Cloud Security:Threats & Mitgations

Vineet Mago
Naresh Khalasi
Vayana

IndicThreads.com Conference On

Upcoming Technology

2010: Cloud Computing

Pune, India

What are we gonna talk about?

- What we need to know to get started
- Its your responsibility
- Threats and Remediations: Hacker v/s Developer

What Security

- Physical security – controls implemented at and for physical facilities (offices, datacenters)
- Network security – controls implemented for network (firewall, anti-DDoS, auth controls)
- System security – controls implemented for the IT systems (anti-virus, active directory)
- Application security – controls implemented for business applications (AAA, API Security, release management)
- Maturity, effectiveness & completeness of security controls implemented

First Step Towards Cloud Security

- Your assets on the cloud - Data, Applications & Processes
- Evaluate all assets in terms of
  - Confidentiality
    - What if the asset becomes publicly accessible?
    - What if the cloud provider employee accessed your asset?
  - Integrity
    - What if the process was manipulated by an outsider?
    - What if the process failed to provide expected results?
    - What if the data got unexpectedly changed?
  - Availability
    - What if the asset were unavailable for a period of time?

Cloud Service Models

IAAS	➢ Provider secures the physical infrastructure (server locations) ➢ Provider may give basic firewall like protection for running instances ➢ Consumer implements additional Network, System and Application security controls ➢ Zero application like features, enormous extensibility
PAAS	• Provider takes care of securing the infrastructure (server locations, servers, network, OS and storage) • Consumer implements Application security controls • Intended to enable developers to build their apps on top of the platform
SAAS	• Provider implements the Network, System & Application security • Service levels, security, liability expectations are contractually enforced • Most integrated functionality • And hence, Least consumer extensibility

Lets Begin the Debate

The first Threat:

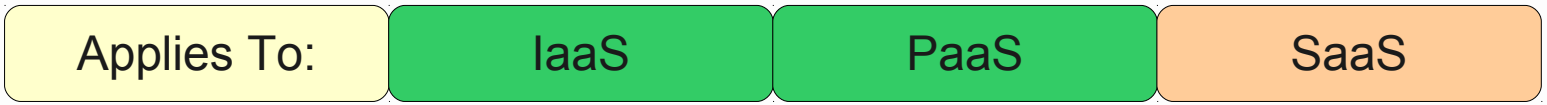
Unknown Risk Profile

Applies To:	IaaS	PaaS	SaaS

Well, Yeah !

- But we have to start somewhere:
  - Educate ourselves
  - Read the Contract Carefully ! Disagree when you are not comfortable
  - Ask the provider for Disclosure of applicable logs and data. Get Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.).
  - Setup best possible Monitoring and alerting on necessary information
  - TOOLS: NAGIOS, AIDE

Abuse and Nefarious Use of Cloud Computing



I choose my friends wisely!

- Look for providers with Stricter initial registration and validation processes.
- Check levels of credit card fraud monitoring and coordination used by the provider
- Is the provider capable of running a Comprehensive introspection of customer network traffic
- Monitor public blacklists for one's own network blocks.

Insecure Interfaces and APIs

Applies To:	IaaS	PaaS	SaaS

Yeah, thats a tough one!

- Analyze the security model of cloud provider's interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the Dependency Chain associated with the API.

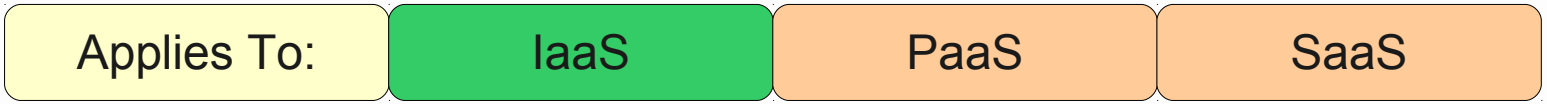
Malicious Insiders

Applies To:	IaaS	PaaS	SaaS

You can trust no one !

- 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



Get your own Bag !

- Implement security best practices for installation/ 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

Data Loss or Leakage

Applies To:	IaaS	PaaS	SaaS

I know its Confidential

- 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

Applies To:	IaaS	PaaS	SaaS

Do I really know you?

- 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 do we do now?"

Lets Brace Ourselves

- Basic Security
  - Install libpam for enforcing stricter password scheme
  - Defined a policy for groups and users
    - Disable root login
    - Don't share user logins
    - Assign user privileges based on requirements
    - Minimize the login accounts that have root access
    - Enable user action logging (**)
    - Don't run webserver and database as root user
    - Restrict SSH access by groups or users
  - Allow SSH login using identity keys only
  - Change default SSH port

Server / OS Hardening

- Chkrootkit – Checks for root kits installed, if any
- SNORT - Intrusion Detection
- AIDE - File Integrity Checking, can alert you if any file is changed on the machine
- psad – Port Scan Attack Detection – Well !
- Bastille – Best Firewall configuration tool
- NAGIOS – Open source remote monitoring of the server and all important services running on it
- Keep a Reference Machine Image

Apache web server Hardening

- Download server binary from trusted sources only and verify download integrity
- Disable modules that are not required
- Change the default webserver user and group
- Follow appropriate security forums & apply security patches ASAP

Application Security -Authentication

- Authentication must be on HTTPS
- Choose strong authentication scheme, especially if you are going to provide an API access
- Prefer Basic authentication over HTTPS as against Digest authentication.
- Maintain a strong password policy
- Implement captcha or response slow down when multiple failed login attempts are detected

Application Security – the rest

- Educate yourself on application security, learn to use a http intercepting proxy – WebScarab/Burp
- Top Ten Vulnerabilities according to the OWASP Project – Remember these are just the TOP TEN
  - Injection, Cross-Site Scripting (XSS), Broken Authentication and Session Management, Insecure Direct Object References, Cross-Site Request Forgery (CSRF), Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards

What happens next?"
"I'm not sure, exactly. But this world is ours now.
It's what we make of it." - 9 (2009)