informatics

Article

What Is This Sensor and Does This App Need Access to It? [†]

Maryam Mehrnezhad * and Ehsan Toreini *

School of Computing, Newcastle University, Newcastle upon Tyne NE4 5TG, UK

* maryam.mehrnezhad@ncl.ac.uk (M.M.); ehsan.toreini@ncl.ac.uk (E.T.)

† This paper was presented at the International Workshop on Socio-Technical Aspects in Security and Trust (STAST), Orlando, FL, USA, 5 December 2017.

Received: 30 November 2018; Accepted: 18 January 2019; Published: 24 January 2019

Abstract: Mobile sensors have already proven to be helpful in different aspects of people's everyday lives such as fitness, gaming, navigation, etc. However, illegitimate access to these sensors results in a malicious program running with an exploit path. While the users are benefiting from richer and more personalized apps, the growing number of sensors introduces new security and privacy risks to end users and makes the task of sensor management more complex. In this paper, first, we discuss the issues around the security and privacy of mobile sensors. We investigate the available sensors on mainstream mobile devices and study the permission policies that Android, iOS and mobile web browsers offer for them. Second, we reflect the results of two workshops that we organized on mobile sensor security. In these workshops, the participants were introduced to mobile sensors by working with sensor-enabled apps. We evaluated the risk levels perceived by the participants for these sensors after they understood the functionalities of these sensors. The results showed that knowing sensors by working with sensor-enabled apps would not immediately improve the users' security inference of the actual risks of these sensors. However, other factors such as the prior general knowledge about these sensors and their risks had a strong impact on the users' perception. We also taught the participants about the ways that they could audit their apps and their permissions. Our findings showed that when mobile users were provided with reasonable choices and intuitive teaching, they could easily self-direct themselves to improve their security and privacy. Finally, we provide recommendations for educators, app developers, and mobile users to contribute toward awareness and education on this topic.

Keywords: mobile sensors; IoT sensors; sensor security; security education; app permission; mobile security awareness; user privacy; user security; sensor attacks

1. Introduction

According to the Economist [1], smartphones have become the fastest-selling gadgets in history, outselling personal computers (PCs) four to one. Today, about half the adult population owns a smartphone; by 2020, 80% will. Mobile and smart device vendors are increasingly augmenting their products with various types of sensors such as the Hall sensor, accelerometer, NFC (Near-Field Communication), heart rate, and iris scan, which are connected to each other through the Internet of Things (IoT). We have observed that around 10 new sensors have been augmented or became popular in mainstream mobile devices in less than two years; bringing the number of mobile sensors to more than 30 sensors. Examples include FaceID, Active edge, depth camera (using infra-red), thermal camera, air sensor, laser sensor, haptic sensor, iris scan, heart rate and body sensors.

Sensors are added to mobile and other devices to make them smart: to sense the surrounding environment and infer aspects of the context of use, and thus to facilitate more meaningful interactions with the user. Many of these sensors are used in popular mobile apps such as fitness and games. Mobile sensors have also been proposed for security purposes, e.g., authentication [2,3], authorization [4], device pairing [5] and secure contactless payment [6]. However, malicious access to sensor streams results in an installed app running in the background with an exploit path. Researchers have shown that the user PINs and passwords can be disclosed through sensors such as the camera and microphone [7], the ambient light sensor [8] and the gyroscope [9]. Sensors such as NFC can also be misused to attack financial payments [10].

In our previous research [11–14], we have shown that the sensor management problem is spreading from apps to browsers. We proposed and implemented the first JavaScript-based side channel attack revealing a wide range of sensitive information about users such as phone calls' timing, physical activities (sitting, walking, running, etc.), touch actions (click, hold, scroll and zoom) and PINs on mobile phones. In this attack, the JavaScript code embedded in the attack web page listens to the motion and orientation sensor streams without needing any permission from the user. By analysing these streams via machine learning algorithms, this attack infers the user's touch actions and PINs with an accuracy of over 70% on the first try. The above research attracted considerable international media coverage (springeropen.altmetric.com/details/18717318/news) including the Guardian [15] and the BBC [16], which reassures the importance of the topic. We disclosed the identified vulnerability described in the above to the industry. While working with W3C and browser vendors (Google Chromium, Mozilla Firefox, Apple, etc.) to fix the problem, we came to appreciate the complexity of the sensor management problem in practice and the challenge of balancing security, usability and functionality.

Through a series of user studies over the years [13,14], we concluded that mobile users are not generally familiar with most sensors. In addition, we observed that there is a significant disparity between the actual and perceived risk levels of sensors. In another work [17], the same conclusion was made by Crager et. al. for motion sensors. In [14], we discussed how this observation, along with other factors, renders many academic and industry solutions ineffective at managing mobile sensors. Given that sensors are going beyond mobile devices, e.g., in a variety of IoT devices in smart homes and cities, the sensor security problem has already attracted more attention not only from researchers, but also from hackers. In view of all this, we believe that there is much room for more focus on people's awareness and education about the privacy and security issues of the sensor technology.

