Cloud Computing Security Issues

Randy Marchany, VA Tech IT Security,
marchany@vt.edu

VirginiaTech
Invent the Future

Something Old, Something New

- New: Cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down providing for an on-demand utility-like model of allocations and consumption
- Old: The Network is the Computer (Sun Microsystems, 1997)

VirginiaTech
Invent the Future

Cloud Computing Parts

- NIST defines cloud computing by:
  - 5 essential characteristics
  - 3 cloud service models
  - 4 cloud deployment models

Essential Characteristics

- On-demand service
  - Get computing capabilities as needed automatically
- Broad Network Access
  - Services available over the net using desktop, laptop, PDA, mobile phone

Essential Characteristics

- Resource pooling
  - Provider resources pooled to server multiple clients
- Rapid Elasticity
  - Ability to quickly scale in/out service
- Measured service
  - control, optimize services based on metering

VirginiaTech
Invent the Future

Cloud Service Models

- **Software as a Service (SaaS)**
  - We use the provider apps
  - User doesn’t manage or control the network, servers, OS, storage or applications
- **Platform as a Service (PaaS)**
  - User deploys their apps on the cloud
  - Controls their apps
  - User doesn’t manage servers, IS, storage

Cloud Service Models

- **Infrastructure as a Service (IaaS)**
  - Consumers gets access to the infrastructure to deploy their stuff
  - Doesn’t manage or control the infrastructure
  - Does manage or control the OS, storage, apps, selected network components

Deployment Models

- Public
  - Cloud infrastructure is available to the general public, owned by org selling cloud services
- Private
  - Cloud infrastructure for single org only, may be managed by the org or a 3rd party, on or off premise

VirginiaTech
Invent the Future

Deployment Models

- Community
  - Cloud infrastructure shared by several orgs that have shared concerns, managed by org or 3rd party
- Hybrid
  - Combo of >=2 clouds bound by standard or proprietary technology

VirginiaTech
Invent the Future

What, When, How to Move to the Cloud

- Identify the asset(s) for cloud deployment
  - Data
  - Applications/Functions/Process
- Evaluate the asset
  - Determine how important the data or function is to the org

VirginiaTech
Invent the Future

Evaluate the Asset

- How would we be harmed if
  - the asset became widely public & widely distributed?
  - An employee of our cloud provider accessed the asset?
  - The process of function were manipulated by an outsider?
  - The process or function failed to provide expected results?
  - The info/data was unexpectedly changed?
  - The asset were unavailable for a period of time?

VirginiaTech
Invent the Future

Map Asset to Models

- 4 Cloud Models
  - **Public**
  - **Private, internal, on premise**
  - **Private, external**
  - **Community**
    - Hybrid
- Which cloud model addresses your security concerns?

Map Data Flow

- Map the data flow between your organization, cloud service, customers, other nodes
- Essential to understand whether & HOW data can move in/out of the cloud
  - Sketch it for each of the models
  - Know your risk tolerance!

VirginiaTech
Invent the Future

Cloud Domains

- Service contracts should address these 13 domains
- Architectural Framework
- Governance, Enterprise Risk Mgt
- Legal, e-Discovery
- Compliance & Audit
- Information Lifecycle Mgt
- Portability & Interoperability

VirginiaTech
Invent the Future

Cloud Domains

- Security, Business Continuity, Disaster Recovery
- Data Center Operations
- Incident Response Issues
- Application Security
- Encryption & Key Mgt
- Identity & Access Mgt
- Virtualization

VirginiaTech
Invent the Future

Security Stack

- **IaaS**: entire infrastructure from facilities to HW
- **PaaS**: application, Middleware, database, messaging supported by IaaS
- **SaaS**: self contained operating environment: content, presentation, apps, mgt

