Intro to Cloud & Cloud Security

Professors: David A. Cass and Kevin McKenzie

Lecture 11

NIST Definition of Cloud

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared

pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that

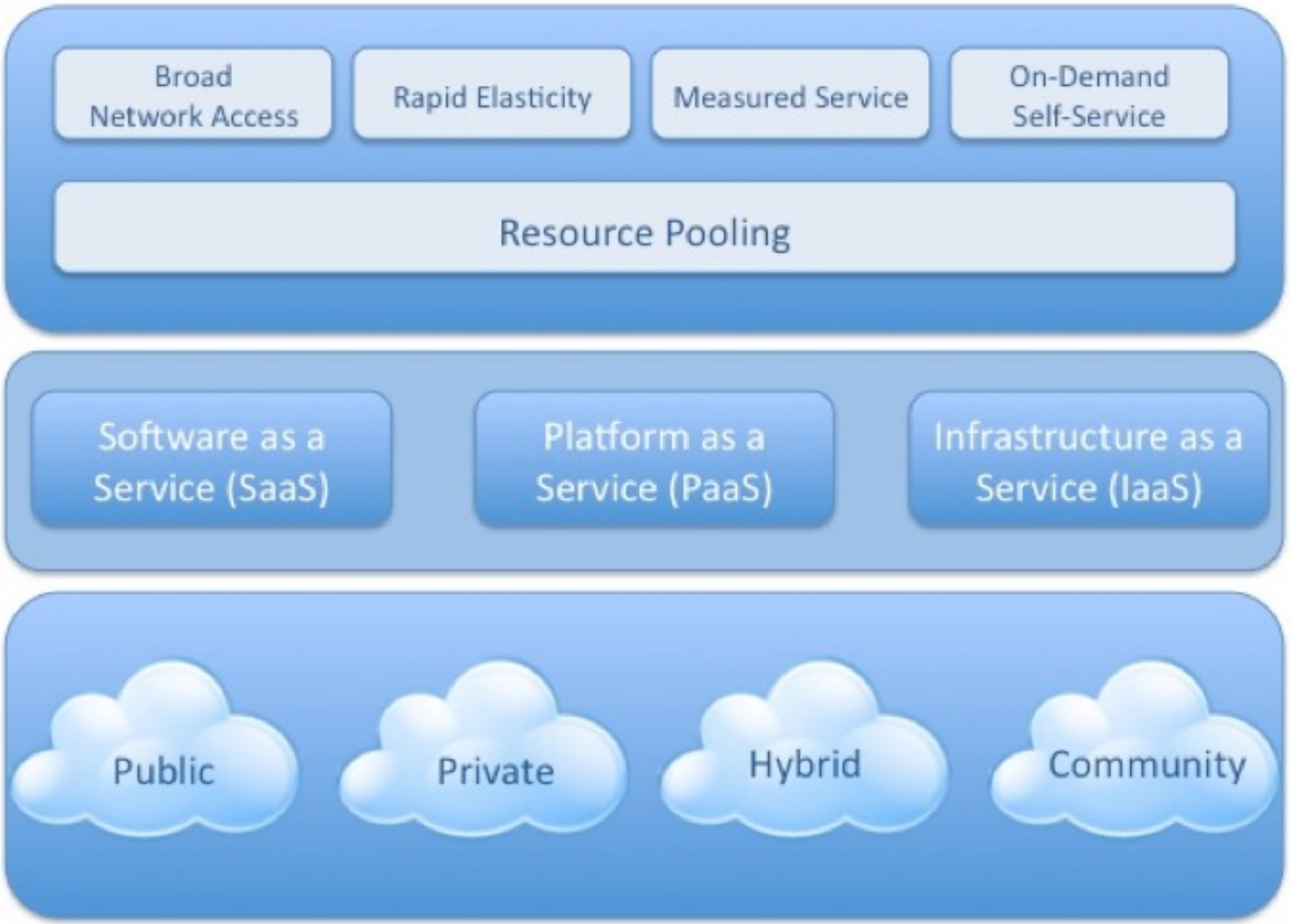
can be rapidly provisioned and released with minimal management effort or service provider interaction.

