Infosys®

Win in the flat world

Cloud security desiderata and user centric identity management for cloud systems

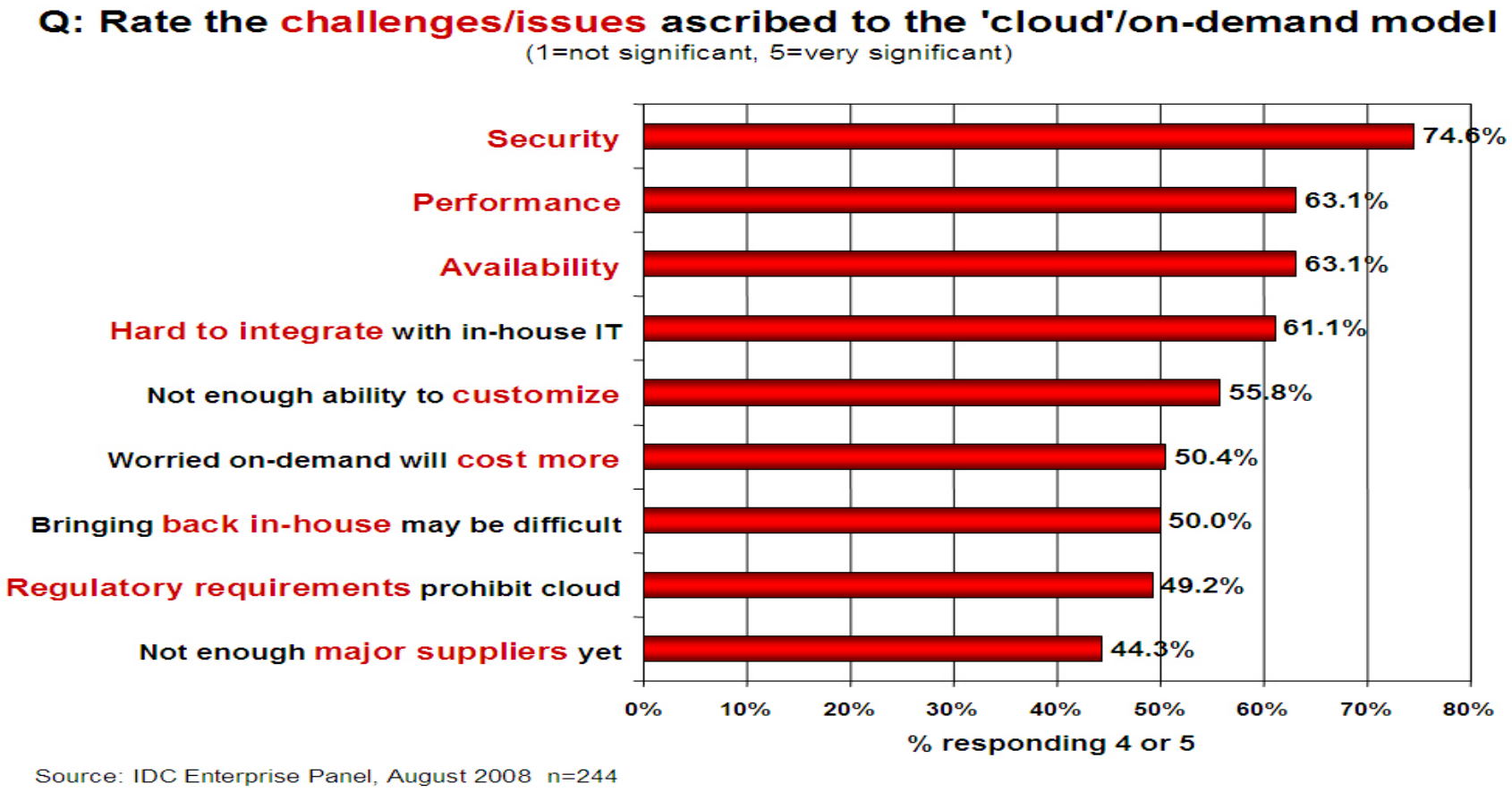
Srinivas Padmanabhuni, Ph.D.
Principal Research Scientist
Infosys Labs
Bangalore, India.
srinivas_p@infosys.com

14th May 2011
Cloud Developer Conference, Bangalore.

