SLA – Service Security

S. Srinivasan
Professor of Information Systems
Texas Southern University

Outline

- State of SLA in Cloud Computing
- Preferred Security Aspects in SLA
- Sample SLA segments on security
- SLA – service provider perspective
- FedRAMP expectations
- Resources to monitor SLA

State of SLA in Cloud Computing

- Cloud Service Providers (CSPs) serve thousands of customers
- CSPs prefer a click through SLA
- Several CSPs use third parties for their service
- At the CSP end mergers and acquisitions occur
- At the customer end Cloud Service Brokers enter the picture

State of SLA in Cloud Computing

- SLAs help with conflict resolution before dispute arises
- SLAs are more mature for IaaS
- Many CSPs offering SaaS and PaaS don't even offer an SLA (e.g., Salesforce)
- Service providers should monitor and gather relevant service metrics

State of SLA in Cloud Computing

- Often, gap exists between CSP metrics and customer expectations for high-level functionality (e.g., backup, software patches)
- Several CSPs offer cloud service using third party IaaS public cloud (e.g., VMware)
- Today's cloud SLAs favor CSP
- Large enterprises are able to negotiate better SLAs while SMBs get only standard SLA

Preferred Security Aspects in SLA

- Seek greater transparency in CSP security practices
- Ability to conduct audit of provider security features using third parties
- Have knowledge of privileged users with access to customer data and processes on the cloud
- In public cloud, protection for customer systems in multi-tenant environments

Preferred Security Aspects in SLA

- CSP should be able to document security controls that are risk based
- CSP should be able to document compliance with security standards such as ISO 27001
- SLA should permit customer to publicly announce any missed service levels
- CSP should carry compliance certifications that help customer meet their requirements

Preferred Security Aspects in SLA

- CSP should document their security policies and practices related to encryption, firewalls and physical security
- Customer expectation on data retention and protection
- Non-proprietary data storage format to facilitate changing CSP

Preferred Security Aspects in SLA

- Administrators with privileged access may create or delete files but do not have right to view content
- Salesforce uses this approach in its service level assurance
- People with physical access to servers cannot identify data storage for a particular customer
- Rackspace uses this approach in its practice

Sample SLA Segment on Availability

Google Apps SLA extract

- 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.

SLA Constraints for Customer

- Customer responsibility mentioned in the SLA requires customer to note the violation and notify the provider within 30 days
- When third parties are involved in service provisioning this becomes difficult
- Remedy is service credit of 3, 7 or at most 15 days
- No mention of any reputational penalty recourse for customer

Sample SLA Segment on Availability

Amazon Web Services SLA extract

- AWS will use commercially reasonable efforts to make Amazon EC2 and Amazon EBS each available with a Monthly Uptime Percentage (defined below) of at least 99.95%, in each case during any monthly billing cycle (the “Service Commitment”).

SLA Constraints for Customer

- Going through the fine details of the rest of the SLA, failure in EBS will not impact EC2's commitment
- Customers are expected to sign up for two Availability Zones in order to enforce SLA
- System downtime calculation is per month for SLA purposes, not per day
- Routine maintenance downtimes are excluded

Sample SLA Segment on Data Storage Location

Extract from Google contract with City of Los Angeles

- Google agrees to store and process Customer's email and Google Message Discovery (GMD) data only in the continental United States. As soon as it shall become commercially feasible, Google shall store and process all other Customer Data, from any other Google Apps applications, only in the continental United States

SLA Constraints for Customer

- SLA shows some data may reside outside US, especially backup data
- Gives customers opportunity to encrypt such data
- All states in US (except Alabama, New Mexico and South Dakota) have laws dealing with data protection and data breach
- Customer, and not the CSP, is responsible for compliance with such laws

Sample SLA Segment on Data Ownership

Extract from Amazon contract

- Other than the rights and interests expressly set forth in this Agreement, and excluding Amazon Properties and works derived from Amazon Properties, you reserve all right, title and interest (including all intellectual property and proprietary rights) in and to Your Content.

SLA Constraints for Customer

- Large CSPs are realizing the importance of clarifying data ownership and including text pertaining to this aspect in SLAs
- It is important to add to this SLA that any information derived from processing such data in CSP's systems are also owned by the customer
- If CSP has compliance certifications for HIPAA, GLBA, SOX, FERPA, FISMA, PCI-DSS, SSAE-16 it would help the customer meet their obligations

Sample SLA Segment on Audit

Extract from CSA Security Guide and Internet2 Wiki Information Security Guide

- Regular and independent audits of critical systems and controls, including the accompanying audit trail and documentation will support improvements in efficiency and reliability.
- Vendor agrees to have an independent third party security audit performed at least once a year.

SLA Constraints for Customer

- Customer should require in SLA that they have the right to verify how the CSP is addressing the results of the audit
- Cost may be an issue for some CSPs for audits. So, a contractual cap on cost may be included in the SLA.

SLA – Service Provider Perspective

- CSPs deal with several thousand customers
- CSPs use third party services for specific areas
- CSPs offer many SaaS applications
- CSP services are distributed
- CSP makes available standard SLA for click-through acceptance
- Any modification to standard SLA will require CSP to have a separate office monitor all SLA related inquiries

FedRAMP Expectations

- FedRAMP Security controls baseline provides minimum set of controls for CSPs to implement
- CSPs must use independent assessors to test the effectiveness of the controls
- Two of the important controls are:
  - Separation of duties
  - Least privilege

FedRAMP Expectations

- CSP must identify all inherited controls
- In order for a CSP to be certified it must meet FedRAMP guidelines

Resources to Monitor SLA

- From customer perspective, they need enough information before developing SLA
- Cloud Security Alliance (CSA) provides several tools such as:
  - Cloud Controls Matrix
  - STAR (Security, Trust, and Assurance Registry)
  - SysTrust Report (includes Veracode security rigor compliance audit)

Resources to Monitor SLA

- Cloud Standards Customer Council has developed a Practical Guide for Cloud SLA
- Rackspace acquired Cloudkick so that its customers can continuously monitor their various cloud services
- All major CSPs such as AWS, Google, Microsoft, Salesforce provide real time status of their cloud service availability

References

- http://cloudsecurityalliance.org
- http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf
- S. Srinivasan, Cloud Computing Basics, Springer, NY, 2014, ISBN: 978-1-4614-7698-6
- S. Bradshaw et al, Contracts for Clouds, Legal Studies Research Paper 63/2010

References

- http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
- http://cloud.cio.gov/fedramp
- http://www.nist.gov/itl/csd/cloud-061113.cfm
- T. Trappler, “If it’s in the cloud, get it on paper: Cloud computing contract issues”, Educause Review Online, June 2010
- S. Bradshaw et al, “Contracts for Clouds”, Queen Mary U of London, Research Paper 63/2010

Thank You

srinis@tsu.edu