Blending Embedded Hardware OTP, SSO, and Out of Band Auth for Secure Cloud Access

Vikas Jain
Director, Product Management
Intel Corporation

Jesper Tohmo
CTO, Nordic Edge
(an Intel company)
Agenda

- Client to Cloud Security Layers
- User to Cloud SSO
- Strong Auth for Cloud
- Cloud App API Security
- Demo
The Goal “Security Connected” Client to Cloud

Extended Enterprise Security Continuum

Security Layers Cross
Hardware & Software

Cloud APIs
App Services
Data
OS/VM
Chip/CPU

On-Prem to Cloud

Private,
Public,
Hybrid

SaaS,
PaaS, IaaS

Security
Connected!

Hardware + Software

Devices & Infrastructure

Intel

RSA CONFERENCE 2012
Effective Client to Cloud Trust Involves Connecting these Layers of Cloud Security
User to Cloud Access Challenges?

- **Multiple Logins / Weak Security**
  - Single Sign On (SSO) & Strong Authentication
  - Manual Provisioning

- **Lack of Visibility**
  - Centralized Management Console
  - Auto Account Provisioning & Profile Sync

- **ID Infrastructure Integration**
  - AuthN & Provisioning Connectors
  - Scalable, Federated Trust

- **Audit Silos**
  - Centralized Audit Logging
  - Standards Based

- **Standards Based**
  - AD & IAM
Ubiquitous Access Requirement: **Any Device, Any Network, Any Cloud App**

- **Client Aware Security**
  - Multiple devices
  - Any network

- Accessing…
  - Apps from multiple cloud vendors

Users:
- Browser
- Desktop
- Mobile

Work, Home, Wireless

Intel

RSACONFERENCE 2012

salesforce.com
Google
amazon web services™
Typical solution should include ...

- **SSO**
- **Provisioning**
- **Strong Auth**

**Combine Enterprise Class Strong Auth with SSO**

**Provision Access**
- Provision/de-provision accounts
- AD integration
- Sync Id Profiles

**Adaptive Strong Auth**
- Selectively apply 2nd factor OTP AuthN
- Variety of software AuthN methods & devices - mobile devices, SMS, email

**Secure SSO**
- Federate windows/AD log in via portal
- To popular SaaS like Salesforce & Google Apps

**Regulatory Compliance**
- Rich audit trail of user login showing AuthN level
- De-provision & orphan account reports
Client Aware, Adaptive Authentication

- Network, IP, Geo Location, Time
- Credential Type
- User Attribute – Role, Group, Dept., etc.
- Device, type of target app
Out of band Signed Authentication

- More secure way for 2nd factor authentication
  - Authentication is performed on a separate channel different from the transaction channel

- Convenient
  - User approves using a simple Approve/Reject button from their mobile phone
Authentication
Authentication
Authentication
Authentication
Authentication

Welcome to iBank

Logged in: username@gmail.com
Digital Signing

![IBank screenshot](image)
Digital Signing

Please use Pledge client to sign transaction.
Transaction ID: 235326
From Account number: 6397583726
To: Apartment Renter
Bank: iBank
Amount: 1123 USD
Routing number: 321345678
Digital Signing
Digital Signing

Transaction ID: 235326
From Account number: 6397583726
To: Apartment Renter
Bank: iBank
Amount: 1123 USD
Routing number: 321345678
Digital Signing
Digital Signing
**Hardware Assisted Security at the Endpoints**

- **Silicon OTP**: Enables frictionless 2-factor user authN. Determines trusted platform.
  
  - **OTP**: 927316250
  
  - **Username** + **Password**

- **Virtual Keypad**: Protects PC display from malware scraping and proves human presence at PC. Great for transaction verification and ACH fraud prevention.

- **TXT Data Center Root of Trust**: Secure boot of VMs in Cloud.

- **PKI certificates**: to authenticate User and Server to each other, digitally sign documents and emails and encrypt files and messages.

---

**Intel**

**RSA Conference 2012**
Cloud Apps- APIs are New Cloud Control Point

- Leverage third-party services
- Applications move off premise

1/3 of Enterprise Traffic is via APIs

- Google: 5 billion API calls / day (April 2010)
- Facebook: 5 billion API calls / day (October 2009)
- Twitter: 3 billion API calls / day, 75% of all traffic (April 2010)
- Netflix: 20 billion API calls / month (Jan 2011)
- eBay: 8 billion API calls / month (Q3 2009)
- Bing: 3 billion API calls / month (March 2009)
- NPR: 1.1 billion API-delivered stories / month (March 2010)
- Over 50% of all traffic via API (March 2009)
- Over 100 billion objects stored in S3 (March 2010)
Service Gateway Broker Technology Makes a lot of Sense

APIs can be exposed, consumed, and proxied to a Service Gateway to offload security & communicate with back end infrastructure vs point to point integration.
Demo
Demo 1- 100% In the Cloud SSO

- Delivers same level of control as on-prem IAM
- Leverage Salesforce or enterprise accounts for SSO
- Trigger mobile & hardware assisted strong authentication
new slide to import SSO Portal
Kelly Anderson, 2/17/2012
Demo #2: Trusted Client to Cloud SSO

User -> Ultrabook -> Trusted Client -> On-Premise

Federation (SAML)

force.com

Intel Cloud SSO

Access

IPT based Trusted Client Authentication

SSO

100+ apps

Custom Apps

Box

webex

Google

Custom Apps

100+ apps
Unique Context Aware Strong Authentication

Configure GoogleApps

<table>
<thead>
<tr>
<th>Configure App</th>
<th>Assign Users</th>
<th>Restrict Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Time Password Requirement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select this option if additional authentication using One Time Password (OTP) is required to access this application. Learn more about how users will use OTP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requires Intel Identity Protection Technology (ITP)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **IP Restrictions**: Specify the subset of IP ranges from which this application may or may not be accessible.
- **Mobile Restrictions**: Specify mobile browsers for which this application may not be accessible.
- **Time restrictions**: Specify time frames when an application may or may not be accessed by users.
- **Day restrictions**: Specify the days of the week when the application may or may not be accessed by users.

Intel Identity Protection Technology Embedded in 120 million Ultra Books

Fast enrollment mobile OTP

Equip IT with Same Level of On-prem Security Controls
How to Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Identify all the cloud applications your Enterprise uses
  - Understand how many passwords are being managed
  - Define appropriate compliance controls for events such as a user leaving the company

- Within six months you should:
  - Select an IAM system which allows policy based integrated SSO portal according to your organization’s needs
  - Drive an implementation project to secure access to cloud applications
Visit Intel Booth for Demos

www.intelcloudsso.com

Free Trial
April 12

Bonus Free Box.net Account

www.intel.com/go/identity

www.mcafee.com/cloudsecurity

Mar 29- Kuppinger Cole Webinar
• How To Outsource Identity to the Cloud

On-Demand Webinar
• Cloud Service Brokers w/CSA & NIST
• Meet the Cloud API w/Forrester Research