- This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Cloud Characteristics

Visual Model Of NIST Working Definition Of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

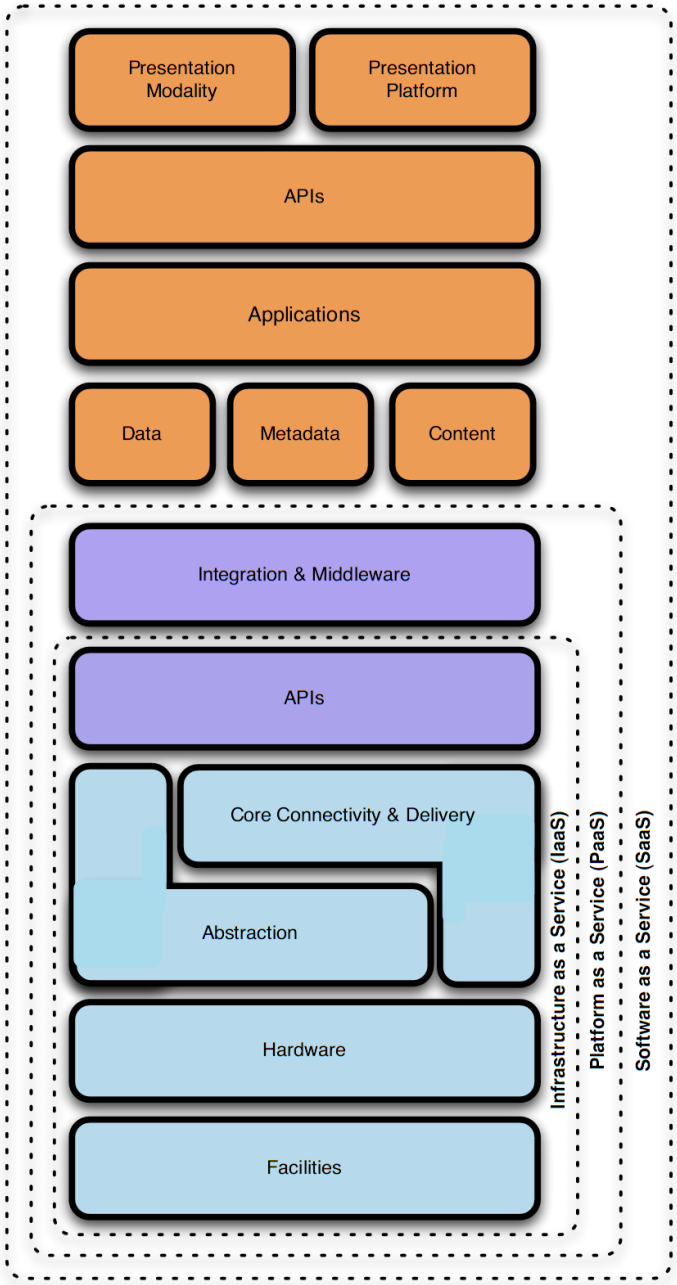


Characteristics of Cloud Computing

- Rapid elasticity
- High availability
- File synchronization
- On-demand
- Metered utilization

Cloud Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)



Common Cloud Models

- Infrastructure as a Service (IaaS)
  - Customers purchase access to data center infrastructure (storage, networking services)
  - Cloud provider covers the cost and work involved in equipment, configuration, and maintenance
  - The provider does not supply software

Common Cloud Models, Continued

- Platform as a Service (PaaS)
  - Enables vendors to develop and deploy application software in a cloud environment
  - A developer using PaaS can concentrate on software features instead of possible issues with server hardware and operating systems.

