OWASP Chapter Meeting | June 2010

SECURE CLOUD COMPUTING

Presented by: Brayton Rider, SecureState Chief Architect

Agenda

- What is Cloud Computing?
  - Cloud Service Models
  - Cloud Deployment Models
- Cloud Computing Security
  - Security Cloud Components
  - Cloud Security Advantages
  - Cloud Security Challenges
- Summary
  - Possible Effects of Cloud Computing

What is Cloud Computing?

Cloud Computing

- NIST defines cloud computing as a model for enabling 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 promotes availability.

- It is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

5 Essential Cloud Characteristics

- **On-demand self-service**
  - Get computing capabilities as needed automatically
- **Broad network access**
  - Services available over the net using desktop, laptop, PDA, and mobile phone
- **Resource pooling**
  - Provider resources are pooled to serve multiple clients, using a multi-tenancy model
  - Location independence
- **Rapid elasticity**
  - Ability to quickly scale in / out service
- **Measured service**
  - Control, optimize services based on metering

3 Cloud Service Models

- **Cloud Software as a Service (SaaS)**
  - Use provider's applications over a network
- **Cloud Platform as a Service (PaaS)**
  - Deploy customer-created applications to a cloud
- **Cloud Infrastructure as a Service (IaaS)**
  - Rent processing, storage, network capacity, and other fundamental computing resources
- To be considered "cloud" they must be deployed on top of cloud infrastructure that has the key characteristics

Cloud Software as a Service (SaaS)

- The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

- SaaS is a model of software deployment whereby a provider licenses an application to customers for use as a service on demand. SaaS software vendors (such as SalesForce.com) may host the application on their own web servers or upload the application to the consumer device, disabling it after use or after the on-demand contract expires.

- **Characteristics:**
  - *Strengths*
    - Sometimes free; easy to use; lots of different offerings; easy to access; good consumer adoption; proven business models
  - *Weaknesses*
    - You can only use the application as far as what it is designed for; no control or knowledge of underlying technology

Examples of SaaS

Cloud Platform as a Service (PaaS)

- PaaS deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications.
- Users gain increased flexibility and control in comparison to SaaS, however this is still somewhat restricted as to what a user can or cannot do.
- **Characteristics:**
  - *Strengths*
    - Great for developers with a particular niche target,
    - Upload a tightly configured applications
    - Simply “runs” within the platform’s framework;
    - More control than SaaS
  - *Weaknesses*
    - Restricted to the platform’s ability only
    - Hard to work “outside the box”
    - Sometimes dependent on Cloud Infrastructure providers

Examples of PaaS

Cloud Infrastructure as a Service (IaaS)

- IaaS delivers computer infrastructure, typically a platform virtualization environment, as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service.

- This service is what PaaS and SaaS are built on. IaaS providers allow users to create completely virtualized (or hybrid cloud/hardware) IT configurations, giving the user complete control of their environments.

- **Characteristics:**
  - *Strengths*
    - Offers full control of a company's infrastructure
    - Not confined to "containers" or "applications" or restrictive instances
  - *Weaknesses*
    - Sometimes comes with a price premium
    - Can be complex to build, manage and maintain (based on provider)