Previous research [14,17] has focused on individual user studies to study human aspects of sensor security. In this paper, we present the results of a more advanced teaching method—working with sensor-enabled apps—on the risk level that users associate with the PIN discovery scenario for all sensors. We reflect the results of two interactive workshops that we organized on mobile sensor security. These workshops covered the following: an introduction of mobile sensors and their applications, working with sensor-enabled mobile apps, an introduction of the security and privacy issues of mobile sensors and an overview of how to manage the app permissions on different mobile platforms.

In these workshops, the participants were sitting in groups and introduced to mobile sensors by working with sensor-enabled apps. Throughout the workshops, we asked the participants to fill in a few forms in order to evaluate the general knowledge they had about mobile sensors, as well as their perceived risk levels for these sensors after they understood their functionalities. After analysing these self-declared forms, we also measured the correlation between the knowledge and perceived risk level for mobile sensors. The results showed that knowing sensors by working with sensor-enabled apps would not immediately improve the users' security inference of the actual risks of these sensors. However, other factors such as the prior general knowledge about these sensors and their risks have a strong impact on the users' perception. We also taught the participants about the ways that they could audit their apps and their permissions including per app vs. per permission. Our participants found both models useful in different ways. Our findings show that when mobile users are provided with reasonable choices and intuitive teaching, they can easily self-direct themselves to improve their security and privacy.

In Section 2, first, we list the available sensors on mobile devices and categorise them. Then, we present the current permission policies for these sensors on Android, iOS, and mobile web browsers. In Section 3, we present the structure of these workshops in full detail. Section 4 includes our analysis on the general knowledge and perceived risk levels that our participants had for sensors and their correlation. Section 5 presents our observations of the apps' and permissions' review activities in the workshops. In Section 6, we present a list of our recommendations to different stakeholders. Finally, in Sections 7 and 8, we include limitations, future work and the conclusion.

2. Mobile Sensors

As stated, there are more than 30 sensors on mobile devices. Both iOS and Android, as well as mobile web browsers allow native apps and JavaScript code in web pages to access most of these sensors. Developers can have access to mobile sensors either by (1) writing native code using mobile OS APIs [18,19], (2) recompiling HTML5 code into a native app [20] or (3) using standard APIs provided by the W3C, which are accessible through JavaScript code within a mobile browser (w3.org/TR/#tr_Javascript_APIs).

As shown in [21], the average number of permissions used by Android apps increases over time, in particular for popular apps and free apps. These permissions are requested for having access to the operating system (OS) resources such as contacts and files, as well as sensors such as GPS and microphone. This has the potential to make apps over-privileged and unnecessarily increases the attack surface.

2.1. Mobile Sensors' Categorization

We present a list of available sensors on various mobile devices. We prepared this list by inspecting the official websites of mainstream mobile devices; iPhone X (support.apple.com/kb/SP770?locale=en_US), Samsung Galaxy S9 (samsung.com/uk/smartphones/galaxy-s9/specs/), Google Pixel 2 (store.google.com/gb/product/pixel_2_specs) and the specifications that W3C (w3.org/2009/dap/) and Android [18] and Apple [19] provide for developers. We propose to categorize these sensors into four main groups: identity-related (biometric) sensors, communicational sensors, motion sensors and ambient (environmental) sensors, as presented in Table 1. Note that this list can be even longer if all mobile brands are included. For example, the Cat S61 smart phone (catphones.com/en-gb/cat-s60-smartphone/#technical-specs) has sensors such as a thermal camera, an air sensor (measures the quality of the environmental air), and a laser sensor (to measure distance).

Table 1. Categorization of current mobile sensors.

Category	Sensors
Identity-related (Biometric)	GPS, Camera, Microphone, Fingerprint (TouchID), FaceID, Iris Scan, Heart Rate (HR), Touch Screen, Active Edge, Haptic Sensor, Body Sensors
Communicational	WiFi, Bluetooth, NFC
Motion	Gyroscope, Accelerometer, Rotation, Orientation, Motion, Sensor Hub
Ambient (Environmental)	Temperature (Ambient, Device), Humidity, Pressure (Barometer), Light, Proximity, Gravity, Magnetic Field, Hall Sensor

In Appendix A, we present a brief description of each sensor. With the growing number of sensors on mobile devices, categorising them into a few groups is much more difficult than before. Some of these sensors can belong to multiple groups. For example, one might argue that GPS belongs to the environmental category; however, since it is associated with people's identities, we propose to keep it in the identity-related category. Similarly, the sensor hub monitors the device's movements, which is associated with the user's activities. Hence, it is difficult to decide to which category (motion or biometric) it belongs.

2.2. Sensor Management Challenges

In Table 2, we present how Android, iOS, and W3C spec (followed by mobile browsers) treat different sensors in terms of access. We have used Android and Apple Developer websites and W3C specifications and caniuse.com to build this table [18,19,22,23]. As can be seen, permission policies for having access to different sensors vary across sensors and platforms. We argue that sensing is still unmanaged on existing smartphone platforms. The in-app access to certain sensors including GPS, camera and microphone requires user permission when installing and running the app. However, as Simon and Anderson discussed in [7], an attacker can easily trick a user into granting permission through social engineering (e.g., presenting it as a free game app). Once the app is installed and the permission approved, usage of the sensor data is not restricted. On the other hand, access to many other sensors including accelerometer, gyroscope and light is unrestricted; any app can have free access to the sensor data without needing any user permission, as these sensors are left unmanaged on mobile operating systems.