Common Cloud Models

- Software as a Service (SaaS)
  - Provider hosts software on servers
  - Customers access the software via a web browser

Types of Clouds

- Public cloud
  - Available to any organization that signs up or pays for it
  - Connection between services and organizations is the public Internet
- Private cloud
  - Available only to authorized users in a single company
  - The company owns and manages the cloud behind its firewall
  - Employees maintain the equipment

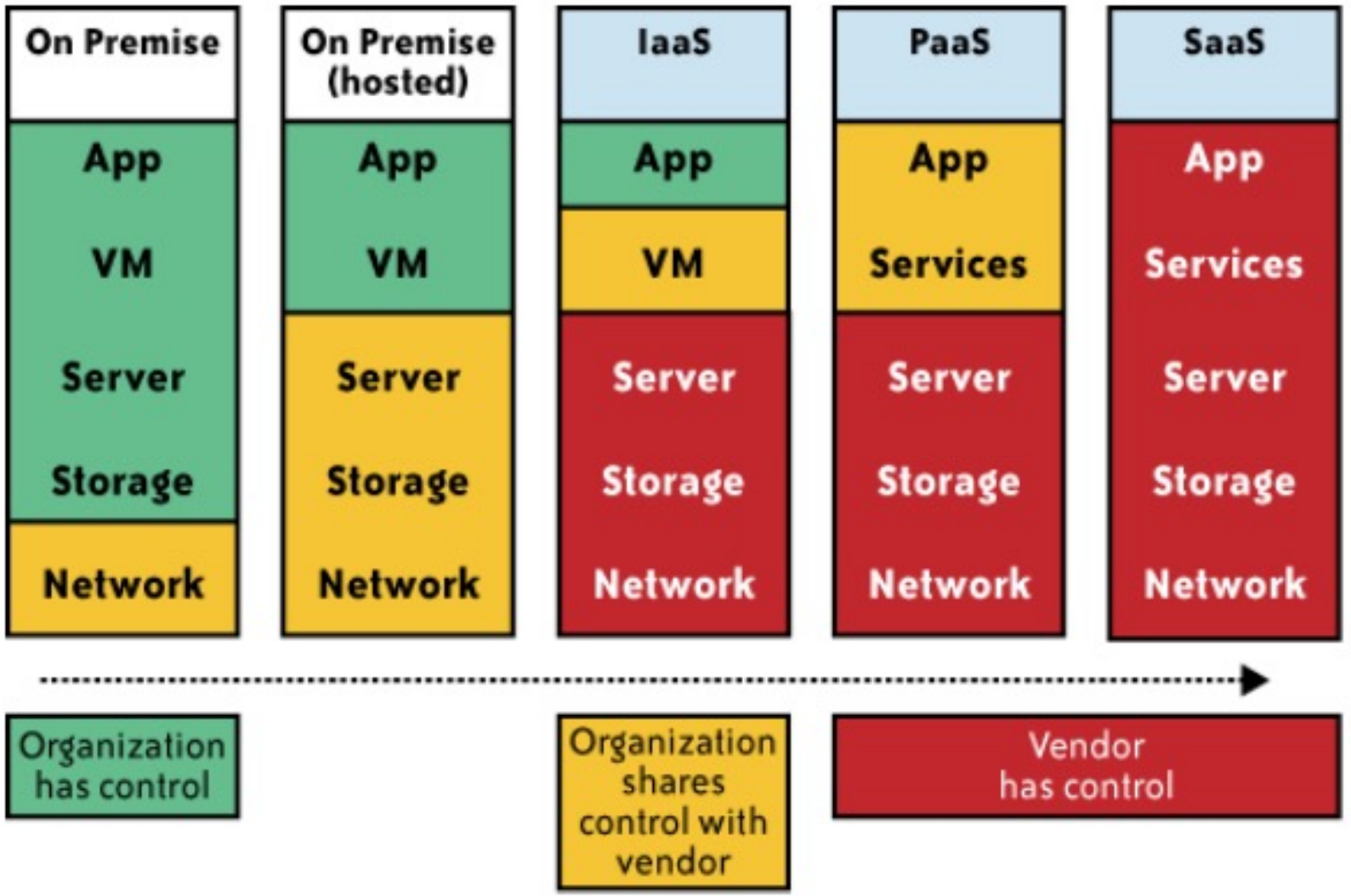
Types of Clouds, Continued

- Hybrid cloud
  - Combines features of public and private clouds
  - Typically includes dedicated and cloud-based servers and high-speed interconnections with load balancing
- Community cloud
  - A type of hybrid cloud that is used by different organizations that are working together
