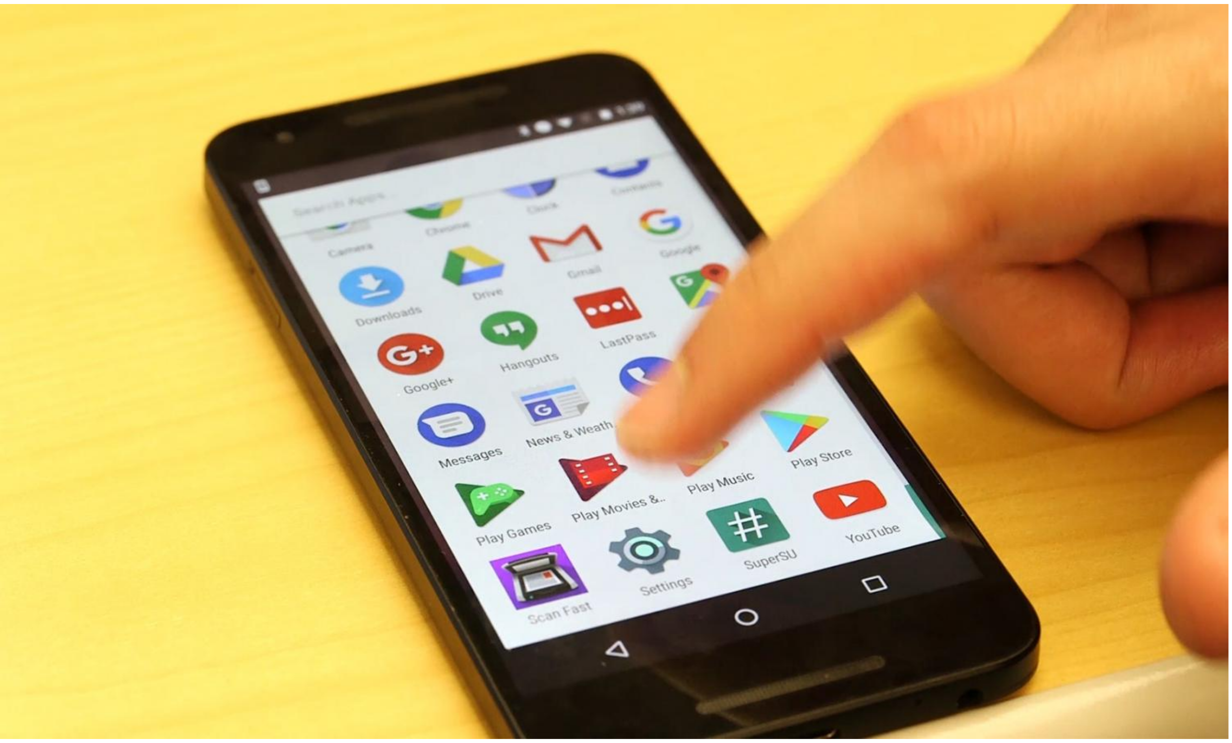
TechXplore

Combination of features produces new Android vulnerability

May 22 2017



Cybersecurity researchers have identified a new vulnerability affecting Android mobile devices that results not from a traditional bug, but from the malicious combination of two legitimate permissions that power desirable and commonly used features in popular apps. Credit: Maxwell Guberman, Georgia Tech

A new vulnerability affecting Android mobile devices results not from a traditional bug, but from the malicious combination of two legitimate permissions that power desirable and commonly-used features in popular apps. The combination could result in a new class of attacks, which has been dubbed "Cloak and Dagger."

The vulnerability, which was identified and tested in closed environments by computer scientists at the Georgia Institute of Technology, would allow attackers to silently take control of a mobile device, overlaying the graphical interface with false information to hide malicious activities being performed underneath - such as capturing passwords or extracting the user's contacts. A successful attack would require the user to first install a type of malware that could be hidden in a pirated game or other app.

Georgia Tech researchers have disclosed the potential attack to Google, maker of the Android system, and details of the vulnerability will be presented May 24 at the 38th IEEE Symposium on Security and Privacy in San Jose, California. But because it involves two common features that can be misused even when they behave as intended, the issue could be more difficult to resolve than ordinary operating system bugs.

"In Cloak and Dagger, we identified two different Android features that when combined, allow an attacker to read, change or capture the data entered into popular mobile apps," said Wenke Lee, a professor in Georgia Tech's School of Computer Science and co-director of the Institute for Information Security & Privacy. "The two features involved are very useful in mapping, chat or password manager apps, so preventing their misuse will require users to trade convenience for security. This is as dangerous an attack as we could possibly describe."

The research was sponsored by the National Science Foundation (NSF), Office of Naval Research (ONR) and the Defense Advanced Research Projects Agency (DARPA).

The first permission feature involved in the attack, known as "BIND_ACCESSIBILITY_SERVICE," supports the use of devices by disabled persons, allowing inputs such as user name and password to be made by voice command, and allowing outputs such as a screen reader to help the disabled view content. The second permission, known as "SYSTEM_ALERT_WINDOW," is an overlay or "draw on top" feature that produces a window on top of the device's usual screen to display bubbles for a chat program or maps for a ride-sharing app.

When combined in a malicious way, "SYSTEM_ALERT_WINDOW" acts as a cloak, while "BIND_ACCESSIBILITY_SERVICE" serves as the dagger. The two could allow attackers to draw a window that fools users into believing they are interacting with legitimate features of the app. The malicious program, operating as the overlay, would then capture the user's credentials for the malware author, while the accessibility permission would enter the credentials into the real app hidden beneath, allowing it to operate as expected, leaving the user with no clue that anything is awry.

