Private Virtual Infrastructure for Cloud Computing

John Krautheim
UMBC Cyber Defense Lab

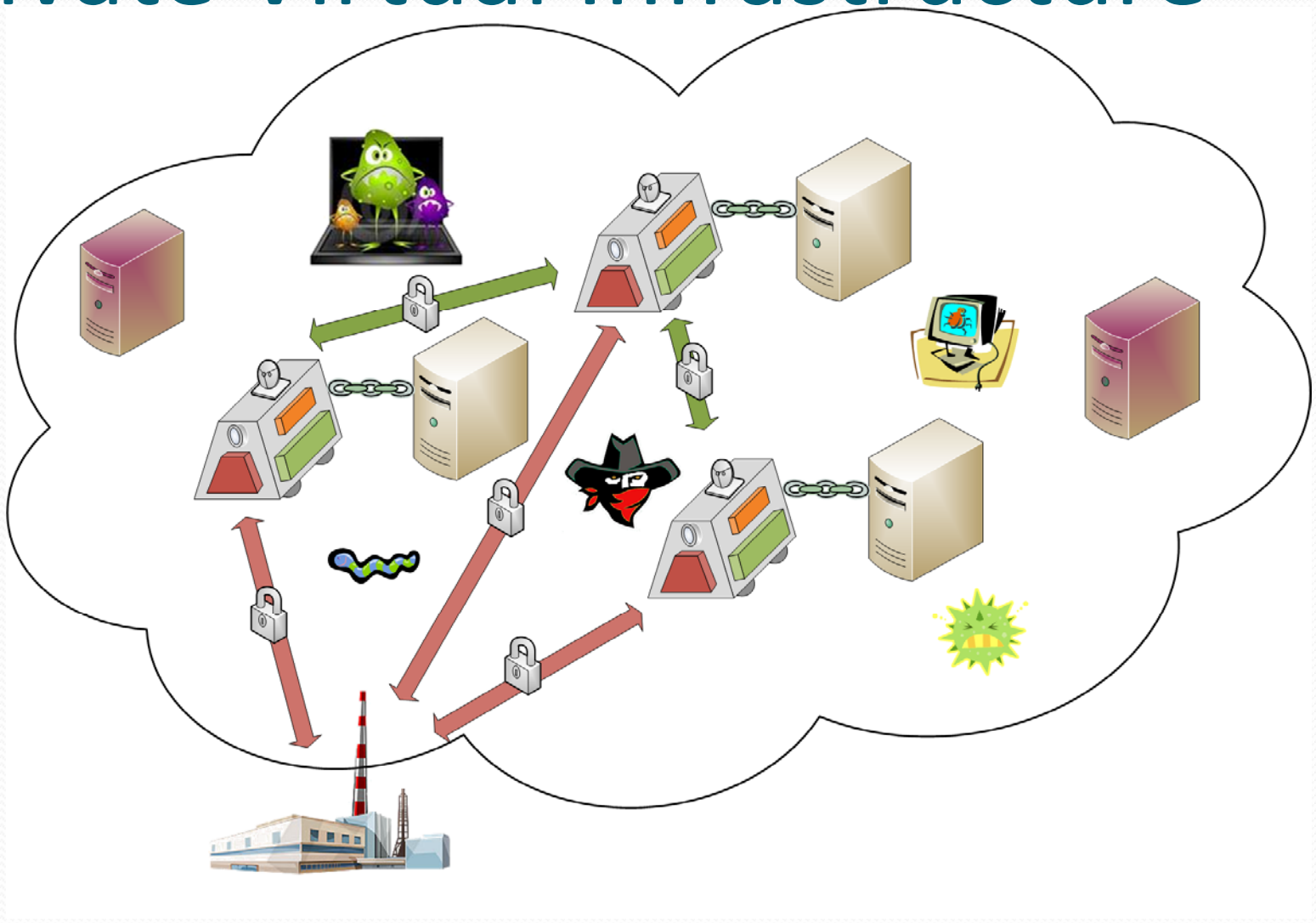
Cloud Computing Security

- Someone else owns the cloud
  - Data in cloud is out of control of data owner
  - Does cloud provides required level of data security?
- Attack models
  - Bad administrator
  - Bad actor within cloud
- Cloud Virtual Machines Issues
  - The Clone Wars
  - Spoofing
  - Data Theft
  - Data Integrity

Five Tenets of Cloud Security

- Provide a trusted foundation
- Provide a secure factory to provision
- Provide a measurement mechanism to validate the security of the fabric
- Provide secure methods for shutdown and destruction of virtual devices to prevent object reuse attacks.
- Provide continuous monitoring and auditing from within as well as from outside of PVI with intrusion detection systems and other devices.