VirginiaTech
Invent the Future

Security Stack Concerns

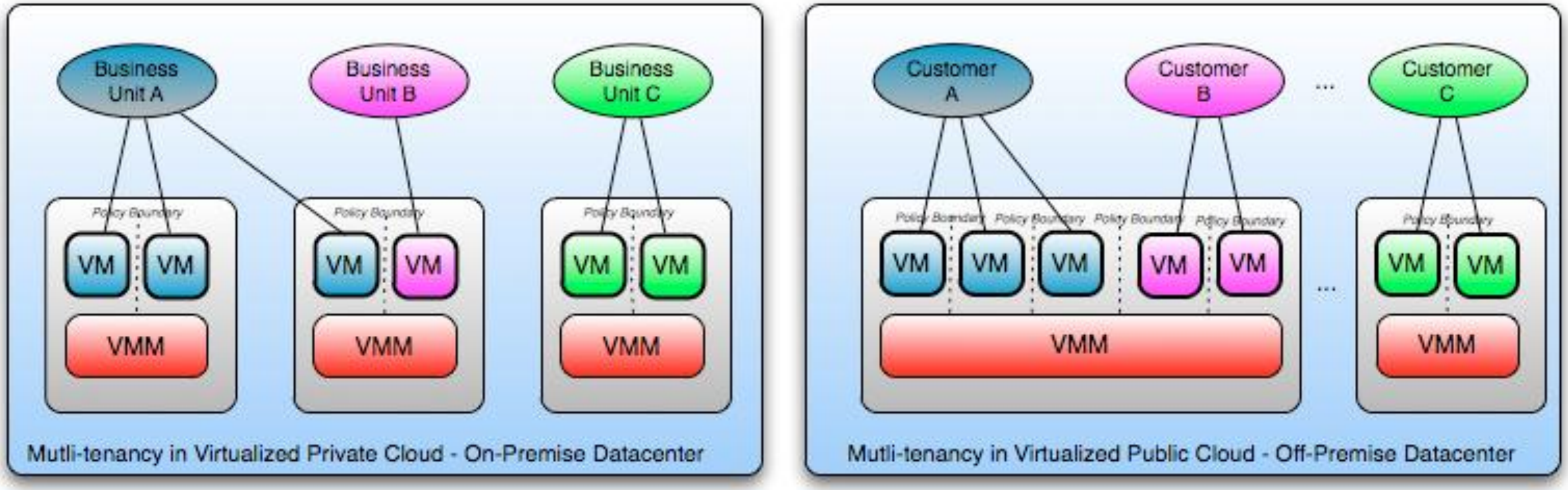
- Lower down the stack the cloud vendor provides, the more security issues the consumer has to address or provide
- Who do you trust?

Key Takeaways

- SaaS
  - Service levels, security, governance, compliance, liability expectations of the service & provider are contractually defined
- PaaS, IaaS
  - Customer sysadmins manage the same with provider handling platform, infrastructure security