Table 2. Current permission policies of sensors on different platforms. ✓: permission required, ✗: permission not required, NA: not supported, and Locked: not open to developers. * NFC should be turned on manually for any program to be able to use it.

Sensor	**Android**	**iOS**	**W3C/Web Browsers**
GPS	✓	✓	✓
Camera	✓	✓	✓
Microphone	✓	✓	✓
Fingerprint/TouchID	✓	✓	NA
Touch Screen	✗	✗	✗
FaceID	✓	✓	NA
Iris Scan	✓	✓	NA
Heart Rate (HR)	✓	✓	NA
Body Sensors	✓	✓	NA
Active Edge	Locked	NA	NA
Haptic Sensor	✗	✗	✗
WiFi	✓	✓	✗
Bluetooth	✓	✓	✓
NFC	✗*	✗*	✗
Accelerometer	✗	✗	✗
Rotation	✗	✗	✗
Gyroscope	✗	✗	✗
Motion	✗	✗	✗
Orientation	✗	✗	✗
Sensor Hub	Locked	Locked	NA
Proximity	✗	✗	✗
Ambient Light	✗	✗	✗
Ambient Pressure/Barometer	✗	✗	NA
Ambient Humidity	✗	NA	NA
Ambient Temperature	✗	NA	NA
Device Temperature	✗	NA	NA
Gravity	✗	✗	✗
Magnetic Field	✗	✗	✗
Hall Sensor	✗	NA	NA

Although the information leakage caused by sensors has been known for years [7–9], the problem has remained unsolved in practice. One main reason is the complexity of the problem; keeping the balance between security and usability. Another reason, from the practical perspective, is that all the reported attacks depend on one condition: the user must initiate the downloading and installing of the app. Therefore, users are relied upon to be vigilant and not to install untrusted apps. Furthermore, it is expected that app stores such as the Apple app store and Google Play will screen the apps and impose severe penalties if the app is found to contain malicious content. However, in the browser-based attacks described in [11–14], we have demonstrated that these measures are ineffective. Apart from academic efforts, there are industrial solutions (e.g., Navenio (navenio.com)) that use some of these sensors such as the accelerometer to track users precisely indoors and outdoors. These products can easily be integrated with illegitimate apps and websites and break user's privacy and security.

With the growing number of sensors, and more sensitive sensor hardware provisioned with new mobile devices and other IoT devices, the problem of information leakage caused by sensors is becoming more severe. Previous research [14,17] suggested that users are not aware of (i) the data generated by the sensors, (ii) how that data might be used to undermine their security and privacy and (iii) what precautionary measure they could and should take. Given that, we believe that raising public knowledge about the sensor technology through education is a very timely matter.

3. Workshop

We ran two rounds of a 90-min workshop entitled: "What Your Sensors Say About You", which was hosted by the Thinking Digital conference in November 2016 (mediaworks.co.uk/insights/news/mediaworks-blog-post-thinking-digital-women-2016/) and May 2018 (thinkingdigital.co.uk/workshops/what-your-sensors-say-about-you/) at Newcastle University, U.K. The attendees could find the following description of the workshop on the event page: "Mobile sensors are everywhere. They're in our smartphones, our tablets and our wearables. They help our devices to detect movement, sense changes in pressure, and notice when other devices are nearby. The data they provide help us to enjoy richer and more personalised apps. But what are the risks to our phones, and the information that lies within them? Discover how these sensors may introduce new security risks to phone users, and make it more complicated to manage them."

3.1. Pedagogical Approach

Our teaching approach, which incorporates taught and research dissemination activities, embodies the principles of constructive alignment and constructivist learning theory. In particular, we deliberately introduce a number of periods of reflection throughout the workshop. Attendees are supported in considering various preventative measures in relation to permission-granting in sensor-related apps and extrapolate their future impacts.

A widely-adopted theory in the public understanding of scientific research, is that of the "deficit model" [24]. The deficit model acknowledges that a lack of available information leads to a lack of popular understanding, which in turn fosters scepticism and hostility. Through our public engagement exercise, and by making available our resources, we seek to equip the public with accessible information, which may inform reasonable precautionary behaviour.

The authors of this paper adopt a challenging role, both as researchers active in mobile sensor security and mediators seeking to popularise research findings. This leads to a tension between providing lay and specialist explanations, a perennial issue in science communication [25]. We acknowledge the role popularisation of science plays in informing future iterations of research [26,27]. Indeed, our observations of participants' interactions serve to inform future technological interventions to support mobile sensor security.