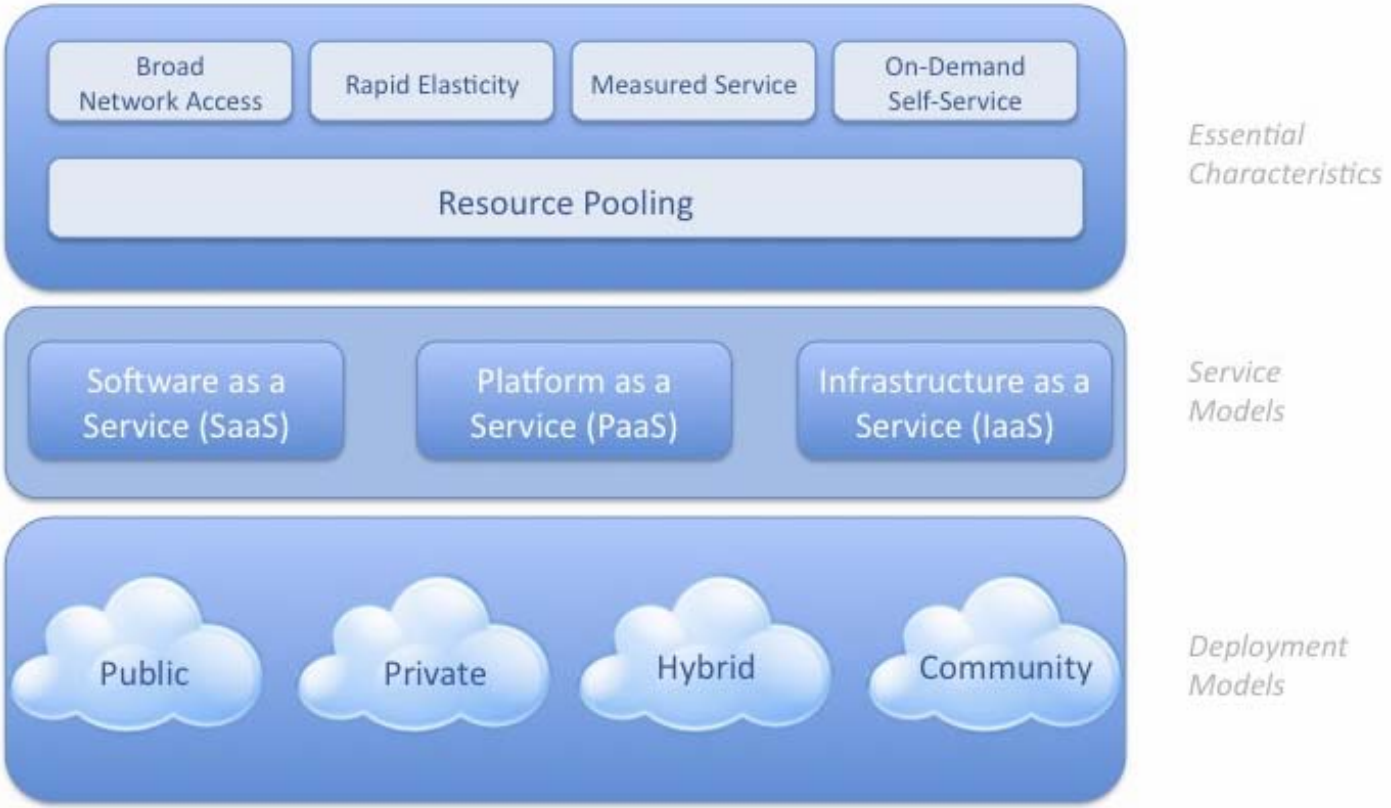
Examples of IaaS

4 Cloud Deployment Models

- **Private cloud**
  - The cloud infrastructure is operated solely for an organization.
- **Community cloud**
  - The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- **Public cloud**
  - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Hybrid cloud**
  - The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Visual Model Of NIST Working Definition Of Cloud Computing

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



Common Cloud Characteristics

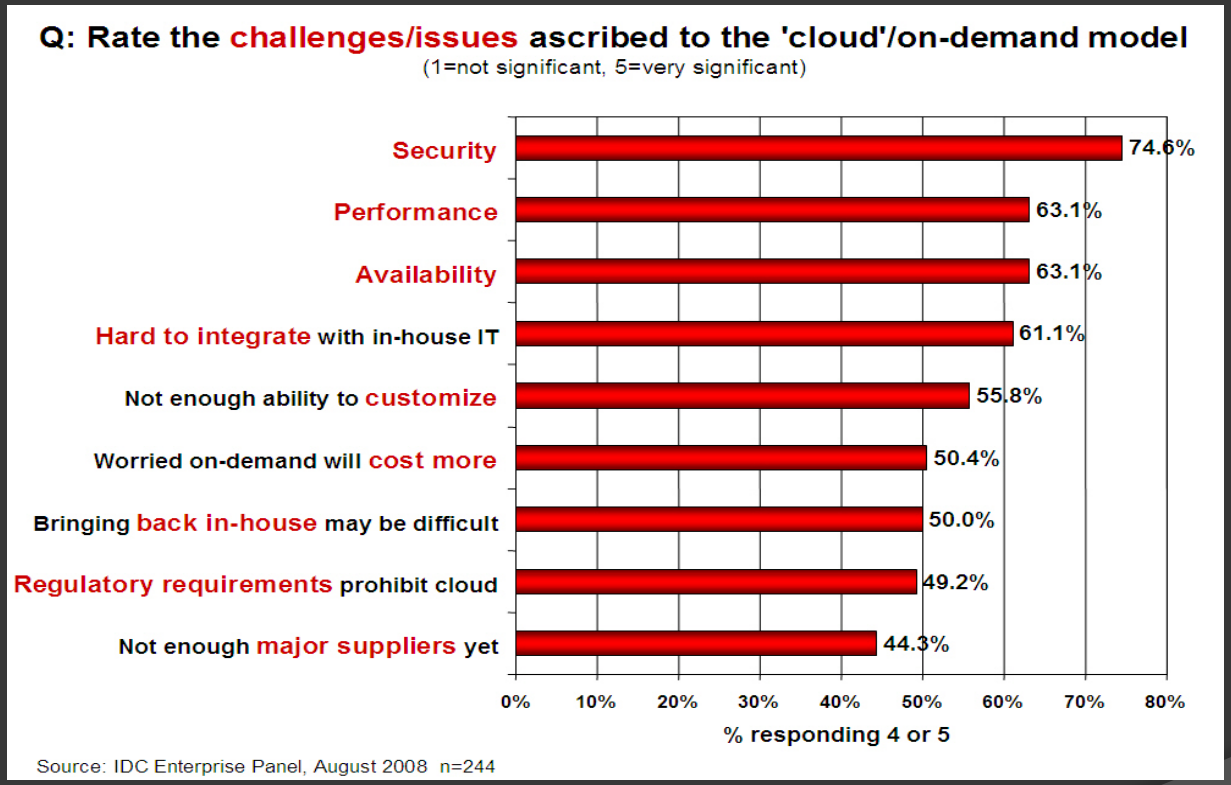
- Cloud computing often leverages:
  - Massive scale
  - Homogeneity
  - Virtualization
  - Resilient computing
  - Low cost software
  - Geographic distribution
  - Service orientation
  - Advanced security technologies

