Information Security Decisions

TechTarget®

Cloud Security: Evaluating Risks within IAAS/PAAS/SAAS

Char Sample
Security Engineer,
Carnegie Mellon University CERT

Disclaimer

- Standard Disclaimer
  - This talk represents the opinions and research of the presenter only and not those of her employer. This talk is NOT a CERT sanctioned talk.

Is Your Data In The Cloud @ Risk?
Introduction

- Credentials etc.
- Acknowledgement

Agenda

- Defining the Cloud
  - General Overview
  - Specific Areas
- Security Implications
  - IaaS
  - PaaS
  - SaaS
- Data Loss Prevention (DLP)
- What You Can Do
- Conclusion & Wrap-up

Defining The Cloud

- What is the Cloud?
  - Difficult to define, no agreement on definition.
  - One definition "The provision of dynamically scalable and often virtualized resources as a service over the Internet on a utility basis. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the 'cloud' that supports them."
  - NIST 800-145 also attempted to define the cloud.

Defining The Cloud

- NIST Standard 800-145 defines 3 Cloud Service Areas.
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)

Defining The Cloud

- According to Mather, Kumaraswamy and Latif, common characteristics of Cloud Computing include:
  - Shared resources
  - Massive scalability
  - Elasticity
  - “Pay as you go”
  - Self-provisioning of resources

Defining The Cloud

- Not a model, a combination of models.
- A type of abstraction.
- Another step (not sure if forward) in the technology arena.
  - Mainframe -> PCs -> client server -> Internet -> Cloud computing
  - Considered a strategic technology

Defining The Cloud

- Cloud Server characteristics:
  - Widely distributed across wide geographic range.
  - Virtualized environments (Amazon EC2), virtualized data centers.
  - Diverse access mechanisms
    - Desktop clients.
    - Mobile clients.
  - Single tenant or multi-tenant apps
    - Single tenant better for security.
    - Multi-tenant more cost effective.

Defining The Cloud

- Public
  - Multi-tenant.
  - CSP provides security.
- Private
  - Owner responsible for security.
  - SLAs (vendor owned and operated)
  - Managed (owner and vendor have different roles)
- Hybrid
  - Mixes both, data sensitivity determines what goes where.
    - Sensitive data and apps: private cloud
    - Public data and apps: public cloud

Defining The Cloud - Specifics

- IaaS
  - Virtual environment
    - Examples: Amazon EC2, Verizon, IBM
    - Management and provisioning
    - Internet connectivity
    - Desktop virtualization
    - AKA Hardware as a Service (HaaS)
    - Servers in the virtualized environment

Defining The Cloud - Specifics

- PaaS
  - Examples: Google App Engine, RedHat
  - Thought of as an outgrowth of SaaS. Where SaaS does processing, background functions such as storage, integration etc. comprise PaaS.
  - Disks in the virtualized environment.
  - The foundation for the development environment.

Defining The Cloud - Specifics

- SaaS
  - Examples: Google Apps, Oracle SaaS, NetSuite
  - Common applications and libraries for customized development.
  - Both disks and servers in the virtualized environment.

Security Implications

- First the good:
  - Cost savings.
  - Improved performance.
  - Better reliability.
  - Scalability as needed.
  - Personnel cost savings.
  - Reduced ownership costs.

Security Implications

- Next the not as good
  - Cloud providers are expected to consolidate.
    - Consolidation means that there will be winners and losers.
    - Also means procedures will migrate to the most common, or most cost effective. Not necessarily the most secure.
    - Increases likelihood of some providers not surviving, what happens to data when that occurs?

Security Implications

- Not as good
  - International issues
    - Transborder data flow
      - How do agreements get enforced.
      - Should some data stay out of the cloud?
  - Cross tenant hacking?
  - Mapping of virtual environments to physical servers.
  - How are the paths between servers managed?
  - How are the different servers and libraries managed?

Security Implications

- Risks
  - DoS attacks.
  - Custom security features unavailable.
  - Legal risks and costs.
  - Excessive trust in CSP.
  - Potential for “fast flux” hacking points.
  - Concerns about data location, ownership, and more.
  - Co-mingled data, even if not co-mingled may use shared memory.

Security Implications

- Risks (continued)
  - Will data be encrypted?
    - When at rest or in motion or both?
    - Encryption adds significant overhead.
    - Key management?
  - Exploitation of hypervisor vulnerabilities.
  - Are CSP data elements really deleted?

Security Implications

- Risks (continued)
  - Insider threat at CSP is much more costly, than at individual sites.
  - Inconsistent security profiles between CSPs and between tenants.
  - Because of the nature of the cloud, threats and vulnerabilities must be dealt with more aggressively than in conventional environments.

Security Implications: IaaS

- IaaS: Platform Virtualization
  - Consider that paths for configurable files are likely to be the same across each virtual environment.
    - Private key paths
    - DNS zone files, and DNSSEC key files.
    - Virtual hosts will still map to physical IP addresses.
    - The hypervisor is under the control of the ISP. A single vulnerability to the hypervisor provides direct and trusted access to all tenants environments.
    - “Client” hosts will need to protect themselves from servers, even if all the hosts belong to the same organization.