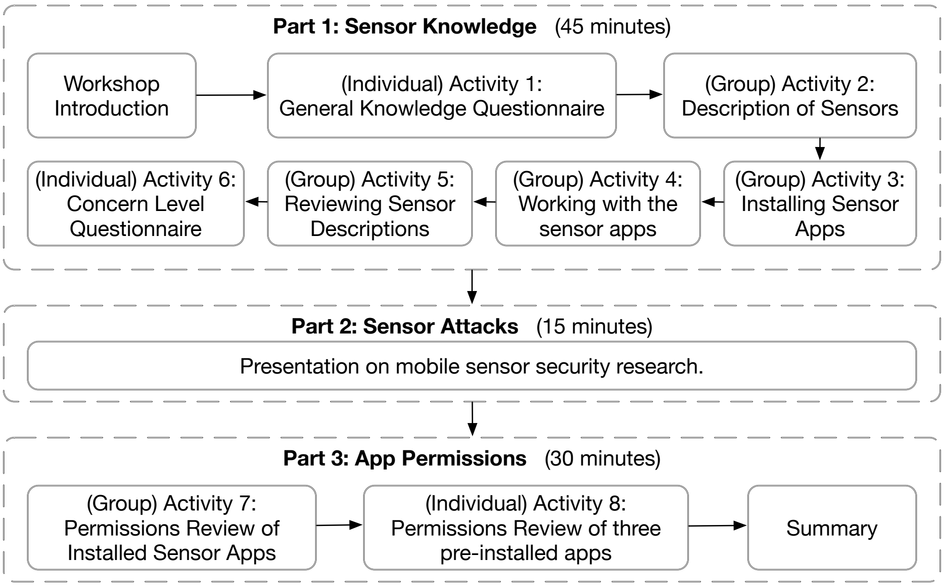
3.2. Participants

In both rounds of the workshop, participation was voluntary, with conference attendees selecting among multiple parallel workshops. We (the authors) presented the workshop to the audience in both rounds. In the first run in 2016, 27 female and three male participants, aged between 22 and 51 attended the workshop. In the second run, two female and 18 male participants aged between 21 and 58 attended the workshop. This brought the total number of our participants to 50 (29 female). In both rounds, the workshop attendees were sitting at tables of five or six and could interact with each other and the educators during the workshop. The attendees owned iOS and Android phones from 1–15 years. Full details of the participants' demography is presented in Appendix B.

3.3. Workshop Content

We ran the workshops by presenting a PowerPoint file, which is publicly available via the first author's homepage. These slides contain all the general and technical content delivered to the attendees and the individual/group exercises they were asked to complete. We explicitly explained to the participants whether they need to complete an activity individually or in a group. We also observed them during the workshop to make sure everyone was following the instructions. We explained to the attendees that their feedback during the workshop, through completing a few forms, would be used for a research project. The attendees could leave the workshop at any stage without giving any explanation. In both rounds of the workshop, all participants completed the session to the end.

These workshops were organised into three parts, as shown in Figure 1. In Part 1, we went through the current mobile sensors by (a) providing the participants with a description of sensors and (b) working with sensor-enabled apps. In Part 2, we explained the sensor-based attacks that have been performed on sensitive user information such as PINs. Finally, in Part 3, we discussed mobile app permission settings.



Part 1: Sensor Knowledge (45 minutes)
Workshop Introduction
(Individual) Activity 1: General Knowledge Questionnaire
(Group) Activity 2: Description of Sensors
(Group) Activity 3: Installing Sensor Apps
(Group) Activity 4: Working with the sensor apps
(Group) Activity 5: Reviewing Sensor Descriptions
(Individual) Activity 6: Concern Level Questionnaire
Part 2: Sensor Attacks (15 minutes)
Presentation on mobile sensor security research.
Part 3: App Permissions (30 minutes)
(Group) Activity 7: Permissions Review of Installed Sensor Apps
(Individual) Activity 8: Permissions Review of three pre-installed apps
Summary

Figure 1. The workshop structure.

3.4. Part 1: Sensor Knowledge

General knowledge questionnaire (Activity 1): After a brief introduction about the workshop, we asked the participants to fill in a five-point scale self-rated familiarity questionnaire on a list of different sensors listed in Section 2.1 (see Appendix C, borrowed from [14]). In the first round of the workshop in 2016, this form had 25 sensors which we had been consistently using in our previous research [14] as well. However, in the second round of the workshop in 2018, we added six new sensors (FaceID, iris scan, heart rate, body sensors, Active Edge and haptic sensor). This was due to the augmentation of popular mobile devices with these new sensors.

In this form, we asked the users to express the level of the general knowledge they had of each sensor by choosing one of the following: "I've never heard of this", "I've heard of this, but I don't know what this is", "I know what this is, but I don't know how this works", "I know generally how this works" and *"I know very well how this works"*. This was an individual exercise, and the list of sensors was randomly ordered for each user to minimise bias.

Description of sensors (Activity 2): After completing the knowledge form, we asked the participants to go through the description of each sensor (see Appendix A) on a printed paper given to everyone. This was a group activity, and the participants could help each other for a better understanding. In case of any difficulty, the attendees were encouraged to interact with the educators. After everyone went through the description page, we gave them examples of the usage of each sensor, e.g., motion sensors for gaming, NFC for contactless payment and haptic sensors for virtual reality applications.