VirginiaTech
Invent the Future

Sample Clouds

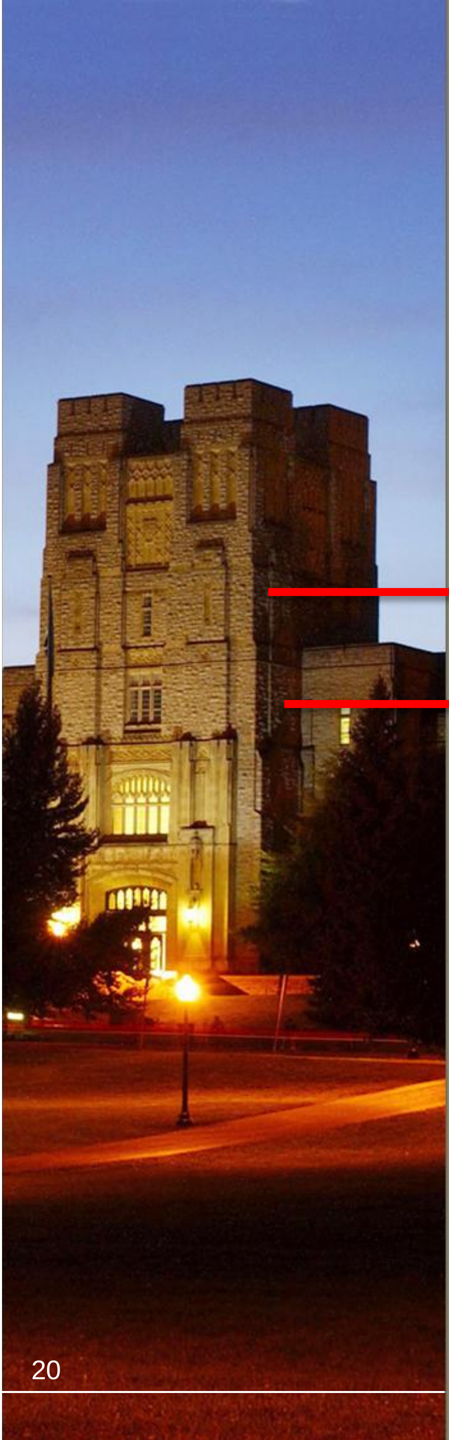

Business Unit A
Business Unit B
Business Unit C
Policy Boundary
VM
VMM
Mutli-tenancy in Virtualized Private Cloud - On-Premise Datacenter
Customer A
Customer B
...
Customer C
Policy Boundary
VM
VMM
Mutli-tenancy in Virtualized Public Cloud - Off-Premise Datacenter

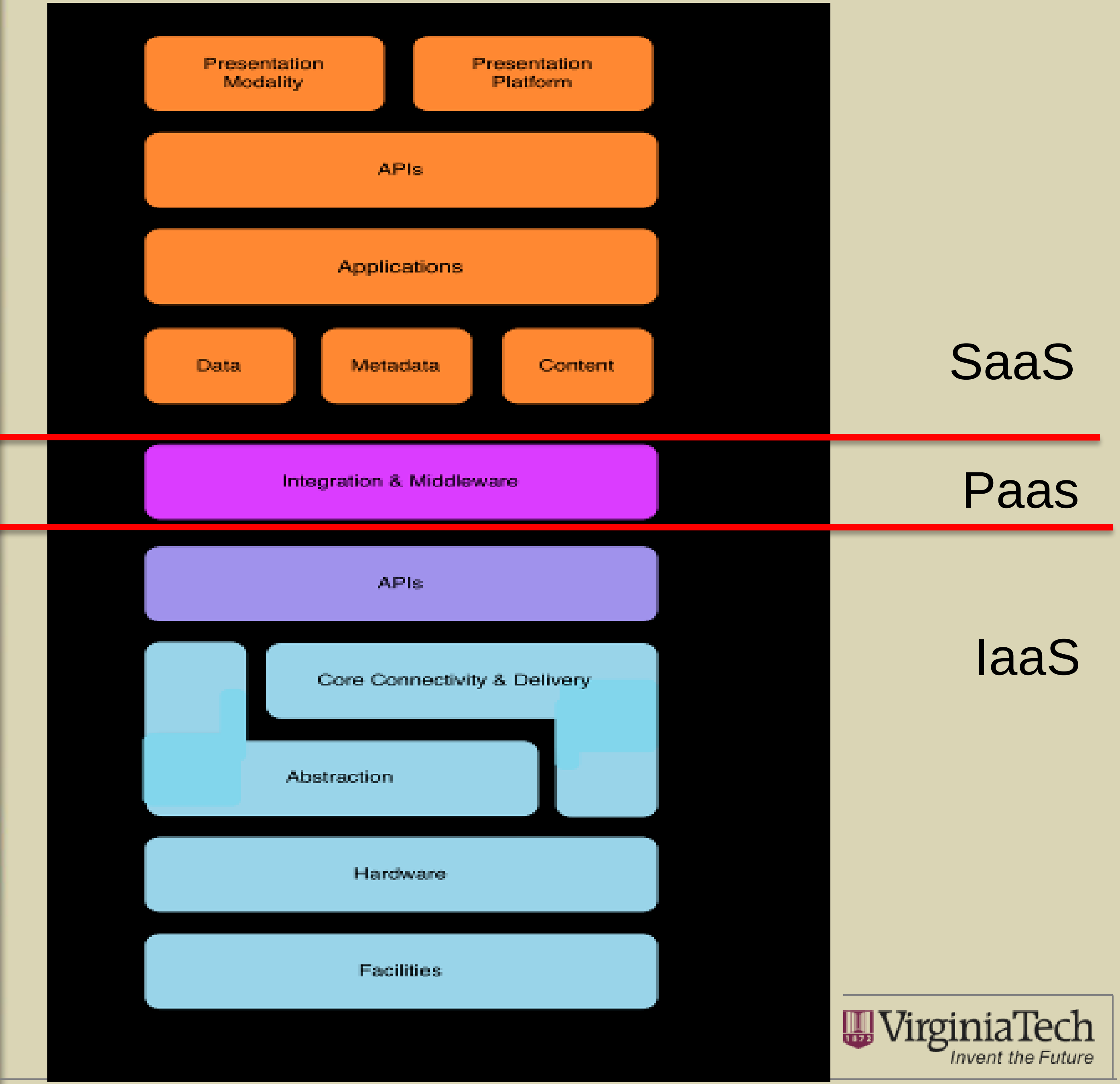
Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure

Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

From “Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, p.18

VirginiaTech
Invent the Future





Presentation Modality

Presentation Platform

APIs

Applications

Data

Metadata

Content

SaaS

Integration & Middleware

Paas

APIs

Core Connectivity & Delivery

Abstraction

Hardware

Facilities

IaaS

Security Pitfalls

- How cloud services are provided confused with where they are provided
- **Well demarcated network security border is not fixed**
- Cloud computing implies loss of control

VirginiaTech
Invent the Future

Overall Security Concerns

- Gracefully lose control while maintaining accountability even if operational responsibility falls upon 3rd parties
- Provider, user security duties differ greatly between cloud models

Governance

- Identify, implement process, controls to maintain effective governance, risk mgt, compliance
- Provider security governance should be assessed for sufficiency, maturity, consistency with user ITSEC process

3rd Party Governance

- Request clear docs on how facility & services are assessed
- Require defn of what provider considers critical services, info
- Perform full contract, terms of use due diligence to determine roles, accountability

VirginiaTech
Invent the Future

Legal, e-Discovery

- Functional: which functions & services in the Cloud have legal implications for both parties
- Jurisdictional: which governments administer laws and regs impacting services, stakeholders, data assets
- Contractual: terms & conditions

VirginiaTech
Invent the Future

Legal, e-Discovery

- Both parties must understand each other’s roles
  - – Litigation hold, Discovery searches
  - – Expert testimony
- Provider must save primary and secondary (logs) data
- Where is the data stored?
  - laws for cross border data flows

VirginiaTech
Invent the Future

Legal, e-Discovery

- Plan for unexpected contract termination and orderly return or secure disposal of assets
- You should ensure you retain ownership of your data in its original form

Compliance & Audit

- Hard to maintain with your sec/reg requirements, harder to demonstrate to auditors
- Right to Audit clause
- Analyze compliance scope
- Regulatory impact on data security
- Evidence requirements are met
- Do Provider have SAS 70 Type II, ISO 27001/2 audit statements?

