A Novel Agent-Based Framework in Bridge-Mode Hypervisors of Cloud Security

M. Janbeglou and W. Yan

AUT University, NZ

KMO 2012, Spain

Content

- Cloud computing
- Virtualization and its risks
- Proposed Virtual Network Model
- Evaluations
- Conclusion

Cloud Computing

Cloud Computing (NIST,USA)

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

Cloud Advantages

- On-demand
- Self-service
- Location independent
- Elastic
- Accessible

Clouds

- **Private Cloud**: This model is for usage of individual organization and not shared among other organizations.
- **Community Cloud**: This model is shared with several set of organizations.
- **Public Cloud**: The most common type of cloud infrastructure that is made to be available for public.
- **Hybrid Cloud**: This model is made by combining two or more deployment models (private, community, or public).

Cloud Components

- **SaaS**: Software as a Service
- **PaaS**: Platform as a Service
- **IaaS**: Infrastructure as a Service

Virtualization and Its Risks

Virtualization

- Visualization provides the ability of installing **multiple OSs** on different VMs on a same physical machine and as a result it **increases the machine utilization**.
- Virtualization is responsible for **splitting resources** on a single physical machine into multiple VMs.
- Virtualization helps **Cloud Service Providers** (CSP) to solve the complexity issues in delivering services, managing **shared resources** and utilizations, **isolating VMs**, and **providing security**.

Risks Towards Virtualization

- Virtualized systems risks
- Hypervisor risks
- Virtual machine risks
- Virtual network risks

Virtualized System Risks

- Visualization makes the **security management** more **complex**.
- Visualization needs **more controlling and monitoring** of the shared resources.
- Larger **security threats** arise when many VMs are combined into a physical machine.
- Systems are dynamic and flexible to changes, defining **security boundaries** will be complicated.

Hypervisor Risks

- Hypervisor is a software program, it is inherently vulnerable to the **growth** of **volume** and **complexity** of application codes.
- Hypervisor provides physical server resources **sharing** and VM/host **isolation**.
- **Vulnerabilities** in current hypervisors are Rogue Hypervisors, External Modification of the Hypervisor, VM Escape, and Denial-of-Service.

Virtual Machine Risks

- Use the shared resources on a physical server to deliver business needs.
  - ➢ Working on a same physical machine
  - ➢ Using the shared resources

Virtual Machine Risks

- Shared clipboard attack
- Keystroke logging attack
- Monitoring VMs from an infected host

Virtual Network Risks

- In physical networks, firewall and encryptions mechanisms are the main tools for applying security.
- In virtual networks, **almost all** the physical network threats are likely to happen.
- **Isolation** does a similar function in virtual networks.

Virtual Network Model

Our Contributions

- This paper proposes a model to improve the **IaaS security** on the **shared network resources** by making **VMs invisible** from attackers, and as a result, **preventing** them from performing the key step of **network-related attacks**.

Proposed Agent

- The proposed model introduce an agent to provide a **centralized virtual network management** for all of the VMs residing in a physical server.
- The agent is to help the hypervisor to **provide security** by **confining the visibility and accessibility** of the VMs network resources.

Proposed Model Steps

1) Generating network-sub-interfaces

and Random IP address configurations

2) Generating PPTP (Point2Point Tunneling Protocol)

configurations

3) Customizing the packet-filtering

Network Sub-interfaces

- Network sub-interfaces refers to sub-interfaces that are created from VM Interface.
- Each of the sub-interfaces will be assigned to corresponding VMs.
- **Randomly generated IP address configurations** are assigned to the VMs by a DHCP (Dynamic Host Configuration Protocol) service running on the agent.

Generating IP addresses in PPTP service

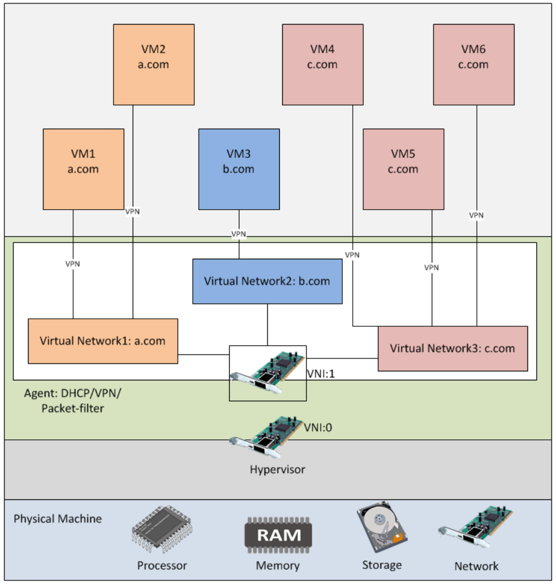
- Counting the **number of domains** available.
- Counting the **maximum number** of VMs in each domain.
- Calculating **appropriate subnet** for each domain. The appropriate subnet is the smallest possible subnet to cover a group of VMs working in a domain.
- **Generating and assigning IPs** to each VM and network-sub-interface.

Customizing the Packet-Filtering

- Packet-filtering improves the security of the whole system by **confining any internal-communications** via dropping packets originating from internal VMs residing in different domains.
- Because the packet-filtering bans any VMs intercommunications within different domains**, the VMs' IP addresses remain invisible** for attackers.

Evaluations

- **CIA**: Confidentiality, Integrity, and Availability.
- **AAA**: Authentication, Authorization, and Accountability.



KMO 2012, Spain

Conclusion

Conclusion

1) **Security risks** towards each virtualized system component have been examined.

2) **A proposed model** was introduced.

3) The **evaluation** of proposed model was addressed.

A Novel Agent-Based Framework in Bridge-Mode Hypervisors of Cloud Security

M. Janbeglou and W. Yan

AUT University, NZ