



Mobile Device (In)Security

Ian Parker

Sentinel Ridge Consulting Group Inc.

Agenda

- Mobile device statistics
- Mobile threats
- Recommended security controls
- Mobile device management

Mobile Device Statistics

- 5.3 billion mobile subscribers – 77% of world population
- China and India added 300 million new subscribers last year!
- Android is now dominant mobile platform with 38.5% market share, iOS is second at 19.4%, Symbian is third at 19.2% and RIM is fourth at 13.4% (and falling)
- Only 4% of mobile devices have any third party security software

New Kid on the Block



ANDROID



"Well, that explains it then. The A2s always were a bit twitchy. That could never happen now with our behavioral inhibitors. It is impossible for me to harm or by omission of action, allow to be harmed, a human being."

- Android Bishop in movie "Aliens"

Mobile Threats

- Malware
- Loss and theft
- Data communication interception
- Youth exploitation
- Corporate misconduct
- Direct attacks

Malware

(Spyware, viruses, trojans and worms oh my)

- Market share and infection rates linked, hence main targets have been Symbian and Windows Mobile devices BUT
 - 400% increase in Android malware since Summer 2010
- Greatest risk comes from installation of applications from untrusted sources
- Greatest threat for Blackberry, Android and iOS users is spyware

Android Malware

- Jan. 2010 – first Android phishing application, Droid09, poses as banking client
- Mar. 2010 – Vodafone Android phones shipped with Mariposa botnet software
- Jul. 2010 – GPS monitoring software masquerades as “Tap Snake” game
- Aug. 2010 – First Android SMS trojan sends SMS messages to Russian premium numbers

Android Malware (cont.)

- Nov. 2010 - “Angry Birds” proof-of-concept malware shows how users can be tricked into downloading unauthorized applications
- Dec. 2010 through Feb. 2011– Many apps available through Chinese third party app stores packed with trojans
- Jan. 2011 - “Soundminer” proof-of-concept “sensory malware” revolutionizes how credit card numbers can be stolen

Android Malware (cont.)

- Mar. 2011 – first Android malware available on Android Market on a large scale affects 50,000 users
- Mar. 2011 – Google's "Android Market Security Tool" is itself trojanized

iOS Malware*

(iPhone, iPad, iPod Touch, Apple TV)*

- Researchers found that almost half of 1400 analyzed apps leaked sensitive data to third parties – pre-packaged code purchased from advertising agencies
- Major threat to iOS users is with “jailbroken” devices – removal of restrictions that only Apple-approved software can be executed

Blackberry Malware

- Several instances of commercial spyware targeted at Blackberry and other devices
 - FlexiSPY – According to Web site: “Receive copies of SMS, call logs, e-mails, locations, listen to conversations, bug meeting rooms, catch cheating spouses
 - also Mobile Spy, MobiStealth, SpyBubble
- Spyware is a major threat if Blackberry connects to corporate resources

Loss and Theft

- One in twenty mobile devices is lost or stolen
- Not only data on device at risk, also:
 - Bookmarked bank accounts with passwords set to auto-complete
 - Contacts with pictures and addresses
 - Calendar events
 - Social media accounts
 - Personal photos
 - Pre-connected corporate e-mail accounts

Loss and Theft (cont.)

- Few users seem to be aware of remote wipe command
- Researchers have found it is trivial to jailbreak an iPhone and decrypt passwords from keychain, including passwords for corporate e-mail, Wi-Fi and VPN, even with screen locking or passcode enabled

Data Communication Interception

- Tools exist to listen to conversations over cellular networks or decrypt data transmissions
- Use of Wi-Fi accentuates threat
 - Man-in-the-middle attacks
 - Wi-Fi hacking
 - Example: Use of FireSheep to steal unencrypted cookies

Youth Exploitation

- 83% of teenagers regularly use mobile devices
- 20% of teenagers have been “cyber-bullied” via a mobile device
- 20% of teens send inappropriate or explicit pictures or videos of themselves

Corporate Misconduct

- Massive amounts of corporate data can be transferred to a mobile device e.g.
 - iPhone 4S up to 64 GB
 - ARCHOS Android tablets up to 250 GB (approx 178,000 times the capacity of a floppy disk)
- Camera can be used to take screenshots of confidential information
 - Most e-mail content management applications don't scan JPEG's

Direct Attacks

- Many direct attacks against mobile devices possible using SMS functionality e.g.
 - Curse of Silence attack against Symbian devices
 - Malformed SMS messages sent to iPhone, Android or Windows Mobile devices can give attacker complete control over device
 - Denial of service attacks using SMS message floods against emergency responders

Direct Attacks (cont.)

- Visiting a malicious Web site e.g. JailBreakMe.com using an iOS-based device can jailbreak the device
- Exploits against mobile browsers will become as big a threat as exploits against Internet Explorer, Firefox etc.

Recommended Security Controls

- Exercise same caution when visiting Web sites as you do from your desktop/laptop computer
- If using an iPhone, don't jailbreak the device !!
- Back up the device regularly
- Pay close attention to services that an application requests access to during installation
- Use built-in or third party anti-X and firewall protection

Recommended Security Controls (cont.)

- Label device with your name and phone number
- Find out how to remotely locate, lock and/or wipe your device BEFORE you need to do it
- Use a complex passcode and change it regularly
- Configure auto-lock function
-
- Encrypt data on device wherever possible

Recommended Security Controls (cont.)

- Turn off Wi-Fi and Bluetooth connectivity when not in use
- Do not connect to company resources over insecure Wi-Fi networks – use a secure network* or a virtual private networking client
- If possible, configure device to prevent outgoing calls while locked

(* preferably a wireless network that uses WPA-Enterprise security protocol)

Mobile Device Management

- Management choice: Mandate use of company-provided mobile devices or let employees use their own devices
- Same result: Employees WILL use their own devices regardless of policy
- Challenge: How to manage heterogeneous mobile devices
- Solution: A mobile device management (MDM) application

Mobile Device Management (cont.)

- What should ideal MDM application do?
 - Only allow company-approved mobile devices to connect to corporate network
 - Remotely locate, lock, wipe, backup and restore lost and stolen devices
 - Enforce security policies on all mobile devices
 - Monitor and control use of messaging and application installation

Mobile Device Management (cont.)

- Determine security posture of mobile devices before granting network access
- Monitor device activity for data leakage and inappropriate use
- Support all major mobile platforms inc. Android, Blackberry, iOS, Windows Phone and Symbian

Recap

- Use of insecure mobile devices represents today's biggest information security risk
- Securing an individual mobile device against most prevalent security threats is quite simple but requires configuration by user
- Supporting large variety of mobile devices is a huge challenge for organizations