Cloud Security Framework (CSF): Gap Analysis & Roadmap

Contributors: Suren Karavettil, Bhumip Khasnabish
Ning So, Gene Golovinsky, and Meng Yu

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

January 07th, 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
  -
-
-

Outline

- Purpose
- Cloud Reference Framework Diagram
- OSI Layers
- Cloud Service Components
- Cloud Service Provider (CSP) Resources
- Content Data Types
- Cloud Service Usage Actors
- CSP Services Requirements Categories
- Administration & Management Requirements
- Application Services Operations Requirements
- Governance, Risk & Compliance Requirements
- Infrastructure Services Requirements
- Gap Analysis
- Other Standards Development Organizations (SDO)
- Roadmap – Next steps

Purpose

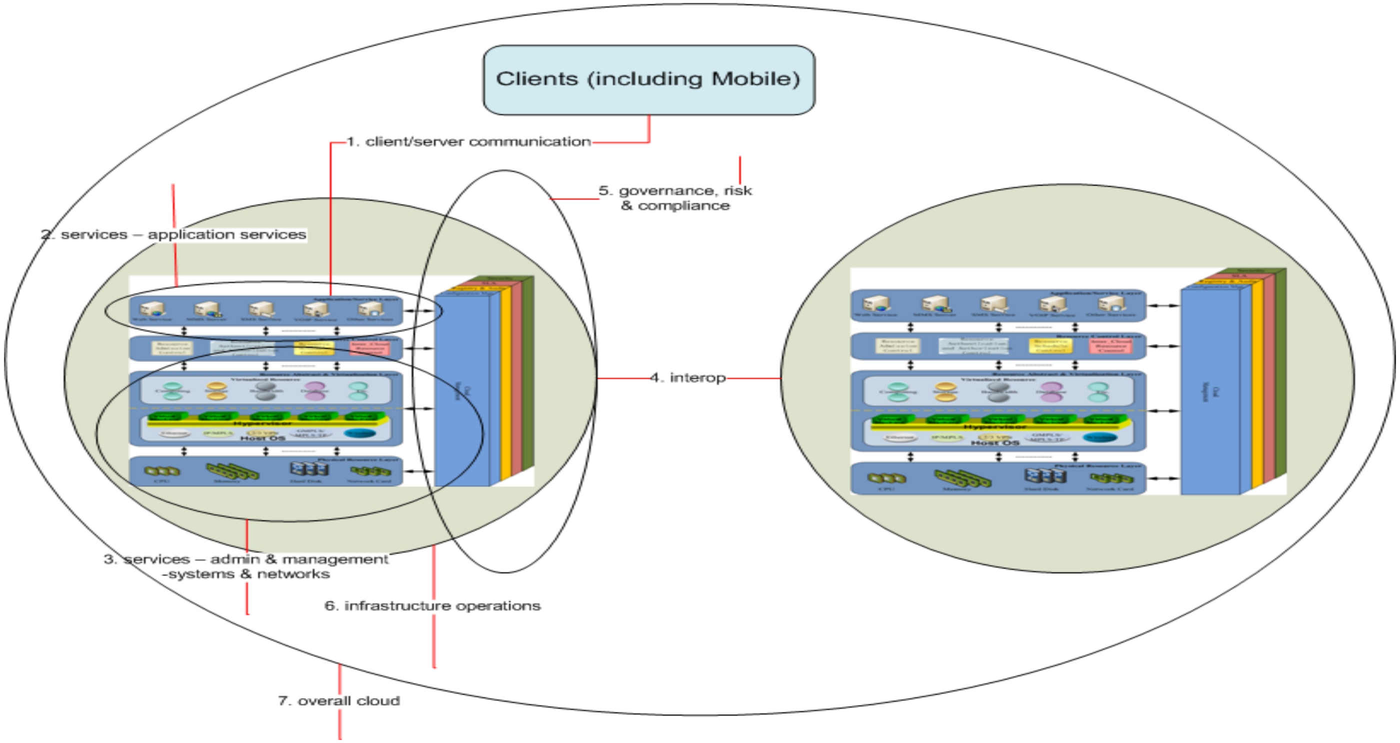
The purpose of the Cloud Security Framework: Gap Analysis & Roadmap is to come up with requirements for:

- 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.

