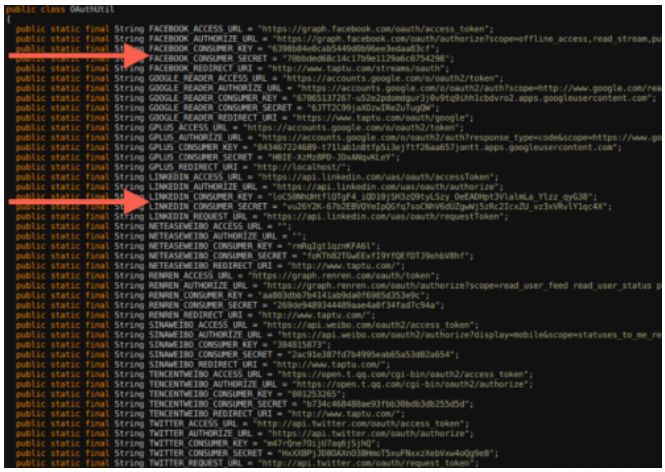
Researchers find thousands of secret keys in Android apps

18 June 2014



Some of the secret keys, including Facebook and LinkedIn, were discovered by PlayDrone, a tool developed by Columbia Engineering researchers that uses hacking techniques to circumvent Google security to successfully download Google Play apps and recover their sources. Credit: Columbia Engineering

In a paper presented—and awarded the prestigious Ken Sevcik Outstanding Student Paper Award—at the ACM SIGMETRICS conference on June 18, Jason Nieh, professor of computer science at Columbia Engineering, and PhD candidate Nicolas Viennot reported that they have discovered a crucial security problem in Google Play, the official Android app store where millions of users of Android, the most popular mobile platform, get their apps.

"Google Play has more than one million apps and over 50 billion app downloads, but no one reviews what gets put into Google Play—anyone can get a $25 account and upload whatever they want. Very little is known about what's there at an aggregate level," says Nieh, who is also a member of the University's Institute for Data Sciences and Engineering's Cybersecurity Center. "Given the huge popularity of Google Play and the potential risks to millions of users, we thought it was important to take a close look at Google Play content."

Nieh and Viennot's paper is the first to make a large-scale measurement of the huge Google Play marketplace. To do this, they developed PlayDrone, a tool that uses various hacking techniques to circumvent Google security to successfully download Google Play apps and recover their sources. PlayDrone scales by simply adding more servers and is fast enough to crawl Google Play on a daily basis, downloading more than 1.1 million Android apps and decompiling over 880,000 free applications.

Nieh and Viennot discovered all kinds of new information about the content in Google Play, including a critical security problem: developers often store their secret keys in their apps software, similar to usernames/passwords info, and these can be then used by anyone to maliciously steal user data or resources from service providers such as Amazon and Facebook. These vulnerabilities can affect users even if they are not actively running the Android apps. Nieh notes that even "Top Developers," designated by the Google Play team as the best developers on Google Play, included these vulnerabilities in their apps.

"We've been working closely with Google, Amazon, Facebook, and other service providers to identify and notify customers at risk, and make the Google Play store a safer place," says Viennot. "Google is now using our techniques to proactively scan apps for these problems to prevent this from happening again in the future."

In fact, Nieh adds, developers are already receiving notifications from Google to fix their apps and remove the secret keys.

Nieh and Viennot expect PlayDrone to lay a

foundation for new kinds of analysis of Android apps. "Big data is increasingly important and Android apps are just one form of interesting data," Nieh observes. "Our work makes it possible to analyze Android apps at large scale in new ways, and we expect that PlayDrone will be a useful tool to better understand Android apps and improve the quality of application content in Google Play."

Other findings of the research include:

- showing that roughly a quarter of all Google Play free apps are clones: these apps are duplicative of other apps already in Google Play
- identifying a performance problem resulting in very slow app purchases in Google Play: this has since been fixed
- a list of the top 10 most highly rated apps and the top 10 worst rated apps in Google Play that included surprises such as an app that, while the worst rated, still had more than a million downloads: it purports to be a scale that measures the weight of an object placed on the touchscreen of an Android device, but instead displays a random number for the weight

Good news for the hundreds of thousands of developers who upload content to Google Play and even more so for the millions of users who download the content!

More information: Paper: www.cs.columbia.edu/~nieh/pubs … cs2014_playdrone.pdf

Provided by Columbia University