Cloud Security Framework (CSF): Gap Analysis & Roadmap

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

Please send comments & suggestions to Suren Karavettil (surenck@gmail.com)

February 11th, 2010
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

• Network (Non-Functional) Requirements

• Governance, Risk & Compliance Requirements

• Facilities Management Services Requirements

• Other Standards Development Organizations (SDO)

• Gap Analysis & 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.

02/11/2011
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

02/11/2011
Cloud Services Security Risks – Consumer vs Provider

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

02/11/2011
## Top Security Risks

<table>
<thead>
<tr>
<th>Top Threats to Cloud Computing, version 1.0 identified by CSA are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Abuse and Nefarious Use of Cloud Computing</td>
</tr>
<tr>
<td>• Insecure Application Programming Interfaces</td>
</tr>
<tr>
<td>• Malicious Insiders</td>
</tr>
<tr>
<td>• Shared Technology Vulnerabilities</td>
</tr>
<tr>
<td>• Data Loss/Leakage</td>
</tr>
<tr>
<td>• Account, Service &amp; Traffic Hijacking</td>
</tr>
<tr>
<td>• Unknown Risk Profile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The OWASP Top 10 Web Application Security Risks for 2010 are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Injection</td>
</tr>
<tr>
<td>• Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>• Broken Authentication and Session Management</td>
</tr>
<tr>
<td>• Insecure Direct Object References</td>
</tr>
<tr>
<td>• Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>• Security Mis-configuration</td>
</tr>
<tr>
<td>• Insecure Cryptographic Storage</td>
</tr>
<tr>
<td>• Failure to Restrict URL Access</td>
</tr>
<tr>
<td>• Insufficient Transport Layer Protection</td>
</tr>
<tr>
<td>• Un-validated Redirects and Forwards</td>
</tr>
</tbody>
</table>
Reasons for Standardizations in Cloud

• Ease of Integration
• Portability
• Transparency
• Inter-operability
• Reuse
• Security
• Others ?
Gap Analysis & Roadmap

General Application Services

Functional Apps Core Services

Functional Admin & Management Services

Non-Functional Virtualized & Hardware Systems Resources

Facilities Management

Non-Functional Network Resources

Governance, Risk & Compliance (GRC)

Network/Transport

client/cloud(s) communication

client/cloud(s) communication

Clients (PC, TV, Mobile)
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 - Network
• Governance, Risk & Compliance (GRC)
  – Governance, Risk Assessment & Mitigation, Compliance
• Facilities Management Services
  – Personnel, premises monitoring, etc
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 – PDF, DOC, 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.
  – Multi-tenant isolation through proper configuration of virtualization & other mechanisms?

• Secure Channels
  – Use of authenticated and encrypted transport layer for apps network traffic
# General Application Security Attributes & Methods

<table>
<thead>
<tr>
<th><strong>Client Attributes</strong></th>
<th><strong>Host Attributes</strong></th>
<th><strong>Data Attributes</strong></th>
<th><strong>Network Channel Attributes</strong></th>
<th><strong>Facility Attributes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>Protocol attributes – referrer, etc</td>
<td>Encrypted or Not</td>
<td>Secure Channel</td>
<td>Personnel Access Control</td>
</tr>
<tr>
<td><strong>Session Id</strong></td>
<td>Hostname (virtual or hard) &amp; port</td>
<td>Location</td>
<td>DMZ or Core</td>
<td>Data center Servers RFIDs</td>
</tr>
<tr>
<td><strong>Page Id</strong></td>
<td>Context root</td>
<td>Sanitized or Not</td>
<td>Bandwidth Available</td>
<td>Data center room cameras</td>
</tr>
<tr>
<td><strong>User Identity</strong></td>
<td>Application Context</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cookie Enabled</strong></td>
<td>Session Context</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Http Only &amp; Secure Flag</strong></td>
<td>Page Context</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Query parameters</strong></td>
<td>Cluster, Load Balanced, Failover &amp; DR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Consumer Id &amp; Location Id</strong></td>
<td>Provider Id &amp; Resource Location Id</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Method Id</strong></td>
<td>Server Configurations (Timeouts)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Identity Management

<table>
<thead>
<tr>
<th><strong>I/O Data Validation</strong></th>
<th><strong>Safe Coding Practices</strong></th>
<th><strong>Safe Install &amp; Config Practices</strong></th>
<th><strong>Facility Management</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor, Single-Sign on Federation, Authentication</td>
<td>Input Sanitization for SQL, LDAP, Header Injection</td>
<td>Encoding, Logging, etc</td>
<td>LDAP/AD config for multi-tenancy</td>
</tr>
<tr>
<td>Authorization</td>
<td>Encoding of output of javascript or HTML data</td>
<td></td>
<td>Database configuration for multi-tenancy</td>
</tr>
<tr>
<td>Auditing</td>
<td>Input Length Check to avoid overflows</td>
<td></td>
<td>VLAN for multi-tenancy</td>
</tr>
</tbody>
</table>

Note: Do not assume all cloud resources are virtualized to support multi-tenancy
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 Failover & Performance Services
  – With different physical infrastructure providers
  – Load Balancing, Backup & Recovery, Business Continuity

• Systems Interoperability
Network (Non-Functional) Requirements

• Network Connectivity Resources (how to handle multi-tenancy)
  – Addressing Services
  – Allocation Services
    • Network resource like Bandwidth, Routing, VLAN, etc for predictable performance
  – Availability

• Network Management Services
  – Virtual network management

• Network Security Services
  – VPN, virtual extension to private cloud (VEPC)

• Network Failover & Performance Resources Allocation Services
  – With different physical infrastructure providers - Load Balancing, Backup & Recovery, Business Continuity

• Network Resource Mobility Resources Allocation Services
  – Virtual resource management

• Interoperability across CSP’s
  – Import/export
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.
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
Gap Analysis

• Thoughts & Ideas for next steps

Generic Header (protocol+)
Functional Header
Non Functional Header
GRC Rules Header
Payload
Roadmap – Next Steps

• Thoughts & Ideas for next steps