CS 5472 - Advanced Topics in Computer Security

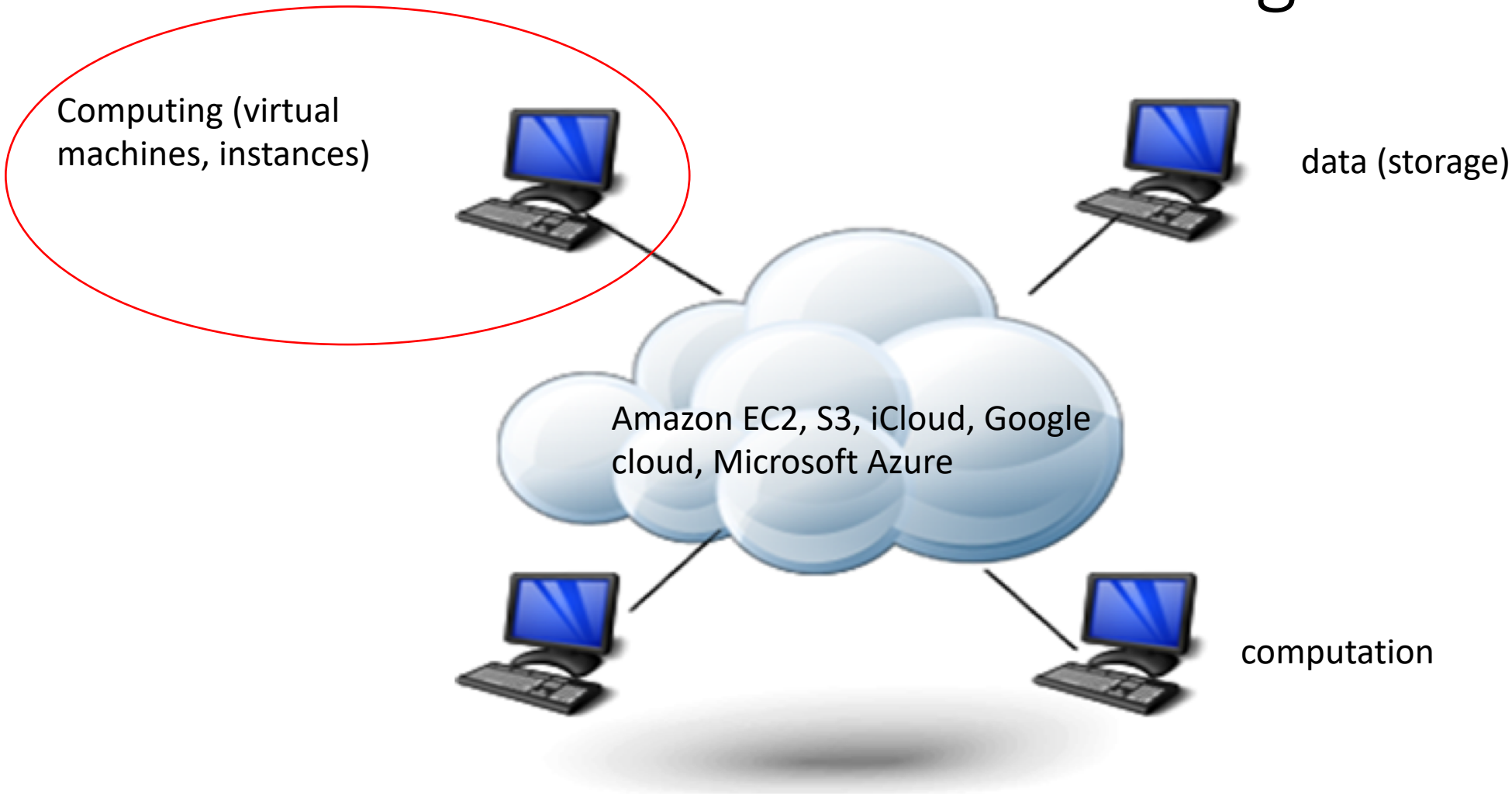
Topic 2: Security in Cloud Computing (2)

Spring 2023 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu

Term Project Proposal Next Week

- Approximately 15 mins for each student (can be a bit more, but don't exceed 20 mins)
- Select the topic (our of the 10 topics we introduce in the class, or other security topic for your own interest)
- What is the specific problem you want to address?
- Why do you want to address this problem (interesting? useful? change the world?)?
- What have been done by other people for this problem (literature review)?
  - Analyze the literature by reading some papers from google scholar
- What is your preliminary/initial idea or thoughts on this problem?
- What is your plan, schedule?
- Any others?

