PHYS.ORG

Georgia Tech uncovers iOS security weaknesses

July 31 2013

Researchers from the Georgia Tech Information Security Center (GTISC) have discovered two security weaknesses that permit installation of malware onto Apple mobile devices using seemingly innocuous applications and peripherals, uncovering significant security threats to the iOS platform.

"Apple utilizes a mandatory app review process to ensure that only approved apps can run on iOS devices, which allows users to feel safe when using any iOS app," said GTISC Associate Director Paul Royal, also a research scientist in the College of Computing. "However, we have discovered two weaknesses that allow circumvention of Apple's security measures."

Using different approaches, research scientists Tielei Wang and Billy Lau learned that malware can be installed onto iOS devices via Trojan Horse-style applications and peripherals. Wang's approach hides malicious code that would otherwise get rejected during the Apple review process. Once the malicious app passes review and is installed on a user's device, it can be instructed to carry out malicious tasks.

Wang's team developed a proof-of-concept attack, called Jekyll, which rearranges its own code to create new functionality that is not exhibited during Apple's approval process. This allows the malicious aspects of the app to remain undetected when reviewed and therefore obtain Apple's approval.

"We were able to successfully publish a malicious app and use it to remotely launch attacks on a controlled group of devices," said Wang. "Our research shows that despite running inside the iOS sandbox, a Jekyll-based app can successfully perform many malicious tasks, such as posting tweets, taking photos, sending email and SMS, and even attacking other apps—all without the user's knowledge."

Taking a different approach, Lau decided to investigate the extent to which security threats were considered when performing everyday activities such as charging a device. Lau and his team created a proof-of-concept malicious charger using a small, inexpensive single-board computer. Called Mactans, it can easily be constructed to resemble a normal iPhone or iPad charger. However, once plugged into an iOS device, Mactans stealthily installs a malicious app.

"Despite the plethora of defense mechanisms in iOS, Mactans was able to install arbitrary apps within one minute of being plugged into current-generation Apple devices running the latest operating system software," said Lau. "All users are affected, as our approach requires neither a jailbroken device nor user interaction."

Both Wang and Lau's teams notified Apple upon the discovery of these security weaknesses. Following GTISC's disclosure of Mactans, Apple implemented a feature in iOS 7 that notifies users when they plug their mobile device into any peripheral that attempts to establish a data connection. Apple has indicated that it is continuing to work on ways to address the weaknesses revealed through Jekyll and, as of yet, has not publicly released a solution.

"These results are concerning and challenge previous assumptions of iOS device security," said Royal. "However, we're pleased that Apple has responded to some of these weaknesses and hope that they will address our other concerns in future updates."

More information: Lau and Wang's findings are summarized in two papers: "Mactans: Injecting Malware into iOS Devices via Malicious Chargers," to be presented at the Black Hat USA 2013 conference July 27-Aug. 1 in Las Vegas; and "Jekyll on iOS: When Benign Apps Become Evil," to be presented at the 2013 USENIX Security Symposium August 14-16 in Washington, D.C.

Provided by Georgia Institute of Technology

Citation: Georgia Tech uncovers iOS security weaknesses (2013, July 31) retrieved 20 March

2024 from https://phys.org/news/2013-07-georgia-tech-uncovers-ios-weaknesses.html