Security & Trust in the Cloud

Ray Trygstad
Director of Information Technology,
IIT School of Applied Technology
Associate Director, Information Technology
& Management Degree Programs
Cloud computing is 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.
Cloud Computing Primer

This cloud model promotes availability and is composed of:

- Five essential characteristics
- Three service models
- Four deployment models
Cloud Five Essential Characteristics

► On-demand self-service
► Broad network access
► Resource pooling
► Rapid elasticity
► Measured Service

http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
Cloud Three Service Models

► **Software as a Service (SaaS)**
  - Use provider’s applications over a network

► **Platform as a Service (PaaS)**
  - Deploy customer-created applications to a cloud

► **Infrastructure as a Service (IaaS)**
  - Rent processing, storage, network capacity, and other fundamental computing resources
  - Now often a key to disaster recovery

http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
Cloud Four Deployment Models

► Private cloud
  ■ Enterprise owned or leased

► Community cloud
  ■ Shared infrastructure for specific community

► Public cloud
  ■ Sold to the public, mega-scale infrastructure

► Hybrid cloud
  ■ Composed of two or more clouds

http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
Cloud Landscape

SaaS

PaaS

IaaS

Value Visibility to End Users

End Users

Application Developers

Network Architects
Cloud Computing Often Leverages…

► Massive scale
► Homogeneity
► Virtualization
► Resilient computing
► Low cost software
► Geographic distribution
► Service orientation
► Advanced security technologies

http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
The NIST Cloud Definition Framework

Deployment Models
- Private Cloud
- Community Cloud
- Public Cloud

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

Essential Characteristics
- On Demand Self-Service
  - Broad Network Access
  - Resource Pooling
- Rapid Elasticity
  - Measured Service

Common Characteristics
- Massive Scale
- Homogeneity
- Virtualization
- Low Cost Software
- Resilient Computing
- Geographic Distribution
- Service Orientation
- Advanced Security
Multi-Tenancy

► Implies a need for
  ■ Policy-driven enforcement,
  ■ Segmentation
  ■ Isolation
  ■ Governance
  ■ Service levels
  ■ Chargeback/billing models

► For different consumer constituencies

http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
Cloud Use in Enterprises

Effective use requires

- Very robust network connectivity
  (i.e. honking big bandwidth)
- Security
- Guarantee of service

Security and guarantee of service at some levels provided by Service Level Agreements
Key Technology: Virtualization

Traditional Stack

Operating System

Hardware

Virtualized Stack

Hypervisor

Hardware

App

OS

App

App

App

OS
Cloud Reference Model

**SaaS**
- Presentation Modality
- Presentation Platform
- APIs
- Applications
- Data
- Metadata
- Content
- Integration and middleware

**PaaS**
- Integration and middleware
- APIs
- Core Connectivity & Delivery
- Abstraction
- Hardware
- Facilities

**IaaS**
- APIs
- Core Connectivity & Delivery
- Abstraction
- Hardware
- Facilities

Security is a Major Issue

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
Cloud Computing Concerns

- Security defects in the technology itself: 54%
- Unauthorized access to or leak of our proprietary information: 51%
- Unauthorized access to or leak of our customers’ information: 49%
- Application/system performance: 34%
- Business continuity/DR readiness of provider: 26%
- Business viability of provider; risk company will fail: 25%
- Vendor lock-in: 17%
- Features and general maturity of technology: 17%
- Unpredictable costs: 13%
- Other: 2%

Note: Three responses allowed
Base: 310 respondents using, planning to use or considering using cloud computing
Data: InformationWeek Analytics 2010 Cloud GRC Survey of 518 business technology professionals, January 2010
Cloud Security Key Issues

► Some key issues:
   ■ Trust, multi-tenancy, encryption, compliance
   ■ Clouds are massively complex systems can be reduced to simple primitives that are replicated thousands of times and common functional units

► Cloud security is a tractable problem
   ■ There are both advantages and challenges
Cloud 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 Challenges

► Trusting the vendor’s security model
► Customer inability to respond to audit findings
► Obtaining support for investigations
► Indirect administrator accountability
► Proprietary implementations that can’t be examined
► Loss of physical control
Cloud Security Standards (!)

► National Institute for Standards and Technology
NIST Special Publication 800-144
Guidelines on Security and Privacy in Public Cloud Computing (Draft)

► Cloud Security Alliance
Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
Guidelines on Security and Privacy in Public Cloud Computing

Wayne Jansen
Timothy Grance
Compliance → Security → Cloud

Who Does Security Where?

The lower down the stack the Cloud provider stops, the more security the consumer is tactically responsible for implementing & managing.

Scope & Control in Cloud Service Models

From NIST Draft Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing by Wayne Jansen and Timothy Grance
SaaS and Security

Provides:

- Most integrated functionality
- Least consumer extensibility
- Relatively high level of integrated security
  - Provider bears a responsibility for security

PaaS and Security

► Enables developers to build their own applications on top of the platform
► Tends to be more extensible than SaaS
► Built in security features and capabilities are less complete
  ■ But there is more flexibility to layer on additional security

IaaS and Security

► Provides few if any application-like features, but enormous extensibility.

