SensorID: Sensor Calibration Fingerprinting for Smartphones*

Jiexin Zhang[1], Alastair R. Beresford[1], Ian Sheret[2]

1 University of Cambridge
2 Polymath Insight Limited

1 Abstract

Sensors are an essential component of many computer systems today. Mobile devices are a good example, containing a vast array of sensors from accelerometers and GPS units, to cameras and microphones. Data from these sensors are accessible to application programmers who can use this data to build context-aware applications. Good sensor accuracy is often crucial, and therefore manufacturers often use per-device factory calibration to compensate for systematic errors introduced during manufacture. In this talk we present a new type of fingerprinting attack on sensor data: *calibration fingerprinting*. A calibration fingerprinting attack infers the per-device factory calibration data from a device by careful analysis of the sensor output alone. Such an attack does not require direct access to any calibration parameters since these are often embedded inside the firmware of the device and are not directly accessible by application developers.

We demonstrate the potential of this new class of attack by performing calibration fingerprinting attacks on the inertial measurement unit sensors found in iOS and Android devices. These sensors are good candidates because access to these sensors does not require any special permissions, and the data can be accessed via both a native app installed on a device and also by JavaScript when visiting a website on an iOS and Android device. We find we are able to perform a very effective calibration fingerprinting attack: our approach requires fewer than 100 samples of sensor data and takes less than one second to collect and process into a device fingerprint that does not change over time or after factory reset. We demonstrate that our approach is very likely to produce globally unique fingerprints for iOS devices, with an estimated 67 bits of entropy in the fingerprint for iPhone 6S devices. In addition, we find that the accelerometer of Google Pixel 2 and Pixel 3 devices can also be fingerprinted by our approach. Following our disclosure, Apple applied one of our suggested fixes for this vulnerability in iOS 12.2.

*This paper will appear at the IEEE Symposium on Security and Privacy (S&P) 2019