  - Organizations share the resources and costs
  - May be temporary for a specific project or goal

Internal vs. External Shared Resources

- Internal vs. external is defined by the ownership of the cloud's resources
  - Internal cloud
    - Provides greater control, security, and guaranteed availability
    - Similar to a private cloud but is built and owned inside the organization
  - External cloud
    - Exists outside an organization's physical boundaries

Impact of cloud computing on the governance structure of IT organizations



Shared responsibility model

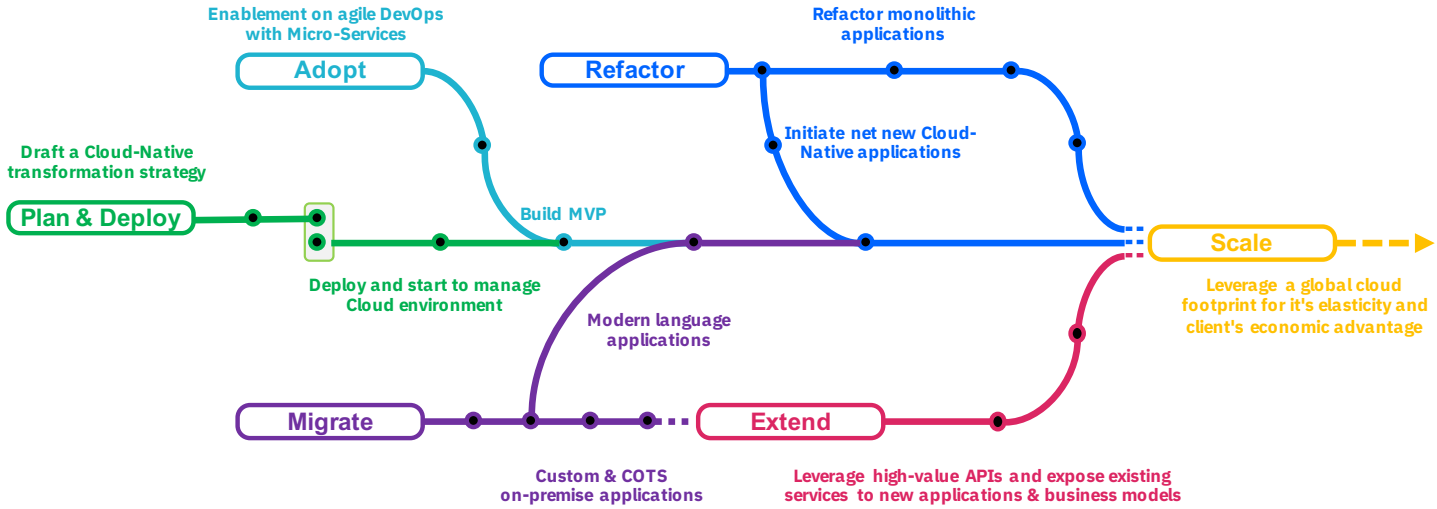
Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely' ?
  - If they can't, can we isolate them?
- How to provide separation between tenants?

- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

Preparing for Cloud

- Understand that cloud is a journey – it is not just a change in technology
- Cloud security must align with overall cloud strategy
- Understand your current cloud maturity level and where are in their journey



Decision Making Process

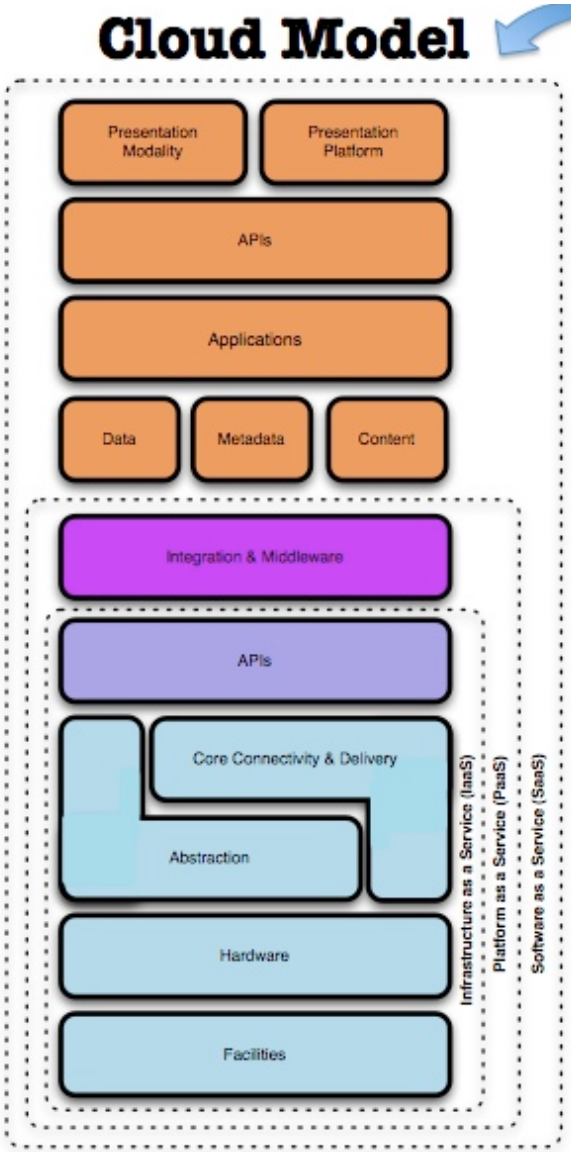
- Identify the asset for cloud deployment
- Evaluate the asset requirements for confidentiality, integrity, and availability
- Map the asset to potential cloud deployment models
- Evaluate potential cloud service models and providers
- Sketch the potential data flow
- Draw conclusions

Regulators expect the same level of control in a cloud environment

Regulators require firms to review the following before deciding to use cloud services

- Location of data and the related legal jurisdiction
- Identity and access management
- Auditability
- Availability
- Data classification
- Encryption management
- Security incident management
- Business continuity

Security Interaction 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

Uses for Cloud Computing

- Off-site email applications
- Cloud file storage services
- Virtual application streaming/cloud-based applications
- Virtual desktop (VDI)
- Virtual NIC

Desktop Virtualization

- Also called thin client networking
- Creating a user interface to a computer that is hosted on a central server or in the cloud
- Virtual desktop infrastructure (VDI)

Virtualization Key Terms

- Virtual machine manager (VMM)
  - Also called the hypervisor
  - Software that creates and manages virtual machines
- Virtual machine (VM)
  - A machine created by a hypervisor that runs like any other computer
- Emulation
  - Software-based reproduction of various operating systems but without the functionality and resource use of virtualization

Virtualization vs. Emulation

- Virtualization
  - Physical resources are divided between VMs that can run independently of each other
  - An OS is loaded into each VM
- Emulation
  - An emulation app creates a full reproduction of a different OS and different hardware
  - The emulation app is then used to run software made for that operating system