► Less integrated security capabilities and functionality beyond protecting the infrastructure itself.

► Requires OS, apps, and content be managed and secured by the consumer.
SaaS Security

► Vendor bears primary responsibility
► Governed/driven by Service Level Agreements
► Gartner suggests 7 issues to settle with vendor
  ■ All should be specified by SLA
Service Level Agreements (SLAs)

- Contract between customers and service providers of the level of service to be provided
- Contains performance metrics (e.g., uptime, throughput, response time)
- Problem management details
- Documented security capabilities
- Contains *penalties* for non-performance
SaaS Security

► Privileged user access
► Regulatory compliance
  ■ Ensure vendor is willing to undergo external audits and security certifications
► Data location
  ■ Ask if they’ll commit to storing/processing data in specific jurisdictions, and if they’ll obey local privacy requirements

SaaS Security

► Data segregation
  ■ Ensure encryption is available at all stages and encryption schemes were designed and tested by experienced professionals

► Recovery
  ■ What will happen to your data and service in a disaster; must replicate data and app infrastructure across multiple sites

SaaS Security

► Investigative support
  ■ Get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities

► Long-term viability
  ■ In case of vendor bankruptcy or acquisition, ensure your data will remain available

SaaS Service Level Agreements

- salesforce.com – the “trust us” model
  - No SLA!
  - AKA “don’t worry be happy”

- Google Apps
  - Standard SLA has NO security clauses
  - Security addressed at security FAQ but incurs no legal obligation
Google Apps Service Level Agreement

Google Apps SLA. During the Term of the applicable Google Apps Agreement (the "Agreement"), the Google Apps Covered Services web interface will be operational and available to Customer at least 99.9% of the time in any calendar month (the "Google Apps SLA"). If Google does not meet the Google Apps SLA, and if Customer meets its obligations under this Google Apps SLA, Customer will be eligible to receive the Service Credits described below. This Google Apps SLA states Customer’s sole and exclusive remedy for any failure by Google to meet the Google Apps SLA.

Definitions. The following definitions shall apply to the Google Apps SLA.

"Downtime" means, for a domain, if there is more than a five percent user error rate. Downtime is measured based on server side error rate.

"Google Apps Covered Services" means the Gmail, Google Calendar, Google Talk, Google Docs, Google Groups and Google Sites components of the Service. This does not include the Gmail Labs functionality, Google Apps – Postini Services, Gmail Voice or Video Chat components of the Service.

"Monthly Uptime Percentage" means total number of minutes in a calendar month minus the number of minutes of Downtime suffered in a calendar month, divided by the total number of minutes in a calendar month.

"Service" means the Google Apps for Business service (also known as Google Apps Premier Edition), Google Apps for Government service, Google Apps for ISPs service (also known as Google Apps Partner Edition), or Google Apps for Education service (also known as Google Apps Education Edition) (as applicable) provided by Google to Customer under the Agreement.

"Service Credit" means the following:

<table>
<thead>
<tr>
<th>Monthly Uptime Percentage</th>
<th>Days of Service added to the end of the Service term, at no charge to Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 59.9% - ≥ 99.0%</td>
<td>3</td>
</tr>
<tr>
<td>&lt; 99.0% - ≥ 95.0%</td>
<td>7</td>
</tr>
<tr>
<td>&lt; 95.0%</td>
<td>15</td>
</tr>
</tbody>
</table>

Customer Must Request Service Credit. In order to receive any of the Service Credits described above, Customer must notify Google within thirty days from the time Customer becomes eligible to receive a Service Credit. Failure to comply with this requirement will forfeit Customer’s right to receive a Service Credit.

Maximum Service Credit. The aggregate maximum number of Service Credits to be issued by Google to Customer for all Downtime that occurs in a single calendar month shall not exceed fifteen days of Service added to the end of Customer’s term for the Service. Service Credits may not be exchanged for, or converted to, monetary amounts.

Google Apps SLA Exclusions. The Google Apps SLA does not apply to any services that expressly exclude this Google Apps SLA (as stated in the documentation for each service) or any performance issues (i) caused by factors described in the “Force Majeure” section of the Agreement, or (ii) that resulted from Customer’s equipment or third party equipment, or both (not within the primary control of Google).
Security and privacy

Two of the most common topics of questions regarding Google in general, and Google Apps specifically, are security and privacy. We take both topics very seriously and truly believe that our offerings are a great option for customers on both fronts. Our business is built on our users' trust: trust in our ability to properly secure their data and our commitment to respect the privacy of the information they place in our systems by not giving that information to others or using it inappropriately.

In order to help answer some of the many questions we receive and to dispel some common misconceptions we encounter, we have created this FAQ and the corresponding Google Apps security whitepaper. We hope this helps to answer some of your questions about Google's position on these important issues!

If you need to report an abuse issue, learn more about reporting abuse issues to our team.

