to the virtual machines.

Even though they differ, both types of hypervisors are useful in different applications. Enterprise cloud data centres utilize Type 1 hypervisors or Bare-metal hypervisors for virtual machine allocation due to their efficiency, scalability, and flexibility. Additionally, a type 1 hypervisor is generally more secure and stable because it doesn't run on top of an operating system.

Type 2 hypervisors are used by administrators due to their ease of use. In situations where users desire to use two or more operating systems simultaneously, but have limited access to one machine, they are also favoured. Installing, configuring, and using Type 2 hypervisors is easier than using Bare-metal hypervisors. It is comparable to the installation and usage of other desktop applications.

AWS (n.d.) *What's the Difference Between Type 1 and Type 2 Hypervisors?* Available at: **https://aws.amazon.com/compare/the-difference-between-type-1-and-type-2-hypervisors/** [Accessed 11 May 2024].

iii) Cloud Service Provider (CSP)

Cost is a significant factor in deciding between going in the Cloud Services Provider or Investing Directly in Hardware. In order to compare cloud costs with on-premises costs accurately, it is important to first calculate the total cost of ownership (TCO), by taking into account factors such as purchase price, maintenance, and lifetime operating costs.

Essentially, TCO = Capital expenditures (CapEx) + Operating expenditures (OpEx)

On-premises TCO calculation is challenging due to numerous hidden costs. The following table shows the breakdown of Capex and OpEx for on-Prem hosting.

On-Premises	
CapEx	**OpEx**
Server Purchase	Lifetime updates and improvements
Storage Fees	Maintenance
Security	Technical Support
Network	Staff training
Internet	Energy Consumption
Software licenses	Temperature monitoring
Infrastructure design	End of life disposal
Backup and disaster recovery system	Equipment replacement
Datacenter	

Chaitanya (Chey) Penmetsa (2024) On-Premises CapEx/OpEx. Available at: https://medium.com/codenx/cloud-vs-on-premises-8f4a3dc1cf18 (Accessed 11 May 2024)

It is undoubtedly important to emphasize the advantages of greater security, total control over IT resources, and independence of the internet connection.

On the other hand, the disadvantages of this approach include high expenses, complex data recovery, and limited flexibility.

In the same way, the breakdown of capital expenditures and operating expenses for cloud services is shown in the following table.

Cloud	
CapEx	**OpEx**
Subscription Fees	Integration costs for connecting systems
Migration costs for data and applications	Management costs for scaling, trouble shooting and complaince costs.
Training	Support
	Data Recovery costs
	Governing limits

Chaitanya (Chey) Penmetsa (2024) Cloud CapEx/OpEx. Available at: https://medium.com/codenx/cloud-vs-on-premises-8f4a3dc1cf18 (Accessed 11 May 2024)

Cloud-based solutions will experience a continuous increase in operating expenses, along with limited control over data ownership and reliance on internet connectivity for data recovery.

Nonetheless, it is notable for offering significant cost efficiency, speeding up time to market, providing advanced security, and improving operational efficiency.

In conclusion, the choice between the two options is dependent on the specific priorities and needs of each organization, which requires a careful analysis of costs and benefits to make a decision.

Medium (2024) *Cloud Vs On-premises*. Available at: https://medium.com/codenx/cloud-vs-on-premises-8f4a3dc1cf18 [Accessed 11 May 2024]

4. CAOSN in Industry

Artificial Intelligence / Machine Learning

Machine Learning (ML) is considered a subfield of AI and computer science that focuses on the application of data and algorithms to duplicate the method humans learn, gradually increasing their precision.

IBM (n.d.) *What is machine learning (ML)?* Available at: https://www.geeksforgeeks.org/logical-and-physical-address-in-operating-system/ [Accessed 12 May 2024]

Companies today often use machine learning as a method to deploy artificial intelligence programs, which is why terms are often used interchangeably and sometimes ambiguous. Computers can learn without being explicitly programmed thanks to machine learning, a subfield of artificial intelligence.

"In just the last five or 10 years, machine learning has become a critical way, arguably the most important way, most parts of AI are done," said MIT Sloan professor Thomas W. Malone, the founding director of the MIT Centre for Collective Intelligence. "So that's why some people use the terms AI and machine learning almost as synonymous … most of the current advances in AI have involved machine learning."

Machine learning is becoming more and more common, resulting in every business requiring practical knowledge in this field. According to the 2020 Deloitte survey, 67% of companies are employing machine learning and 97% intend to do so next year.

Machine learning is a key component of certain companies' business models. For other companies, while not their main business proposition, they are deeply engaged with machine learning.

