The Cloud, Virtualization, and Security
The Cloud, Virtualization, and Security

A Cloud:
Large groups of remote servers that are networked to allow centralized, shared data storage and online access to computer services or resources.
The Cloud, Virtualization, and Security

A Cloud:
Large groups of remote servers that are networked to allow centralized, shared data storage and online access to computer services or resources

A Public Cloud:
A cloud service provider offers cloud services to many organizations - Amazon Elastic Compute Cloud, IBM Blue Cloud, Google AppEngine, Windows Azure
The Cloud, Virtualization, and Security

A Cloud:
Large groups of remote servers that are networked to allow centralized, shared data storage and online access to computer services or resources

A Public Cloud:
A cloud service provider offers cloud services to many organizations - Amazon Elastic Compute Cloud, IBM Blue Cloud, Google AppEngine, Windows Azure

A Private Cloud:
The cloud infrastructure is open to one organization with many tenants - Intel's Cloud
The Cloud, Virtualization, and Security

A Hybrid Cloud:
Use of two or more service delivery models -
ex: *cloudbursting*
where an application runs in a private cloud or
data center and bursts into a public cloud when
the demand for computing capacity spikes.
The Cloud, Virtualization, and Security

A Hybrid Cloud:
Use of two or more service delivery models -
ex: *cloudbursting*
where an application runs in a private cloud or
data center and bursts into a public cloud when
the demand for computing capacity spikes.

A Community Cloud:
A cloud that is organized for a community of groups
with similar interests, such as security.
The Cloud, Virtualization, and Security

What's so good about a public Cloud?

1. Easy and inexpensive to set-up because hardware, application, and bandwidth costs are covered by the cloud provider.

2. Can be **elastic** – that is, the resources and services available to the user are what the user requests and requests can change with time - if the user wants less, less is provided, if the user wants more, more is provided. This can even be done automatically!

3. The user pays only for what it uses

4. There are several delivery models available to the user
The Cloud, Virtualization, and Security

What's so bad about a public Cloud?

1. Generally, the user has lost some or all control of its data

2. Generally, the user does not know where its data is or even how many copies of it are floating around or even who is able to view the data

3. Generally, configuration management is difficult. Updates may be unwanted or maybe desired updates are not provided

4. Cloud APIs are readily available but the implementation of those APIs is proprietary so modifications are not allowed

5. Downtime may occur unexpectedly
The Cloud, Virtualization, and Security

Delivery Models:

1. **DSaaS**:
   - Data Storage as a Service
     providers rental space to subscribers
     price based on amount and transfers
   - Delivery Server as a Service
     user can provide services, serve information
   - Deep Security as a Service
     enables quick and easy security to be added to cloud workloads for instant protection.
The Cloud, Virtualization, and Security

Delivery Models:

2. **IaaS**: Infrastructure as a Service
   - User self-provisions the resources it needs to run platforms and applications.
   - User “outsources” hardware equipment to be used in normal operations (HDs, NICs, etc)
   - Service provider owns the equipment and is responsible for housing, running, and maintaining it
   - pay-as-you go billing automation of administrative tasks
   - dynamic scaling - elastic
desktop virtualization - virtual OSes on same comp
- policy-based services - supports analysis of usage
The Cloud, Virtualization, and Security

Delivery Models:

2. **IaaS**: Infrastructure as a Service
   - Resource is available as and when the client needs it so there are no delays in expanding capacity or the wastage of unused capacity
   - Underlying physical hardware supporting IaaS is set up and maintained by the cloud provider, saving time and cost of doing so on the client side
   - Can usually be accessed from any location with internet connection and cloud access policy accept
   - Physical security of the infrastructure is good
   - No single point of failure – hardware can get moved around
The Cloud, Virtualization, and Security

Delivery Models:

3. **PaaS**: Platform as a Service
   - User develops cloud-aware applications using development tools
   - User rents virtual OSes to run specific applications
   - OS features can be changed and upgraded frequently
   - Developers on the same project can be anywhere with IaaS several duplicated infrastructures may be needed to do this
   - Developers may even be non-expert (wordpress)
   - Services can cross international boundaries
The Cloud, Virtualization, and Security

Delivery Models:

4. **SaaS**: Software as a Service
   - User runs applications via devices on the cloud infrastructure from anywhere because provider manages both applications and data
   - All users see the same version of the software therefore, collaboration may be easier
   - No worries about getting licenses, asking for Hardware or OS
   - Can be done either by the provider supplying commercial software or software specially crafted for the cloud
   - User has no control over patching & configuration management
The Cloud, Virtualization, and Security

Delivery Models:

4. **SaaS**: Software as a Service
   - Processing power required to run the apps is supplied by the cloud provider (no extra cost)
   - No initial setup costs
   - New services or storage can be accessed on demand without having to supply extra software
   - Can be accessed by any Internet-enabled device
   - Customization of software services is possible
The Cloud, Virtualization, and Security

Configuration Management:
- process for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design and operational information throughout its life
- provides visibility and control of product performance, functional and physical attributes
- ensures documentation is consistent with design
- absence of a CM plan can be disastrous in 2010 Wordpress applied a bad patch and caused a very serious service outage
- Originated with U.S. D.o.D. in the 1950s, is now a standard practice in nearly all industries
The Cloud, Virtualization, and Security

Configuration Management:
- CM may be difficult in PaaS across OSes
- In SaaS CM is used to ensure proper control of assets required to deliver services – information on this is accessible when needed
The Cloud, Virtualization, and Security