Installing sensor apps (Activity 3): Afterwards, we asked the participants to visit the app stores on their devices and download and install a particular sensor-enabled app (sensor app). Sensor apps are those that visually allow the users to choose different sensors on the screen and see their functionality. For Android users, we recommended the participants install Sensor Box for Android (play.google.com/store/apps/details?id=imoblife.androidsensorbox\&hl=en_GB), as shown in Figure 2, left. This app detects most of the available sensors on the device and visually shows the user how they work. This app supports the following sensors: accelerometer, gyroscope, orientation, gravity, light, temperature, proximity, pressure and sound. For iPhone users, we recommended the Sensor Kinetics app (itunes.apple.com/us/app/sensor-kinetics/id579040333?mt=8), as shown in Figure 2, right. This app mainly supports motion sensors (gyroscope, magnetometer, linear accelerometer, gravity, attitude).

Both apps were chosen based on the popularity, number of installs, rating and the features they offered. We also had a few extra Android phones with the sensor app installed on them. These phones were offered to participants who were unable to install the app and use their own phones. Since the features offered by the Android sensor app were richer, we made sure that each table had at least one Android phone. This was a group activity, and the attendees could help each other find the app on the store and install it. We observed that all users were able to install the app, except two cases in Round 1 and one case in Round 2, who had connection and storage problems. There was another case in Round 2 who did not wish to install the app on his phone due to security and privacy concerns. We lent the Android phones to these users.

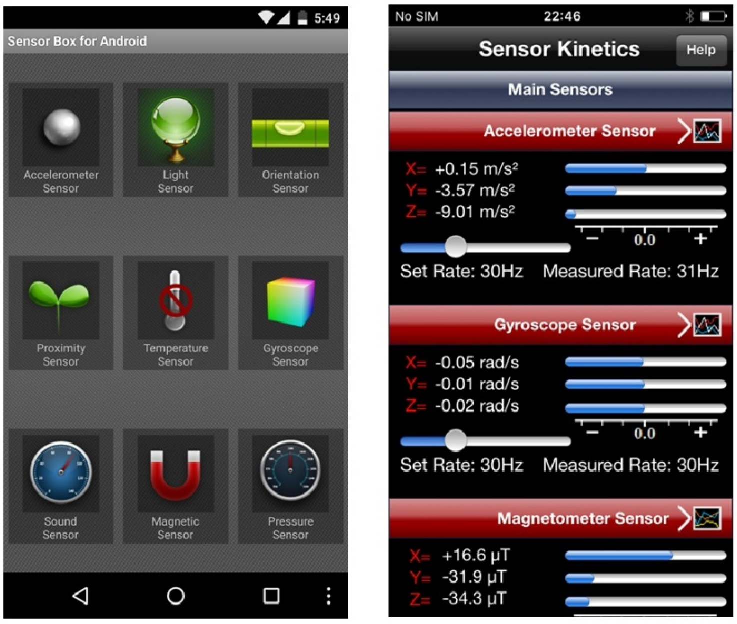


Figure 2. Android (**left**) and iOS (**right**) sensor apps used in the workshop.

Working with the sensor apps (Activities 4 and 5): At this point, we invited the participants to work with the installed apps on their devices. We asked everyone to go through each sensor and find out about its functionality by using the app. Meanwhile, the participants were advised to keep the sensor description page to refer to if necessary. This was a group activity, and the participants could exchange ideas about the app and sensors, as well as help each other to understand the sensors better. During this activity, we worked with individuals either separately or in small groups of two or three and reviewed at least two sensors in the app, including one motion sensor, using the Android app. Through this pair-working activity, we made sure all participants had the chance to observe a few different sensors on the Android device since it offered more features in comparison to the iOS app. At the end of these activities, by asking the participants to review the sensor description page again (Activity 5), we made sure nobody expressed difficulties in understanding the general functionalities of mobile sensors.

Concern level questionnaire (Activity 6): At this stage, we wanted to assess the effect of teaching about sensors to mobile users—via working with mobile sensor apps—on the perceived risk level for each sensor. Similar to our previous research [14], we described a specific scenario: "Now that you have more knowledge about the sensors, let us describe a scenario here. Imagine that you own a smartphone which is equipped with all these sensors. You have opened a game app which can have access to all mobile sensors. You leave the game app open in the background, and open your banking app which requires you to enter your PIN. Do you think any of these sensors can help the game app to discover your entered PIN? To what extent are you concerned about each sensor's risk to your PIN? Please rate them in the table. In this part, please make sure that you know the functionality of all the sensors. If you are unsure, please have another look at the descriptions, or ask us about them."

Then, we asked each participant to fill in a questionnaire (see Appendix C), which included five different levels of concerns: "Not concerned", "A little concerned", "Moderately concerned", "Concerned" and "Extremely concerned". At the end of this individual activity, we asked the participants to complete a demography form. This form included: age, gender, profession, first language, mobile device brand and the duration of owning a smartphone (see Appendix C). We explained to the participants that these forms will be used anonymously for research purposes, and they could refuse to fill it out (partially or completely).