Security Implications: IaaS

- IaaS: Platform virtualization
  - Running multiple copies of software platforms (most often OSs) on a single piece of hardware
  - A quick analysis revealed 20 environments per server.
  - Each piece of software behaves as if there is a one-to-one relationship between it and the hardware.
  - No awareness whatsoever of the other VMs that run on the same physical hardware.
  - VMs can all have the same MAC address.
  - Ability to remove the entire environment.
  - Myth of virtualization improving security

Security Implications: PaaS

- PaaS: Virtual Environments
  - Provides dynamic load balancing capacity across multiple file systems and machines.
  - Provides ability to pool computing resources (e.g., Linux clustering).
  - Provides convenience for users in accessing different OSs (as opposed to systems with multiple boot capability).
  - Allows custom VMs, each of which can serve as a container for delivery of applications.

Security Implications: PaaS

- PaaS: Virtual Environments
  - Can be implemented through software apps or hardware and software hybrid appliances.
  - Can utilize storage area networks (SANs)
  - Hides complexity of SAN functions.

Security Implications: SaaS

- SaaS: Virtual Environments
  - Application security is not easy nor cheap.
  - Apps, especially client apps, are being developed for a variety of platforms. Each interface represents a potential attack vector.
  - Lack of standards.
    - Software
    - Developers
  - Rush to market.

Security Implications: SaaS

- SaaS: Virtual Environments
  - Even if the app is secure, that may not be enough.
    - Libraries
    - Environment or “sand box”.
  - CSPs are largely in control of application security
    - In IaaS, should provide at least a minimum set of security controls
    - In PaaS, should provide sufficiently secure development tools
  - Customers can control access & authentication into their network.
  - SLAs can be written to further tighten controls and determine roles and responsibilities.

DLP

- There are many concerns about data safety with the cloud.
  - Data in motion.
  - Data at rest.
- Depending on your security posture there are ways to navigate DLP issues.
  - Some encrypt objects before they go to the cloud.
  - Encrypt the path (SSL)
  - Encrypt objects when they are stored.
  - Policy: No sensitive data in the cloud (processed or stored)…ever.
  - Auditing of the CSP’s cloud.

DLP

- Consider confidentiality of data in motion.
- Consider integrity of data in motion.
- Consider availability of data in motion.
- Consider the integrity of audit logs and “permanence”.
- Consider the impact of IP address re-cycling on access control devices.

DLP

- End user issues
  - Acceptable use policy
  - Training and awareness

Other

- How to secure the transition to the cloud.
- Who owns what in the cloud?
- How does clustering and back-ups work?
- How will identity management be supported? How will tokens or other related software be secured in the cloud?
- How will the cloud be audited?

What Can You Do?

- First determine what is of value.
  - Not everything needs to be migrated to the cloud.
  - Determine the various levels of security to associate with the data.
- Develop cloud policies and procedures.
- Avoid over trusting, minimal trust and verify that!

What Can You Do?

- Create SLAs/SOWs for your CSP. Do not accept the CSP SLA/SOW.
  - Determine how breaches will be handled.
  - Determine if foreign servers will be used for backups.
  - Data destruction.
  - If you like your present security posture insist on re-creating it in the cloud.
  - Audit
  - Monitor

Conclusion

- Cloud rhetoric is starting to quiet down.
- The “cloud” means different things to different people. When embarking on a migration be sure to find out which cloud areas your organization plans to utilize.
- CSPs are getting to work on answering many of the early security questions.
- CSPs are also consolidating.

Conclusion

- Each layer has it’s own unique security challenges.
  - Software – poorly written code.
  - Platform – weak access controls, cross tenant target.
  - Infrastructure - vulnerabilities in this environment can expand dramatically across tenants and go undetected.
  - Hypervisor – Vulnerabilities at this layer provide trusted access to each environment.

Conclusion

- Threat detection in the cloud will improve.
- Cloud audits will become part of the landscape.
- Trust assurance or certification will be used as a differentiator.
- Cloud Security Standard are being developed.
    - Implementation
    - Adherence

Conclusion

- SLAs and SOWs will need to be carefully written.
- Ultimately the customer owns the data; therefore, great care and planning is required for DIT and DAR.
- The black hat community is focusing on creating tools to exploit virtual environments, eventually something will work, be prepared.

Conclusion

- Securing the data against DLP requires:
  - Careful planning.
  - Understanding of security implications for your data and connections.
  - Determining via cost benefit analysis which data should migrate to the cloud.
  - Creating and enforcing policies that enforce your goals.
  - Use of technology to ensure: confidentiality, integrity and availability.

Q&A

- Questions and answers

Contact

Char Sample

Security Engineer,

Carnegie Mellon University CERT

char_sample@yahoo.com

TechTarget
Editorial
Speaker Bureau
2012

**Featured Member of the
TechTarget Editorial
Speaker Bureau**