Publishing Enterprise Web Applications to BYOD using a Granular Trust Model

Shachaf Levi
IT Client Security & Connectivity
May 2013
Legal Notices

This presentation is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2013, Intel Corporation. All rights reserved.
Agenda

• IT Risk And Security ‘A Balancing Act’: Protect to Enable

• Solution:
  • Access Web applications based on dynamic and granular security controls
  • web applications’ mobile friendly UI
  • Seamless OTP Authentication and Single-Sign-On using Kerberos
Open Access
Controls increased cost and constrains use of data and systems

How Do We Balance?
• Keeping us legal
• Availability of information
• Protection of information
• Industry influence
• Cost effectiveness of controls

Locked Down
Information assets should be fully protected

Our Mission is to Protect to Enable
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain trust level</td>
<td>The process of obtaining trust level is explained.</td>
</tr>
<tr>
<td>Intel TAP</td>
<td>An overview of Intel Trust Application Portal is provided.</td>
</tr>
<tr>
<td>Bingo Validation Tester</td>
<td>Status of validation tester is shown.</td>
</tr>
<tr>
<td>Continuous Integration</td>
<td>CI 2.0 Dashboard provides real-time view of developer's check-in, driver</td>
</tr>
<tr>
<td>Dashboard - VPG</td>
<td>build, smoke, and CI regression tests.</td>
</tr>
<tr>
<td>GEDI</td>
<td>GEDI translates to Global Equipment Downtag and Inventory tool.</td>
</tr>
<tr>
<td>Intel Capital</td>
<td>Further details on Intel Capital are provided.</td>
</tr>
<tr>
<td>Intel News (SMG)</td>
<td>Information about Intel News (SMG) is included.</td>
</tr>
<tr>
<td>PayStub-US</td>
<td>Details about PayStub-US, providing US employees access to their paychecks</td>
</tr>
<tr>
<td></td>
<td>for last 18 months.</td>
</tr>
</tbody>
</table>
How does it work

- User launches the TAP client application
- TAP client application performs the trust calculation
- TAP client application triggers an API to the McAfee* Pledge OTP
  - User confirms the generation of the OTP
- The One-Time-Password being validated on the Gateway
- Gateway requests Kerberos ticket on user’s behalf
- Backend web application is being accessed.
Components

Application Gateway

TAP client application

Web Applications

Trust Broker
Components – cont.

• TAP client application
  • A lightweight client application
  • Responsible for the client trust calculation

• Application gateway and authentication layer.
  • Resides in the enterprise demilitarized zone (DMZ)
  • Provides the layer of enforcement by filtering the access

• Trust broker
  • Calculates and responds with the trust level decision
  • Contains the business logic and the granular trust level
Scenario A: BYO Smartphone
Joe has a personally owned smartphone. He is in a coffee shop.

<table>
<thead>
<tr>
<th>Trust Level</th>
<th>Device Trust Level</th>
<th>Access granted?</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Smartphone + Coffee Shop</td>
<td>No</td>
<td>Level 5: Top Secret</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>Level 4: Top Secret</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>Level 3: Restricted Secret</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Level 2: Confidential</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Level 1: Unclassified</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Level 0: Internet access only</td>
</tr>
</tbody>
</table>

Authentication Method = user OTP plus PIN

Remote display of confidential data but no local content storage

Container based apps

Copyright © 2013, Intel Corporation. All rights reserved.
Scenario B: Intel-managed BYO smartphone

Bob’s BYO smartphone has an approved MDM solution installed and is running most current version of OS. OS has “defined” features. Bob is in an airport.

Trust Level
- Device Trust Level = 3

BYO Smartphone with MDM + Airport

Authentication Method = device PIN plus embedded certificate

Access granted?
- No
- Yes

Access Level
- Level 5: Top Secret
- Level 4: Top Secret
- Level 3: Restricted Secret
- Level 2: Confidential
- Level 1: Unclassified
- Level 0: Internet access only
Trust Calculation

- Dynamically determine what information is accessible based on several factors:
  - User identity
  - Type of device
  - Security controls
  - Physical location (on or off site)
- allow access, deny access, or allow limited or mitigated access
  - Can deny change permissions on certain content
  - Allow view-only permissions
  - Block a download
McAfee* Pledge One-Time-Password authentication

- Using McAfee* Pledge One-Time-Password
- API to generate OTP from the client application
- User experience – no need to enter a password
Single Sign On using Kerberos

- The Gateway authenticates the user
- The Gateway requests a Kerberos ticket on the user’s behalf
- The Gateway presents the Kerberos Ticket to the backend web application

Benefits:
- No passwords being transferred, only the Kerberos ticket
- Removes the need for Active Directory credentials on BYOD
- Single Sign On – login once, access multiple times
User Experience

• our Trusted Application Portal (TAP) is customizable using scripts and HTML5 to support most SFF devices.
• adheres to the guidelines and standards for human factors engineering.
Results

- > 25 enterprise web applications, Smart phones friendly
- > 15 device types, multiple Operating Systems
- > 10,000 installs (35% of BYOD total devices)
- >12,000 accesses to backend applications per week
Next Steps

Content Protection based on Trust Level

Trust Calculation

Version 1
Web App

Version 2
Web App  Hybrid App  Native App

Enterprise App Store
Trust SDK
App Development
Key Messages

Rethink information security in light of new technologies and attack trends

Capitalize on the opportunity to reduce risk while enabling new technologies

No silver bullet – security still requires “defense in depth”
Thank You
Additional Resources

- Information Security Protect to Enable Strategy video
- Rethinking Information Security
- Intel IT's Security Business Intelligence Architecture
- Granular Trust Model Improves Enterprise Security

Learn more about Intel IT’s Initiatives at Intel.com/IT
IT@Intel  Sharing Intel IT Best Practices with the World

Learn more about Intel IT’s Initiatives at www.intel.com/IT