Gap Analysis & Roadmap

- Focus areas



Clients (including Mobile)

1. client/server communication

2. services – application services

3. services – admin & management -systems & networks

4. interop

5. governance, risk & compliance

6. infrastructure operations

7. overall cloud

OSI Layers – Relevance to Cloud

- Layers impacted by Cloud based services model
  - Application Layer – Processes & Apps - HTTP, SMTP, VoIP, IPTV, Telnet, FTP, NFS, NIS
  - Presentation Layer – Data Representation & Encryption - SSL/TLS, VPN
  - Session Layer – Inter-host communication - P2P, SIP
  - Data link Layer - Ethernet WAN
- Layers minimally impacted
  - Transport Layer – TCP, UDP
  - Network Layer – IP + ARP/RARP/ICMP
  - Physical Layer – Media - Fiber Optics

Cloud Service Components

- Resources – Assets & Personnel
- Application Services
- Users & Access Control
- Inter-operability (across CSPs)
- Infrastructure Management & Operational Services

These components mentioned above can be classified based on:

- Cloud Client Side (thick client, mobile), Cloud Server (Hosting) Side and Cloud Network Infrastructure
- CloudApps and CloudOps
- Category of Cloud Services provided

Cloud Service Provider (CSP) Resources

Assets

- Hard Assets Categories
  - Computer Assets – Processors, Memory, etc
  - Storage Assets – Disks, etc
  - Network Elements - Routers, Switches, Load Balancers, Firewalls Appliances, cell towers, etc
  - Mobile Devices – smart phones, pads, etc
  - Device Assets – Cameras, Access Card Readers, RFID Tags, etc
  - Others
- Soft Assets Categories
  - Software(s) and their licenses
    - **OS, High Level Language(s) IDE & Runtime**
    - **Server side** - Application Servers, Databases
    - **Mobile & Client side** software
    - **Network** - Firewalls, VPN, etc
- Virtual Assets
  - Database Connection Pools
  - Clusters, Load Balancers
  - Bandwidth, Frequency, VLANs

Personnel

- Users
- Administrators
- Management
- Security Guards
- Maintenance Employees
- Their vendors, etc

Cloud Content Data (MIME) 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

Cloud Service Usage Actors

- Public/Enterprise
  - Cloud Application Services Users
- Cloud Application Services Providers (CASP) Development Organization (Enterprise)
  - Development Users
  - System Administration Users
  - Management Users – CSO, CIO, Engineering
- CASP Enterprise & Cloud Service Provider(s) (CSP)
  - System Administration Users
  - Network Administration Users
  - Management Users – CXO, etc
- Others
  - Peer CSP, Regulators & Compliance Auditors
  - Investigations & Forensics

CSP Services Requirements Categories

- Administration & Management (A&M)
  - Allocation, Status, Statistics
- Application Services Operations (ASO)
- Governance, Risk & Compliance (GRC)
  - Governance, Risk Assessment & Mitigation, Compliance
- Infrastructure Management & Operations Services (IMOS)

Administration & Management (A&M) Requirements

- Computer Resource Allocation Services
  - System, Storage, etc
- Connectivity Resource Allocation Services
  - Routing, VLAN, etc
- Failover & Performance Resources Allocation Services
  - Load Balancing, etc
- Service Mobility Resources Allocation Services
  - Availability, etc
- Security Configuration Services
  - Identity Management, Access Control, Transport Layer, Encryption, etc
- Management Services
  - Asset tracking, Status & Statistics of various Services

Application & Services Operations (ASO) Requirements

- Runtime user authentication & session management
- Authorized access to data and resources
- Secure token identifiers for applications, instances of systems (servers), device types (clients), request/response (pages), etc
- 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)
- Securing the persistent data/ information
- Use of authenticated and encrypted transport layer for apps network traffic
- Inter-operability across CSP's
  - Applications usage of services across CSP's.
  - Seamless secure configuration of applications.
  - Secure forwards and redirects of requests.
- Multi-tenant isolation
- Track access and usage of services, data and other resources (auditing & logging)

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

Infrastructure Management & Operations Services (IMOS) Requirements

- Interoperability across CSP’s (import/export)
- Backup & Recovery of information
- Business continuity planning
- Resources Tracking (assets scan)
- Manage personnel access to assets/resources by business hours, location, etc.
- Track assets/resources.

Gap Analysis

- Work in progress

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