Mobile Application Security

Rebecca Finnin, AT&T
ISACA Geek Week
08/20/2013
AGENDA

Mobile Application Development

• Review Gartner Framework of Mobile App Development Challenges
• Outline Security Implications of Each
• Discuss Unique AT&T Solutions
Mobile App Development: Challenges

• Gartner Field Research Summary: Mobile Application Development
  – Jan 24 2013, Kirk Knoernschild & Danny Brian

• Strategy and Governance
• Development and Delivery
• Platforms and Frameworks
• Management and Security
Mobile App Development: Challenges

• Mobile Application Development – Strategy and Governance
  • Operating Without a Plan
    – Security Concern: Threat modeling and architecture review with agile development?
  • IT’s Second Chance
    – Security Concern: Percentage of mobile applications developed by 3rd parties?
• Cross-Functional Strategy
  – Security Concern: Critical mass to form Mobile Center of Excellence (COE)?
Mobile App Development: Challenges

• Mobile Application Development – Development and Delivery
  • Adopting Agile
    – Security Concern: Developer experience with mobile platforms (much less security)?
  • RESTful Service Orientation
    – Security Concern: Who is testing the API on back end application?
  • Distribution Challenges
    – Security Concern: Public or private app stores?
• Testing Complexity Squared
  – Security Concern: Testing via devices or simulators?
  – AT&T Solution: Application Resource Optimization (ARO)
AT&T Solution: ARO

• Mobile Application Design Challenges
  • Mobile code not being written mindful of unique aspects of wireless network environment
  • Leads to issues with user experience, battery life and network efficiency
  • Most common pitfalls: excessive radio activity, inefficient use of pre-fetching, unnecessary duplicate content downloads
AT&T Solution: ARO

• AT&T Solution - Application Resource Optimizer (ARO)
  • http://developer.att.com/ARO
  • Free java-based, open source diagnostic tool
  • Available for use with Android and Windows, iOS (network usage only via proxy)
  • Measures data traffic, GPS, bluetooth and camera usage
  • Grades application (Pass/Fail) against 12 best practices
  • Ex Benefits: 46% energy savings from clustering data transfers, eliminate 17% of network traffic from unnecessary download of unaltered HTTP content

Based upon research papers from AT&T and UMich, ACM Mobisys conference
AT&T Solution: ARO

• Security Features
  • Integration with Lookout - Mobile Security API
  • Provides assessment of mobile code for indications of malware, spyware or other security vulnerabilities
  • 6-10 High / 5-1 Medium / 0 Low Severity Readout
  • Available for Android Application Packages (APK) upon release in March 2013
Mobile App Development: Challenges

• Mobile Application Development – Platforms and Frameworks
  • A Tale of Two Platforms
    – Security Concern: Standards for device OS, cross-platform mobile development framework or all of the above?
  • Betting on HTML5
    – Security Concern: HTML5 may become operational best practice, but as it matures will it incorporate better security measures?
  • A Framework Dilemma
    – Security Concern: How to Develop Security SMEs with such a diverse toolset?
• The App Residency Decision
  – Security Concern: Should native app be required for certain situations or mandate additional security controls for mobile web apps?
Mobile App Development: Challenges

• Mobile Application Development – Management and Security
  • Relying on MDM
    – Security Concern: Is MDM enough or too device-centric?
  • Dealing with Data
    – Security Concern: Do you trust device storage?
    – AT&T Solution: TOGGLE

© 2012 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
AT&T Solution: TOGGLE

• Mobile Device Paradox
  • Cost pressures / user preferences mean use of personal devices is desirable
  • Security concerns about corporate data on personal device is undesirable
## AT&T Solution: TOGGLE

<table>
<thead>
<tr>
<th>Technology Options</th>
<th>MDM</th>
<th>Container</th>
<th>Hypervisor</th>
<th>Dual Persona</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Email</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Centralized configuration management and trouble-shooting, device wipe/lock</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Role-based policy mgmt for access to apps and Data</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Basic Enterprise App Store</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Application Push</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Device and App Usage reporting</td>
<td>Y</td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>BTF Server deployment</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud deployment</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Separation of user and business data</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Basic Security (Password / AV / Malware/ VPN / Encryption)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Enhanced Security (real-time network based scanning)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-User and IT Self Service</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Personal Applications, Data, and Usage not seen by IT</td>
<td></td>
<td></td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Multi-OS Support</td>
<td>Y</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
</tbody>
</table>
AT&T Solution: TOGGLE

• AT&T Solution - TOGGLE
  • Establishes two containers on a single device: Personal and Work
  • Available with any domestic carrier and on iOS and Android platforms
  • ToggleHub provides centralized enterprise application, document and media distribution portal.
  • Work mode also provides access to corporate email, contact lists, calendars, browser, messenger tools and access to encrypted attachments.
  • Administrative Interface provides device inventory, user and application management, policy based administration, configuration management and reporting.
AT&T Solution: TOGGLE

• How Does It Work?
  • Mobile application client creates encrypted, password protected workspace on the device
  • Management console is a cloud-based service
  • Security Features Include:
    – Anti Virus / Anti Malware features
    – Application Level VPN
    – LDAP/Active Directory Integration
  • Mobile Device Management
    – Application and Content Management
    – Document Viewer
    – AT&T Toggle Browser
    – Toggle Email
    – Enhanced Application Wrapping

© 2012 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.