Privacy

- Who owns the data that organizations put into Google Apps?
- When can Google employees access my account?
- Who can gain access to my Google Apps administrative account?
- Who can gain access to my end-users' accounts?
- Does Google give third parties access to my organization's data?
- What kind of scanning/indexing of user data is done?
- How long do Google keep my organization's data?
- How does Google handle law enforcement requests?
- How does Google process objectionably illegal content?
- Is my organization compliant with the European Commission Directive on Data Protection if we use Google Apps?
- Where can I find more information on Google's Privacy Policy?

Security

- What does a Google Apps SAST/20 Type II audit mean to me?
- Where is my organization's data stored?
- Is my organization's data safe from your other customers when it is running on the same servers?
- An administrator/end-user deleted a number of email messages, how can I recover them?
- How do you protect your infrastructure against hackers and other threats?
- How do you prevent and resolve security flaws in your applications?
- How do you protect against machine failures or natural disaster?
- Is it safe for my organization to access Google Apps over the internet?
- I'm being asked to sign in at a different page. Why?
- How do you protect my organization against spam, viruses and phishing attacks?
- What is CAPTCHA?
- How do I prevent spammers from spoofing my domain name?
- How does Google respond to users in my domain who are sending spam?
- Can my organization use our own authentication system to provide user access to Google Apps?
- Does Google Apps offer SSL connectivity?
- What is FISMA?
SaaS Service Level Agreements

► Microsoft SaaS offerings
  ■ Office 365 – no default SLA
  ■ Microsoft Exchange Online
  ■ SharePoint Online
  ■ Office Communications Online
  ■ Common SLA
    ● Virus protection
IaaS Security

► Trusting the Virtual Machine Image

■ If using VM image from IaaS vendor, it should have the same level of security verification and hardening for hosts in the enterprise

■ Best alternative is to provide own image conforming to same security policies as internal trusted hosts or use virtual images from a trusted third party.
IaaS Security

- Hardening Hosts
  - All precautions used to harden hosts in the DMZ should be applied to VM images
  - Best practice is to build custom OS and app platform images with only capabilities necessary to support the application stack
IaaS Security

► Securing Inter-host Communication
  ■ Design in explicit controls to prevent disclosure of sensitive information between hosts

► Managing Application Keys
  ■ IaaS platforms use a “secret key” to identify a valid account
  ■ Normal enterprise standards and practices for handling key material will need some modification for application keys
IaaS Security

► Additional Requirements for Handling Sensitive Information

■ Apps on IaaS must ensure sensitive information does not leak during processing

■ All precautions for handling sensitive info for enterprise apps apply to IaaS hosted applications
IaaS Security

- Treat IaaS VM instances as a “weak instance” of normal enterprise systems
- Ensure strong OS-level firewall protections are in place
  - Bi-directional stateful firewall
IaaS Service Level Agreements

► Rackspace
  ■ Agrees to follow security procedures at least as stringent, in Rackspace’s reasonable judgment, as described at http://www.rackspace.com/information/legal/securitypractices.php
Security Practices

Physical Access
The Rackspace servers used to provide the Services will be located in a controlled access data center operated by Rackspace US, Inc. or a Rackspace affiliated company. Access to the datacenter will be restricted to Rackspace employees or its agents who need access for the purpose of providing the services. The data center will be staffed 24/7/365 and will be monitored by video surveillance. Entrance to the data center will be authorized by proximity-based access cards and biometric hand scanners or other approved security authentication methods.

Rackspace Personnel
• Screening. Rackspace will perform pre-employment background screening of its employees who have access to customers’ accounts.
• Access. Rackspace will restrict the use of administrative access codes for customer accounts to its employees and other agents who need the access codes for the purpose of providing the services. Rackspace personnel who use access codes shall be required to log on using an assigned user name and password.

Reports of and Response to Security Breach.
Rackspace will immediately report to you any unauthorized access or release of your information of which we become aware. Upon request, we will promptly provide to you all information and documentation that we have available to us in connection with any such event.

©2011 Rackspace US, Inc.
November 23, 2009 revision
IaaS Service Level Agreements

► Amazon.com

■ No mention of security in SLA
■ Overview of security in “Amazon Web Services: Overview of Security Processes”
  ● Implicit but no explicit contract
  ● SAS70 Type II audit procedures in place

Amazon Web Services: Overview of Security Processes

August 2010

(Please consult http://aws.amazon.com/security for the latest version of this paper)
Negotiate with Public Cloud Vendors

► Vetting of vendor employees
► Data ownership and exit rights
► Isolation of tenant applications
► Data encryption and segregation
► Tracking and reporting service effectiveness

From NIST Draft Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing by Wayne Jansen and Timothy Grance
Negotiate with Public Cloud Vendors

► Compliance with laws and regulations
► Use of validated products meeting federal or national standards

From NIST Draft Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing by Wayne Jansen and Timothy Grance
Essential Reading…

► https://cloudsecurityalliance.org/csaguide.pdf
Ray Trygstad
► trygstad@iit.edu
► 630.447.9009
► http://trygstad.rice.iit.edu/
The End

► Questions?