Mobile Devices Boom Hackers Are Ready. What About You?

Tomáš Rosa

crypto.hyperlink.cz



The one can be happy who has the technique. The one can survive, provided they understand it, too.

Jailbreak and Root

- Firmware patching aimed at user privileges escalation.
 - Finally, we can have unauthorized applications running with no sandbox and the root account at their disposal.
- On Android, installing a set-uid binary is usually enough.
 - So the term "rooting".
- On iOS, the situation is considerably more complicated.
 - Achieving root privileges is often just the beginning, since the runtime is still under Apple tight control.
 - So the term "jailbreaking".

iKee Worms Hit Jailbreakers in 2009

- Exploited default root password "alpine" in SSH on jailbroken phones.
- iKee.A was merely a joke of Australian hacker.
 - It offended users by Rick Astley pictures.
- iKee.B from Europe (probably different author) was a regular malware.
- The whole community of Jailbreakers is still so big to be an attractive target of tailored attacks.



photo by AFP

What Does It Mean Anyway

- Besides obvious warnings, there is one more thing to add.
- Do you wonder whether smart phone OS security can be broken?
 - You do not need to ask anymore.
- The worldwide verified proof is right here.
 - It is the Jailbreak in itself!

Failbreak

Privilege escalation exploit that does not end up with the full-fledged Jailbreak or Root.

- Anyway, suitable exploit with proper payload is far enough for real attack.
- Developer's profile registered at the iDevice is a perfect position to perform a kind of Failbreak.

Failbreak Detection

- Jailbreak/Root detectors usually check for its full-fledged variants including many macro-markers.
- Failbreak has a very good chance to pass undetected.
 - In other words can the mobile device protect company data against any determined attacker? No.

So, Be Careful!

- But... what does it mean to "be careful"?
 - Do not participate in pilot projects.
 - Since provisioning profiles open the door for untrusted code execution.
 - Avoid Mobile Device Management.
 - Since the mDM server has nearly full control over its enrolled devices.
 - Use HTTP<u>S</u> only and check the server certificate carefully.
 - Since remote exploits are probably never ending story.
 - Avoid any suspicious communication (Bluetooth, NFC, optical codes, etc.).
 - Since any data is a possible malware vector.
 - Et cetera, et cetera, et cetera...

Security Add-Ons ...and all the things like that

- In the best case, it would be a false notion of security.
 - Mobile attacks are highly specific and targeted ones.
 - Without radical privilege escalation, the "guarding" application is just an ordinary sandboxed(!) process.
- In the worst case, it would open a vital malware installation vector.
 - Imagine phishing attack recommending some "security enhancement".
 - The current model is that the ultimate device admin is its manufacturer. This will hardly get changed.
 - Memento: Quis custodiet ipsos custodes?

X-Platform Attacking

- Cross-Platform Attack (CPA)
 - Any dishonest interoperation of several malware components running on different computing platforms.
- Cross-Platform Infection (CPI)
 - Any way of CPA components spreading to their respective destinations.

True Lies

Eurograbber: A Smart Trojan Attack

Hackers' Methods Reveal Banking Know-How





Listen to Audio

The Eurograbber banking Trojan is an all-in-one hit, researchers say. It successfully compromises desktops and **mobile** devices, and has gotten around commonly used two-factor **authentication** practices in Europe.

How can banking institutions defend themselves and their customers

against this super-Trojan attack? It may seem cliché, but Darrell Burkey, who oversees intrusion prevention products at Internet-threat-protection provider Check Point Software Technologies, says defense hinges on consumer behavior.

http://www.bankinfosecurity.com/eurograbber-smart-trojan-attack-a-5359/op-1

No Client Cooperation Required

- Contrary to the pioneering approaches used by ZitMo, Spitmo, and the Eurograbber scenario...
 - ... the cross-platform infections reflected hereafter run smoothly with <u>no points of</u> <u>particular cooperation with the client</u>.
 - We can think about generation-2 attacks.

