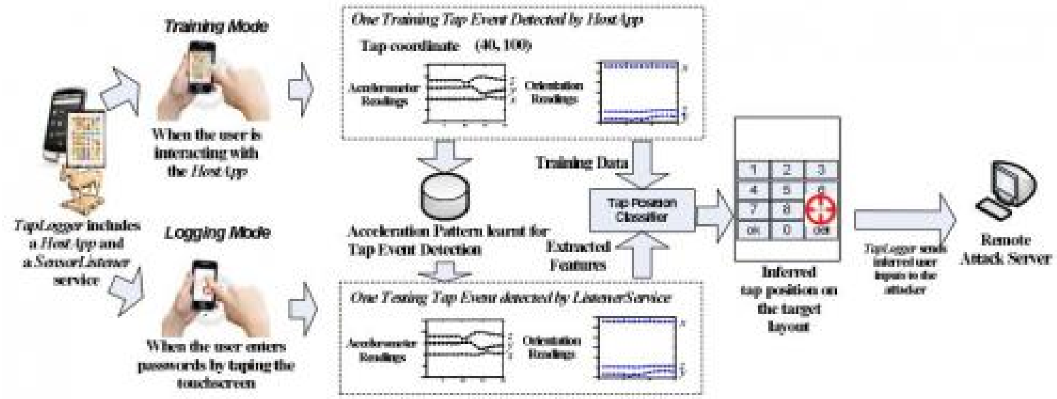
Stealth game steals info from Android sensors

April 24 2012, by Nancy Owano


Training Mode
When the user is interacting with the Host App
TapLogger includes a HostApp and a SensorListener service
Logging Mode
When the user enters passwords by taping the touchscreen
One Training Tap Event Detected by HostApp
Tap coordinate (40, 100)
Accelerometer Readings
Orientation Readings
Training Data
Acceleration Pattern learnt for Tap Event Detection
Tap Position Classifier
Extracted Features
One Testing Tap Event detected by ListenerService
Accelerometer Readings
Orientation Readings
1 2 3
4 5 6
7 8
ok 0 del
Inferred tap position on the target layout
TapLogger sends inferred user inputs to the attacker
Remote Attack Server

The attack overview

(Phys.org) -- No joke. A proof-of-concept application for phones running Android pretends to be a fun challenge asking the user to identify identical icons from a bunch of images. All the while the app monitors sensors to identify user information such as PINs and SS numbers. In brief, you are looking at a Trojan that can track what you type into your phone using your phone's motion sensors. The Trojan’s final feat is uploading the info on to the attacker’s controlled computer. The sensor-snooping app is called TapLogger and it was designed to prove a point: Android has yet another security design weakness that allows installed apps free access to motion sensor readings.

In the case of the rogue game, it picks up the Android phone‘s accelerometer, gyroscope, and orientation sensors to infer digits entered into the device. Attackers would not directly get your keystrokes, but they would get the screen area where you tapped, and reference that with how that lines up with the digital keyboard. *Ars Technica* details how it works: “By logging the precise changes along three dimensions—azimuth, pitch, and roll—the Trojan makes educated guesses about the touchscreen regions that were tapped to generate the orientation changes. TapLogger then maps those regions to the user interface of the screenlock or dial pad of a specific Android phone.”

To crack a four-digit PIN using information from TapLogger, a thief can narrow the number of tries to 81 with an average of a 100-percent chance of success. Using TapLogger to crack a six-digit PIN generates a search space of 729 likely combinations with an average success rate of 80 percent.

The team from Pennsylvania State University and IBM who designed the Trojan app are Zhi Xu, a PhD candidate at PSU, Kun Bai, a researcher at IBM and Sencun Zhu, an associate professor at PSU. They presented their paper, “TapLogger: Inferring User Inputs On Smartphone Touchscreens Using On-board Motion Sensors” to the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks in Tucson, Arizona, which ran from April 16 to April 18.

If mobile sensors are the next big thing for the mobile device industry to pursue as new features, mobile sensors will also be the next big area for security thieves to exploit. The problem, say the researchers, is that thieves may get a head start toward an easy target. “While the applications relying on mobile sensing are booming, the security and privacy issues related to such applications are not well understood yet,” say the paper’s authors. “People are still unaware of potential risks of unmanaged sensors on smartphones. To prevent such types of attacks, we see an urgent need for sensing management systems on the existing commodity smartphone platforms.”

In implementing TapLogger as an Android application, the proof-of-concept app did not require any security permission to access the accelerometer and orientation sensors. While the team worked up an Android application, Android may not be the only platform at issue.“The fundamental problem here,” Zhi Xu told *Ars Technica*, “is that sensing is unmanaged on existing smartphone platforms." iOS devices are not vulnerable to such attacks, unless they are jailbroken. The authors did not discuss on-board sensors in Blackberry devices but they said,”We will address it in our future work.”

More information: Research paper: www.cse.psu.edu/~szhu/papers/taplogger.pdf

Citation: Stealth game steals info from Android sensors (2012, April 24) retrieved 27 April 2024 from https://phys.org/news/2012-04-stealth-game-info-android-sensors.html