In general, machine learning is being employed by companies in different ways, such as, *Recommendation Algorithms,* providing recommendations that are based on Netflix and YouTube suggestions, *Image Analysis and Object Detection,* identifying people and distinguishing them by analysing images, *Fraud Detection*, detecting credit card transactions that may be fraudulent by analysing patterns, and other related areas, such as Medical Imaging and Diagnostics, and Self-Driving Cars.

It is believed that quantum computing will lead to developments in speed optimization for machine learning in the coming decades. Furthermore, the upcoming years are predicted to inaugurate a significant innovation, a multipurpose device capable of carrying out multiple tasks simultaneously.

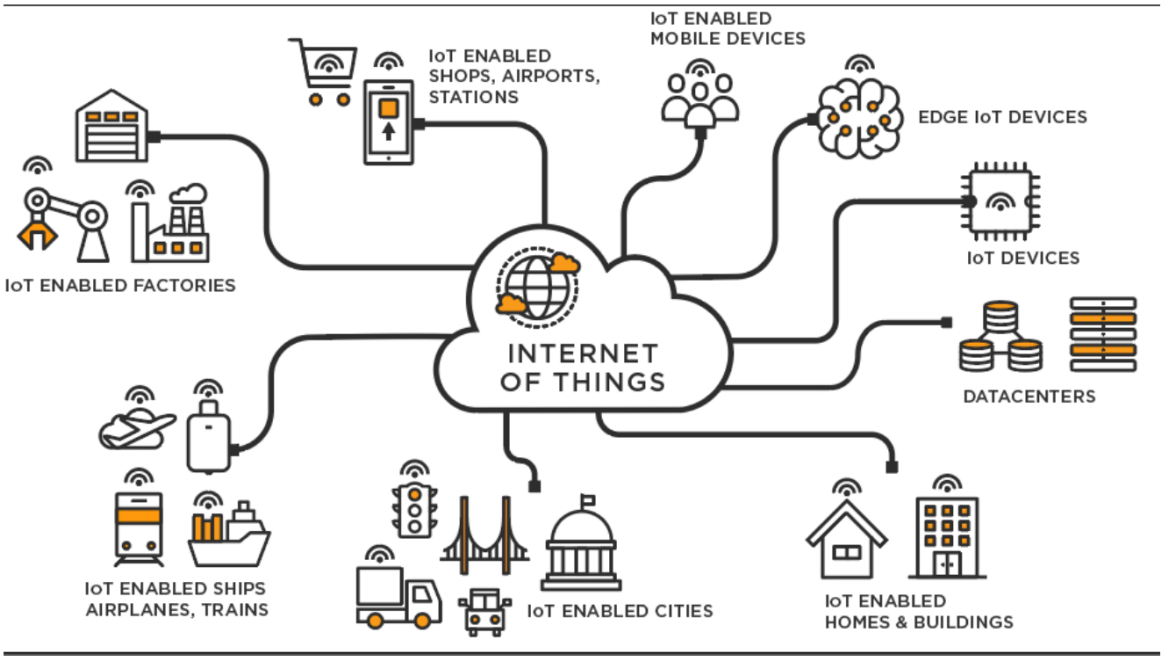
MIT (2021) *Machine learning, explained.* Available at: https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained [Accessed 12 May 2024].

Internet of Things/Internet of Everything

The Internet of Everything (IoE) is a system that connects and manages a large number of computing elements and sensors, inanimate and living entities, people, processes, and data through the Internet infrastructure. To put it simply, it involves a network of connected devices and the technology that enables them to communicate, including the cloud and other services.

A high-level view of IoT components can be seen in the following image.

IoE (n.d.) The *Internet of Everything (IoE)* Available at: https://ioe.org [Accessed 13 May 2024]



University of Michigan (2023) Internet of Things. Available at: https://businesstech.bus.umich.edu/uncategorized/tech-101-internet-of-things/ (Accessed 11 May 2024)

Increasingly, everyday devices like kitchenware, televisions, lights, and thermostats are being connected to the Internet, which allows for more features and customization for users. Smart cities, smart cars, and wearable devices (like Fitbit and Apple Watch) are all common examples of IoT.

The impact of IoT on pre-existing industries can be seen in the way devices like sensors and equipment are used, giving industries detailed real-time data that can be used to improve business processes. They offer insights into supply chain management, logistics, human resources, and production, which leads to cost savings and increased revenue streams.

IoT is frequently used in different verticals like manufacturing, automobiles, logistics, transportation, and retail.

The impact of the Internet of Things on human life and work is extensive. The ability to perform more heavy work, handle tedious tasks, and improve life by making it healthier, more productive, and more comfortable.

A world of IoT offers unlimited possibilities, fostering a future that goes beyond Innovation Acceleration, through advanced analytics, including security assessment, through continuous digital monitoring, optimizing performance, improving efficiency, and reducing safety risks.

