Clouds on the Horizon

Cloud Security in Today’s DoD Environment

Bill Musson
Security Analyst
Cloud [ klaüd ]
vb. to make obscure, to confuse.

SO THAT'S WHY THEY CALL IT 'CLOUD' COMPUTING!
Agenda

- Overview of Cloud architectures
  - Essential characteristics
  - Cloud service models
  - Cloud deployment models

- Security Issues
  - Confidentiality
  - Integrity
  - Authentication
  - Availability
  - Data Remanence
  - Regulatory Requirements
What is the “Cloud”
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
Deployment Models

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

**SaaS**
Cloud Infrastructure

**PaaS**
Cloud Infrastructure

**IaaS**
Cloud Infrastructure

Software as a Service (SaaS)
Providers
Applications

Platform as a Service (PaaS)
Deploy customer created Applications

Infrastructure as a Service (IaaS)
Rent Processing, storage, N/W capacity & computing resources
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 get 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
Deployment Models

- **Community**
  - Cloud infrastructure shared by several orgs that have shared concerns, managed by org or 3rd party

- **Hybrid**
  - Combo of multiple clouds bound by standard or proprietary technology
Organizations are still afraid to use clouds

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)

- Security: 74.6%
- Performance: 63.1%
- Availability: 63.1%
- Hard to integrate with in-house IT: 61.1%
- Not enough ability to customize: 55.8%
- Worried on-demand will cost more: 50.4%
- Bringing back in-house may be difficult: 50.0%
- Regulatory requirements prohibit cloud: 49.2%
- Not enough major suppliers yet: 44.3%

Source: IDC Enterprise Panel, August 2008  n=244
A Massive Concentration of Resources

Also a massive concentration of risk

- expected loss from a single breach can be significantly larger
- concentration of “users” represents a concentration of threats
- “Ultimately, you can outsource responsibility but you can’t outsource accountability.”
Cloud Security Issues

- Most security problems stem from:
  - Loss of control
  - Lack of trust (mechanisms)
  - Multi-tenancy

- These problems exist mainly in 3rd party management models
  - Self-managed clouds still have security issues, but not related to above
Loss of Control in the Cloud

- Loss of control
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources
Lack of Trust in the Cloud

- Trusting a third party requires taking risks

- Defining trust and risk
  - Opposite sides of the same coin

- Defunct third party management schemes
  - Hard to balance trust and risk
Multi-Tenancy

- 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
Security Issues

O Confidentiality
   O Fear of loss of control over data
     O Will the sensitive data stored on a cloud remain confidential?
     O Will cloud compromises leak confidential client data
     O Will the cloud provider itself be honest and won’t peek into the data?

O Integrity
   O How do I know that the cloud provider is doing the computations correctly?
   O How do I ensure that the cloud provider really stored my data without tampering with it?
Security Issues

○ Availability
  ○ Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  ○ What happens if cloud provider goes out of business?
  ○ Would cloud scale well-enough?
  ○ Often-voiced concern
    ○ Although cloud providers argue their downtime compares well with cloud user’s own data centers
Security Issues

• Privacy issues raised via massive data mining
  – Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients

• Increased attack surface
  – Entity outside the organization now stores and computes data, and so
  – Attackers can now target the communication link between cloud provider and client
  – Cloud provider employees can be phishing
Security Issues

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don’t maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?
Attacks

- Distributed Denial Of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks.
- IP Spoofing
- Port Scanning
- Packet sniffing by other tenants
Encryption

"One ring to rule them all, one ring to find them, one ring to bring them all and in the darkness bind them."
Availability

Nirvanix Customers,

For the past seven years, we have worked to deliver cloud storage solutions. We have concluded that we must begin a wind-down of our business and we need your active participation to achieve the best outcome.

We are dedicating the resources we can to assisting our customers in either returning their data or transitioning their data to alternative providers who provide similar services including IBM SoftLayer, Amazon S3, Google Storage or Microsoft Azure.

We have an agreement with IBM, and a team from IBM is ready to help you. In addition, we have established a higher speed connection with some companies to increase the rate of data transfer from Nirvanix to their servers.

We are working hard to have resources available through October 15 to assist you with the transition process, and have set up a rapid response team that can be reached at (619) 764-5650 [press 2 for customer support during normal business hours] or (888) 751-0365 after business hours, or contact customersupport@nirvanix.com.

Please check back to this web page periodically for status updates.

We thank you for your support and patience.

The Nirvanix team

UPDATE ON NIRVANIX

On October 1, 2013, Nirvanix voluntarily sought Chapter 11 bankruptcy protection in order to pursue all alternatives to maximize value for its creditors while continuing its efforts to provide the best possible transition for customers.
Identity and Access Management

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

- 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
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?
Data Remanence

- Cloud computing crime poses unique forensics challenges
- Over time,
  - it's expected that clouds will contain more and more evidence of criminal activity
  - the use of digital evidence in criminal and civil matters will continue to expand.
- Cloud providers and customers need to set up their infrastructures to meet these lawful requests or face fines and other legal repercussions.
Forensics

- Traditional computer forensics must address the following steps:
  - Collection of media at the crime scene or location where the media was seized
  - Preservation of that media; and validation, analysis, interpretation, documentation and courtroom presentation of the results of the examination.
  - Forensic challenges raised by cloud computing are related to control of the evidence, including collection, preservation and validation
Auditing and Monitoring

- 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.
Governance

- DOD Memorandum July 2012 (draft)
  - Cloud Computing Strategy

- NIST SP800-145
- NIST SP500-292
- NIST SP500-299
- NIST SP 800-53 security controls
- NIST SP 800-53a assessment procedures

- FedRAMP
Reference

O Security Guidance for Critical Areas of Focus in Cloud Computing v2.1
   http://www.cloudsecurityalliance.org
O NIST Cloud Model:
   www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
O Cloud Security Alliance (CSA)
O Various cloud working groups
   O Open Cloud Computing Interface Working Group, Amazon EC2, Splunk, McAfee, Microsoft, and Dell among others