3.5. Part 2: Sensor Attacks

After a short break, we presented a few sensor attacks. In particular, we explained the attacks that we have performed on user sensitive information by using motion and orientation sensors via either installed apps or JavaScript code [11–14]. These attacks could reveal phone call timing, physical activities (sitting, walking, running, etc.), touch actions (click, hold, scroll, zoom) and PINs. For the exact content presented in this part, please see the PowerPoint file.

3.6. Part 3: App Permissions

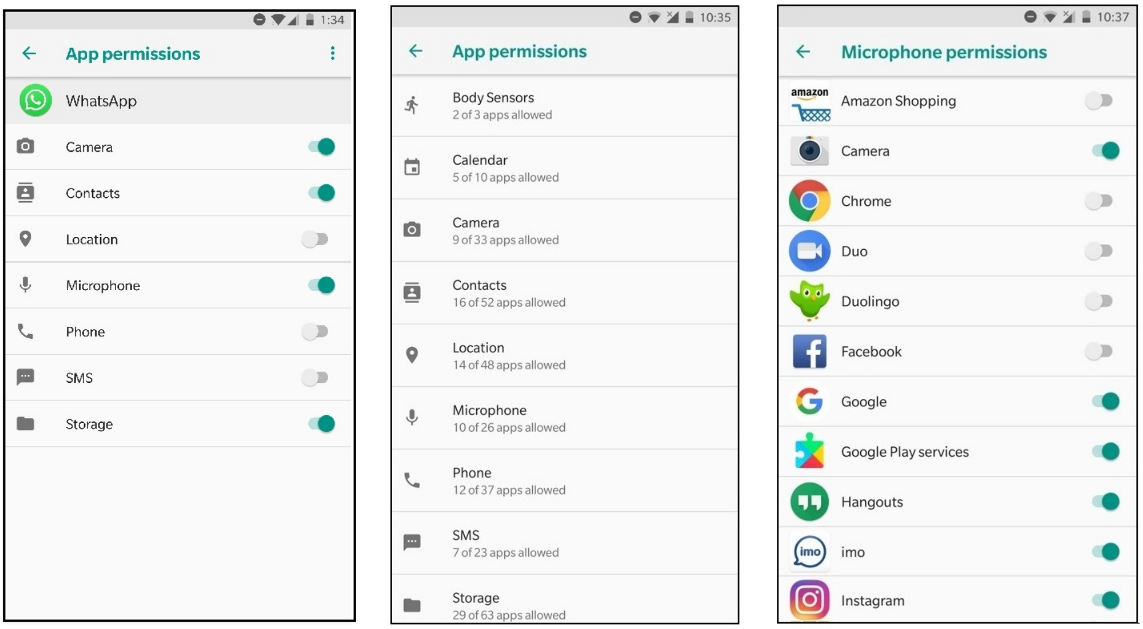
After another short break, we explained the problem of over-privileged apps to the participants. We showed examples of such apps, e.g., Calorie Counter-MyFitnessPal, Zara and Sensor Box for Android (the one that we used in this workshop). These apps ask for extra permissions, e.g., Sensor Box does not need to have access to WiFi and Phone information to function.

Permission review of sensor apps (Activity 7): In this group activity, we invited the participants to go to the system settings of their mobile phones (or the borrowed ones) and check the permissions of the sensor app that they installed during the workshop. We also explained to them that in both Android and iOS devices, it is possible to disable and enable permissions via the system settings (the option of limiting the access to while using the app was discussed with iPhone users.)

Permission review of three pre-installed apps (Activity 8): At this stage, we asked the participants to go through the pre-installed apps on their own devices and choose three apps to review their permissions. We asked them to individually complete a form by naming the app, explaining the purpose of the app, listing the (extra) permissions and expressing whether they would keep the app or uninstall it, and why. This form is provided in Appendix D.

Note that when we ran the workshop in 2016, most Android users were not updated with Android 6 (Lollipop) and had only one way of accessing permissions, which was through each app's settings

(Figure 3, left). From Android Lollipop onward, another permission review model was offered; the user can go to the settings app and see which apps can access certain permission (Figure 3, middle and right). We noticed that in our second workshop in 2018, the participants used both models, as we explain in the Results Section.



1:34
App permissions
WhatsApp
- Camera ●
- Contacts ●
- Location ○
- Microphone ●
- Phone ○
- SMS ○
- Storage ●

10:35
App permissions
- Body Sensors 2 of 3 apps allowed
- Calendar 5 of 10 apps allowed
- Camera 9 of 33 apps allowed
- Contacts 16 of 52 apps allowed
- Location 14 of 48 apps allowed
- Microphone 10 of 26 apps allowed
- Phone 12 of 37 apps allowed
- SMS 7 of 23 apps allowed
- Storage 29 of 63 apps allowed

10:37
Microphone permissions
- Amazon Shopping ○
- Camera ●
- Chrome ○
- Duo ○
- Duolingo ○
- Facebook ○
- Google ●
- Google Play services ●
- Hangouts ●
- imo ●
- Instagram ●

Figure 3. Android permission models; **left**: per app, **middle** and **right**: per permission.