Agenda

- Cloud overview and Concerns
- How Cloud is good for Security
- Security Concerns
- Key Issues
- Insecure SOA
  - SOA Security Threat Profile
  - Solutions for SOA Security
- REST Security
  - Key Issues
  - Solutions
- User Centric Identity Management for Cloud
  - OpenId
- Conclusions

Security is the #1 Issue on Cloud Adopters Mind



Source: IDC Enterprise Panel, August 2008 n=244

Cloud need not be bad from a security perspective?

- Security measures are cheaper when implemented on a large scale.
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management (e.g. default virtual machine images and software updates can be pre-hardened and updated with the latest patches and security settings)
- Cloud catalyzes Redundancy / Disaster Recovery
- Managed offering of security as a service enables experts with deep pockets to invest in security services

Are Cloud Security Concerns all new?

- Likewise, SOA is a key enabler for modularization of Software to be provisioned as a cloud, so the SOA threat profile carries over
- All Cloud Interfaces to be Web Based, the Web threat Profile carries over, primarily REST based interfaces
- Clouds' inherent reliance on external environment for execution, coupled with elastic nature brings a host of new problems..
- **Before that, let us examine what other paradigms carry over to cloud..**

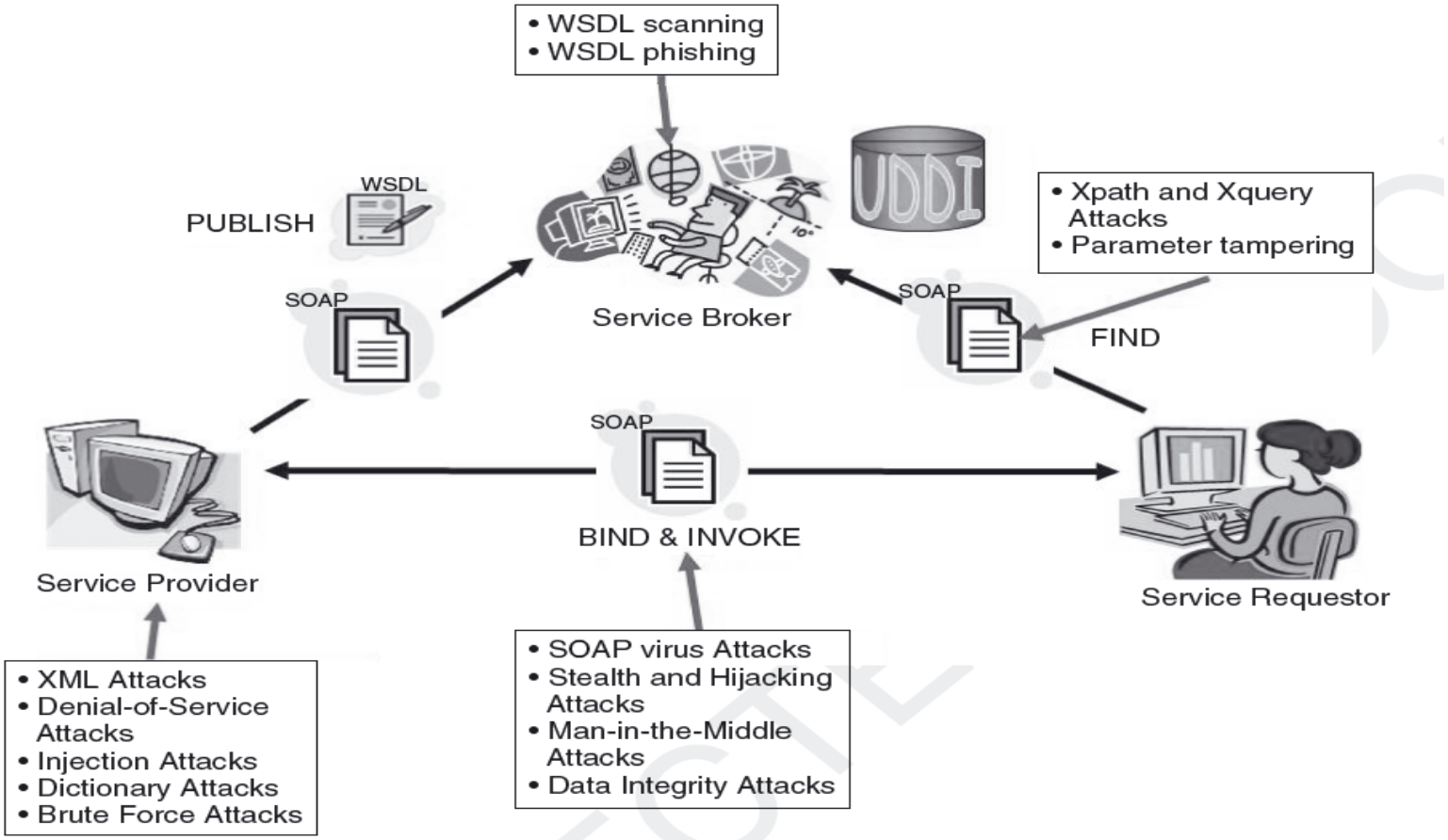
Evolving Cloud Threat Profile (Source: CSA)