Cloud's Basic Model - Outsourcing



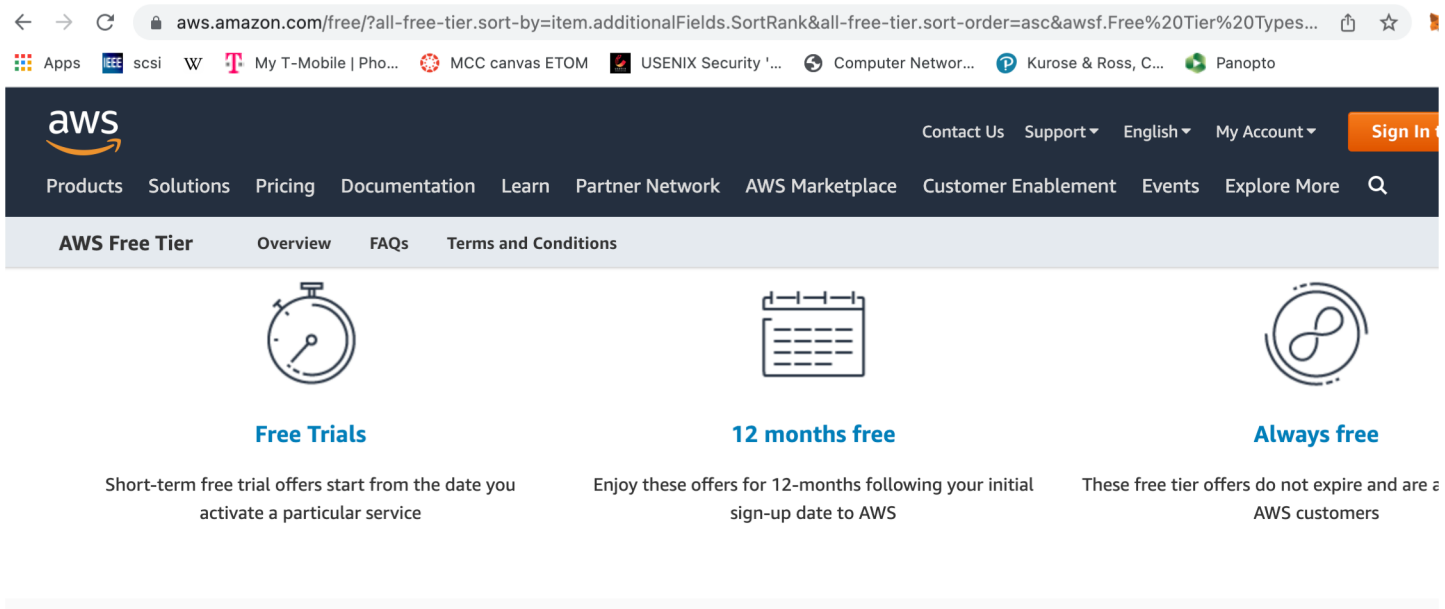
Outsource Computing Infrastructures

- **Ex-"cloud era"** – in a "hard" way
  - Buy/Rent a computer/ server, rent the space/bandwidth from the provider

- **Cloud era** – in a "soft" way
  - Simply launch virtual machines (virtualization) with promised computational resources
  - In this say, selling computing service is just like selling utility (electricity, water, gas, etc) – the first time to make selling computing possible
  - Great for the small and medium size businesses, since they cannot afford to construct their own data centers, but can afford to buy some computing services just like buying electricity, water, and "pay as they go"

