Research finds novel defense against sophisticated smartphone keyloggers

September 5 2016, by Tiffany Westry

Credit: University of Alabama at Birmingham

Researchers at the University of Alabama at Birmingham have found a novel and practical way to combat malicious attacks on motion sensors inside mobile devices.

In a study published in proceedings of the 9th Association for

Computing Machinery Conference on Security & Privacy in Wireless and Mobile Networks, associate professor Nitesh Saxena, Ph.D., and Ph.D. students Prakash Shrestha and Manar Mohamed have created a way to defend mobile device users against motion-based touchstroke leakage with the injection of noise.

Previous research shows that, much like the way a hacker can covertly capture inputs made from a regular computer keyboard, it is also possible to capture a user's inputs on a touchscreen. Currently, motion sensors on Android devices can be accessed by any application downloaded to the device, without a user's being prompted to give permission. By tricking a user into unknowingly downloading a malicious program, hackers could obtain sensitive information like passwords and PINs by tracking the vibrations made from the touchscreen and decoding the movements based on a keyboard's layout. Given the accuracy rate of this type of attack, mobile security experts consider it a significant threat to user privacy and are exploring methods to combat it.

"Most mobile platforms have established a sensor security access control model," Saxena said. "Android follows a model where read access to many sensitive sensors, like a phone's camera or microphone, is very restrictive or requires special permissions granted by the user. However, the read access to other sensors, like inertial sensors, is not restricted because Android may not consider these sensors explicitly sensitive. This openness in the Android sensor security architecture has given rise to potentially significant threat of motion-based side channel attacks."

By utilizing a recently developed framework called SMASheD (Sniffing and Manipulating Android Sensor Data), initially created as a malicious application, the study's authors built a defense mechanism called Slogger that can be used to thwart sensor-based touchstroke logging attacks. As a user enters sensitive information, Slogger transparently inserts noisy

sensor readings in order to obscure the original readings. Slogger works in the background of a device and is completely unnoticeable to a user and other trusted applications. It can be installed through the Android Debug Bridge, without the need to root the device or change its operating system.

To test Slogger's effectiveness, the authors compromised an Android device using two of the latest touchstroke logging algorithms developed for touchstroke detection and inference. During this type of attack, the start and end points of a user's taps are monitored. With data recorded by the accelerometer, a hacker could determine whether a user is holding the device vertically or horizontally. They can also predict what areas of the screen were tapped by applying machine learning tools. Later, by mapping the predicted areas with the standard keyboard layout, a hacker can determine the series of taps.

After installing the malicious application, the authors also installed Slogger. Upon being installed, Slogger prompts the user to do a series of typing tests, holding the device in various positions. This allows Slogger to learn the range of the sensor values based on the user's typing style. The user types while holding the phone in his or her hand and while it is lying on a flat surface. The values are later used to set the range of values for injecting noise during an attack.

"During the evaluation phase, we implemented Slogger in such a way that, whenever the user launches the application used for the attack, a noise inject request is sent to the Slogger server," Saxena said. "When the user closes the application, a request to stop Slogger is sent. The application can also be updated to send an inject request whenever the keyboard is running or whenever a user is entering sensitive information."

Slogger searches for system files related to motion sensors such as an

accelerometer or gyroscope, and injects noise until it receives a request to stop, like when the application being used for the malicious attack is closed. Without Slogger, the touchstroke detector had an 85 percent rate of accuracy. Once the Slogger application was enabled, the touchstroke detector was unable to detect any touchstrokes. During the touchstroke inference test, there was a 90 percent accuracy rate without Slogger. Slogger was able to reduce inference accuracy to 56 percent while the device lay on a flat surface. While the user held the device, inference accuracy was reduced by more than 20 percent.

During the evaluation, the authors discovered Slogger was also highly effective in minimizing touchstroke leakage even when more than one motion sensor is leveraged by an attacker.

More information: Slogger: Smashing Motion-based Touchstroke Logging with Transparent System Noise. dl.acm.org/citation.cfm?id=2939924

Provided by University of Alabama at Birmingham