- Insecure Service Oriented Architecture
- REST based
  - Unprotected APIs
  - Web application attacks
- Hypervisor Attacks
- L1/L2 Attacks (Cache Scraping)
- Trojaned AMI Images

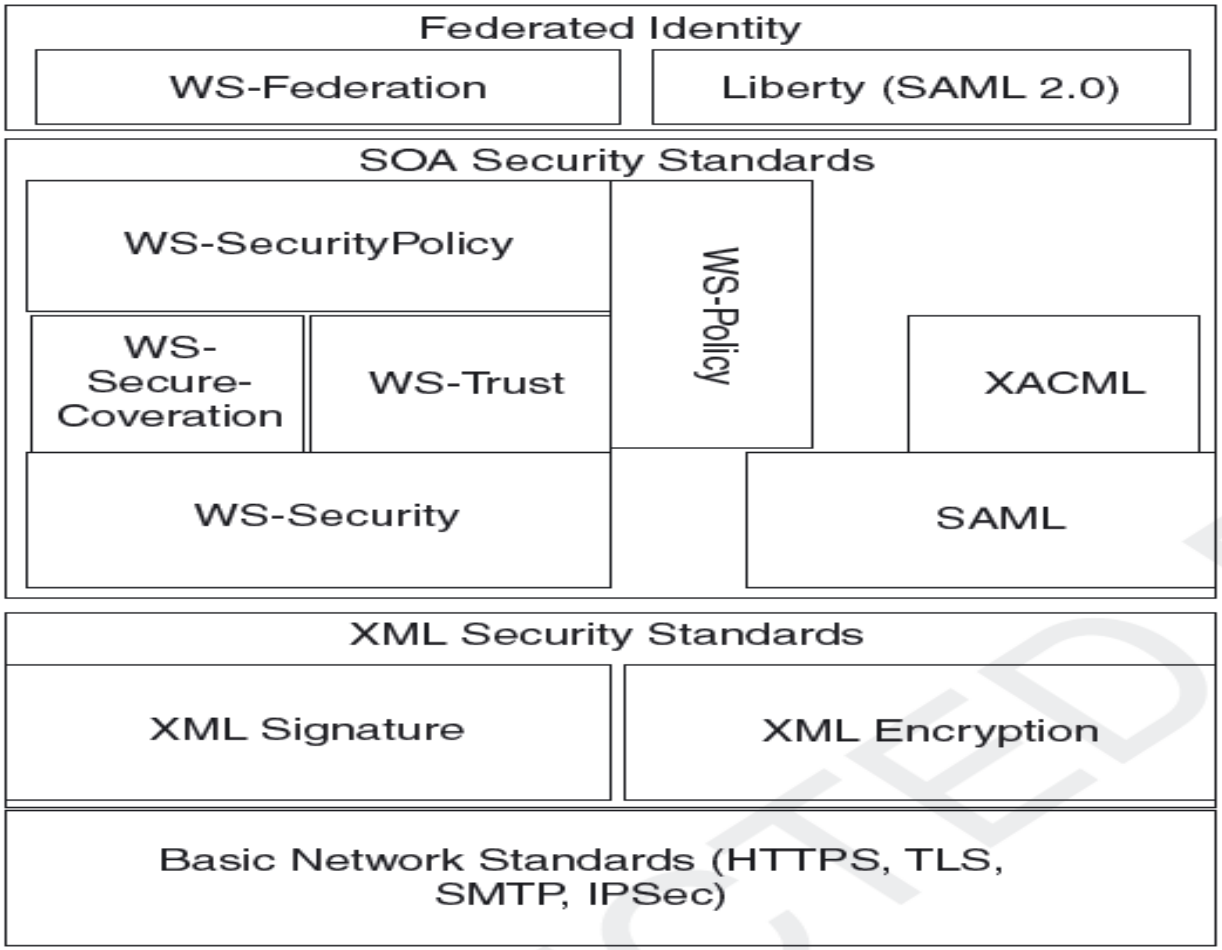
- VMDK / VHD Repurposing
- Key Scraping
- Infrastructure DDoS
- Data leakage
- Poor account provisioning
- Cloud provider insider abuse
- Financial DDoS
- "Click Fraud"