Categories of Virtualization

- Host/guest virtualization
- Server-hosted
- Client-side virtualization

Uses for Virtual Machines

- Help desk and support specialists can run older OSes without changing computers
- Application developers can test new software in a variety of OS environments
- Network administrators can run several kinds of servers on a single hardware box
- A VM can serve as a sandbox for testing new or risky software
- The same apps can be run across different platforms

Resource Requirements for Virtualization

- Fast, multi-core processors
- As much RAM as possible
- 64-bit processor and host OS, if possible
- BIOS/UEFI firmware support for virtualization
  - Not required but improves performance and increases the VMMs that are supported
- VMM applications such as Hyper-V or Virtual Box
- Legal copy of the OS to be installed on the VM

Infrastructure Security

- Network Level
- Host Level
- Application Level

The Network Level

- Ensuring confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- Ensuring availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
- Replacing the established model of network zones and tiers with domains

The Network Level - Mitigation

- Note that network-level risks exist regardless of what aspects of “cloud computing” services are being used
- The primary determination of risk level is therefore not which *aaS is being used,
- But rather whether your organization intends to use or is using a public, private, or hybrid cloud.

The Host Level

- PaaS/SaaS
  - Both the PaaS and SaaS platforms abstract and hide the host OS from end users
  - Host security responsibilities are transferred to the CSP (Cloud Service Provider)
    - You do not have to worry about protecting hosts
  - Customer still owns the risk of managing information hosted in the cloud services.

Local Host Security

- Are local host machines part of the cloud infrastructure?
  - Outside the security perimeter
  - While cloud consumers worry about the security on the cloud provider's site, they may easily forget to harden their own machines
- The lack of security of local devices can
  - Provide a way for malicious services on the cloud to attack local networks through these terminal devices
  - Compromise the cloud and its resources for other users

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

The Application Level

- DoS
- End user security
- Who is responsible for Web application security in the cloud?
- SaaS/PaaS/IaaS application security
- Customer-deployed application security

Data Security and Storage

- Several aspects of data security, including:
  - Data-in-transit
    - Confidentiality + integrity using secured protocol
    - Confidentiality with non-secured protocol and encryption
  - Data-at-rest
    - Not encrypted by default
  - Processing of data, including multitenancy
    - For any application to process data not encrypted

The Need for Strong IAM

- Organization's trust boundary will become dynamic and will move beyond the control and will extend into the service provider domain.
- Managing access for diverse user populations (employees, contractors, partners, etc.)
- Increased demand for authentication
  - personal, financial, medical data will now be hosted in the cloud
  - S/W applications hosted in the cloud requires access control
- Need for higher-assurance authentication
  - authentication in the cloud may mean authentication outside F/W
  - Limits of password authentication
- Need for authentication from mobile devices

Cloud-based vs. On-premises Attacks

- Cloud computing security includes many of the same functionalities as traditional IT security.
- Some types of cloud computing attacks include:
  - Session hijacking
  - DNS attack
  - Cross-site scripting (XSS)
  - SQL injection
  - Session riding
  - Distributed denial-of-service (DDoS) attack
  - Man-in-the-middle cryptographic attack
  - Side-channel attack
  - Authentication attack
  - API attacks

Top Security Threats

- Abuse and nefarious use of cloud computing
- Insecure interfaces & API's
- Unknown risk profile
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking

Security Issues and Requirements

- Monitoring network traffic
- Backing up VMs
- Updates and patches
- Sandboxing
- Best security practices for VMMs and VMs

Threat Mitigation

Abuse and nefarious use of cloud computing	▪ Stricter initial registration and validation processes. ▪ Enhanced credit card fraud monitoring and coordination. ▪ Comprehensive introspection of customer network traffic. ▪ Monitoring public blacklists for one's own network blocks.
Insecure interfaces & API's	▪ Analyze the security model of cloud provider interfaces. ▪ Ensure strong authentication and access controls are implemented in concert with encrypted transmission. ▪ Understand the dependency chain associated with the API.
Unknown risk profile	▪ Disclosure of applicable logs and data. Partial/full disclosure of infrastructure details ▪ Monitoring and alerting on necessary information.