Business Benefits

- **Cost Containment**
  - Pay for use, little to no upfront capital expenditure.
- **Immediacy**
  - Services are provisioned quickly.
- **Availability**
  - Infrastructure has high bandwidth and load balancing capabilities.
- **Scalability**
  - Infrastructure capacity allows for traffic spikes and minimizes delays.
- **Efficiency**
  - Reallocating some operational activities to the cloud can free up resources to work on innovation.
- **Resiliency**
  - Cloud providers have mirrored solutions to minimize downtime in the event of a disaster. This type of resiliency can give businesses the sustainability they need during unanticipated events.

Cloud Computing Security

Security is the Major Issue



Key Security Issues

- **Trust**
- **Multi-Tenancy**
- **Encryption**
- **Compliance**

General Security Advantages

- Shifting public data to a external cloud reduces the exposure of the internal sensitive data.
- Cloud homogeneity makes security auditing/testing simpler.
- Clouds enable automated security management.
- Redundancy / Disaster Recovery.

Cloud Security Advantages

- Data Fragmentation and Dispersal
- Dedicated Security Team
- Greater Investment in Security Infrastructure
- Fault Tolerance and Reliability
- Greater Resiliency
- Hypervisor Protection Against Network Attacks
- Possible Reduction of C&A Activities (Access to Pre-Accredited Clouds)

- Simplification of Compliance Analysis
- Data Held by Unbiased Party (cloud vendor assertion)
- Low-Cost Disaster Recovery and Data Storage Solutions
- On-Demand Security Controls
- Real-Time Detection of System Tampering
- Rapid Re-Constitution of Services
- Advanced Honeynet Capabilities

General Security Challenges

- Trusting vendor’s security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can’t be examined
- Loss of physical control

Cloud Security Challenges

- Data dispersal and international privacy laws
  - EU Data Protection Directive and U.S. Safe Harbor program
  - Exposure of data to foreign government and data subpoenas
  - Data retention issues
- Need for isolation management
- Multi-tenancy
- Logging challenges
- Data ownership issues
- Quality of service guarantees

- Dependence on secure hypervisors
- Attraction to hackers (high value target)
- Security of virtual OS in the cloud
- Possibility for massive outages
- Encryption needs for cloud computing
  - Encrypting access to the cloud resource control interface
  - Encrypting administrative access to OS instances
  - Encrypting access to applications
  - Encrypting application data at rest
- Public cloud vs. internal cloud security
- Lack of public SaaS version control

Keep in Mind

- Issues with moving PII and sensitive data to the cloud
  - Privacy impact assessments
- Using SLAs to obtain cloud security
  - Suggested requirements for cloud SLAs
  - Issues with cloud forensics
- Contingency planning and disaster recovery for cloud implementations
- Handling compliance
  - FISMA
  - HIPAA
  - SOX
  - PCI
  - SAS 70 Audits

Possible Effects of Cloud Computing

- Small enterprises use public SaaS and public clouds and minimize growth of data centers
- Large enterprise data centers may evolve to act as private clouds
- Large enterprises may use hybrid cloud infrastructure software to leverage both internal and public clouds
- Public clouds may adopt standards in order to run workloads from competing hybrid cloud infrastructures

References

NIST on Cloud Computing

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

Cloud Security Alliance

- http://www.cloudsecurityalliance.org/

Thank you for your time!

Any questions? Contact brider@securestate.com