Mobile Security Threats

Adi Sharabani
About me

**Adi Sharabani**
CEO & co-founder, Skycure

- Over 15 years of security experience
- Built and managed Watchfire's research group
- Built and led IBM's worldwide Rational security initiative, was responsible for IBM software products, developed by thousands of developers worldwide
- Author of more than 20 patents
- Fellow at Yuval Ne'eman's workshop
- High school teacher
• Provides seamless security for mobile devices
• Sell to large organizations
• Backed by Pitango Venture Capital
• Team consists of elite security experts coming from IBM, Google, CheckPoint and more
5 Biggest Mobile Threats
The Simple Threat
Physical Access
The Known Threat
Malware

Skycure
The Known Threat
Malware

2

Skycure
2012: The year of Android malware

Android Threat Growth

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

App Characteristics
- One Store
- Heavy Screening
- App Sandboxing

Source: Apple's App Sandbox Design Guide
iOS Security Model

App Characteristics
- One Store
- Heavy Screening
- App Sandboxing

Profile Characteristics
- No Store
- No Screening
- No Sandboxing

Profiles break the iOS security model
For iOS, the incarnation of malware is malicious configuration profiles.

Profiles break the iOS security model

Recent relevant Skycure discovery
http://blog.skycure.com/2013/03/malicious-profiles-sleeping-giant-of.html
Welcome to iOS Streamer

Watch TV shows and movies free online. Stream your favorite content directly to your iOS device.

Click to install streaming profile

Hacker gains access to your mail, business apps, cloud services, bank accounts and more, even if traffic is encrypted.
The Biggest Threat
Wi-Fi Networks
Mobile Security Threats

Wi-Fi Attacks

Are you comfortable connecting to Wi-Fi networks?

Did you know that connecting to a public Wi-Fi could lead to **persistent** control over your device?
Wi-Fi attacks become more prevalent with mobile use. These attacks have two main requirements:

- Attacker has to be in a nearby location
- User has to actively connect to the Wi-Fi

Mar 2013: Malicious iOS profiles
MiTM has become fully remote
“I hardly connect to wi-fi networks, so I’m protected. Right?”
“I hardly connect to Wi-fi networks. Is that right?”

Wrong!
Auto Connect
“I have never connected to Wi-Fi networks, so I’m protected. Right?”
“I have never connected to Wi-Fi networks. I'm not sure if that's right?”

Wrong!
In practice, many carrier settings configure wi-fi networks on user behalf.
In practice, many carrier settings configure Wi-Fi networks on user behalf.

```
AIS_th.bundle CW_tt.bundle Claro_gt.bundle
ATT_US.bundle CW_wi.bundle Claro_hn.bundle
AVEA_tr.bundle CarrierLab.bundle Claro_jm.bundle
Aircel_in.bundle Celcom_my.bundle Claro_ni.bundle
Bell_ca.bundle CellC_za.bundle Claro_pa.bundle
BhartiAirtel_in.bundle Cellcom_il.bundle Claro_pe.bundle
Bouygues_fr.bundle Chunghwa_tw.bundle Claro_pr.bundle
CMCC_cn.bundle Claro_ar.bundle Claro_py.bundle
CSL_hk.bundle Claro_br.bundle Claro_sv.bundle
CTM_mo.bundle Claro_cl.bundle Claro_uy.bundle
CW bs.bundle Claro_cr.bundle Comcel_co.bundle
CW_pa.bundle Claro_do.bundle Comviq_se.bundle
Sakin:/System/Library/Carrier Bundles/iPhone root#  
```
In practice, many carrier settings configures wi-fi networks on user behalf.

Setting-up such a network would automatically initiate an attack on all nearby carrier customers.
Putting the attack to test

Attack - During the cyber security conference

• Location: Smolarz Auditorium, TAU
Attack - During the cyber security conference

- Location: Smolarz Auditorium, TAU
- **448** devices connected to our in **2.5** hours
So what should you do about this?

- **Users and Organizations:**
  - Close the Wi-Fi connection when not in use
  - Use a mobile firewall protection

- **Carriers and Wi-Fi network providers:**
  - If you need to provide Wi-Fi access, enable client-side firewall capabilities on it

Contact us for more information:

Join our beta program
contact@skycure.com
The Growing Threat

Vulnerabilities in Apps and OS
The Growing Threat

Vulnerabilities in Apps and OS
The Growing Threat

Vulnerabilities in Apps and OS

iOS 6.0.1
Apple Inc.
69.9 MB

This update contains improvements and bug fixes.

Learn More

Download and Install
The Leaking Threat

Privacy

2012: Skycure uncovers a major privacy violation in the LinkedIn app

LinkedIn leaked out its users’ calendar information

Skycure’s discovery in the news

```json
{"calendar":{"calendarOptIn":true,"values":{"events":[]}}}
```

The New York Times
Forbes
BBC
The Verge
The Huffington Post
Washington Post
The Next Web
Gizmodo
Ars technica
Apple Insider
CSO Online
cnet
Following our work, LinkedIn changed their app to ask the user for permission to leak out the information.

When it comes to organizations, the problem is still unsolved.
Following our work, LinkedIn changed their app to ask the user for permission to leak out the information.

When it comes to organizations, the problem is still unsolved.
A Few Tips

1. Enable “Find Phone” features
2. Do not automatically click “Continue”
3. Be cautious when using public Wi-Fi networks
4. Always update your software
5. Follow me on Twitter: 
   My Twitter @AdiSharabani

Contact us contact@skycure.com
Website http://www.skycure.com
Blog http://blog.skycure.com
Twitter @SkycureSecurity
Backup Slides