

iOS Devices

Sebastien Andrivet
#Days Management Session 2011
Lucerne, October 27

Agenda

- Mobile and iOS devices
- iOS and Companies
- Threats and Controls
- Predictions
- Conclusion, Q&A

Mobile Devices

- Are easy to loose, easy to steal, ...
- Contain more and more data
 - E-mails, contacts, documents, passwords, VPN accesses...
 - Facebook, LinkedIn, Twitter...
 - Geolocation
- Are often (always) connected to untrusted networks
 - Wi-Fi, GSM, CDMA...
 - Many mobile devices have IPv6 activated by default
- Represent money
 - SMS and premium numbers, Stores
 - Payment system (near future)

iOS Devices

- Every application, every release is reviewed by Apple
 - Contrary to Android
 - But... they do not care much about apps security
- Only four distribution channels
 - AppStore (iTunes)
 - Enterprise distribution (in-house)
 - Ad Hoc (max 100 devices - testing)
 - Development (your device)

iOS and Companies

- Corporate data synchronization
 - Exchange ActiveSync, Contacts, Calendar...
 - VPN, WPA/WPA2 Enterprise
 - In-house applications
- Only 1 user profile
 - Mix of private and corporate identities (mails, contact), problematic, especially with iPad
- Difficult to manage
 - Despite some solutions like MobileIron, Good Technologies...
 - No control over AppStore apps

Two points of view

- Companies are concerned by iOS threats in two ways:
 - As user of iPhones and iPads where end users are employees
 - As publisher of iOS Applications where end users are customers, general public, journalists, ...
- Different threat scenarios apply in each case

Relevant iOS Threat Scenarios

- Hackers obtain your company data (jailbroken devices)
- Competitors steal company data (Lost or stolen devices)
- Hackers attack your apps (Releasing security fixes)
- These are only few examples, there are many more...

Jailbreaking

- Cool, fun, but...
- ... It exposes your device to other threats
 - `root/mobile password = alpine`
- ... It attacks your device
 - Uses exploits, rootkit...
- ... It disables several security features
- ... if you buy apps from the jailbreaking community (Cydia), you give your credit card number to hackers!

Threat Scenario: Hackers obtain your company data

- Agents
 - Hackers community
- Action
 - Add a Trojan to a jailbreak
 - Malware exploiting vulnerabilities extracted from jailbreaks
- Asset
 - Almost all your employee's data

Controls

- Do not jailbreak
- But if you have to ...
 - ... Use dedicated devices, not your own
 - ... Set (strong) passwords
 - ... Evaluate the security consequences
- Company policies & training

Lost or stolen devices

- Lots of data is unencrypted
 - Apple apps
 - Third-party (AppStore) apps
 - In-house apps
- Hard-disk drive is encrypted (AES)
 - PINs are attackable
 - Passwords have to be strong
 - Russian company is selling a cracking software

Threat Scenario: Competitors steal Company Data

- Agents
 - Thieves, competitors, ...
- Actions
 - Steal the device
 - Jailbreak the device (matter of minutes)
- Asset
 - Almost all your employee's data

Controls

- Training of employees
 - How to detect, how to react
- Configuration Profiles
- Mobile Device Management Systems
 - MobileIron, Good, Apple Lion Server, ...
 - Manage other mobiles (Android, Windows)
 - In-house app deployment, policy mgmt, remote/automatic wipe, etc.
- Strong password

Releasing a security fix

- For Apple, there is no notion of minor or major releases
- Every release is checked by Apple
- What happens if you have an urgent release?
 - You have to wait
 - The attackers will not

Threat Scenario: Hackers attack your apps/customers

- Agents
 - Hackers
- Actions
 - A security vulnerability is discovered and published for your app
 - You build a fix, you wait for Apple's approval
 - In the meantime, your customers are attacked
- Asset
 - Your apps, i.e. your customers
 - Your reputation

Controls

- Make a security review before releasing
 - Pentest, audits, code review, remember the server side
- Training, SDL, OWASP
- Use iOS Security Services
 - Encryption, SSL/TLS, ...
- If it happens, remove app from AppStore
 - But will protect only new customers
 - Companies are not able to remove or “kill” already installed apps

Predictions 2011-2012

- Nokia (Symbian) was dominant
 - 38.1% in 2010, 15.2% in 2011
 - Still number 1 if you take into account S40
- Today, Apple is number one in terms of revenue and profit
 - 18.5%, Q2 2011
- Future major player: Google
 - Has already 39% of US market, but fragmented
 - Will be the “Microsoft” of Mobiles

Predictions 2011-2012

- Mobile malwares
 - iOS: a few but lot of buzz
 - Android: too many for buzz
- Social engineering attacks
 - Phishing, like on PCs
- Attacks against browsers
 - Safari, embedded Safari
- Attacks against PDFs
- Stolen certificates
 - Fake “in-house” app distribution
- Privacy concerns

Predictions 2011-2012

- New jailbreaks
 - Despite efforts of Apple
 - Against iPad 2, iPhone 4S, ...
 - Exploits in Apple chip (A5...)
 - Cannot be patched (hardware)
- Some malware will use exploits extracted from jailbreaks
- Some malicious sites will use jailbreak exploits

Thank you

To contact me:

sebastien@advtools.com

Twitter:

@AndrivetSeb

@ADVTOOLS

www.advtools.com



ADVTOOLS

- Swiss company founded in 2002 in Geneva
- Specialized in Information Security & Problems Diagnosis
 - Pentesting mobile devices (iPhone, iPad...)
 - Training (secure development of iOS apps, pentesting iOS apps)
 - Forensics
 - Security Audits
 - Pentesting web apps and services

References

- A. Apple now top smartphone vendor in the world with 140% growth
<http://www.bgr.com/2011/07/29/sa-agrees-apple-now-top-smartphone-vendor-in-the-world-with-240-growth/>
- B. Symantec Security Response – A Window Into Mobile Device Security
http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf
- C. Apple iOS 4 Security Evaluation – Black Hat USA 2011
https://media.blackhat.com/bh-us-11/DaiZovi/BH_US_11_DaiZovi_iOS_Security_WP.pdf
- D. Five New Userland Exploits Found For iPad 2 And iPhone 5, Future Jailbreak Imminent!
<http://www.redmondpie.com/jailbreak-iphone-5-ios-5-untethered-announced-by-chronic-dev-team/>

References

- In the U.S. Smartphone Market, Android is Top Operating System, Apple is Top Manufacturer
http://blog.nielsen.com/nielsenwire/online_mobile/in-u-s-smartphone-market-android-is-top-operating-system-apple-is-top-manufacturer/
- Apple iPad Security Overview
http://images.apple.com/ipad/business/pdf/iPad_Security_Overview.pdf
- Apple Enterprise Deployment Guide
http://manuals.info.apple.com/en_US/Enterprise_Deployment_Guide.pdf
- Press Release – Securing and managing smartphones with Swisscom
http://www.swisscom.ch/en/ghq/media/mediareleases/2011/06/20110607_MM_Firmen_Smartphones.html
- Good on iPhone, iPad and iPad Touch
<http://www.good.com/iphone/>
- MobileIron iOS Management for Enterprise
<http://www.mobileiron.com/en/multi-os-management/ios-management>
- Around 23 companies in this market today (Boxtone, NetHawk, Sybase, McAfee/Intel...)