Dealing with Insecure SOA

SOA Threat Profile carries over to Cloud

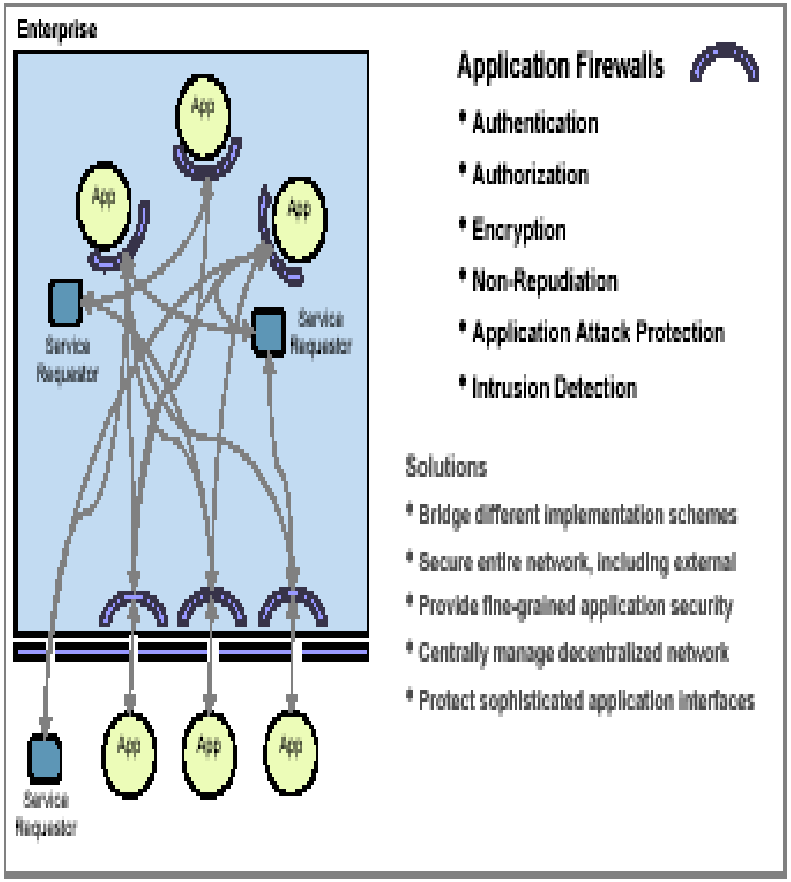


Solution: Follow SOA Security Standards Stack



Solution: Deploy XML Firewalls With Strict Policy Framework

- Unlike conventional firewalls, new generation firewalls do not work at packet filtering level
- Capable of SOAP content inspection
- Can detect SOAP level repeated / malicious attacks
- DOS detection
- Good to deploy at the enterprise gateway
- Both in Hardware and Software
- Capable of handling XML security standards
- Now extended to REST message filtering too.



Dealing with REST Security

REST API /Web Security Considerations for Cloud

- REST does not have predefined security methods so developers define their own due to proprietariness of REST implementations
- Most APIs handle authentication using a key but lack shared secret(For a sample analysis check out most of the APIs on http://www.programmableweb.com)
- Huge Problems due to letting a cloud REST service use HTTP basic authentication (need at least digest enabled or SSL).
- Cloud APIs highlight need to protect against typical Web threats like XSS, XML/JSON content manipulation, DoS attacks, session hijacking attacks etc.

Best Practices for REST Security

- Extend Web Security mechanisms for your REST APIs
- Deploy Access Control Rules to Methods
- Validate Validate Validate QUERYSTRING (No Shortcuts)
- Add a password requirement in addition to API Key (enable a shared secret)
- Encrypt communications
- Use hash-based message authentication code (HMAC) using SHA-2 or above (Used in S3 and other AWS)
- Check for XML firewalls' additional capability for JSON and other REST content filtering

Solution 1: Digest HTTP Authentication

HTTP Authentication can be of two types

- Basic
- Digest

Basic Authentication –

- User name and password sent as plain text
- Can be used in any Servlet Container with JaaS.
- Jguard is widely used for JaaS based authentication
- This is stateless

Digest Authentication –

- MD5 of username and password is passed
- Can be used any Servlet Container
- JaaS authentication and authorization is supported
- Stateless

Deployment Descriptors: Web.xml

<login-config>

<auth-method>BASIC</auth-method>

<realm-name>admin</realm-name>

</login-config>

<security-constraint>

//Specifies which URLs to be protected

</ security-constraint>

Auth Method BASIC, DIGEST, CLIENT_CERT

In Java program @RolesAllowed({“role1Allowd”,”roll2Allowed”})

