DUDE, WHERE IS MY LAPTOP? - RELOADED

Dublin 2013
Simón Roses Fenerling

- Founder & CEO, VULNEX  www.vulnex.com
- Blog:  www.simonroses.com
- Twitter:  @simonroses
- Former Microsoft, PwC, @Stake
- DARPA Cyber Fast Track award on software security project
- Black Hat, RSA, OWASP, SOURCE, AppSec, DeepSec, TECHNET
TALK OBJECTIVES

• Examination of Anti-Theft products
• In a mobile world are we safe?
• If stolen, what can they do?
All Anti-Theft solutions are considered safe until proven guilty by a security review.

Neither the authors or VULNEX support in any way the robbery and/or manipulation of electronic devices, nor shall be held liable or responsible for the information herein.
AGENDA

1. Overview
2. Issues & Weaknesses
3. Vulnerabilities & Attacks
4. Conclusions
1. Overview
1. TERMINOLOGY NIGHTMARE: NO ESCAPE!

- **BYOx Family**
  - **BYOD:** Bring Your Own Device
  - **BYOT:** Bring Your Own Technology
  - **BYOP:** Bring Your Own Phone
  - **BYOPC:** Bring Your Own PC

- **Mxx Family**
  - **MDM:** Mobile Device Management
  - **MAM:** Mobile Application Management
  - **MDP:** Mobile Data Protection
  - **MDS:** Mobile Data Security
1. PHONES & LAPTOPS CONTAIN YOUR LIFE

- Emails
- Contacts
- Photos
- Social Networks
- Bank Accounts
- Password Managers
- Access to corporate / internal servers
- Apps
- You name it...
1. LOST & STOLEN STATISTICS

- “10,000 mobiles phones stolen per month in London” (that’s 314 phones per day)
  London Metropolitan Police (2013)

- “Lost and stolen cellphones could cost U.S. consumers more than $30 billion this year”
  Lookout (2012)

- “Laptop theft totaled more than $3.5 million dollars in 2005”
  FBI

- FBI statistics reveal that 221,009 laptops were reported stolen in 2008 and 2009

- 67,000 phones likely to be lost or stolen during London Olympics
  http://www.venafi.com/67000-phones-likely-to-be-lost-or-stolen-during-london-olympics/
1. ANTI-THEFT FEATURES

- Encrypt & protect information
- Remote Wipe files, directory or system
- Lock screen
- Sound alarm & alert window
- Sent info to C&C:
  - Screenshot
  - Webcam photo
  - Wireless (Access Point) name
  - GPS location
  - IP
- Claim to:
  - Offer strong security
  - Help recovering device
1. SEA OF ANTI-THEFT: PRODUCTS BY NUMBERS

- Antivirus houses have also joined the party...
1. ANTI-THEFT CLAIMS: JUST RELAX

Rest safe.

What we do
We Simplify
Enterprise
Mobility

THE SECURE
WORKSPACE

Find your laptop, see who's using it, even what they're wearing!

Lose it. Track it. Find It!

Keep your device safe & your safer
2. Issues & Weaknesses
2. PREVIOUS WORK ON THE SUBJECT

• “Deactivate the Rootkit”
  Alfredo Ortega & Anibal Sacco
  http://www.blackhat.com/presentations/bh-usa-09/ORTEGA/BHUSA09-Ortega-DeactivateRootkit-SLIDES.pdf

• Issues
  – Huge privacy risk (bad/no authentication)
  – Anyone could activate it with enough privileges
  – Anyone can change the configuration
  – Anyone can de-activate it (at least in certain known cases)
  – Whitelisted by AV (potentially undetectable)
2. LACK OF THREAT MODELING (TM)

- How data is protected (Rest / Transit)?
- If stolen can Anti-Theft really:
  - Can data really be wiped?
  - Can device be recovered?
  - Can tampering be detected and stopped?
  - How resilient are we?
- No understanding of the threats