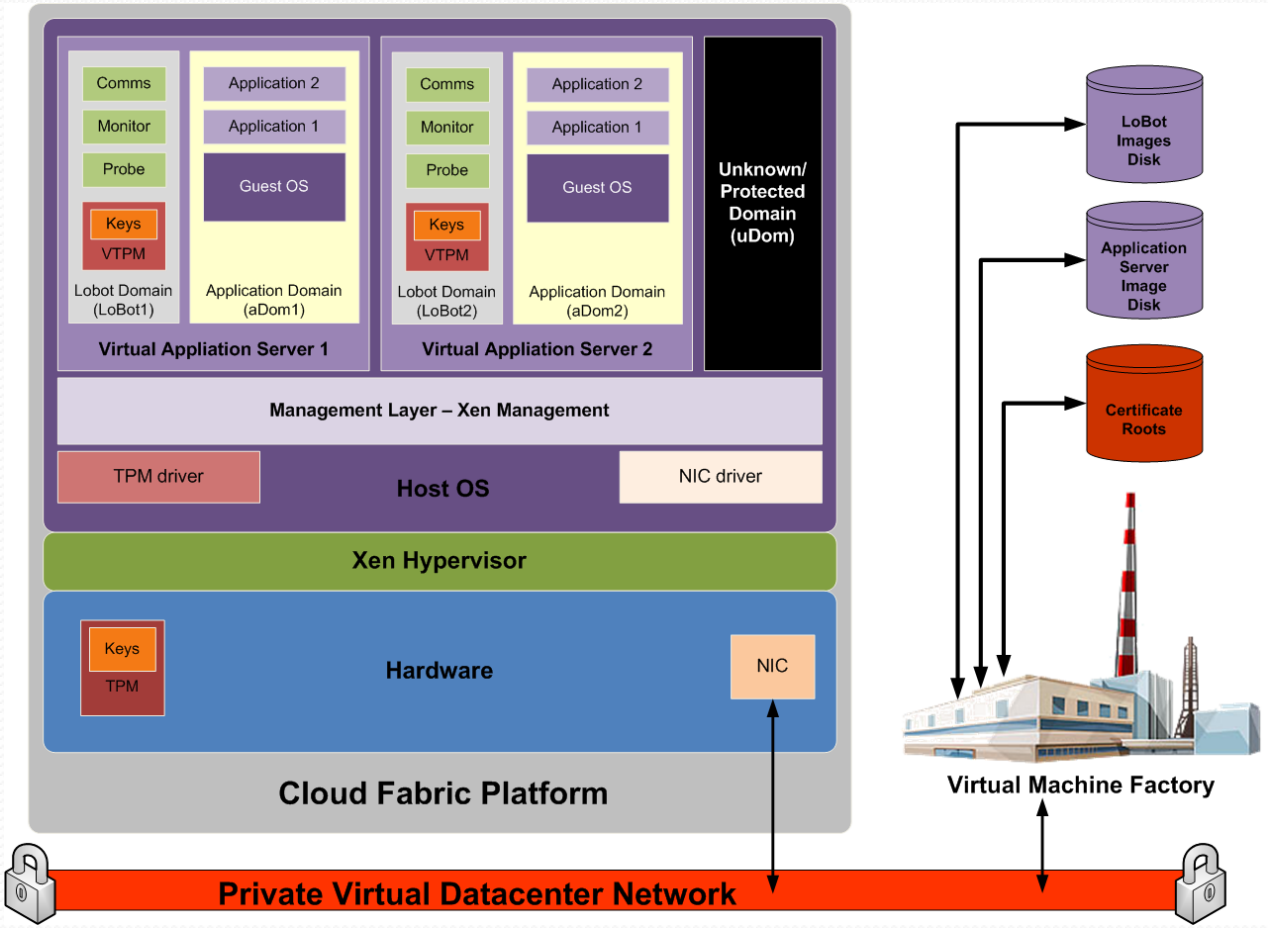
Private Virtual Infrastructure



Trusted Cloud Fabric Platform

- Provides Trusted Platform Module
  - Platform Root of Trust
- Secure Hardware
  - Intel vPro (TXT)
  - Create Measured Launch Environment
  - Late launch of domains
- Secure Hypervisor (sHype)

Trusted Cloud Fabric Platform

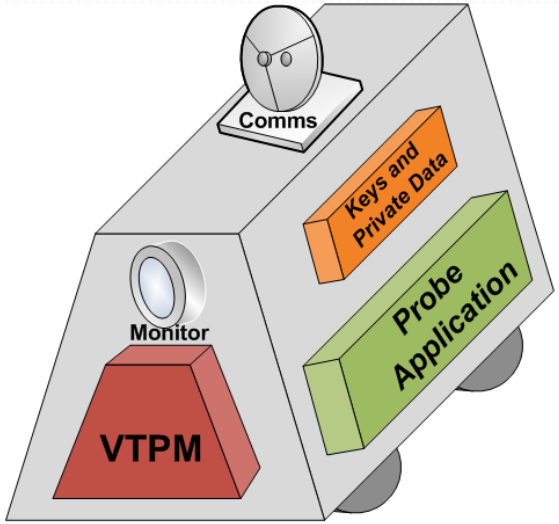


PVI Factory

- Root of Trust for PVI
- Certificate Authority for PVI
  - Generates Endorsement Keys (EKs) for TPMs
- Policy Decision Point for PVI
- Manages VM Provisioning for PVI
- Performs Security Monitoring for PVI

Secure Provisioning

- Measure the environment prior to provisioning
  - Utilizes a LoBot
- Ensures environment is “safe”



LoBot Features

1) Pre-measures cloud computing fabric
2) Provisions virtual machines in cloud
3) Enables secure migration
4) Monitors for abnormal behavior
5) Secure data storage
6) Secure data destruction
7) Communicates with other LoBots for total situational awareness

Cloud Security Research

- Private Virtual Infrastructure
- Locator Bot
- Trusted Virtual Machine Identification

Conclusion

- Vendors are responsible to provide a secure fabric
- Information owners are responsible to protect their data
- Cooperation between vendor and customer will result in an increased security while lowering the overall cost of ownership for IT infrastructure.