Cloud Security Framework (CSF): Gap Analysis & Roadmap

Contributors: Suren Karavettill, Bhumip Khasnabish
Ning So, Gene Golovinsky, Meng Yu & Wei Yinxing

Please send comments & suggestions to
Suren Karavettill (surenck@gmail.com)
April 15th, 2011
IETF IPR and Copyright Statements

• This document (future Internet-Draft) is being prepared for IETF in full conformance with the provisions of BCP 78 and BCP 79

• Copyright Notice
  – Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

• This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info)

•
List of Acronyms

• IETF – Internet Engineering Task Force
• CSF - Cloud Security Framework
• GRC – Governance, Risk & Compliance
• CSA – Cloud Security Alliance
• SDO – Standards Development Organizations
• OWASP – Open Web Application Security Project
• XSS – Cross-Site Scripting
• CSRF – Cross-Site Request Forgery
• PCI - Payment Card Industry
• DSS - Data Security Standards
• SOX – Sarbanes Oxley
Outline

• Purpose
• Background on Cloud from Cloud Security Alliance
  – Essential Characteristics of Cloud
  – Cloud model to security control & compliance model
  – Cloud Service security risks – consumer vs provider
• Top Security Risks
• Reasons for Standardizations in Cloud
• Gap Analysis & Roadmap
• CSP Services Requirements Categories
• Typical Web Application Architecture & Content Types
• General Application Security Requirements
  – Security Attributes & Methods
• Functional Apps & Systems
  – Core Services Requirements
  – Administration & Management Requirements
• Non Functional – Apps & Systems
  – Security, Business Continuity, etc
• Governance, Risk & Compliance Requirements
• Facilities Management Services Requirements
• Gap Analysis - Cloud Protocol Framework
• Other Standards Development Organizations (SDO)
• Roadmap – Next steps
Purpose

The purpose of the Cloud Security Framework: Gap Analysis & Roadmap is to come up with requirements for:

– Protocol & Profiles
– Interfaces
– API’s

That helps develop & provide secure applications for users and reduce human interventions in provisioning & management of resources for these cloud applications & services.

04/15/2011
Essential Characteristics of Cloud

- On-demand self-service
- Broad network access
- Resource pooling using Multi-Tenant model
- Rapid elasticity
- Measured service

*Courtesy of Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*
Cloud Model to Security Control & Compliance Model

Diagram is courtesy of Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
Cloud Services Security Risks – Consumer vs Provider

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

Figure 7 - How Security Gets Integrated

Portion of diagram is courtesy of Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

04/15/2011
## Top Security Risks

<table>
<thead>
<tr>
<th>Top Threats to Cloud Computing, version 1.0</th>
<th>The OWASP Top 10 Web Application Security Risks for 2010 are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>identified by CSA are:</td>
<td></td>
</tr>
<tr>
<td>• Abuse and Nefarious Use of Cloud Computing</td>
<td>• Injection</td>
</tr>
<tr>
<td>• Insecure Application Programming Interfaces</td>
<td>• Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>• Malicious Insiders</td>
<td>• Broken Authentication and Session Management</td>
</tr>
<tr>
<td>• Shared Technology Vulnerabilities</td>
<td>• Insecure Direct Object References</td>
</tr>
<tr>
<td>• Data Loss/Leakage</td>
<td>• Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>• Account, Service &amp; Traffic Hijacking</td>
<td>• Security Mis-configuration</td>
</tr>
<tr>
<td>• Unknown Risk Profile</td>
<td>• Insecure Cryptographic Storage</td>
</tr>
<tr>
<td></td>
<td>• Failure to Restrict URL Access</td>
</tr>
<tr>
<td></td>
<td>• Insufficient Transport Layer Protection</td>
</tr>
<tr>
<td></td>
<td>• Un-validated Redirects and Forwards</td>
</tr>
</tbody>
</table>
Reasons for Standardizations in Cloud Security

- Ease of Integration
- Portability
- Transparency
- Inter-operability
- Reuse
- Security
- Others?
CSP Services Requirements

Categories

• General Applications Security
• Functional - Apps & Systems
  – Core Services API
  – Administration & Management API (incl. Non Functional for systems)
    • Resources Allocation, Locking, Control & Management
• Non Functional – Apps & Systems
  – Security – anti-virus, LDAP
  – Business Continuity & Disaster Recovery Planning
• Governance, Risk & Compliance (GRC)
  – Governance, Risk Assessment & Mitigation, Compliance
• Facilities Management Services
  – Personnel, premises monitoring, etc

04/15/2011
Typical Internet Application Architecture

Application Security

Network Security

Systems Security

Data Security

Physical Security

Client Attributes

Network Attributes

Host Attributes

Information (Data) Attributes

Facility (Physical) Attributes

04/15/2011
Cloud Content Data Types

Live
• Web Application Form Data (Structured text/html)
• Image
• Voice
• Video
• Attachments (unstructured/MIME data types)
• Unstructured data

Archive
• Structured Data (Database, etc)
• Files
  ▪ Data – DOC, PDF, Excel, etc
  ▪ Image - JPEG, GIF, PNG, etc
  ▪ Voice archive – MP-3, etc
  ▪ Video Archive – MPEG-4, MPEG-2, MJPEG, AVCHD, etc
• Unstructured data