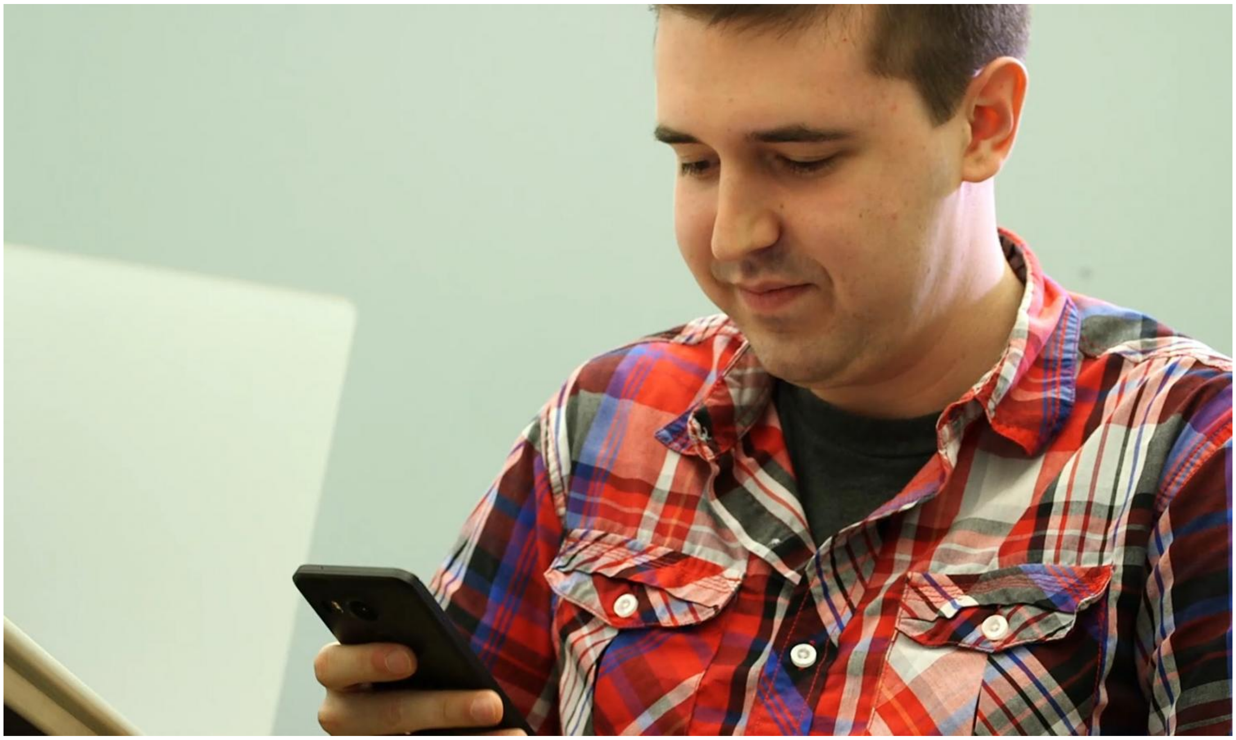
The researchers tested a simulated attack on 20 users of Android mobile devices and found that none of them noticed the attack.

Of most concern to Georgia Tech's researchers is that these permissions may be automatically included in legitimate apps from the Google Play store, meaning users do not need to explicitly grant permissions for the attack to succeed.

"This is a design flaw that some might say allows the app functionality to work as intended, but our research shows that it can be misused," said Yanick Fratantonio, the paper's first author and a Georgia Tech Ph.D. summer intern from the University of California Santa Barbara. "Once the phone is compromised, there may be no way for the user to understand what has happened."

Nearly 10 percent of the top 5,000 Android apps use the overlay feature, noted Fratantonio, and many are downloaded with the accessibility feature enabled.

While both permissions have been used separately as user-interface redressing attacks and "a11y attacks," previous research did not examine what happens when they are combined, noted Simon P. Chung, a research scientist at Georgia Tech's School of Computer Science and one of the study's co-authors.



Carter Yagemann, a graduate research assistant in Georgia Tech's School of Computer Science, checks permissions on an Android phone. Cybersecurity researchers have identified a new vulnerability affecting Android mobile devices that results not from a traditional bug, but from the malicious combination of two legitimate permissions that power desirable and commonly used features in popular apps. Credit: Maxwell Guberman, Georgia Tech

Creating vulnerabilities when permissions are combined may be a reality that system developers will have to consider more seriously in the future, Fratantonio said. "Changing a feature is not like fixing a bug," he explained. "System designers will now have to think more about how seemingly unrelated features could interact. Features do not operate separately on the device."

Android versions up to and including the current 7.1.2 are vulnerable to this attack. The researchers caution that it may be difficult to determine the status of the settings required for the attack.

There are two key precautions, Lee and Fratantonio agree. One is to avoid downloading apps from providers other than branded outlets such as the Google Play store. A second step is to check the permission requests that apps make before allowing them to operate.

"Users need to be careful about the permissions that new apps request," said Lee. "If there are very broad permissions, or the permissions don't seem to match what the app is promising to do, you need to be sure you really need that app."

The researchers have produced a video that shows the attack and how to check these permissions, which are in different locations depending on the mobile operating system version.

"Apps from name-brand sources such as Facebook, Uber and Skype should be okay," said Lee. "But with a random game or free versions of paid apps that you might download, you should be very careful. These features are very powerful and can be abused to do anything you could do as a user - without you knowing."

More information: Yanick Fratantonio, et al., "Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop," 38th IEEE Symposium on Security and Privacy, 2017.

Provided by Georgia Institute of Technology

Citation: Combination of features produces new Android vulnerability (2017, May 22) retrieved 2 May 2024 from https://techxplore.com/news/2017-05-combination-features-android-vulnerability.html