USB Link Cross-Platform Infection

- Discussed by Stavrou and Wang at BlackHat DC 2011.
 - O Exploits USB protocol stack
 vulnerabilities for infection spreading in
 both ways (CPI computer ↔ mobile).
- The original proof-of-concept can be further extended.

Immediate Extensions

- CPI computer → iPhone during iTunes synchronization via e.g.:
 - limera1n boot ROM exploit (iPhone 4, 3GS),
 - http://theiphonewiki.com/wiki/Limera1n
 - AFC2 service running on Jailbroken devices.
 - http://theiphonewiki.com/wiki/AFC

Yet-Another Incarnation

- Discussed by Lau, Jang, and Song at BlackHat US 2013 this summer.
 - Malicious public charging station silently installs malware into connected iDevices.
 - Exploits weak authorization concept of USB protocol stack under iOS 6.
 - Does not require (but allows instead) Jailbreak or Failbreak.
 - Employes otherwise honest X-platform library www.libimobiledevice.org.
 - Protection is expected to get better with iOS 7.

NY: Solar Malware For Free



-Gmail Link Cross-Platform Infection

- Discussed by Rosa in 2011-2012.
 - o <u>http://crypto.hyperlink.cz/files/rosa_scforum12_v1.pdf</u>
 - Exploits Android services convergence in the Google portal.
- Based on reverse engineering of certain forensic technique by Cannon and Hoog (2011).
 - Originally named Screen Lock Bypass.
- CPI computer \rightarrow Android device.

Wi-Fi Link Cross-Platform Infection

- Discussed by Dmitrienko et al. at BlackHat AD 2012.
 - Exploits tight interconnection and certain implicit trust of devices in the WLAN of a typical home Wi-Fi.
- CPI computer \rightarrow Android device.
 - This was just a proof-of-concept demo.
 - CPI computer \rightarrow iOS device is also achievable.

Bring Your Own Device

■ My Devices						
macfric.local/mydevices/ C Search						
My Devices						
Devices	Profiles					
This iPhone						
Enroll this iPhone to allow it to be remotely managed.						
Once enrolled you will also be able to wipe all data from and lock access to this iPhone.						
Enroll						
Logout						

On One Hand

- There is a risk of company data disclosure.
 - Failbreak is the tool of first choice.
 - Passes bellow the Jailbreak radar.
 - Allows breaking into the company sandbox.
 - Brodie and Shulov at BlackHat US 2013

On the Other Hand Bring Break Your Own Device

Since: "By agreeing to the profile installation, the user's device is automatically enrolled without further interaction."

-- http://images.apple.com/iphone/business/docs/iOS_6_MDM_Sep12.pdf

- Zdziarski in "*Hacking and Securing iOS Applications*", 2012
- Sharabani at Herzliya 2013
- o Medin at Shmoocon 2013

BYOD Risks

- Ideal phishing or X-platform vector.
- Remote admin (hacker) is in perfect position to:
 - Sniff and modify internet communication incl. SSL/TLS.
 - Perform a Failbreak to install a malware.
 - Reset screen lock PIN.
 - Schuetz at BH US 2011 and Shmoocon 2012.

Hackers Are Ready...

Apple malware 'mobileconfig' allows remote hijacking of iPhones, iPads

March 25, 2013 10:52am



Configuration profile warning reminds us not to carelessly tap and install things on our iPhones and iPads

Still think your iPhone and iPad are safer than their Android counterparts? Don't get too smug J By Rene Ritchie, Wednesday, Mar 13, 2013 a 11:06 am yet.

Malicious profiles, or so-called "mobileconfigs," may yet show hackers the way into your Apple devices running iOS, security firm Skycure warned.

"A malicious profile could be used to remote control mobile activity and hijack user sessions," it said in a blog post.

Security firm: iOS Configuration Profiles could be vector for Apple's first big malware wave

By Matthew Panzarino, Tuesday, 12 Mar '13, 10:00am



ATA Scenario

Definition. Let the After-Theft Attack (ATA) be any attacking scenario that assumes the attacker has unlimited physical access to the user's smart device.

