October 17,2011 - Cloud computing security

Kyle MacNamara

1 What is Cloud Computing?

According to NIST(National Institute of Standards and Technology), cloud computing is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction”

1.1 Service Models

NIST categorizes cloud computing into three different service models.

1.1.1 Software as a service (SaaS)

This model delivers software as a service over the Internet which eliminates the need to install and run the application on the customer’s own computer.

1.1.2 Platform as a service (PaaS)

In this model, consumer runs consumer-created applications on the cloud with provider- supported tools.

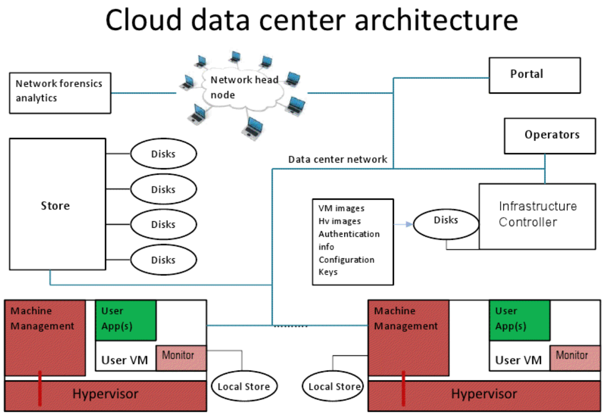
1.1.3 Infrastructure as a service (IaaS)

In this model, a customer uses a cloud provider’s processing, storage, and networks.

2 Building a cloud data center

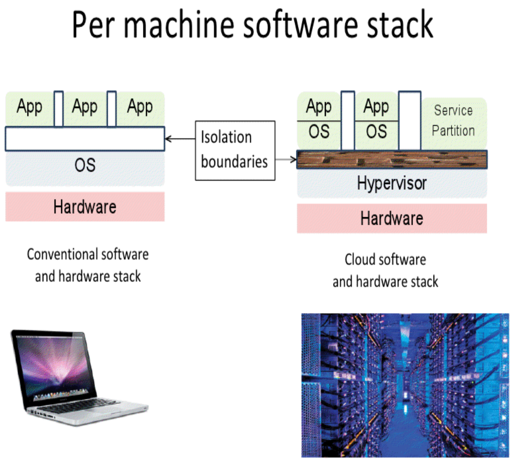
- Large number of homogeneous machinse set up to operate together in clusters
- Often built where power and cooling can be acquired cheaply such as near a dam.
- A management system must be set up to manage and monitor the machines and applications. A cluster typically contains around 250,000 machines.
- Each data center will often contain a centralized redundant storage that is often encrypted. This is done in order to avoid saving state on the individual machines. If a particular machine goes down, ideally no data will be lost.

Figure 1



3 Attack model/Adversaries

Figure 2


Per machine software stack
App
App
App
OS
Hardware
Isolation boundaries
App
App
OS
OS
Service Partition
Hypervisor
Hardware
Conventional software and hardware stack
Cloud software and hardware stack

- Insiders
  - Each data center is managed by usually less than 25 people. This is approximately one person per 10,000 machines. They essentially have access to all of the data stored in the data center.
- Vulnerabilities inside TCB of cloud components
  - For example, a hypervisor is a trusted component that serves as the virtual machine manager. It is a allows multiple VMs to share a single hardware host. This can be seen in Figure 2.
- Opacity of third party data center operations
  - There is no economic incentive to report breaches. If a breach happens, you will probably not know about it.
- The actual data center might not be trustworthy.
- The hardware that the cloud center uses could be tampered with before installation.
- Other tenants located in the cloud might be malicious.
- Advanced Persistence Threats (APT)

4 Attacking the cloud

- The operators of the cluster could be targeted and blackmailed.
- The data coming into the data center is often unencrypted for performance reasons. This communication could potentially be tapped.
- The disk near the infrastructure contains the keys. Since disks often fail due to the large number of machines, an operator could potentially steal the keys from one of these disks
- As seen in the paper "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Cloud", malicious tenants may use side channel attacks to read the data of other tenants on the same physical machine.
- Malicious tenants could steal shared resouces or find ways to charge resources to other tenants
- An attacker could launch a denial of service attack by targeting the shared resources.
- Fortunately, cloud centers generally have good physical security in which the racks of machines have cameras watching them at all times.

5 Making the cloud possible - Historical milestones

5.1 Virtualization

- IBM System/360 Model 67(1965)
  - First IBM system with virtual memory
  - Contained a Dynamic Address Translation facility (DAT box)

5.2 Internet and local networks

- Packet switching was chosen instead of circuit switching.
- Standards were decided upon (DNS, TCP/IP, HTTP)
- Distributed control and routing
- LANs have improvements in terms of latency and increased throughput

5.3 the PC

- Massive increase in computing power
- Quantity drives out quality, uniformity drives out diversity.

6 Cloud as a marketing concept

- Huge cost savings
  - Generally, computing for cloud data centers is considered 10 times cheaper. This is due to the data centers being located where cheap power is abundant. In addition, the machines used are also highly utilized. However, it is not always cheaper to use cloud services. Consider that storing 1 TB of data for one year might cost as much as 2000 dollars.
- Rent vs buy
- Resiliency through redundancy
- Software as a service
  - Outsource IT
- Increase security by professional management
  - This concept refers to the fact that each data center has around 25 operators. This "increased security" is most likely just a marketing ploy.

7 Discussions on Papers

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

- This paper discusses how the sharing of resources between VMs can be used to launch an attack. If an attacker is capable of placing a VM on the same physical machine as the target, then cross-VM side-channel attacks can potentially be used to extract information from a target VM
- Compared to the severity of the other security vulnerabilities mentioned earlier, this vulnerability is not as critical.

7.2 Protecting Your Critical Assets: Lessons Learned from "Operation Aurora"

- This paper briefly described the attack "Operation Aurora" . The attack preceded as follows:
  1. A targeted user receives a link from a supposed "trusted" source.
  2. By clicking on the link, the user was taken to a malicious website.
  3. The malicious website contains Javascript which contained a zero-day Internet Explorer exploit.

4. The exploit downloaded a binary which was disguised as an image. A malicious payload was then executed.
5. This payload set up a backdoor to command and control servers located in Taiwan

- As a result of the above attack, the attackers had complete access to internal systems of the companies targeted.
- The attack "Operation Aurora", an example of an Advanced Persistent Threat(APT), wasn't an attack on the cloud directly, but instead on client machines.
- The goal was access to steal intellectual property from companies by taking advantage of flaws in software configuration management (SCM) systems such as Perforce.
- One of the reasons why this attack was so successful was that many of the targeted companies lacked defense in depth.

8 A better design for a cloud data center

In order to improve the security of cloud data centers, the following is required:

1. Users should have the ability to confirm remotely that the software running on the VM is the software they intend to run.
2. The VM should have access to keys that only it knows.

In order to accomplish this, hardware support is necessary. A TPM (Trusted Platform Module) is required. This is a secure cryptoprocessor that will be used to store the cryptographic keys. This hardware will be used to sign statements that it is given. In order to remotely confirm the software, during boot-up, the VM can be hashed and then stored and signed. Now, data can be sent securely between the VM and the owner by negotiating keys and encrypting all future data with the negotiated keys.