Solution 2: Identity Management for Cloud

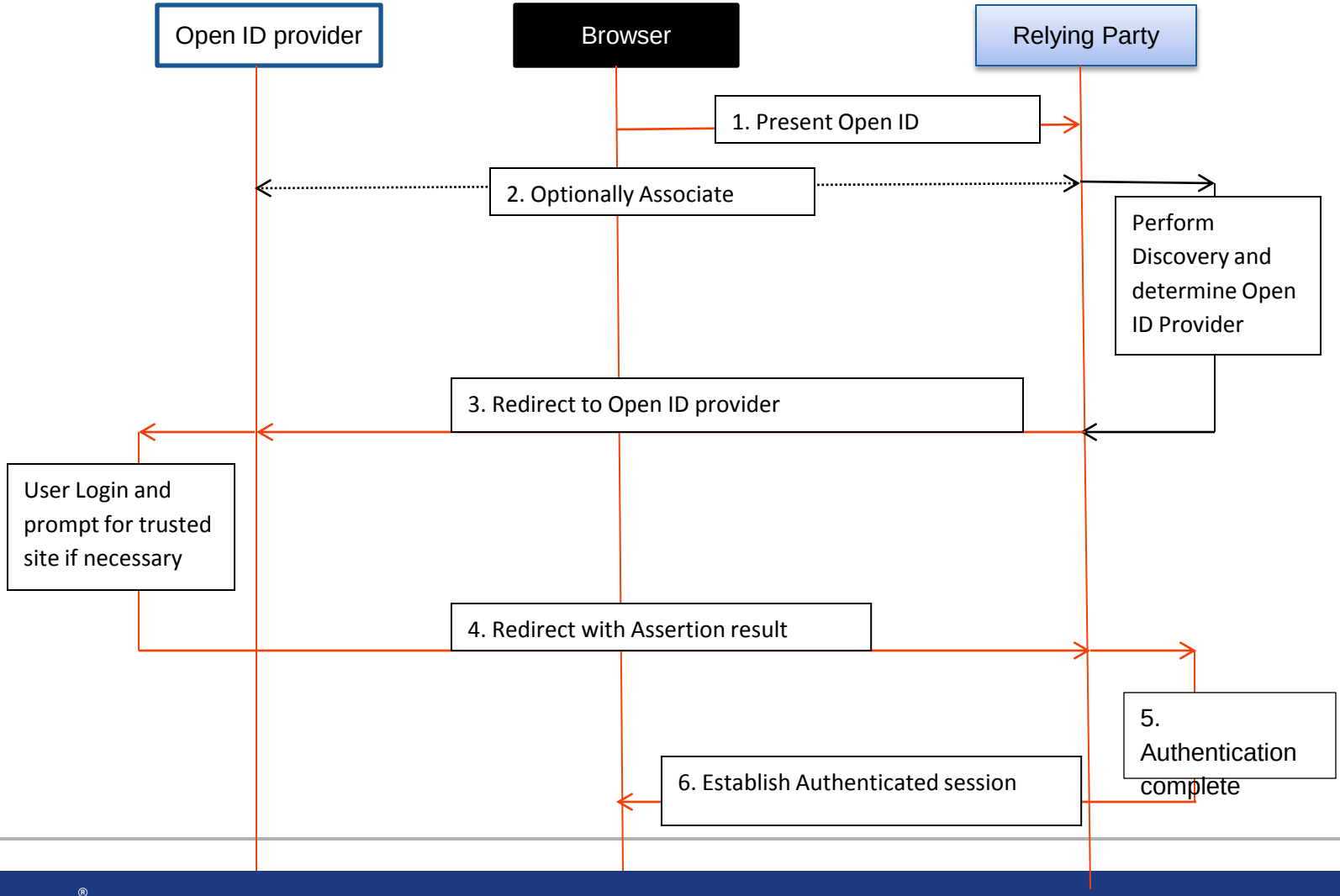
User centric Identity for Cloud

- Non applicability of Application-centric access control, where each application keeps track of its collection of users and manages because:
  - user space maybe shared across applications that can lead to data replication
  - mapping of users and their privileges a herculean task
  - Users need to remember multiple accounts/passwords and maintain them.
- A preferred model is User centric approach which leaves the user with the ultimate control of their digital identities.
  - The user has a consistent user experience
  - every user request to any service provider is bundled with the user identity and entitlement information
  - the application lets user the provider dynamically when authentication/authorization is needed

A UCID solution: OpenId

- OpenID is a user centric identity system
- It allows you to use an existing account to sign in to multiple websites, without needing to create new passwords
- Popular with leading Cloud Providers
- With OpenID, you control how much of that information is shared with the websites you visit.
- Typical Details involve:
  - Provider URL
  - Ex: https://www.google.com/accounts/o8/id
  - Call Back URL
  - OpenID token
  - OpenID attribute

Open ID Authentication Process



Steps Forward And Desiderata

- Industry Leaders both from Security and Cloud Provider Industry should come forward for
  - Standardization (Cloud Security Alliance is a good move)
  - API Standardization , Metadata standardization etc.
  - Contribute to Knowledge Dissemination (CSA Report on Risks is a good move)
  - Educate Cloud Providers on Secure APIs
  - Consumers awareness of REST security needs enhancement
  - Expand OpenID, Oauth and standardize them
  - Research onto advanced Cloud security issues
  - Certification Activities (CSA launched one recently)
  - Outreach

Q&A
Thank You

Contact srinivas_p@infosys.com