TechXplore

Researchers uncover a hardware security vulnerability on Android phones

April 4 2022, by Maggie Lindenberg

Credit: Unsplash/CC0 Public Domain

Could your smartphone be spying on you?

Hopefully not, and if so, not for long, thanks to a team of researchers at the University of Pittsburgh Swanson School of Engineering.

Their recent study found that the Graphics Processing Unit (GPU) in some Android smartphones could be used to eavesdrop on a user's credentials when the user types these credentials using the smartphone's on-screen keyboard, making it an effective target for hacking. This hardware security vulnerability exposes a much more serious threat to user's sensitive personal data, compared to the previous attacks that can only infer the user's coarse-grained activities, such as the website being visited or the length of the password being typed.

"Our experiments show that our attack can correctly infer a user's credential inputs, such as their username and password, without requiring any system privilege or causing any noticeable shift in the device's operations or performance. Users wouldn't be able to tell when it's happening," said Wei Gao, associate professor of electrical and computer engineering, whose lab led the study. "It was important to let manufacturers know that the phone is vulnerable to eavesdropping so that they can make changes to the hardware."

A phone's GPU processes all of the images that appear on the screen, including the pop-up animations when a letter of the on-screen keyboard is pressed. The researchers were able to correctly infer which letters or numbers were pressed more than 80 percent of the time, based only on how the GPU produces the displayed keyboard animations.

"If someone were to take advantage of this weakness, they could build a benign application—like a game or other app—and embed malicious code into it that would run silently in the background after it's installed," said Gao. "Our experimental version of this attack could successfully target usernames and passwords being entered in online banking, investment, and credit reporting apps and websites, and we have proved that the embedded malicious codes in the app cannot be correctly detected by the Google Play Store."

The researchers focused their experiments on the Qualcomm Adreno GPU, but this method could potentially be used for other GPUs, as well. The team reported their findings to Google and Qualcomm, and Google confirmed that they will release an Android security update later this year to address the concern.

The paper, "Eavesdropping User Credentials via GPU Side Channels on Smartphones," was coauthored by Boyuan Yang, Ruirong Chen, Kai Huang, Jun Yang, and Wei Gao. It was presented at the ASPLOS Conference, held Feb. 28 through March 4, 2022, in Lausanne, Switzerland.

More information: Conference: asplos-conference.org/

Provided by University of Pittsburgh

Citation: Researchers uncover a hardware security vulnerability on Android phones (2022, April 4) retrieved 18 April 2024 from https://techxplore.com/news/2022-04-uncover-hardware-vulnerability-android.html