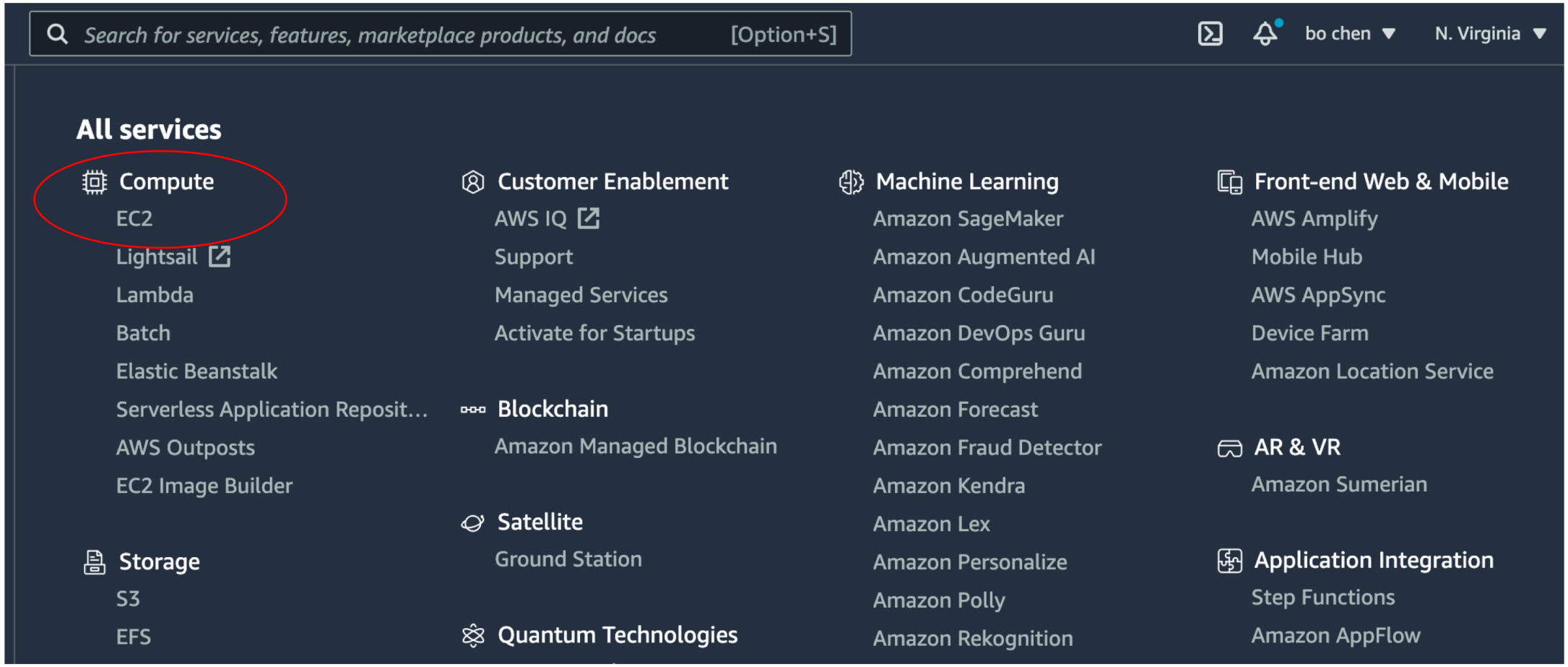
Try The Public Cloud Computing Service Yourself

- AWS free tier allows you to use the cloud computing service for free for one year
  - https://aws.amazon.com/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc



- https://aws.amazon.com

Amazon Elastic Compute Cloud (EC2)



https://aws.amazon.com/

Create a AWS account, and you can easily launch some cloud instances, and run your services/business …

Outsource Computing Infrastructures in a “Soft” Way

Amazon EC2 instance (virtual machine):

	vCPU	ECU	Memory (GiB)
General Purpose - Current Generation			
t2.nano	1	Variable	0.5
t2.micro	1	Variable	1
t2.small	1	Variable	2
t2.medium	2	Variable	4
t2.large	2	Variable	8
t2.xlarge	4	Variable	16
t2.2xlarge	8	Variable	32
m4.large	2	6.5	8
m4.xlarge	4	13	16
m4.2xlarge	8	26	32
m4.4xlarge	16	53.5	64

What is The Technology Behind Cloud Computing - Virtualization?