Note: Assuming data security as part of application security for this discussion purposes
General Application Security Requirements

• Authentication, Authorization & Auditing (AAA)
  – Runtime user authentication & session management
  – Authorized access to data and resources
  – Track access and usage of services, data and other resources (auditing & logging)
  – Secure token identifiers for applications, instances of systems (servers), device types (clients), request/response (pages), etc

• Data Validation
  – Sanitized data (user or systems) input into applications (from Browsers, CLI, Web Services, etc to avoid injection into OS, SQL, LDAP, etc).
  – Validated and appropriately escaped data output to the clients (browser, CLI, etc)
  – Checking length of data to avoid overflows.
  – Securing the persistent data/information

• Data Security
  – Appropriate encryption of data.
  – Data confidentiality
  – Multi-tenant isolation through proper configuration of virtualization & other mechanisms?
# General Application Security

## Attributes & Methods

### Client Attributes
- URL
- Session Id
- Page Id
- User Identity
- Client Type Id
- Cookie Enabled
- HttpOnly, Secure Flag
- Query parameters
- **Consumer Id & Location Id**
- Method Id

### Host Attributes
- Protocol attributes – referrer, etc
- Hostname (virtual or hard) & port
- Context root
- Session Context
- Resource Id
- Page Context
- Cluster, Load Balanced, Failover & DR
- **Provider Id & Resource Location Id**
- Server Configurations (Timeouts)

### Data Attributes
- Encrypted or Not
- Location
- Sanitized or Not
- Page Context
- LDAP/AD config for multi-tenancy

### Additional Attributes
- Secure Channel
- DMZ or Core
- Bandwidth Available
- Connection Type
- Route
- PKI Certificates
- LDAP, RADIUS, Kerberos

### Facility Attributes
- Personnel Access Control
- Data center Servers RFIDs
- Data center room cameras
- Time of Day rules
- Access Controls
- VLAN for multi-tenancy

### Identity Management
- Multi-factor, Single-Sign on Federation, Authentication
- Authorization
- Auditing

### I/O Data Validation
- Input Sanitization for SQL, LDAP, Header Injection
- Encoding of output of javascript or HTML data
- Input Length Check to avoid overflows

### Safe Coding Practices
- Encoding, Logging, etc
- Database configuration for multi-tenancy
- Time of Day rules

### Safe Install & Config Practices
- LDAP/AD config for multi-tenancy
- Database configuration for multi-tenancy

### Facility Management
- Time of Day rules
- Access Controls

---

**Note:** Do not assume all cloud resources are virtualized to support multi-tenancy

04/15/2011
Functional Apps & Systems – Core Services Requirements

• Identity & Access Management (IAM)
• Virtual Desktop Infrastructure (VDI)
• Video Streaming
• Directory Services (DS)
• Database Management Systems (DBMS)
• Logging
Functional Apps & Systems - Admin & Management Requirements

- Systems Resource Allocation Services
  - System, Storage (private/public, or varying provider), etc for multi tenancy
- Systems Resource Mobility Resources Allocation Services
  - Availability, etc
- Systems Resource Configuration Services
  - Security
    - Single Sign On, Multi-Factor Authentication, Access Control, Encryption
- Named Services
- Systems Management Services
  - Asset tracking, Status & Statistics of various Services
- Systems Interoperability
Non-Functional Apps & Systems Requirements

• Systems Security
  – Anti-virus
  – LDAP
  – Kerberos/RADIUS

• Systems Failover & Performance Services
  – With different physical infrastructure providers
  – Load Balancing, Backup & Recovery, Business Continuity
Governance, Risk & Compliance (GRC) Requirements

- Payment Card Industry (PCI) Data Security Standards (DSS) – PCI DSS
- Health Insurance Portability & Accountability Act (HIPAA)
- Sarbanes Oxley Act (SOX)
- Personal Identification Information (PII) - Massachusetts Regulation 201 CMR 17.00
- SAS 70 Auditing Standards
- NERC CIP Standards
- Gramm Leach Bliley Act (GLBA) for Financial Services

GRC applies to CSP and their clients
Facilities Management Services
Requirements

• Resources Tracking (assets scan)
• Manage personnel access to assets/resources by business hours, location, etc.
• Track assets/resources.
Gap Analysis – Cloud Protocol Framework

• Few factors influencing the Cloud Protocol Framework:
  – On-demand self service
  – Client Type (PC, TV, Smartphone, Auto)
  – User & Session (identity)
  – Data Type (video, voice, image, data [e.g. HTTP POST])
  – Channel (bandwidth, availability, mobility, security)
  – Host/Service (resource virtualization, availability, location)
Other Standards Development Organizations (SDO)

- Cloud Security Alliance (CSA)
- VMWare’s DMTF – vCloud API & Open Virtualization Format (OVF)
- TM Forum’s Cloud Program
- Open Cloud Computing Interface Working Group
- Amazon EC2 API
- Sun’s Open Cloud API
- Rackspace API
- GoGrid API
Roadmap – Next Steps

• Thoughts & Ideas for next steps