BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2024
http://excel.fit.vutbr.cz

Security Risks of Mobile Device Sensors

Kateřina Henclová*

Abstract

In this work, we present the threats to mobile security and privacy exposed by mobile sensors. We introduce the Generic Sensor API, the mobile sensors, and ways they can be misused. Using the mobile sensors like the accelerometer, gyroscope and magnetometer, we demonstrate such an attack on mobile sensors in the browser. The chosen attack is activity recognition, which performs its activity prediction using machine learning.

*xhencl02@vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

Privacy and security in today's world are ever-growing concerns. With smartphones that we carry with us everywhere in our daily lives, we are constantly connected. Smartphones get many opportunities to collect data about their users without user consent, such as through Web API when the user visits websites. Unfortunately, it is a common practice to use data collected through such methods to track users across the internet, exposing their privacy and exploiting user information for monetary gain or other benefits [1].

The options to capture people's lives are greater when we take into account the power of mobile sensors. What was designed to help users seems to be more often used to monitor users and their environment. The mobile phone sensors, such as the accelerometer, gyroscope, ambient light sensor, or magnetometer, can also be accessed by websites via the Generic Sensor API, without asking for user permission.

2. What kind of attacks are possible using mobile sensors?

In many previous studies on this subject, we can find that it is possible to attack users with the data collected from the sensors.

Users can be subject to PIN skimming [2], map the inside of the building [3] recognize the video being played on TV [4] or cross device linking [5, 3], all with just using the ambient light sensor.

The accelerometer can be used for decoding vibrations from a nearby keyboard [6], classify human walking patterns [7] and infer the trajectory of a route [8].

With the gyroscope, you can do speech recognition [9] and or identify the speaker or gender [10] and use Magnetometers to detect and identify nearby objects [5] or track what apps run on the phone [11, 12].

Although these studies may be fascinating, the threats stemming from them are dire.

3. Activity recognition

The chosen attack on mobile sensors to demonstrate is activity recognition. With the use of data from the Accelerometer, Gyroscope and Magnetometer, we can determine what the current action of the user holding the phone is. The attack page is online and accessible on the URL `https://feta5.fit.vutbr.cz/attack/`.

An activity recognition attack can provide many pieces of information about the user, especially if we collect a whole set of records of daily actions and activities. For example, it wouldn't be hard to assume when the user regularly leaves their home to commute to work and deduce if the mode of transport is by car or a bus. Or we could monitor how much of an active lifestyle the user has, or if they are sick or old. Overall, these cases can hint information about the user's daily routines, living conditions or their social status if enough data is collected.

The attack is carried out through using the Generic Sensor API, not needing user permission to access the mobile sensor readings. This attack is possible on Android phones, with browsers that expose sensor

data by default, such as Chrome, Edge, Opera and other Chromium based browsers. Firefox, Brave, Safari and other privacy-oriented browsers don't enable access to sensor readings, as well as iOS phones. Also, important to mention, that access to the sensors is only granted to websites that are currently active and visible on the phone, limiting opportunities to collect sensor data in the background.

To implement this attack, we trained an activity classifier that receives live sensor data every 5 seconds, extracts features, predicts the current activity and logs the results. To train this classifier, we collected a large set of sensor readings corresponding to an activity, such as lying, sitting, standing, walking, phone on table, taking the bus, taking the car, taking the train or taking the tram. A training and testing dataset of 1282 items worth the time of 13 hours was collected, from November 2023 till April 2024, and used to build the activity classifier.

4. Classifier results

What we produced by this work is a proof of concept example of an attack that could be realized through the Generic Sensor API. We created 3 classifier models, each with a different classifier algorithm. We created a Decision tree model, which reached a prediction accuracy of 0.5836, a Random forest model with an accuracy of 0.7030 and a LightGBM model, which we are currently using for the activity recognition, reaching the best accuracy rate of 0.7128. There is still a lot of room for future improvement of the classifiers, but the results are good enough to use for our attack to show users the risks resulting from exposing sensor data.

More interesting is studying the confusion matrix we use to visualize the individual classifier testing results. We can see in our LightGMB classifier, that recognizing walking and phone on table activities is something our classifier can do very well. It manages well enough car recognition, confusing it with a bus, and tram recognition, also confused with the other rail vehicle which is the train. Most problematic is standing and sitting, which the classifier confuses with most of the other activities.

5. Conclusions

The Generic Sensor API is a useful tool that allows developers to access and use sensor data in a consistent and standardized way, but unfortunately gives opportunity to violate user privacy and security. In order to mitigate these threats, the user can make some changes on their mobile device.

The first thing the user may consider, especially if they see their sensor data being exposed on our page, is to choose a better browser that increases user privacy, such as Brave or Firefox. They may also consider getting a different device, such as iOS, that requires permission before sensors can be accessed. But if they do not want to change their digital environment, they should at least visit the browser settings and disable access to the sensors in Site Settings.

To illustrate the potential risks to sensor security, an attack using the mobile sensor data was devised. We hope this serves as a reminder of the importance of considering the security implications of sensor data and taking appropriate measures to protect it.

Acknowledgements

For valuable advice, help and information throughout the year, I would very much like to thank Ing. Radek Hranický, Ph.D., who provided me with his expert guidance. I would also like to thank Ing. Libor Polčák, Ph.D., for his assistance in the data collection process and everyone who helped collect sensor data.

References

[1] Gunes Acar Amogh Pradeep Anupam Das, Nikita Borisov. The web's sixth sense: A study of scripts accessing smartphone sensors. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 1515–1532. Association for Computing Machinery, October 2018.

[2] Raphael Spreitzer. Pin skimming: Exploiting the ambient-light sensor in mobile devices. volume 2014, 11 2014.

[3] Lukasz Olejnik. Privacy analysis of ambient light sensors. online, 08 2016.

[4] Lorenz Schwittmann, Viktor Matkovic, MatthE4;us Wander, and Torben Weis. Video recognition using ambient light sensors. In *2016 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 1–9, 2016.

[5] Libor Polčák, Giorgio Maone, Marek Saloň, and Radek Hranický. Jshelter website. online.

[6] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp)iphone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, page 551–562, New York,

NY, USA, 2011. Association for Computing Machinery.

[7] Akram Bayat, Amirhossein Bayat, and Sina Amir. Classifying human walking patterns using accelerometer data from smartphone. 12 2017.

[8] Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, and Joy Zhang. Accomplice: Location inference using accelerometers on smartphones. pages 1–9, 01 2012.

[9] Yan Michalevsky, Dan Boneh, and Gabi Nakibly. Gyrophone: Recognizing speech from gyroscope signals. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 1053–1067, San Diego, CA, August 2014. USENIX Association.

[10] S Abhishek Anand, Chen Wang, Jian Liu, Nitesh Saxena, and Yingying Chen. Motion sensor-based privacy attack on smartphones, 2020.

[11] Nikolay Matyunin, Yujue Wang, Tolga Arul, Kristian Kullmann, Jakub Szefer, and Stefan Katzenbeisser. Magneticspy: Exploiting magnetometer in mobile devices for website and application fingerprinting. In *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*, CCS '19. ACM, November 2019.

[12] Lukasz Olejnik. Privacy analysis of web browser access to magnetometer sensor. online, 06 2020.