At the end of this workshop, we invited the attendees to discuss their opinions on mobile sensor security with their peers and the educators and gave them a few tips to improve their mobile security, as we present in our Discussion Section.

4. Results

In this section, we present the results of our analysis of different stages of the two rounds of the workshop including the general knowledge level about sensors and their perceived risk level, as well as the correlation between them.

4.1. General Knowledge

Recall that our participants completed the general knowledge form at the beginning of the workshop, before being presented with any information. We present this knowledge level in a stacked bar chart in Figure 4 (left) for the two rounds. The top bars represent the participants of the first round of the workshop in 2016, and the bottom bars are for the second round in 2018. We categorized these sensors into four groups, as suggested in Section 2.1. In each category, sensors were ordered based on the aggregate percentage of participants in the first round of the workshop declaring they knew generally or very well how each sensor works. This aggregate percentage is shown on the right-hand side; the first number for Round 1, the second number for Round 2. In the case of an equal percentage, the sensor with a bigger share of being known very well by the participants is shown earlier. Not that the bars for some of these sensors (FaceID, heart rate, iris scan, body sensors, haptic sensor and Active Edge) are solo since they were studied only in our second workshop. We conclude the following observations from Figure 4, left.

Identity-related sensors: Our participants knew most of identity-related sensors (very) well, and there was not much difference between the two groups of participants. Some of these sensors such as touch screen, camera, microphone and GPS have been available on mobile devices for a longer time. However, some of them such as FaceID, iris scan and body sensors are relevant.

Yet, since the applications of these sensors are immediate and they are named after their functionalities, our participants felt confident about them. The only two less-known sensors in this group were haptic sensor and Active Edge. We believe that since these sensors are used in a more implicit way (see their descriptions in Appendix A) and were introduced more recently with limited applications, they were less known to the users.

Communicational sensors: Apart from NFC (which was extensively adopted by users after the introduction of ApplePay and Google Pay), other communicational sensors (WiFi and Bluetooth) were well known to the users. When we explained the usage of NFC for contactless payment, our participants could recognize it, though its name did not contribute to their knowledge they expressed for it. Although, the second group of our participants expressed more knowledge for NFC, it still remains the least-known sensor in this category.

Motion sensors: The sensors of this category are generally less known to our participants in comparison to biometric and communicational sensors. However, there was a significant increase in the general knowledge about these sensors in the second group of our participants. On the other hand, in the first group of participants, low-level hardware sensors such as the accelerometer and gyroscope seemed to be less known in comparison with high-level software ones such as motion, orientation and rotation, which were named after their functionalities. This was true only about the gyroscope in the second group of participants. Both groups expressed little familiarity about the sensor hub.

Ambient sensors: Our participants were generally less familiar with ambient sensors. Some of these sensors, such as ambient light and device temperature, were better known to both groups. However, similar to motion sensors, the second group of our participants expressed more knowledge of ambient sensors. Though generally, the environmental sensors remained the least known ones between all our participants.

When reading the sensors' list and later their descriptions, our participants were generally surprised to hear about some sensors and impressed by the variety. An overall look at Figure 4, left, shows that identity-related and communicational sensors were better known to the users in comparison to the other two categories. We suspect that this is due to the fact that these sensors have explicit use cases (such as taking a picture, unlocking the phone, exchanging files), which users can easily associate with. These explicit use cases contributed to a better knowledge people expressed for the first two categories. In contrast, the usage of ambient and motion sensors was not immediately clear to the users, and they felt less confident about them. These results are consistent with the results of our previous research [14]. Through multiple rounds of user studies over years, we have witnessed that the level of the knowledge that mobile users have of most sensors is increasing gradually.