Why the rush to adopt private clouds?
- public clouds are considered more risky
- private cloud offers speed, agility, and efficiency while maintaining control of sensitive workloads
- user can be up and running in hours or minutes, with minimal interaction with IT – full interaction with IT could takes weeks
- accelerate customer application deployment and promote cloud-aware application design principles
- enables extensions to public clouds, when needed, to manage spikes in demand
The Cloud, Virtualization, and Security

But public clouds may be better
- they tend to have newer software and hardware
- they shift capital expenses to operational expenses
- they offer spare resources instantly (elastic)
- infrastructure costs are lower for new projects
- they move enterprises out of the datacenter business
- economy of scale (compete with Amazon?)
- they attract great security people (they can pay big)
- perimeter complacency - internal network is secure!?
- they are hardened due to continual attacks (better be)
- better penetration testing – more frequent, higher competence of staff
Virtualization is different from cloud computing
- virtualization abstracts compute resources typically as VMs with associated storage and networking connectivity. the cloud determines how those virtualized resources are allocated, delivered, and presented.
- virtualization is not necessary to create a cloud environment, but it enables rapid scaling of resources in a way that nonvirtualized environments find hard to achieve.
- most clouds are built on virtualized infrastructure technology.
- faster service deployment and dynamic placement of workloads
Virtualization is a natural for cloud computing
- provides intelligent abstraction layer which hides the complexity of underlying hardware or software.
- partitioning may be used to support many applications and operating systems in a single physical system.
- since each VM is isolated, each is protected from crashes and viruses in other VMs. In other words, software is decoupled from hardware
- a VM can be represented (and even stored) as a single file, making it easy to identify and present to other applications.
- but I/O bound applications do poorly in virtualized clouds
Virtualization can help with security
- since each VM is isolated, each is protected from crashes and viruses in other VMs. In other words, supports single points of control over multiple systems
- easier and faster disaster recovery
- supports role-based access
- supports additional auditing and logging capabilities for large infrastructures.
The Cloud, Virtualization, and Security

Virtualization has problems wrt security
- monitoring systems are based on device history but now devices are virtualized
- there are a vast number of configuration options that security and system administrators need to understand, with an added layer of complexity that has to be managed by operations teams
- access controls must be carefully and competently planned since so many virtualized technologies can connect to network infrastructure
- access to sensitive outsourced data has to be limited to a subset of privileged users to mitigate the risk of abuse of high privilege roles
The Cloud, Virtualization, and Security

Security considerations
- **access**: access to sensitive outsourced data must be limited to a subset of privileged users
- **data segregation**: one instance of customer data has to be fully segregated from other customer data
- **privacy**: exposure of sensitive information stored on platforms implies legal liability and loss of reputation
- **bug exploitation**: prevent exploit of software bug to steal data or grab resources and allow further attacks
- **recovery**: must provide an efficient replication and recovery mechanism should a disaster occur
- **accountability**: monitoring is often a mandatory requirement because it enhances security and reduces risk
The Cloud, Virtualization, and Security

Security considerations
- **privacy**: exposure of sensitive information stored on platforms implies legal liability and loss of reputation
- **accountability**: monitoring is often a mandatory requirement because it enhances security and reduces risk

**Note the tradeoff:**
If something goes wrong, an investigation may be launched. This may expose faulty components or internal cloud resource configuration details. Then, a cloud customer might be able to learn information about the internal structure of the cloud that could be used to perform an attack.
The Cloud, Virtualization, and Security

Cloud Security Model

SU and SP have no physical control over the cloud machines

Cloud machine status cannot be observed by SU and SP

Attacks:
- CP resources – steal to mount...
- SP resources – botnet attack
- CP data – steal to modify...
- SP data – service or node conf
- SU data – steal sensitive data

SP=Service Provider
SU=Service User
HP=Hosting Platform
SI=Service Instance
SLA=Service Level Agreement
CP=Cloud Provider
The Cloud, Virtualization, and Security

Cloud Threat Model

Host Integrity is assumed

Guest Integrity is assumed at setup, when a VM is supplied but assumption is not valid when VM is deployed and exposed to the network

Guest VMs provided by SU are not trusted and will be monitored

Attackers can be SP or SU

Victims can be SP, CP, or SU

SP=Service Provider
SU=Service User
HP=Hosting Platform
SI=Service Instance
SLA=Service Level Agreement
CP=Cloud Provider
The Cloud, Virtualization, and Security

Core requirements of cloud monitoring system

- **effectiveness**: detection of most kinds of attacks
- **precision**: few false-positives (mistake good for malware)
- **transparency**: minimize visibility from VMs; SP, SU, and potential intruders should not detect the monitoring system
- **non-subvertability**: host system, cloud infrastructure and sibling VMs are protected from attacks from a compromised guest; cannot disable monitoring system
- **deployability**: should be deployable on the vast majority of available cloud middleware and HW/SW configurations.
- **dynamic reaction**: detect intrusion attempt over a cloud component and mitigate and notify security management
- **accountability**: collect data and snapshots to enforce accountability policies
The Cloud, Virtualization, and Security

Eucalyptus
The Cloud, Virtualization, and Security

OpenECP
The Cloud, Virtualization, and Security

- Suspicious guest activities (e.g. system_call invocation) can be noticed by the **Interceptor** and recorded by the **Warning Recorder** into the **Warning Pool**, where the potential threat will be evaluated by the **Evaluator** component.

- **ChecksumDB** has checksums for critical code, data, files

- The **Interceptor** does not block or deny any system call to prevent the monitoring system from being detected

- **Evaluator** and **Hasher** are always active, running and continuously performing security checks.

- **Warning Pool** caches warnings so evaluation does not choke **Warning Pool** also allows setting priorities wrt evaluation order thereby increased invisibility

- Hot recovery by replacement of compromised service via **Snapshots**

- **Snapshots** support recording of guest machines for forensics