PHYS.ORG

Hacking Gmail with 92 percent success

August 21 2014, by Sean Nealon

A team of engineers have developed a method that allows them to successfully hack into apps up to 92 percent of the time.

(Phys.org) —A team of researchers, including an assistant professor at the University of California, Riverside Bourns College of Engineering, have identified a weakness believed to exist in Android, Windows and iOS mobile operating systems that could be used to obtain personal information from unsuspecting users. They demonstrated the hack in an Android phone.

The researchers tested the method and found it was successful between 82 percent and 92 percent of the time on six of the seven popular apps they tested. Among the apps they easily hacked were Gmail, CHASE Bank and H&R Block. Amazon, with a 48 percent success rate, was the only app they tested that was difficult to penetrate.

The paper, "Peeking into Your App without Actually Seeing It: UI State Inference and Novel Android Attacks," will be presented Friday, Aug. 22 at the 23rd USENIX Security Symposium in San Diego. Authors of the paper are Zhiyun Qian, of the Computer Science and Engineering Department at UC Riverside; Z. Morley Mao, an associate professor at the University of Michigan; and Qi Alfred Chen, a Ph.D. student working with Mao.

The researchers believe their method will work on other operating systems because they share a key feature researchers exploited in the Android system. However, they haven't tested the program using the other systems.

The researchers started working on the method because they believed there was a security risk with so many apps being created by some many developers. Once a user downloads a bunch of apps to his or her smart phone they are all running on the same shared infrastructure, or operating system.

"The assumption has always been that these apps can't interfere with each other easily," Qian said. "We show that assumption is not correct and one app can in fact significantly impact another and result in harmful consequences for the user."

The attack works by getting a user to download a seemingly benign, but actually malicious, app, such as one for background wallpaper on a phone. Once that app is installed, the researchers are able to exploit a newly discovered public side channel—the shared memory statistics of a process, which can be accessed without any privileges. (Shared memory is a common operating system feature to efficiently allow processes share data.)

The researchers monitor changes in shared memory and are able to correlate changes to what they call an "activity transition event," which includes such things as a user logging into Gmail or H&R Block or a user taking a picture of a check so it can be deposited online, without going to a physical CHASE Bank. Augmented with a few other side channels, the authors show that it is possible to fairly accurately track in real time which activity a victim app is in.

There are two keys to the attack. One, the attack needs to take place at the exact moment the user is logging into the app or taking the picture. Two, the attack needs to be done in an inconspicuous way. The researchers did this by carefully calculating the attack timing.

"By design, Android allows apps to be preempted or hijacked," Qian said. "But the thing is you have to do it at the right time so the user doesn't notice. We do that and that's what makes our attack unique."

The researchers created three short videos that show how the attacks work. They can be viewed below:

Here is a list of the seven apps the researchers attempted to attack and their success rates: Gmail (92 percent), H&R Block (92 percent), Newegg (86 percent), WebMD (85 percent), CHASE Bank (83 percent), Hotels.com (83 percent) and Amazon (48 percent).

Amazon was more difficult to attack because its app allows one activity to transition to almost any other activity, increasing the difficulty of guessing which activity it is currently in.

Asked what a smart phone user can do about this situation, Qian said, "Don't install untrusted apps." On the operating system design, a more careful tradeoff between security and functionality needs to be made in the future, he said. For example, side channels need to be eliminated or more explicitly regulated.

More information: The paper is available online: www.cs.ucr.edu/~zhiyunq/pub/se … tivity_inference.pdf

Provided by University of California - Riverside

Citation: Hacking Gmail with 92 percent success (2014, August 21) retrieved 24 April 2024 from https://phys.org/news/2014-08-hacking-gmail-percent-success.html