Android apps can conspire to mine information from your smartphone

April 3 2017, by Amy Loeffler

Associate Professor of Computer Science Daphne Yao (left), Fang Liu, doctoral candidate (center), and Assistant Professor of Computer Science Gang Wang (right), are co-authors on a first-of-its-kind large scale and systematic study that evaluated collusion between Android smartphone apps. Credit: Virginia Tech

Mobile phones have increasingly become the repository for the details

that drive our everyday lives. But Virginia Tech researchers have recently discovered that the same apps we regularly use on our phones to organize lunch dates, make convenient online purchases, and communicate the most intimate details of our existence have secretly been colluding to mine our information.

Associate Professor Daphne Yao and Assistant Professor Gang Wang, both in the Department of Computer Science in Virginia Tech[1]s College of Engineering, are part of a research team to conduct the first ever large-scale and systematic study of exactly how the trusty apps on Android phones are able to talk to one another and trade information.

Yao will present the team[1]s findings in Dubai at the Association for Computing Machinery Asia Computer and Communications Security Conference on April 3.

"Researchers were aware that apps may talk to one another in some way, shape, or form," said Wang. "What this study shows undeniably with real-world evidence over and over again is that app behavior, whether it is intentional or not, can pose a security breach depending on the kinds of apps you have on your phone."

The types of threats fall into two major categories, either a malware app that is specifically designed to launch a cyberattack or apps that simply allow for collusion and privilege escalation. In the latter category, it is not possible to quantify the intention of the developer, so collusion, while still a security breach, can in many cases be unintentional.

In order to run the programs to test pairs of apps, the team developed a tool called DIALDroid to perform their massive inter-app security analysis. The study, funded by the Defense Advanced Research Projects Agency as part of its Automated Program Analysis for Cybersecurity initiative, took 6,340 hours using the newly developed DIALDroid

software, a task that would have been considerably longer without it.

First author of the paper Amiangshu Bosu, an assistant professor at Southern Illinois University, spearheaded the software development effort and the push to release the code to the wider research community. Fang Liu, a fifth year Ph.D. candidate studying under Yao, also contributed to the malware detection research.

"Our team was able to exploit the strengths of relational databases to complete the analysis, in combination with efficient static program analysis, workflow engineering and optimization, and the utilization of high performance computing. Of the apps we studied, we found thousands of pairs of apps that could potentially leak sensitive phone or personal information and allow unauthorized apps to gain access to privileged data," said Yao, who is both an Elizabeth and James E. Turner Jr. '56 andL-3 Faculty Fellow.

The team studied a whopping 110,150 apps over three years including 100,206 of Google Play[1]s most popular apps and 9,994 malware apps from Virus Share, a private collection of malware app samples. The set up for cybersecurity leaks works when a seemingly innocuous sender app like that handy and ubiquitous flashlight app works in tandem with a receiver app to divulge a user[1]s information such as contacts, geolocation, or provide access to the web.

The team found that the biggest security risks were some of the least utilitarian. Apps that pertained to personalization of ringtones, widgets, and emojis.

"App security is a little like the Wild West right now with few regulations," said Wang. "We hope this paper will be a source for the industry to consider re-examining their software development practices and incorporate safeguards on the front end. While we can[1]t quantify

what the intention is for app developers in the non-malware cases we can at least raise awareness of this security problem with mobile apps for consumers who previosuly may not have thought much about what they were downloading onto their phones."

Provided by Virginia Tech