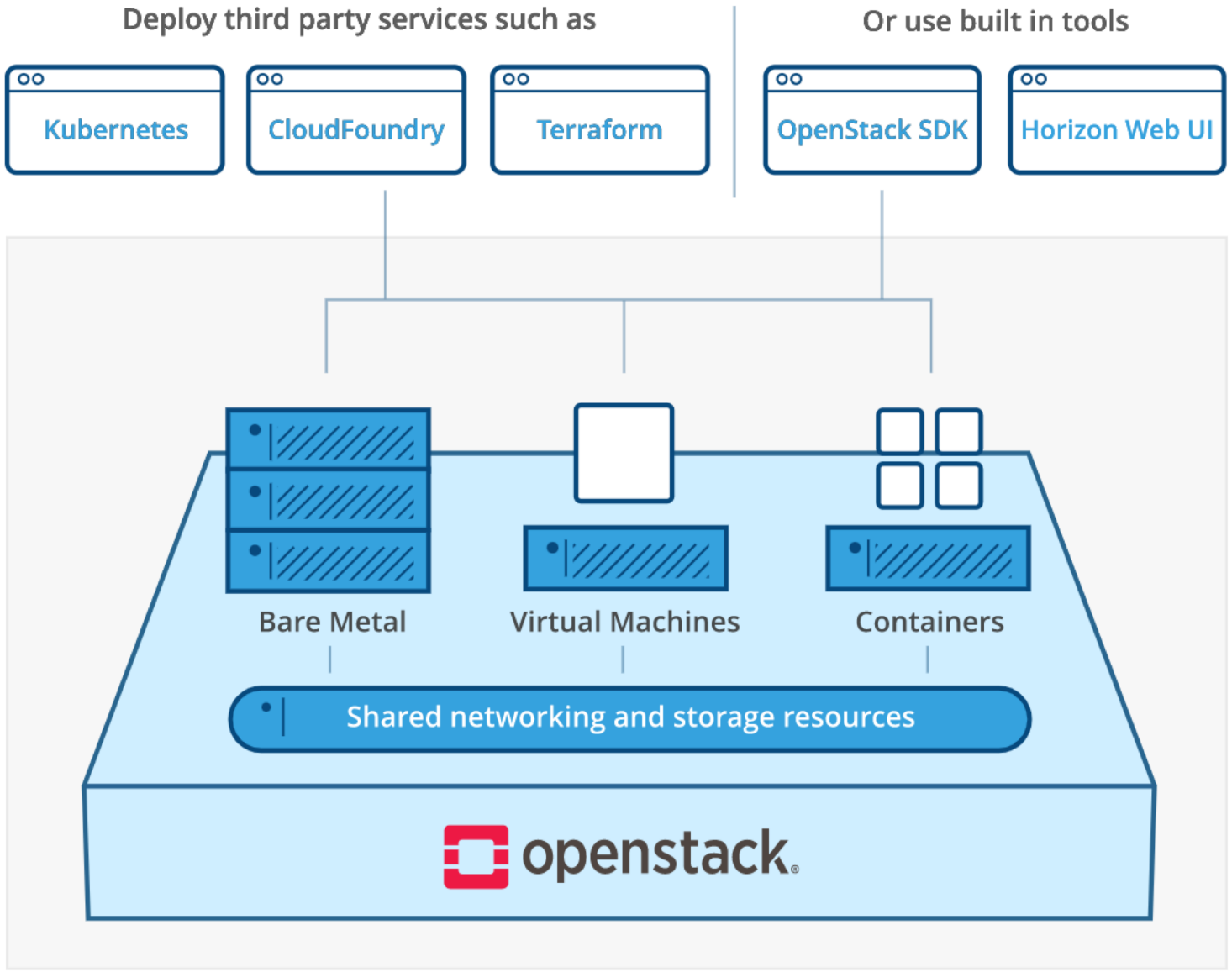
- Virtualbox can allow to create multiple virtual machines, each running a different operating system

- Cloud computing simply follows this idea, but
  - The cloud provider (e.g., Amazon) maintains a large number of physical computers (organized into data centers around the world)
  - Users can easily create their own virtual machines
  - A “virtualbox”-like software system is incorporated into the cloud to schedule which virtual machine will occupy which physical computer

OpenStack

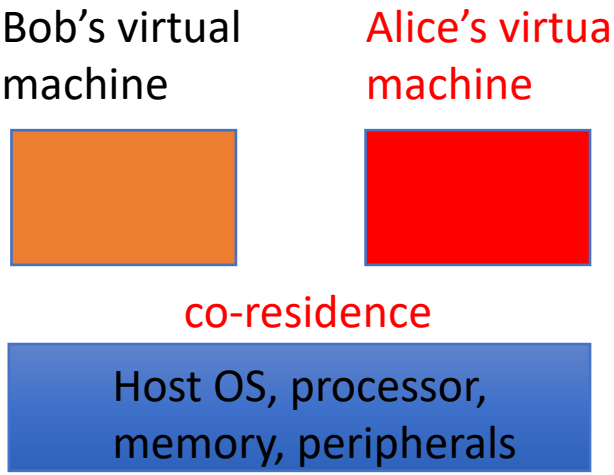
- You can even create your own cloud computing service using OpenStack
  - A free open standard cloud computing platform, mostly deployed as infrastructure-as-a-service (IaaS) in both public and private clouds where virtual servers and other resources are made available to users
  - It consists of interrelated components that control diverse, multi-vendor hardware pools of processing, storage, and networking resources throughout a data center.
  - Nova is the OpenStack component that provides a way to provision compute instances (aka virtual servers). Nova supports creating virtual machines, baremetal servers. Nova runs as a set of daemons on top of existing Linux servers to provide that service
- https://www.openstack.org/

OpenStack


Deploy third party services such as
Or use built in tools
Kubernetes
CloudFoundry
Terraform
OpenStack SDK
Horizon Web UI
Bare Metal
Virtual Machines
Containers
Shared networking and storage resources
openstack.