Threat Mitigation

Malicious insiders	▪ Enforce strict supply chain management and conduct a comprehensive supplier assessment. ▪ Specify human resource requirements as part of legal contracts. ▪ Require transparency into overall information security and management practices, as well as compliance reporting. ▪ Determine security breach notification processes.
Shared technology issues	▪ Implement security best practices for installation and configuration. ▪ Monitor environment for unauthorized changes/activity. ▪ Promote strong authentication and access control for administrative access and operations. ▪ Enforce service level agreements for patching and vulnerability remediation. ▪ Conduct vulnerability scanning and configuration audits.

Threat Mitigation

Data loss or leakage	▪ Implement strong API access control. ▪ Encrypt and protect integrity of data in transit. ▪ Analyze data protection at both design and run time. ▪ Implement strong key generation, storage and management, and destruction practices. ▪ Contractually demand providers wipe persistent media before it is released into the pool. ▪ Contractually specify provider backup and retention strategies.
Account or service hijacking	▪ Prohibit the sharing of account credentials between users and services. ▪ Leverage strong two-factor authentication techniques where possible. ▪ Employ proactive monitoring to detect unauthorized activity. ▪ Understand cloud provider security policies and SLAs.

What Are the Key Privacy Concerns?

- Typically mix security and privacy
- Some considerations to be aware of:
  - Storage
  - Retention
  - Destruction
  - Auditing, monitoring and risk management
  - Privacy breaches
  - Who is responsible for protecting privacy?

Storage

- Is it commingled with information from other organizations that use the same CSP?
- The aggregation of data raises new privacy issues
  - Some governments may decide to search through data without necessarily notifying the data owner, depending on where the data resides
- Whether the cloud provider itself has any right to see and access customer data?
- Some services today track user behaviour for a range of purposes, from sending targeted advertising to improving services

Retention

- How long is personal information (that is transferred to the cloud) retained?
- Which retention policy governs the data?
- Does the organization own the data, or the CSP?
- Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?

Destruction

- How does the cloud provider destroy PII at the end of the retention period?
- How do organizations ensure that their PII is destroyed by the CSP at the right point and is not available to other cloud users?
- Cloud storage providers usually replicate the data across multiple systems and sites—increased availability is one of the benefits they provide.
  - How do you know that the CSP didn't retain additional copies?
  - Did the CSP really destroy the data, or just make it inaccessible to the organization?
  - Is the CSP keeping the information longer than necessary so that it can mine the data for its own use?

Auditing, monitoring and risk management

- How can organizations monitor their CSP and provide assurance to relevant stakeholders that privacy requirements are met when their PII is in the cloud?
- Are they regularly audited?
- What happens in the event of an incident?
- If business-critical processes are migrated to a cloud computing model, internal security processes need to evolve to allow multiple cloud providers to participate in those processes, as needed.
  - These include processes such as security monitoring, auditing, forensics, incident response, and business continuity

Privacy breaches

- How do you know that a breach has occurred?
- How do you ensure that the CSP notifies you when a breach occurs?
- Who is responsible for managing the breach notification process (and costs associated with the process)?
- If contracts include liability for breaches resulting from negligence of the CSP?
  - How is the contract enforced?
  - How is it determined who is at fault?

Data Security in the Cloud: Takeaways

1. Best practices to secure data in the cloud include using security fundamentals, securing cloud infrastructure, encrypting data, and complying with regulations.
2. Organizations can use the CIA triad as a guide to securing data in their cloud environment.
3. The shared responsibility model shows which parts of the cloud the customer is responsible for.
4. Organizations should use security services from cloud providers to encrypt data.
5. Organizations should be vigilant about the laws and regulations that apply to them and when those laws and regulations change or are added to.

Questions