In a nutshell, IoT is rapidly altering our approach to the world around us, From household devices to industrial supply chains, improving processes, improving efficiency, and providing valuable insights in real-time.

The evolution and expansion of IoE is expected to lead to an era of even deeper connectivity. Further expansion of the reach and impact of IoE is expected due to advances in artificial intelligence, cybersecurity, and data integration.

Despite the exciting opportunities, there are also significant challenges, including issues of privacy, security, and accessibility fairness.

IoE's future is promising, with the potential to enhance our lives, foster innovation, and shape a more connected and efficient world.

University of Michigan (2023) TECH 101: INTERNET OF THINGS. Available at: https://businesstech.bus.umich.edu/uncategorized/tech-101-internet-of-things/ [Accessed 13 May 2024]

5. Memory Management and Scheduling

i) Physical and Logical memory

During the execution of a program, the CPU generates a logical address, also known as a virtual address, since it is not physically present in the main memory. This logical address represents the exact location of the data required in memory and is translated to a physical address. This translation is performed by the Memory Management Unit (MMU).

The logical or virtual address is what the process sees and is related to the address space of the program. This address is used by the process to access memory, and is then translated by the operating system into a physical address. During program execution, the CPU creates this logical address as a reference to access memory.

On the other hand, the physical address refers to the exact location in the main memory where the data is stored. Instead of a virtual address, the physical address represents a real location in memory. It is the MMU that uses the physical addresses to translate the logical addresses into corresponding physical addresses. To access the physical address, the user must use the logical address that corresponds to it instead of accessing it directly.

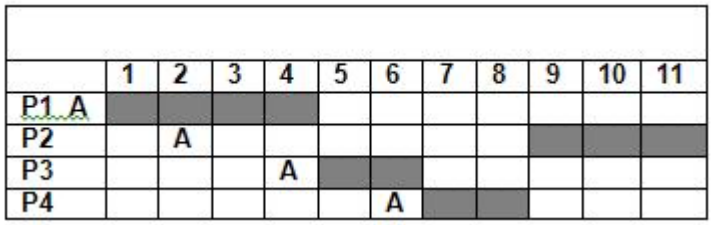
Both logical and physical addresses share similarities, such as, both are used to identify a specific location in memory, both can be represented in different formats, such as binary, hexadecimal or decimal, also both have a finite range, which is determined by the number of bits used to represent them.

To sum up, managing memory in computer systems involves converting logical addresses generated by the CPU during program execution into physical addresses in the main memory. The MMU is responsible for mapping the logical addresses to their physical equivalents during this translation process. Physical addresses are used by the process to locate data in main memory, while Logical addresses represent the program's address space. Both types of addresses have differences, but they both have the ability to identify a specific location in memory and represent it in different formats. Understanding logical and physical addressing concepts can enable computer systems to manage and optimize memory usage to ensure program performance and efficiency.

Geeks for Geeks (2024) *Logical and Physical Address in Operating System*. Available at: https://www.geeksforgeeks.org/logical-and-physical-address-in-operating-system/ [Accessed 11 May 2024]

ii) The following diagrams show four processes, with their respective Arrival Times and Burst Times.

Process Name	Arrival Time	Burst Time
P1	0	4
P2	2	3
P3	4	2
P4	6	2



If the algorithm used was non pre-emptive, which of the following is it most likely to be:

Shortest Process First (SPF) is the answer. Due to Burst Time being superior to processes P3 and P4, process P2 was executed after the shortest process were executed.(Non-pre-emptive).

Geeks for Geeks (2023) *Program for Shortest Job First (or SJF) CPU Scheduling | Set 1 (Non- pre-emptive).* Available at: https://www.geeksforgeeks.org/program-for-shortest-job-first-or-sjf-cpu-scheduling-set-1-non-preemptive/ [Accessed 13 May 2024]

iii) Calculate the average waiting time of the system for the processes depicted above.

Response (Waiting) Time = (Total BT – Arrival Time)

P1 = 0 times unit

P2 = (8 – 2) = 6 times unit

P3 = (4 – 4) = 0 times unit

P4 = (6 – 6) = 0 times unit

Average Response Time = AvgRespTime = [(P1 + P2 + P3 + P4) / 4]

AvgRespTime = (0 + 6 + 0 + 0)/4 = 1.5 times unit

Geeks for Geeks (2023) *Program for Shortest Job First (or SJF) CPU Scheduling | Set 1 (Non- pre-emptive).* Available at: https://www.geeksforgeeks.org/program-for-shortest-job-first-or-sjf-cpu-scheduling-set-1-non-preemptive/ [Accessed 13 May 2024]