Cloud Security

M. G. Sarwar Murshed

What is Cloud Computing?

- What do you think?
- It’s internet computing
  - Computations are done through the Internet
  - No worry about any maintenance or management of actual resources
- Car rental services, instead of car we rent computing infrastructure and IT-services
- The cloud computing system is an organized series of computers, located in data centers, all over the world
- Cloud Service Providers (CSPs) make cloud services available for us (for a price)
  - Computing
  - Storage
  - IT supports
  - Many more

Cloud Computing Standard by NIST

Five Essential Cloud Characteristics

- On-demand self-service
  - Users can provision computing resources without human intervention from the service provide
- Broad network access
  - Cloud services are accessible over the network and can be accessed by clients using a variety of devices
- Resource pooling
  - The provider's computing resources are pooled to serve multiple customers, with different physical and virtual resources
- Rapid elasticity
  - The provider can quickly scale up or down the amount of resources allocated to a customer, often automatically, to meet changing demand
- Measured service
  - Cloud systems automatically control and optimize resource use by leveraging a metering capability

Cloud computing is a model for enabling convenient, ondemand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (from NIST)

[3] Mell, P. and Grance, T. (2011), The NIST Definition of Cloud Computing

Three Cloud Service Models

- Cloud Software as a Service (SaaS)
  - To use the provider’s applications
  - Gmail, Dropbox, Salesforce
- Cloud Platform as a Service (PaaS)
  - To deploy customer-created and acquired applications
  - Google App Engine, Azure App Service
- Cloud Infrastructure as a Service (IaaS)
  - To provision processing, storage, networks, and other fundamental computing resources
  - Amazon Web Services (AWS)

If Cloud Computing is So Great, Why isn't Everyone Doing It?

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Security and Privacy Issues in Cloud Computing

- Infrastructure Security
- Data Security and Storage
- Identity and Access Management (IAM)
- Privacy
- And more

[2] Bhargava et al., **Security and Privacy in Cloud Computing,** Computer Science, Purdue University, https://www.cs.purdue.edu/homes/bb/cs448_Fall2016/lecture-files/pdf/cloud-complete.pdf

Infrastructure Security

- Host Level
  - Involves various measures to secure the servers, operating systems, applications, and data that reside on the machines.
- Network Level
  - Involves securing the communications channels that connect cloud-based services and data with users, devices, and other services over the internet.
- Application Level
  - Involves securing the applications and services that run on cloud-based infrastructure.

[1]. Cloud Security and Privacy by Mather and Kumaraswamy

The Host Level (Infrastructure Security)

SaaS and PaaS Host Security

- Both the PaaS and SaaS platforms abstract and hide the host OS from end users
- Host security responsibilities are transferred to the Cloud Service Provider (CSP)
  - You do not have to worry about protecting hosts
- However, as a customer, you still own the risk of managing information hosted in the cloud services

[1]. Cloud Security and Privacy by Mather and Kumaraswamy

The Host Level (Infrastructure Security)

Host security threats in the public IaaS

- Vulnerabilities in the virtualization layer
  - enables the creation and management of virtual machines
  - can be exploited by attackers to gain access to other virtual machines
- Misconfigured virtual machines
  - most common security threats in public IaaS environments
  - expose sensitive data or services to unauthorized access
- Stealing keys used to access and manage hosts (e.g., SSH private keys)
- Hijacking accounts that are not properly secured (i.e., weak or no passwords for standard accounts)
- Attacking systems that are not properly secured by host firewalls
- Deploying Trojans embedded in the software component in the VM or within the VM image (the OS) itself

[1]. Cloud Security and Privacy by Mather and Kumaraswamy

Securing Host Servers

- **Image inventory tracking**: Track the inventory of VM images and OS versions that are prepared for cloud hosting.
- **Image integrity protection**: Protect the integrity of the hardened image from unauthorized access.
- **Private key safeguarding**: Safeguard the private keys required to access hosts in the public cloud
- **Firewall implementation**: Run a host firewall and open only the minimum ports necessary to support the services on an instance.

[1]. Cloud Security and Privacy by Mather and Kumaraswamy

Securing Host Servers

- **Service reduction**: Run only the required services and turn off the unused services (e.g., turn off FTP, print services, network file services, and database services if they are not required).
- **Auditing and logging**: Enable system auditing and event logging, and log the security events to a dedicated log server. Isolate the log server with higher security protection, including accessing controls.
- **Compromise response**: If you suspect a compromise, shut down the instance, snapshot your block volumes, and back up the root filesystem.
- **Log review**: Periodically review logs for suspicious activities

The Local Host Security (Cont.)

Case study: Amazon's EC2 infrastructure (Exploring Information Leakage in Third-Party Compute Clouds)

- Multiple virtual machines (VMs) of different organizations with virtual boundaries separating each VM can run within one physical server.
- VMs have internet protocol, or IP, addresses, visible to anyone within the cloud.
- VMs located on the same physical server tend to have IP addresses that are close to each other and are assigned at the same time
- An attacker can set up lots of his own virtual machines, look at their IP addresses, and figure out which one shares the same physical resources as an intended target
- Once the malicious virtual machine is placed on the same server as its target, it is possible to carefully monitor how access to resources fluctuates and thereby potentially glean sensitive information about the victim

[2] Bhargava et al., **Security and Privacy in Cloud Computing,** Computer Science, Purdue University, https://www.cs.purdue.edu/homes/bb/cs448_Fall2016/lecture-files/pdf/cloud-complete.pdf

The Local Host Security (Cont.)

With mobile devices, the threat may be even stronger

- Users misplace or have the device stolen from them
- Security mechanisms on handheld gadgets are often times insufficient compared to say, a desktop computer
- Provides a potential attacker an easy avenue into a cloud system.
- If a user relies mainly on a mobile device to access cloud data, the threat to availability is also increased as mobile devices malfunction or are lost
- Devices that access the cloud should have
    - Strong authentication mechanisms
    - Tamper-resistant mechanisms
    - Strong isolation between applications
    - Methods to trust the OS
    - Cryptographic functionality when traffic confidentiality is required

References

1. Mather, Tim, S. Kumaraswamy and Shahed Latif. “Cloud security and privacy.” (2009).
2. Bharat Bhargava, Anya Kim ,and YounSun Cho, Security and Privacy in Cloud Computing, Computer Science, Purdue University, https://www.cs.purdue.edu/homes/bb/cs448_Fall2016/lecture-files/pdf/cloud-complete.pdf
3. Mell, P. and Grance, T. (2011), The NIST Definition of Cloud Computing, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-145 (Accessed April 13, 2023)
4. Salim Hariri, Fundamental of Cloud Security, The University of Arizona. https://projet.liris.cnrs.fr/cyber/WS3Presentations/Hariri.pdf

Thank you!
Q&A