Because...
2. NOT ALL THIEVES ARE SO SEXY...
2. THIEF TACTICS

- Network Analysis & Attacks
- System Analysis & Attacks
- Reverse Engineering Apps
  - Android
  - iOS
  - Windows
  - MacOS
3. Vulnerabilities & Attacks
4. HIDE IN PLAIN SIGHT... RIGHT!
3. ALL KIND OF INFORMATION DISCLOSURE

Thief: snooping the network

<table>
<thead>
<tr>
<th>Person Names</th>
<th>Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS coordinates</td>
<td>OS version</td>
</tr>
<tr>
<td>Phone Numbers</td>
<td>Application Internals</td>
</tr>
</tbody>
</table>

Emails
3. CLEAR TEXT SECRETS (IN TRANSIT): LOCATEMYLAPTOP (WINDOWS)
3. CLEAR TEXT SECRETS (IN TRANSIT): MITRACKER (WINDOWS)

POST /control/Interface/GetInfo.ashx? HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: WebQueryLib
Host: www.mitracker.com
Content-Length: 72
Cache-Control: no-cache

\[\text{name=\text{johnhard}, pword=\text{temp}, mac=00-0C-29-4A-F1-3A, position=, tag=query} HTTP/1.1 200 OK\]
Content-Type: text/plain; charset=utf-8

\[
\{
\text{name":"ok", pword":"ok", mac":"ok", ip":"213.37.127.115", email":"john.hardverga@gmail.com", privilege:"0", regdate:"2013-02-10", status:"0", description":", adddate:"2013-02-10 11:44:11"}
\]

Entire conversation (702 bytes)
3. CLEAR TEXT SECRETS (IN TRANSIT): PREY (IOS)
3. PHYSICAL ACCESS TO DEVICE

• Thief
  – Shield device in a Faraday box / bag

  – Break device security
    • Recovery modes
    • Android
      – Maybe already rooted?
      – USB debugging
    • Passcode bypass
    • Forensic LIVE CD
    • Jailbreak tools
3. CLEAR TEXT SECRETS (AT REST): ANTIDROIDTHEFT (ANDROID)
3. CLEAR TEXT SECRETS (AT REST): WHERE’S MY DROID (ANDROID)

```
hellraiser:platform-tools conde$ ./adb shell
# cd /data/data/com.alienmanfc6.wheresmyandroid/shared_prefs
# ls
Pontiflex.xml
PrefFile.xml
openudid_prefs.xml
# cat PrefFile.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <boolean name="enable_passcode" value="true" />
  <string name="response_log">02/10 11:14PM-App opened~02/10 11:16PM-Declined new terms~02/10 11:24PM-App opened~02/10 11:24PM-Accepted new terms~02/10 11:26PM-Correct passcode entered~02/20 08:23PM-App opened</string>
  <int name="run_count_two" value="1" />
  <long name="last_login_time" value="1360535198217" />
  <int name="nag_count" value="1" />
  <string name="attention_string">WMD Ring</string>
  <boolean name="setup_finished" value="false" />
  <int name="terms_acct" value="1" />
  <string name="saved_passcode">1234</string>
  <long name="Pontiflex_last_ad_time" value="1360535098085" />
  <string name="attention_gps_string">WMD GPS</string>
</map>
```
3. ANTI-THEFT CRYPTO FAILS

• No crypto at all...

• Weak cryptographic algorithms
  – MD5 no salt
  – SHA1
3. LOCK DOWN BYPASS: PREY

- DEMO
3. SECURE WIPE (AND RECOVERY) I

- Apps do not have secure delete capabilities, relies on a delete() call from OS

- SD Cards many times do not get deleted
  - Some Apps not configured by default
3. SECURE WIPE (AND RECOVERY) II

- Thief: Remove SD Card as soon device is stolen!
- Use forensic tools to recovered Data if device wiped
  - Windows: Use any LIVE CD/DVD forensic
  - Android
    - Open Source Android Forensics Toolkit
      http://sourceforge.net/projects/osaftoolkit/
    - iCare Recovery Android
  - iPhone
    - Iphone Analyzer
      http://sourceforge.net/projects/iphoneanalyzer/
    - iOS Forensic research
      http://www.iosresearch.org/
3. SECURE WIPE (AND RECOVERY) III
3. SECURE WIPE (AND RECOVERY) IV
3. JHV DEFUSER I

