RetroScope opens doors to the past in smart phone investigations

August 3 2016

Purdue University researchers are working on a new technique that could aid law enforcement in gathering data from smart phones when investigating crimes.

A research team led by Dongyan Xu, professor of computer science and interim executive director of Center for Education and Research in Information Assurance and Security, and fellow Purdue computer science professor Xiangyu Zhang will detail findings of the technique, called RetroScope, during the USENIX Security Symposium Aug. 10-12 in Austin, Texas.

The increasing use of mobile technology in today's society has made information stored in the memory of smart phones just as important as evidence recovered from traditional crime scenes.

Xu said RetroScope was developed in the last nine months as a continuation of the team's work in smart phone memory forensics. The research moves the focus from a smart phone's hard drive, which holds information after the phone is shut down, to the device's RAM, which is volatile memory.

"We argue this is the frontier in cybercrime investigation in the sense that the volatile memory has the freshest information from the execution of all the apps," he said. "Investigators are able to obtain more timely forensic information toward solving a crime or an attack."

Although the contents of volatile memory are gone as soon as the phone is shut down, it can reveal surprising amounts of forensic data if the device is up and running.

The team's early research resulted in work published late last year that could recover the last screen displayed by an Android application. Building on that, Xu said, it was discovered that apps left a lot of data in the volatile memory long after that data was displayed.

To uncover that data, Purdue doctoral student Brendan Saltaformaggio theorized that rather than focusing on searching for that data, the phone's graphical rendering code could be retargeted to specific memory areas to obtain and bring up several previous screens shown by an app.

RetroScope makes use of the common rendering framework used by Android to issue a redraw command and obtain as many previous screens as available in the volatile memory for any Android app. Improving on the previous research, RetroScope requires no previous information about an app's internal data.

The screens recovered, beginning with the last screen the app displayed, are presented in the order they were seen previously. "Anything that was shown on the screen at the time of use is indicated by the recovered screens, offering investigators a litany of information," Xu said.

In testing, RetroScope recovered anywhere from three to 11 previous screens in 15 different apps, an average of five pages per app. The apps ranged from popular social media platforms Facebook and Instagram to more privacy-conscious apps and others.

"We feel without exaggeration that this technology really represents a new paradigm in smart phone forensics," he said. "It is very different from all the existing methodologies for analyzing both hard drives and

volatile memories."

Xu said RetroScope takes care of a lot of manual "dirty work" for a smart phone forensics investigator. However, it also raises questions about how much is available for recovery from a person's smart phone.

"I was personally amazed by the lack of in-memory app data protection," he said. "One would expect these privacy-sensitive apps to have more completely shredded the information that was previously displayed.

"I should get peace of mind that none of my privacy-sensitive information lingers in the live memory. I know by doing this research that we don't get that."

Purdue researchers looked at the issue from the other side, attempting to determine how to disrupt the RetroScope tool. Xu and his team characterized efforts to disrupt RetroScope as a trade-off between privacy and usability.

"We realize the dilemma that arises from zeroing every bit and byte of information previously displayed. By doing that your app will run very slowly to regenerate that information when needed again and the usability of the app will degrade," he said. "We don't see an easy solution or easy way to bypass this."

More information: Purdue researchers are scheduled to present "Screen after Previous Screens: Spatial-Temporal Recreation of Android App Displays from Memory Images" from 4-6 p.m. Aug. 12 at the USENIX Security Symposium in Austin, Texas.

Provided by Purdue University