Midterm

Due Mar 24 at 9:15pm **Points** 100 **Questions** 10
Available Mar 24 at 6:30pm - May 27 at 11:59pm 2 months **Time Limit** 180 Minutes

Instructions

- **The exam is open-book: you may use the text book in a hard or electronic copy, but *nothing* else;**

- **You must be alone answering questions. No communication with anyone else is allowed, nor is it permitted to use web search.**
- **You have to respond to each of the 10 questions in the shortest way possible, never to exceed the space allowed on the page. The CA may deduct points for irrelevant discussions. If you feel that you don't understand the question or don't know the answer, write just this—it is perfectly all right!**

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	167 minutes	0 out of 100 *

* Some questions not yet graded

ⓘ Correct answers are hidden.

Score for this quiz: **0** out of 100 *
Submitted Mar 24 at 9:17pm
This attempt took 167 minutes.

Question 1

Not yet graded / 5 pts

1. **(5 points)** Give one example of each a) SaaS, b) PaaS, and c) IaaS. (Try to think of your own examples rather than the ones that are given in the book.)

Your Answer:

a) SaaS: SaaS stands for Software-as-a-Service. SaaS provides the capabilities to the customer to use the provider's application running on a Cloud infrastructure. The application running is accessible from various client devices through either a thin client interface.

Example: Dropbox, Slack

b) PaaS: PaaS stands for Platform-as-a-Service. PaaS provides capabilities to the customer to deploy onto the cloud infrastructure or acquired applications created using programming languages, libraries, services, and tools supported by the provider but does not manage or control the cloud infrastructure.

Example: Windows Azure, AWS Elastic Beanstalk

c) IaaS: IaaS stands for Infrastructure-as-a-Service. IaaS provides the capabilities to the customer to provision processing, storage, network, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which even includes operating systems and applications but does not manage or control Cloud infrastructure.

Example: AWS EC2, Google Compute Engine (GCE)

Question 2

Not yet graded / 5 pts

1. **(5 points)** Explain what problem the HSMs solve and how exactly an HSM helps with the security of outsourcing IT to the Cloud.

Your Answer:

A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.

You can store your keys within an HSM and use them to encrypt and decrypt data while keeping them safe and sound and under your full control. You are the only one with access to the keys stored in an HSM.

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud. With CloudHSM, you control the encryption keys and cryptographic operations performed by the HSM.

AWS CloudHSM runs in your own Amazon Virtual Private Cloud (VPC), enabling you to easily use your HSMs with applications running on your Amazon EC2 instances. With CloudHSM, you can use standard VPC security controls to manage access to your HSMs. Your applications connect to your HSMs using mutually authenticated SSL channels established by your HSM client software. Since your HSMs are located in Amazon datacenters near your EC2 instances, you can reduce the network latency between your applications and HSMs versus an on-premises HSM.

Question 3

Not yet graded / 10 pts

1. **(10 points)** Explain what it means that an instruction is *not* virtualizable and give an example of such an instruction's behavior. Provide several examples of x86 instructions that are not virtualizable.

Your Answer:

Popek and Goldberg's requirements must be met for instructional be virtualizable, but in the case when the instruction is not virtualizable these requirements are overruled. The operating system runs in modes i.e. user mode or system mode. When any privileged or sensitive instruction which is supposed to run under only system mode and the instruction traps and when executed in user or guest mode. This attempt of utilizing or modifying any system application or resource by the user is termed as not virtualizable instructions.

Non-virtualizable instructions fall into three classes. In first-class, A major problem is that the processor has only one register for each of these, which means that they need to be replicated for each virtual machine. In the second class, the instructions that copy parts of the STATUS register into either general registers or memory and in third class, instructions that

reference the storage protection system, memory, or address relocation systems.

The problem with x86 instructions is that the instructions were allowed while being executed in the user mode to transfer the value of the STATUS register to a general register. This instruction is behavior-sensitive in the Popek and Goldberg taxonomy because it allows a user program to discover which model is running in it.

Examples of x86 instructions that are not virtualizable are:

1) Instructions that read and write the values of the segment table registers as well as the interrupt table register.

2) Instructions that copy parts of the STATUS register into either general registers or memory (including the stack).

3) Instructions that depend on memory protection and address relocation mechanisms.

4) Instructions that are supposed to execute only in system mode and do not trap when executed in the user mode.

Question 4

Not yet graded / 10 pts

1. **(10 points)** Explain how a hypervisor can be run on top of a hypervisor and provide an example where such a feature is being used. Can KVM run on top of XEN?

Your Answer:

A hypervisor is a crucial piece of software that makes virtualization possible. It abstracts guest machines and the operating system they run on, from the actual hardware.

Nested virtualization refers to virtualization that runs inside an already virtualized environment. In other words, it's the ability to run a hypervisor inside of a virtual machine (VM), which itself runs on a hypervisor.

With nested virtualization, you're effectively nesting a hypervisor within a hypervisor. The hypervisor running the main virtual machine is considered

a level 0, or LO hypervisor, and the initial hypervisor running inside the virtual machine is referred to as a level 1 or L1 hypervisor. Further nested virtualization would result in a level 2 (L2) hypervisor inside the nested VM, then a level 3 (L3) hypervisor within that nested VM, and so forth.

VMware supports installing one or more ESXi servers within an instance of ESXi.

Yes, KVM can run on top of XEN

Question 5

Not yet graded / 10 pts

1. **(10 points)** Explain the problem that the I/O MMU solves. What problems are introduced when using the I/O MMU?

Your Answer:

A virtual machine may not have direct access to an I/O device since each I/O device is “married” to its machine. Therefore a hypervisor must either directly emulate a device or use para-virtualized drivers.

