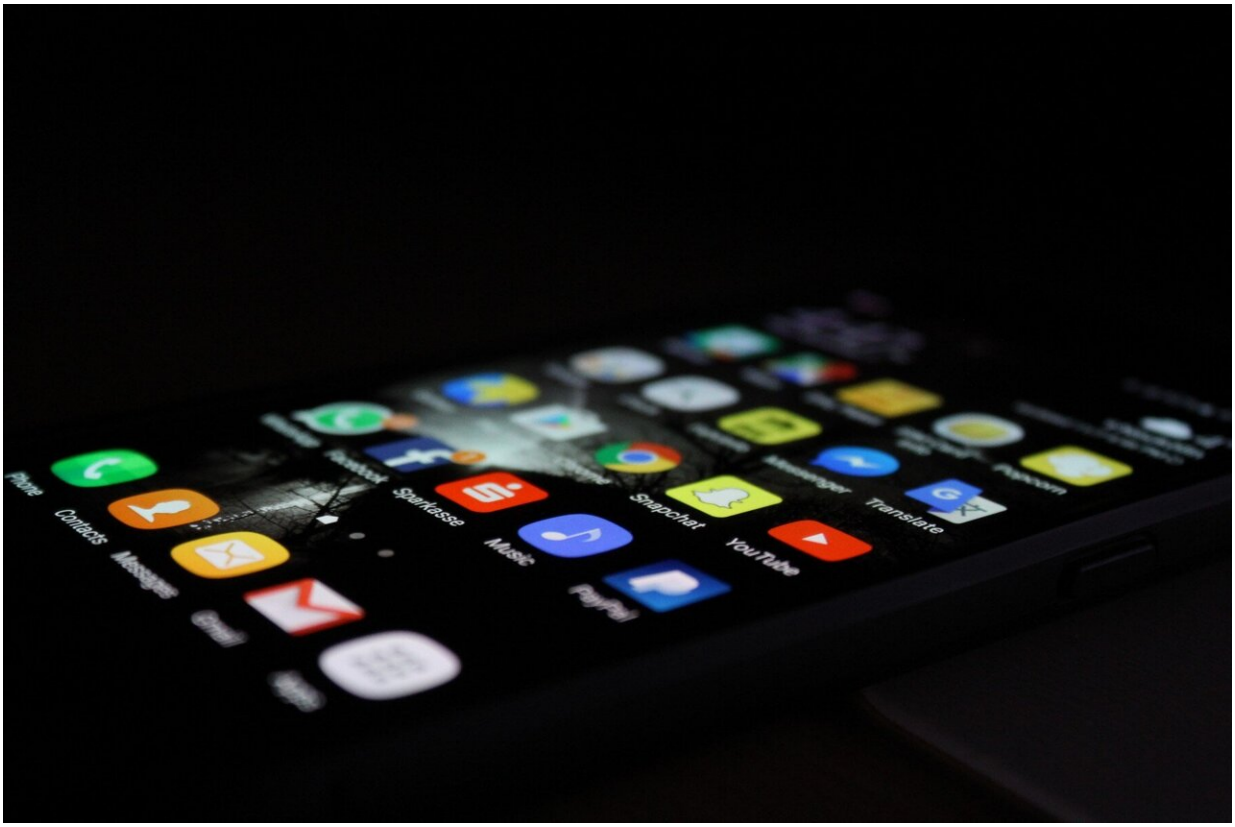
Some mobile phone apps may contain hidden behaviors that users never see

March 31 2020, by Laura Arenschield



A team of cybersecurity researchers has found that some apps have hidden "backdoor" secrets that could make them vulnerable to hacking. Credit: Rami Al-zayat on Unsplash

A team of cybersecurity researchers has discovered that a large number

of cell phone applications contain hardcoded secrets allowing others to access private data or block content provided by users.

The study's findings: that the apps on mobile phones might have hidden or harmful behaviors about which end users know little to nothing, said Zhiqiang Lin, an associate professor of computer science and engineering at The Ohio State University and senior author of the study.

The study has been accepted for publication by the 2020 IEEE Symposium on Security and Privacy in May. The conference has moved online because of the global coronavirus (COVID-19) outbreak.

Typically, mobile apps engage with users by processing and responding to user input, Lin said. For instance, users often need to type certain words or sentences, or click buttons and slide screens. Those inputs prompt an app to perform different actions.

For this study, the research team evaluated 150,000 apps. They selected the top 100,000 based on the number of downloads from the Google Play store, the top 20,000 from an alternative market, and 30,000 from pre-installed apps on Android smartphones.

They found that 12,706 of those apps, about 8.5 percent, contained something the research team labeled "backdoor secrets"—hidden behaviors within the app that accept certain types of content to trigger behaviors unknown to regular users. They also found that some apps have built-in "master passwords," which allow anyone with that password to access the app and any private data contained within it. And some apps, they found, had secret access keys that could trigger hidden options, including bypassing payment.

"Both users and developers are all at risk if a bad guy has obtained these 'backdoor secrets,'" Lin said. In fact, he said, motivated attackers could

reverse engineer the mobile apps to discover them.

Qingchuan Zhao, a graduate research assistant at Ohio State and lead author of this study, said that developers often wrongly assume reverse engineering of their apps is not a legitimate threat.

"A key reason why mobile apps contain these 'backdoor secrets' is because developers misplaced the trust," Zhao said. To truly secure their apps, he said, developers need to perform security-relevant user-input validations and push their secrets on the backend servers.

The team also found another 4,028 apps—about 2.7 percent—that blocked content containing specific keywords subject to censorship, cyber bullying or discrimination. That apps might limit certain types of content was not surprising—but the way that they did it was: validated locally instead of remotely, Lin said.

"On many platforms, user-generated content may be moderated or filtered before it is published," he said, noting that several social media sites, including Facebook, Instagram and Tumblr, already limit the content users are permitted to publish on those platforms.

"Unfortunately, there might exist problems—for example, users know that certain words are forbidden from a platform's policy, but they are unaware of examples of words that are considered as banned words and could result in content being blocked without users' knowledge," he said. "Therefore, end users may wish to clarify vague platform content policies by seeing examples of banned words."

In addition, he said, researchers studying censorship may wish to understand what terms are considered sensitive.The team developed an open source tool, named InputScope, to help developers understand weaknesses in their apps and to demonstrate that the reverse engineering

process can be fully automated.

Provided by The Ohio State University

Citation: Some mobile phone apps may contain hidden behaviors that users never see (2020, March 31) retrieved 23 February 2024 from https://techxplore.com/news/2020-03-mobile-apps-hidden-behaviors-users.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.