Jekyll on iOS: When Benign Apps Become Evil

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

In addition to various standard security features, Apple adopts the mandatory app review and code signing mechanisms, to provide additional security. App review inspects every third party app, while code signing mechanism makes app signing mandatory and rejects unsigned app. Paper proposes a new attack method, which defeats both of those mechanisms. Using their attack method, an attacker can publish the malicious app, in spite of all the security mechanisms. The idea is, instead of submitting the app with malicious code, attackers create remotely exploitable backdoor, "decomposes the malicious logic into small code gadgets and hides them under the cover of the legitimate functionality"[1] or in other words, it lets the attacker to attack remotely by running the code gadgets, after it passes the initial app store review. Authors created "Jekyll" app which appears to be benign, but are capable of carrying out the malicious logic. This app is also capable of acting as a medium to attack other apps. Authors claim that their app, successfully passed Apple's review and they were able to launch malicious operations using this app.

2 Contribution

Authors showed that in spite of the app store security mechanisms, they were able to publish "Jekyll" app having a backdoor. They were able to breach Apple store's mandatory app review and code signing mechanisms. They claim that there are first to propose a dynamic analysis technique to discover the private APIs that can be used to do malicious activity (send messages, post tweets, etc.), without user's consent. They were able to launch remote attacks using the app backdoor, showing the ineffectiveness of the Apple's policy.

3 Strengths

I like that they showed that apple doesn't have any "backdoor check mechanism", which is a serious security flaw. I liked that they discussed the possible countermeasures which can be useful in general for most of the attacks.

4 Limitations

Some of those attacks (Like rebooting the device), may not work with iOS 6x, because of the introduction of new security features. The idea of run time security mechanisms are good but I think that this may incur a large overhead.

5 Future Work

Similar attack can be reproduced on Android phones, by publishing "Jekyll" kind of apps on play store. Authors provided some countermeasures, tough they have some flaws, building a flawless defense against these kind of attacks can be a future research work.

References

[1] Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee, *Jekyll on iOS: When Benign Apps Become Evil*, USENIX Security 13