Comp 116 Final Paper Outline

Stefan Dimitrov

October 31, 2013

Introduction

Problem: iOS jailbreaking has been stigmatized as a potential invitation for malware and security risks, while too much trust is placed in the walled garden model of software distribution through the App Store. How can we turn jailbreaking into an advantage?

To the Community

1. Jailbreaking allows for:
   - unrestricted security research on the iOS platform.
   - third party patches in response to security vulnerabilities.
2. This paper:
   - points out some security and privacy benefits of jailbreaking
   - uncovers pitfalls that could make jailbreaking a security risk

Privacy issues

1. UDID leaks [b]
2. Path address book fiasco
3. Apps sharing too much for no reason other than identification, data collection, etc.
4. ...

Security issues of stock-iOS devices

1. Methods for subverting the signing process on non jailbroken devices - a GBA emulator?s source code used to be available on github and could be compiled and installed without a developer account. ad hoc distribution using leaked udids

2. Methods for injecting obfuscated malicious code into an App Store app
3. Other methods of delivering malware
4. ...

Security issues of jailbreaken devices

1. Malicious/untrusted repositories
2. SSH attacks with default root password
3. Retaining a jailbreak means not updating to the latest iOS
4. ...

Security benefits of jailbreaking

1. Delivery of patches (jailbreak.me fix for pdf vulnerability)
2. Allows for security research, finding flaws and patching them
3. Enhancing privacy - on stock iOS7 camera access still unrestricted, ad location tracking [a]
4. Prevents *other* users from jailbreaking for malicious purposes (bypassing the lockscreen passcode lock for example) [c]
5. ...

Summary

References

iSAM: An iPhone Stealth Airborne Malware
`http://www.icsd.aegean.gr/publication_files/conference/62773319.pdf`

PiOS: Detecting Privacy Leaks in iOS Applications
`http://seclab.cs.ucsb.edu/media/uploads/papers/egele-ndss11.pdf`

Jekyll on iOS: When Benign Apps Become Evil
`http://www.cc.gatech.edu/~klu38/publications/security13.pdf`

A survey of mobile malware in the wild
`http://dl.acm.org/citation.cfm?id=2046618`

Exploiting the iOS Kernel
`http://media.blackhat.com/bh-us-11/Esser/BH_US_11_Esser_Exploiting_The_iOS_Kernel_WP.pdf`

Articles

[a] http://ios.wonderhowto.com/how-to/18-sneaky-privacy-betraying-settings-every-iphone-owner-must-know-about-ios-7-0148682/

[b] http://www.crowdstrike.com/blog/finspy-mobile-ios-and-apple-udid-leak/index.html

[c] http://www.zdnet.com/ios-7-apples-war-against-jailbreaking-now-makes-perfect-sense-7000016623/