Cloud Security and The Open Group

A Birds of A Feather Session
Topics

- Introduction and objectives
- Review status of “Sec-Cloud-SOA” project
- Other Open Group Cloud Security initiatives
- What do you think is important and valuable?
- What can you contribute?
- Where shall we go now?
Security for the Cloud and SOA Project

Objectives:

- Develop a Best Practice Guide to implementing effective security in SOA environments;
- Understand Security, Privacy, Services and authorization in the hybrid (enterprise & public) cloud arena;
- Describe the application of SOA security standards to provide a secure Cloud foundation; and
- Understand Cloud security and Cloud security architecture

Leaders:

- Omkhar Arasaratnam, IBM  
  omkhar@ca.ibm.com  
- Stuart Boardman, CGI  
  stuart.boardman@cgi.com  
  (and World Cup finalists!)
Planned outputs of the Cloud/SOA Security Project

- Ultimate output: A Cloud/SOA Security Reference Architecture which Open Group will standardize
  - Informative, not normative standard (as of now)
  - Aligned to the SOA & Cloud Reference Architectures
Draft ToC for Cloud/SOA Security

- Challenges in Cloud/SOA Security
- Security Architecture Principles for Cloud & SOA
- Terminology
- Security Requirements
  - Use Cases
  - NFR support, i.e. limitations & constraints around non-functional issues such as performance & scalability
  - Policy & Compliance issues
- Cloud Security Reference Model
- Architecture Building Blocks for Cloud Security
- Security Policy Handling
- Gap Analysis between the existing Enterprise Cloud Security Architecture and Cloud/SOA security Architecture
  - Note that this assumes an enterprise security architecture. For a public or hybrid cloud, we should think about differences
- Cloud/SOA Security Scenarios & Patterns
- Security Monitoring & Logging for Cloud & SOA security
- Candidate Architectural Decisions
- Issues in mapping ABBs to Technologies for Realization
What We’ve Produced

- Security Building Blocks
- Security Principles
- Whitepapers
- Framework for Architecture Decisions (and the “rodeo”)
Cloud / SOA Security Architecture

Building Blocks

Command and control management

Security policy management

Risk and compliance assessment

Knowledge

Entity, access and entitlement management

Data and information protection management

Software, system and service assurance

IT Service management

Threat and vulnerability management

Physical asset management

Policies

Delegation of authority

Service directives and objectives

Compliance metrics

Events and artifacts

Risk exposure

Compliance reports

IBM Cloud Computing Management Platform donation
The Whitepapers

- An Architectural View Of Security For Cloud
- Security Principles for Cloud and SOA
- Data and Information Protection (WIP)