To deal with this problem, a type of MMU (appropriately called the I/O MMU—sometimes also spelled IOMMU) is employed, where the MMU performs virtual-to-real memory translation for the CPU, the I/O MMU performs this function for DMA. With that, the memory space is partitioned among the devices, and the translation and partitioning caches are typically included with hardware, which often provides memory protection.

This approach supports virtual machine isolation and provides a degree of security. Yet, the challenge here is posed by dynamic translation mappings. The issues are similar to general paging, and the overarching problem is the performance penalty resulting from the extra work that the hypervisor needs to perform. In fact, this work needs to be performed before DMA has finished a memory transfer, which brings yet another problem of the tolerable delay in DMA operations.

Question 6

Not yet graded / 10 pts

1. (**10 points)** Explain how XEN supports I/O processing in a guest operating systems.

Your Answer:

Xen supports both para-virtualized and fully virtualized guests, respectively called PV and HVM. For guests running in HVM, XEN emulates low-level hardware and firmware components—such as graphic, network, and BIOS adapters, using techniques described in the previous section. Predictably, emulation often results in degraded performance. XEN deals with this by creating yet another mode, called PV-on-HVM (or PVHVM), in which an HVM guest is para virtualized only partly. Xen's approach to handling physical I/O devices is straightforward and elegant. XEN creates a special environment—called a domain—for each guest.

Question 7

Not yet graded / 10 pts

1. (**10 points)** What is the difference between the virtual machine and a container? Provide an example of a situation where you would use a Linux container rather than a virtual machine.

Your Answer:

Virtual Machine versus Container:

1) Virtual Machines are used to run only a single application in an operating system, but Container are used to run many applications.

2) The resources (like memory, disk space, and CPU utilization) available in Virtual Machine are much lesser in size as compared to Containers.

3) Containers have more economical ways than Virtual Machines to move to the cloud.

4) Containers are more efficient than Virtual Machines as it provides more and necessary resources for any computation or processing.

5) Virtual Machines can run more user or guest operating system and operating system have full control of the machine, whereas Contains have control of operating system userspace.

Situations to use Container rather than a Virtual Machine

1) While rewriting an application based on microservices, the user must use Container.

2) Containers should not be used while writing an application from scratch.

Question 8

Not yet graded / 10 pts

1. (**10 points)** NAT prevents the internal IP addresses from being seen outside. Can an ISP assign to a host behind a NAT box an IP address that is already assigned to some other host, which is not shielded by NAT)? If yes, explain why. If not, show what may be a problem with that.

Your Answer:

Yes, it is possible because it translates the IP address of the hosts within its network and stores in Network Address Table and gives out a mapped address to communicate outside the NAT box, which differs from the original address. Hence, that IP is never visible to the hosts outside the NAT network, and hence the two IPs would never be the same and the communication between the hosts can flow seamlessly without conflict.

Question 9

Not yet graded / 10 pts

1. **(10 points)** Given the implementation of a NAT box that we discussed in class, what is the major factor (independent on the memory capabilities) that limits the number of the active connections that a single NAT box can support at any given time? (In other words,

consider the UDP packet header below and provide the absolute upper bound for the number of all possible UDP-based “connections.” (You don’t need to be concerned with the number of reserved ports.)

Your Answer:

NAT Stands for Network Address Translation, it is used to send the request to the internet from a private virtual cloud. This safeguards the internal network from the security attacks.

The maximum number of connections that a single NAT box can maintain is 2^{16} ie 65,536, and support up to a maximum of 64k bit connections. The factor determining the maximum number of connections is the number of ports of the source and destination IPs and the ports associated with it.

UDP ports range from 0 to 65,535, hence 65535 UDP connection could be made.

Question 10

Not yet graded / 20 pts

1. **(20 points)** You are building your own cloud with two remote data centers, each of which runs an Ethernet LAN. The respective sets of LAN addresses in these centers are A, and B. The data centers are interconnected with the MPLS-supporting networks, and so each data center has its own MPLS switch capable of performing layer-2 switching function. Show how you can implement the Layer-2 WAN supporting the combined range of addresses, **A** U B. (You need to describe the switch logic in deciding how to handle outbound and inbound frames based on the destination addresses and define the LSPs needed for the WAN operation.)

Your Answer:

The servers of a data center need to be interconnected, and they need to connect to the outside world as well. As the number of servers increases, more cables have to fit into a given space. Top-of-Rack (ToR) and End-of-Row (EoR) are two approaches to connectivity resulting in different cabling options. In the ToR approach, each rack has a switch at the top to which all servers in the rack connect. As a result, the cable connecting a server to the ToR switch does not need to be longer than the height of the rack. A ToR switch typically provides external network access. Normally, it is sufficient for a ToR switch to have just enough ports to support the servers within the same rack. In the EoR approach, each row (of racks) has a switch at its end to which all nearby servers and switches in other racks in the same row connect. This may require long cables of different lengths running between the servers and switches. Depending on its actual length and required bandwidth, a fiber-optic cable may be needed (where a copper connection would suffice in the ToR case). Here the cost of cabling could exceed the cost of a server supporting multiple links. An EoR switch is placed in a rack (possibly all by itself due to its size). It may provide network access and aggregation. Both ToR and EoR switches are typically implemented using Ethernet technology. We will return to this subject later. For now, we just note that Ethernet technology is particularly important to data centers because of its potential to eliminate employing separate transport mechanisms (e.g., FC) for storage and interprocessor traffic. Depicts a next-generation data center with common Ethernet transport. Finally, note that the data-center aggregation network connects to the Wide Area Network (WAN) through a gateway. On the other side of the WAN may be a single user device or a full-blown data center

Quiz Score: **0** out of 100