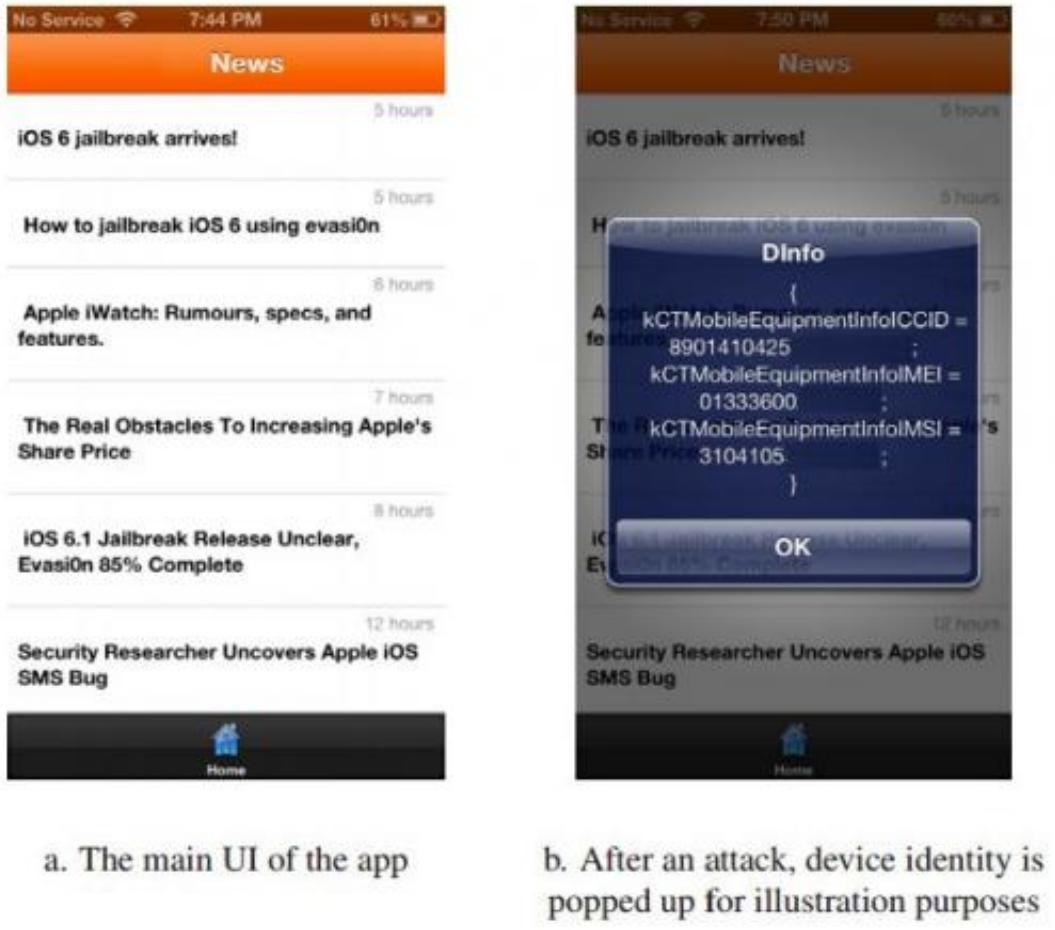
Apple's App Store review process missed Georgia Tech Jekyll

August 19 2013, by Nancy Owano



a. The main UI of the app

b. After an attack, device identity is popped up for illustration purposes

Snapshots of the app. Credit: Tielei Wang et al.

(Phys.org) —Georgia Tech researchers figured out a way to bypass Apple's safeguards in allowing new apps on the App Store. Apple adopts

review mechanisms to ensure that only approved apps can run on iOS devices and enjoys a good reputation for keeping malware at bay. That good reputation, however, cannot stop curious researchers from testing. They did succeed. They introduced some malware that the Apple Store review process did not catch. Why were they able to sneak past security screening and place a malicious app for sale? The team last week presented their paper which detailed their research, at the Usenix security symposium, which ran from August 14 to 16 in Washington, DC.

Titled "Jekyll on iOS: When Benign Apps Become Evil," authors Tielei Wang, Kangjie Lu, Long Lu, (a Stony Brook University researcher who participated with the team at Georgia Tech), Simon Chung, and Wenke Lee described how they were able to bypass security review. This is an app that can transform itself—over time. "Our method allows attackers to reliably hide malicious behavior that would otherwise get their app rejected by the Apple review process. Once the app passes the review and is installed on an end user's device, it can be instructed to carry out the intended attacks."

The Jekyll malware hit the jackpot in what a criminal would want to achieve. It could post tweets, send e-mails and texts, steal personal information and device ID numbers, take photos, and could direct Safari to a website with more malware. They introduced malicious control flows by rearranging signed code. Since the new control flows do not exist during the app review process, such "Jekyll" apps can elude detection when reviewed and can get Apple's approval. "Speci?cally," the authors wrote, "attackers can carefully plant a few arti?cial vulnerabilities in a benign app, and then embed the malicious logic by decomposing it into disconnected code gadgets and hiding the gadgets throughout the app code space."

New execution paths not in the app code mean the app appears benign at

the time of review, not violating any rules or seeming to have any functional malice. "However, when a victim downloads and runs the app, attackers can remotely exploit the planted vulnerabilities and in turn assemble the gadgets to accomplish various malicious tasks," they wrote. Overall, the paper highlighted shortcomings of the pre-release review approach and, as a recommendation, the authors called for more runtime monitoring mechanisms to protect iOS users in the future. "In summary," they said, "we advocate the of?cial support for runtime security monitoring mechanisms on iOS."

The Jekyll app was live for only a few minutes in March; it was not installed by anyone except the researchers, who used it on their Apple devices, attacking themselves and then withdrawing the app so that there would be no victims. The team made a full disclosure of the attack scheme to Apple in March and since then were in correspondence with Apple. An Apple spokesman told *MIT Technology Review* that the company, in response to issues raised in the paper, made some changes to the iOS mobile operating system.

More information: www.usenix.org/system/files/co … c13-paper_wang_2.pdf