- Imagine somebody steals your mobile phone...
- Despite being really obvious threat, it is often neglected in many contemporary applications.
- By a robbery, the attacker can even get access to <u>unlocked screen or a synced computer</u>, hence receiving another considerable favor!

Be Aware of PIN Prints

- This can be any direct or indirect function value that:
 - o once known to the attacker,
 - can be used for a successful brute force attack on the PIN,
 - o under the particular attack scenario.
 - Rosa: The Decline and Dawn of Two-Factor Authentication on Smart Phones, ISS 2012
 - Rosa: Discovering PIN Prints in Mobile Applications, Security 2013
- Principally, the same applies to general passwords, too.
 - However, we can mitigate the risk by enforcing strong password policy here.

PIN Prints Examples

Plaintext obtained for the correct PIN:

RSAPrivateKey ::= SEQUENCE {

version Version. INTEGER, modulus publicExponent INTEGER, -- e privateExponent INTEGER, -- $d, d^*e \equiv 1 \pmod{\lambda(N)}$ INTEGER, $--p, p \mid N$ INTEGER, $--q, q \mid N$ prime1 prime2 INTEGER, INTEGER, exponent1 exponent2 coefficient INTEGER.

```
-- N, N = p^{*}q(\text{*other_factrs})
-- d_p, d_p = d \mod (p-1)
-- d_q, d_q = d \mod (q-1)
 - q_{inv}, q_{inv}^* q \equiv 1 \pmod{p}
```

-- ...

How to Exploit

- Plaintext obtained for <u>a wrong PIN</u> can be considered as a pseudorandom sequence.
 - The ASN.1 format rules as well as the algebraic relations are probably corrupted.
 - PIN searching hint do you remember analog TV tuning?
 - ...just turn the tuning knob until you get <u>any</u> <u>plausible</u> picture and sound...

TLS – Safe Forever, Whenever?

The fundamental rule is that higher levels must be cognizant of what their security requirements are and <u>never transmit</u> information over a channel less secure than what they require.

-- RFC 2246 (TLS 1.0), RFC 4346 (TLS 1.1), RFC 5246 (TLS 1.2)



In God We Trust. The others...

Implementations and users must be careful when deciding which certificates and certificate authorities are acceptable; <u>a dishonest</u> <u>certificate authority can do tremendous</u> <u>damage.</u>

-- RFC 2246 (TLS 1.0), RFC 4346 (TLS 1.1), RFC 5246 (TLS 1.2)



SSL Routinely Inspected? Sure.



Cryptographer's Comment

TLS protocol family is secure up to a finite set of vulnerabilities that can be practically avoided, provided we care about them actively.







Example of Blockwise Adaptive Chosen Plaintext Attack



Example of Adaptive Chosen Ciphertext Attack



To Have	and	То	Understand

N th	ice, but ere is only RC4 supported!	Certificate Protocol Support Key Exchange Cipher Strength 0 20 40	100 85 90 60 80 100
	Cipher Suites (sorted by strength; the server has no preference)		
<u> </u>	SSL_RSA_WITH_RC4_128_SHA (0x5)	128	
Ξ	Handshake Simulation	100	
		scanned by ww	w.ssllabs.com

- There is a feasible refined ciphertext-only attack rendering RC4 broken by AlFardan et al. at USENIX 2013.
- "...given the rather small security margin provided by RC4... [it] should henceforth be avoided in TLS, and deprecated as soon as possible..."

Conclusion

- Smart phones offer the highest security they ever did.
- However, the attacks intensity is also very high and still increasing.
- The threat model is changing significantly.
 - New attacks induced by new use-cases, rather than by e.g. astonishing cryptanalytic advances (X-platform, SSL/TLS, etc.).
- We really need to move very fast to even stand still. --JFK

Thank You For Attention



IT Security Trends and DMS Safety, Prague, Sep 17th 2013

Tomáš Rosa, Ph.D.

http://crypto.hyperlink.cz