• “John Hard Vegas, Anti-Theft defuser”

• Features:
  – Fingerprint Anti-Theft
  – Steal credentials
  – Disable Anti-Theft

• .NET (XP-Win8)
3. JHV DEFUSER II

• Current Anti-Theft apps defused
  (* Windows only):
  – Prey
  – LaptopLock
  – Bak2u / Phoenix
  – Snuko
  – LocateLaptop

• More to come and other platforms...
3. JHV DEFUSER III

- Detect Anti-Theft
- Disable Anti-Theft
- Steal Credentials
3. INSERT ROOTKIT TO STOLEN DEVICE – SUBVERTING ANTI-THEFT

1. Stolen device
2. Shield device
3. Tamper device
4. Install Rootkit
5. Enable Anti-Theft and return device
6. User happy again 😊
3. MITM ATTACK ON ANTI-THEFT

• DEMO
3. ANOTHER MITM ATTACK

You have 3 days left of Trial period! Please activate your copy to protect your device!
3. ANOTHER MITM ATTACK
3. ANOTHER MITM ATTACK

HTTP/1.1 200 OK
Date: Thu, 28 Feb 2013 12:09:06 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=vgxcmvtdfhyv8ouq4x0ms030b7; path=/
Vary: Accept-Encoding
Content-Type: text/html
Content-Length: 90

{"response":{"status":"failure","message":"The activation pin is invalid.","key":"00000"}
3. ANOTHER MITM ATTACK

![Error message for activation pin is invalid]

The activation pin is invalid. Try again.
3. ANOTHER MITM ATTACK

Response from http://www.bak2u.com:80/api/registerWin/?api_key=1234567890&firstName=john%20hard%20vegas&email=john@hardhardvegas.com&macAddress=00-0C-29-35-99-1E&operatingSystem=jnv%20005%2.

HTTP/1.1 200 OK
Date: Thu, 28 Feb 2013 12:07:10 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=fa255pg5ol1isd9dv4gmxb6b27; path=/

"response":{"status":"success","message":"The activation pin is invalid.","key":"00000"}
3. ANOTHER MITM ATTACK
3. WE WILL CONTROL THE HORIZONTAL. WE WILL CONTROL THE VERTICAL...
3. THIEF CRAFT

- Disable Anti-Theft remote if possible
- Mute sound on device
- Remove SD Card
- Shield it
- Break device security
- Collect user data
- Recover deleted data
3. AVOID BEING...

BUSTED

You know what you did.
4. Conclusions
4. RISKS SUMMARY

- Clear Text Secrets
  - At-Rest: Mobile Top 10 2012-M1 Insecure Data Storage
  - In-Transit: Mobile Top 10 2012 - M3 Insufficient Transport Layer Protection

- Poor Cryptographic Algorithm
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm

- Insecure Development Practices
  - Shipped with Debug
  - No data validation
  - NO SSL certification checks

- Privacy Violations

- Wiped data can be recovered (most of the time)

- Lack of Resilient & Security Defenses

- Easily defeated
4. OWASP MOBILE TOP 10 RISKS

- Insecure Data Storage
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Client Side Injection
- Poor Authorization and Authentication
- Improper Session Handling
- Security Decisions Via Untrusted Inputs
- Side Channel Data Leakage
- Broken Cryptography
- Sensitive Information Disclosure
4. THE UGLY TRUTH

• Anti-Theft products need to improve their security

• Some products need to change their claims
4. USER SECURITY

- Keep up on updates

- Enforce security defenses (usual suspects)
  - Firewall
  - Anti-virus
  - Encrypt device
  - Strong passwords
  - VPN

- Beware of public networks

- If Anti-Theft app installed, make sure it does what it claims!
4. ANTI-THEFT VENDORS

- Understand your threats!

- Build secure software, not security software

- Protect user data effectively
4. BE SAFE IF YOU CAN
4. Q&A

- Thanks!

- @simonroses / @vulnexsl