What Are The Potential Security Issues?

Different virtual machines may share the same physical hardware (e.g., processors, memory) – co-residence



Bob is a victim, and Alice is an hacker.

A physical computer from Amazon AWS

What Are The Potential Security Issues (cont.)?

Different virtual machines may share the same physical hardware (e.g., processors, memory)

Bob's virtual machine

Alice's virtual machine

Bob is a victim, and Alice is an hacker.

A physical computer from Amazon AWS

Host OS, processor, memory, peripherals

Share processor

User space (attacker)

Meltdown

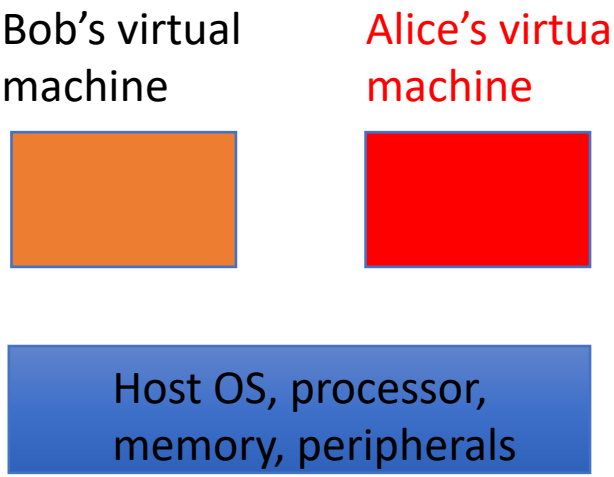
Kernel space (victim)

App 1 (attacker)

Spectre

App 2 (victim)

What Are The Potential Security Issues (cont.)?



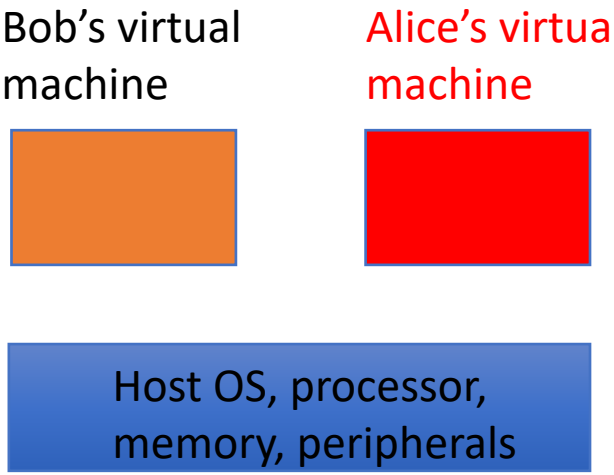
Bob is a victim, and Alice is an hacker.

Share cache/memory

A physical computer from Amazon AWS

Can the attacker infer something about the victim virtual machine by this shared cache/memory (side channel attacks)?

What Are The Potential Security Issues (cont.)?



Bob is a victim, and Alice is an hacker.

A physical computer from Amazon AWS

But how can the attacker approach the victim virtual machine so that it will be co-resident with the victim virtual machine to perform various attacks?

How to Approach A Victim Instance (Virtual Machine) in The Public Cloud?

To make sure the attack can be successful, a major issue the attacker needs to address is to launch an instance which is co-resident with the victim instance

- How to find out where in the cloud infrastructure the victim instance is located? (Cloud Cartography)
- How can an adversary launch instances that will be co-resident with the victim's instance?
- How to verify whether two instances are co-resident on the same physical machine?
- How to exploit cross-VM information leakage once co-resident?

The Future of Cloud Computing

- Our society will rely more and more on cloud computing
  - AI and big data: a lot of AI computation and big data storage need the cloud platform since no organization would be able to afford the cost of a computation/storage intensive applications
  - IoT (Internet of things): IoT needs cloud, since 100 billion IoT devices would not be easily handled
    - Amazon, Microsoft, Google etc have specifically built IoT clouds (could be a research project for you)
  - Blockchain would be integrated with the cloud computing:
    - You have seen FileCoin previously which can decentralized cloud storage using the blockchain technique. There are more …

    - There are emerging technologies which decentralize cloud computing using the blockchain technique

Paper Presentation

- Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds

- Presented by Suruchi Kushwaha