iOS Security
The Never-Ending Story of Malicious Profiles

SESSION ID: BR-R02

Adi Sharabani
CEO & Co-Founder
Skycure
@AdiSharabani

Yair Amit
CTO & Co-Founder
Skycure
@YairAmit
About the Presenters

Yair Amit
- CTO & co-founder of Skycure
- Web, network and mobile researcher
- Inventor of 15 patents
- Former manager of the Application Security & Research group at IBM

Adi Sharabani
- CEO & co-founder of Skycure
- Watchfire's research group [Acquired by IBM]
- Lead the security of IBM software
- Fellow at Yuval Neeman’s workshop
- Teacher at Ohel Shem high-school
Agenda

- iOS security model
- Malicious profiles
- iOS 7.1 security fix
- Impact on MDMs
- Afterthoughts
Starting With the Obvious

- Android malware threat growth:

iOS malware in 2012: less than 1% of mobile malware

Source: Trend Micro 2012 Mobile Threat and Security Roundup
iOS Security Model

App Characteristics
- One Store
- Heavy Screening
- App Sandboxing

Profile Characteristics
- No Store
- No Screening
- No Sandboxing

Source: Apple’s App Sandbox Design Guide
Configuration Profiles – Where Do We Find Them?

- Mobile Device Management (MDM)
- Cellular carriers
  - Usually used for APN settings
- Mobile applications
- Service providers
Malicious Profiles

Hacker gains access to your mail, business apps, cloud services, bank accounts and more, **even if traffic is encrypted**
Time for a demo
(so take out your iOS device)
Malicious Profiles – Where Do We Find Them?

- Malicious “service providers” (apps/services/etc.)
- Malicious Wi-Fi networks
- Vulnerable services
Am I Safe?

- Profile listing could indicate suspicious profiles
- Cat-and-mouse game: attackers can name their profile to look benign
So let’s remove the attack
The Invisible Profile

- iOS vulnerability allowing a profile to hide itself.
- Identified by Assaf Hefetz, researcher and developer, Skycure
- So what happened:
  - Victim was lured into installing a special crafted profile
  - Due to iOS bug, profile is not listed in the Profiles pane
  - Malicious profile is active and yet hidden

- Additional technical details pending on iOS 7.1 release
Malicious Profiles and MDMs
Mobile Device Management

- Enrollment:
  1. A configuration profile is sent to the device
  2. User installs the MDM profile
  3. Device connects to MDM Server to enroll

- Commands:
  4. Server sends an APNS command
  5. Device connects directly to the server over HTTPS (Server sends commands or requests information)
Mobile Device Management

- MDM profile could potentially act as a powerful “malicious profile”.
- However:
  - Alarming installation message
  - Barriers to become an MDM
  - Only one MDM is allowed on device
MDM Security Issues

- David Schuetz presented a great research on MDM security

- Problem increases when malicious profiles are used to exploit MDM protocol shortcomings
MDM Piggybacking

- Attack scenario:
  - IT/user enrolls an iOS device to a legitimate MDM service
  - Victim installs a malicious profile
  - Attacker waits …
  - MDM server sends an APNS command
    (attacker has no control over this part)
  - iOS device asks the MDM server for commands
    (attacker does have control over this)
  - Attacker impersonates the MDM server
Possible Attacks – Removal of MDM

- A simple 401 HTTP response leads to the removal of the MDM (and associated settings or apps) from the device

HTTP/1.1 401 Unauthorized
Content-Type: text/html
Cache-Control: must-revalidate,no-cache,no-store
Transfer-Encoding: chunked
Content-Encoding: gzip
Full Demo Flow
Impact

- Things an attacker can do:
  - Remove the MDM profile (along with associated apps, configuration and data)
  - Send MDM query commands (e.g., list apps, profiles, certificates)
  - Perform an action (lock, remote wipe)
  - Configure additional stuff (Wi-Fi/APN proxy settings, install apps)
Some Challenges

- Challenge: Client-side certificate validation
  - Not all MDMs enforce them
  - Mdm-Signature HTTP header
- Challenge: Reliance on APNS calls
  - Chaining consequent commands
- Challenge: MDM can query the profile list
  - The “invisible profile” is also hidden from the MDM
Current Status

- We reported to Apple the issue at the end of September, 2013
- Apple fixed the issue in 7.1 code (GA should be released soon)
- We are not aware of live exploitation of the issue
- We acknowledge Apple’s security team for dedication to the security of their products
Recommendations

- **End users:**
  - Maintain an up to date OS
  - Check your iOS for suspicious profiles
  - If you don’t have profiles, make sure you don’t have the profile menu

- **Organizations:**
  - Enforce OS updates
  - Implement network based solutions for your mobile devices

- **MDM Vendors:**
  - Verify client side certificates
  - Work with Apple on the MDM protocol issues
Thank you!

- twitter: @YairAmit, @AdiSharabani
- email: {yair,adi}@skycure.com
- blog: http://www.skycure.com/blog