Agenda

The Mobile World - Trends

Mobile devices - threats and risks

BYOD Security Top Five

Consumer App Security Action Items
The Mobile World - Trends
What's a mobile device?
No other technology adoption trend compares

- 4 BILLION mobile phones in use among 7 billion people.
- By 2013, mobile use is expected to overtake desktop and laptop use.
- By 2015, there are expected to be 500 million mobile banking users worldwide.
- 40% of consumers say losing their mobile phone is worse than losing their wallet.
There’s an App for That

- Payment data
- Corporate email
- Corporate apps
- VPN credentials
- Banking data
- Healthcare ePHI
- Home automation
- Automotive
- Social
- Dropboxes

We can’t wait to manage sensitive data on
Mobile Devices – Threats and Risks
The Problem Space....

Vulnerabilities and attacks affecting an m-payment system

Protocol
- Design flaws in the mobile standards/protocols
- Weak cryptographic algorithms
- Design vulnerabilities in GSM, Bluetooth, etc

Platform
- Design flaws in the m-payment protocol
- Vulnerabilities Demonstrated on various platforms
- SIM Card cloning
- Spyware
- Unauthorized access
- Impersonation
- Repudiation
- Replay attacks

Hardware
- Side-channel attacks on APIs in the development platform (e.g., J2ME, C++)

Software
- Android
- Windows 7
- iOS
- <15% use ANY AV/AM

Technology + Human Factors

Security Issues in Mobile Payment Systems
Agarwal, Khapra, Menezes and Uchat
Threats and attacks are increasing

Mobile’s proliferation and access to sensitive data make it the new target

- **Loss / Theft**: Smartphones are 90% more likely to be lost than laptops.
- **Phishing**: Phishing is many times more successful on mobile devices.
- **Malware**: Android Market had over 400,000 downloads of malicious apps identified in 2011.
- **Spy-ads**: Legitimate-sounding applications from the Dark Side.
- **“Repackaging”**: Multi-media whiz-bang idea, can be used for evil.
- **QR attacks**: Man-in-the-middle attacks, just like using a laptop.
- **Wi-Fi**
- **Botnet**
Vulnerabilities of the mobile platform today

- Security awareness and usage.
- Confusion over security “ownership”.
- Small size increases loss and theft.
- Authentication and access control not designed for multi-user or secure application management
- Mobile security standards are immature
Vulnerabilities of the mobile platform today

‣ “Mostly-On” carrier network, location services, Wi-Fi, Bluetooth, and NFC can amplify exposure to networking vulnerabilities.

‣ Secure configuration and system management are difficult for both consumer and the enterprise.

‣ Security tools and services emerging with slow adoption or consistency across platforms.
Mobile (In)Security

- < 15% of smartphones run anti-virus and/or anti-malware (or have proven options)
- Malware attacks on Android have increased 400% since mid-2010
- Industry focus is on Mobile Device Management (MDM) to address enterprise-level risk
  - This includes ‘private’ marketplaces replacing the Apple App Store and Android Marketplace
  - Preventing ‘rooted’ or ‘jailbroken’ devices from accessing corporate information assets
  - Does not begin to address the consumer space
- Remote exploitation, command & control, Botnet attacks are increasing
BYOD Security Top Five
1. Establish a Corporate Position

- Mobile Device Risk Assessment
- Mobile Device Usage Policy
- Acceptable Use Policy
- Device Inventory
- Data Classification Policy and Controls
- Supported vs. Unsupported

A goal without a plan is just a wish.
Antoine de Saint-Exupery – French Writer (1900-1944)
2. Use a Mobile Device Management Platform

Agent-based
- Third Party MDM Solutions

Agent-less
- Exchange Active Sync
- “GoogleSync” (beta)
- Blackberry Enterprise Server
- System Center: Windows Mobile Device Manager / SC:MDM

Mobile device management (MDM) has become a critical service for IT departments needing to manage the increasing number of smartphones and tablet devices entering the enterprise. MDM systems facilitate policy setting, enforcement and support of mobile devices. Architectures of these solutions include agent-based and zero agent. Gartner 12 February 2012

Gartner Magic Quadrant, MDM Third Party
3. Enable a Password / PIN

MDM Commonalities

• PIN or Password strength, length and history *
• Lockout after \{X\} failures
• Delay between attempts *
• Remote Wipe after \{X\} failures

Device Options

• Fingerprint authentication *
• Password authentication *
• PIN authentication
• Pattern authentication *

* options vary per OS flavor and additional applications may be required.
4. Disable “Untrusted” Application Installation

Enterprise

• App Whitelists / Blacklists
• iOS: Private App Store
• Blackberry Enterprise Server Policy
• Windows: ActiveSync Policy
• Android: Third Party MDM

Personal

• Read the fine print regarding permissions before installing
• Do not install ‘non-market’ applications (Android)
• Do not ‘jailbreak’ or ‘root’ your phone
5. Report Lost / Stolen Devices Immediately

MDM Commonalities

• On-Demand Remote Lock
• On-Demand Remote Wipe

Personal Devices

• MobileMe / iCloud remote wipe
• Third Party Security Applications
• Deactivate SIM with provider
• New FCC Ruling related to stolen devices
Consumer Apps
Payments - Yesterday...

...and Today
Types of Consumer Apps

‣ e-Banking apps - moves the online banking model to the mobile platform (but with stored data)

‣ Retail apps - personalized shopping experience right from your mobile device (i.e. Nordstrom, Amazon and many other retailers)

‣ Retail Loyalty Payments – (i.e. Starbucks) proving new paradigm by the millions

‣ Many more that are being realized and
Consumer Apps
Mobile Security Action Items
Mobile security action items

You cannot ignore it and praying isn’t changing risks – every organization has a mobile environment to manage today.

Establish a mobile security culture – take ownership of the risks with the opportunities.

Education and training for your employees and customers are the greatest tools available today.

Conduct a mobile risk assessment annually to drive strategy.
Mobile security action items

Policies must match risk and have a way of enforcing

Security should be a key component of any new mobile initiative

Security in the development process is a necessity for consumer apps

Prepare for dynamic changes

Leverage compliant and secure services when available
Require Security Deliverables in the SDLC

- Requirements Gathering
  - Identify security controls

- Development and testing
  - Require security control testing

- Deployment
  - Test in an ‘as-built’ environment

- Maintenance
  - Re-test on change

- Outsourced? Third Party Apps?
  - Ensure contracts require these steps!
  - Vendor management and third party reviews
More mobile security action items

Don’t trust anything – take a whitelist approach

Train, train and train users about phishing with web, email, social media and SMS on mobile

Emerging security tools can help

Test, test, test and then test again (use forensic and other tools to identify app vulnerabilities and unprotected data)

Consider third-party solution security validation
Drive business value with mobile security

Consumers are going to use their mobile devices for purchasing – the landscape is still wide-open to determine the mobile payments winners.

Mobile payments are opening up great opportunities for innovative merchants, emerging technology vendors and traditional payments players.
Drive more business value with mobile security

Mobile security is at the heart of any successful solution and is likely the puzzle piece that determines adoption.

Companies that invest in security now as they implement mobile payments can overcome the fears and risks as they accelerate business value through consumer trust.
Golden Rule

Trust Nobody

Test Everything
Thank You

Adam Shnider, Coalfire
Adam.Shnider@Coalfire.com
206.604.5047 ext. 7519