VirginiaTech
Invent the Future

Info Lifecycle Mgt

- Data security (CIA)
- Data Location
  - All copies, backups stored only at location allowed by contract, SLA and/or regulation
  - Compliant storage (EU mandate) for storing e-health records

VirginiaTech
Invent the Future

Portability, Interoperability

- When you have to switch cloud providers
- Contract price increase
- Provider bankruptcy
- Provider service shutdown
- Decrease in service quality
- Business dispute

Security, BC, DS

- Centralization of data = greater insider threat from within the provider
- Require onsite inspections of provider facilities
  - Disaster recover, Business continuity, etc

Data Center Ops

- How does provider do:
  - On-demand self service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service

Incident Response

- Cloud apps aren't always designed with data integrity, security in mind
- Provider keep app, firewall, IDS logs?
- Provider deliver snapshots of your virtual environment?
- Sensitive data must be encrypted for data breach regs

VirginiaTech
Invent the Future

Application Security

- Different trust boundaries for IaaS, PaaS, Saas
- Provider web application security?
- Secure inter-host communication channel

Encryption, Key Mgt

- Encrypt data in transit, at rest, backup media
- Secure key store
  - Protect encryption keys
  - Ensure encryption is based on industry/govt standards.
    - NO proprietary standard
  - Limit access to key stores
  - Key backup & recoverability
    - Test these procedures

VirginiaTech
Invent the Future

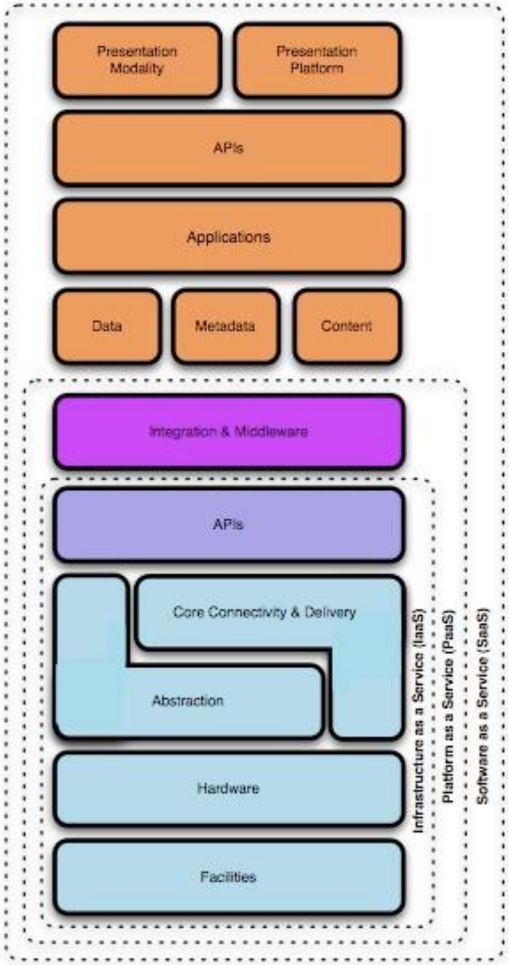
ID, Access Mgt

- Determine how provider handles:
  - Provisioning, deprovisioning
  - Authentication
  - Federation
  - Authorization, user profile mgt

Virtualization

- What type of virtualization is used by the provider?
- What 3rd party security technology augments the virtual OS?
- Which controls protect admin interfaces exposed to users?

Cloud Model



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

☑ Firewalls
☑ Code Review
☑ WAF
☑ Encryption
☑ Unique User IDs
☑ Anti-Virus
☑ Monitoring/IDS/IPS
☑ Patch/Vulnerability Management
☑ Physical Access Control
☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

Summary

- We already do some sort of cloud computing
  - NFS, Samba shares, SAN, NAS, Web applications
- Decide on public or private cloud
- Public cloud implies loss of control

VirginiaTech
Invent the Future

Reference

- All material from “Security Guidance for Critical Areas of Focus in Cloud Computing v2.1”, http://www.cloudsecurityalliance.org
    - All figures in this talk taken from this paper
- NIST Cloud Model: www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
- Various cloud working groups
    - Open Cloud Computing Interface Working Group, Amazon EC2 API, Sun Open Cloud API, Rackspace API, GoGrid API, DMTF Open Virtualization Format (OVF)

VirginiaTech
Invent the Future