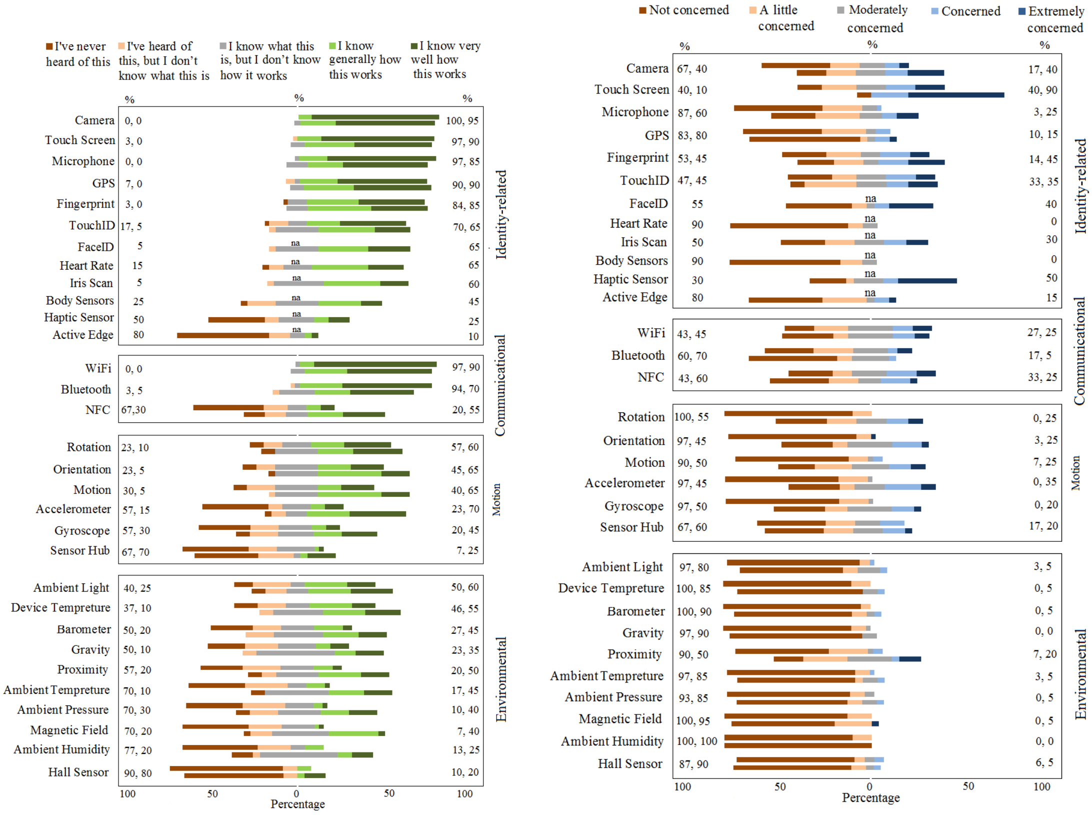


Figure 4. (**Left**) Self-declared knowledge of sensors; (**right**) self-declared perceived risk of sensors. Top bars and left percentages are for Workshop 1 (2016); bottom bars and right percentages are for Workshop 3 (2018).

4.2. Perceived Risks of Sensors

Similar to the above, we present the concern level that our participants expressed for each sensor. Following our previous work [14], we also limited our study to the level of perceived risks users associate with their PINs being discovered by each sensor since finding one's PIN is a clear and intuitive security risk. The actual risks of mobile sensors to people's PINs and passwords are briefly discussed in Section 1. Note that when our participants completed the concern form, they had not been given any security knowledge about sensors. This activity was done after they had the description about the sensors and worked with the sensor apps. As can be seen in Figure 4, right:

Identity-related sensors: Both groups of our participants generally expressed more concern for biometric sensors. Yet, apart from touch screen in the second workshop, none of these sensors received an aggregated percentage declaration of *Concerned*and *Extremely Concerned* more than 50%. Among these sensors, touch screen, TouchID/fingerprint and camera were on top of the list for both groups. FaceID, haptic sensor and iris scan had higher concern levels as well. Our participants did not think that heart rate, body sensors and Active Edge can contribute to the PIN discovery attack scenario much.

Communicational sensors: The participants of the two groups showed consistent levels of concern for WiFi, Bluetooth and NFC. Most of the participants were either *Not*, *A little* or *Moderately concerned* about these sensors.

Motion sensors: The first group of our participants expressed *No* or *Little concern* about these sensors. However, similar to the knowledge level, the second group showed higher concern levels about motion sensors, and the gap was even more noticeable. This correlation between the knowledge and concern levels is interesting, as we discuss later. Note that despite the actual risks of these sensors and with this increase in the concern level of the participants of the second group, most of them were still *Not*, *Little* or *Moderately concerned* about motion sensors being able to reveal their PINs.

Ambient sensors: Almost all of our participants felt *Not* or only a *Little concerned* about ambient sensors in relation to their risk to PINs. The only exception is proximity, where the participants of our second workshop showed a little more concern.

In our previous study [14], we concluded that providing only the description of mobile sensors would not affect the concern level considerably. In some cases, people expressed less concern after knowing the sensor description since they felt more confident about the functionality of the sensor. However in some other cases, they became more concerned after they knew about the sensor description. The same conclusion was stated in [17], where the participants were generally unaware of keystroke monitoring risks due to motion sensors.

In this study however, the concern level varied across the sensor categories. While the percentages have not changed for ambient sensors much, the perceived risk level for the PIN discovery scenario was slightly lower for most biometric and communicational sensors than what was examined in [14]. However, the concern level for motion sensors fluctuated for the participants of our first and second workshops. We observed a reduction in the concern level of the participants of the first group and a noticeable rise in the second group. This increase in the perceived risk levels for motion sensors in the second group was not expected. When we discussed it with our participants, we concluded that this could be due to various reasons including having more knowledge about the actual risks of these sensors via different ways. As a matter of fact, a few of our participants pointed out that they had previously seen articles and news on the risks of motion sensors to sensitive information such as PINs. We believe that this could have contributed to this finding.

4.3. General Knowledge vs. Risk Perception

Figure 4 (right and left) suggests that there may be a correlation between the relative level of knowledge users have about sensors and the relative level of risk they express for them. We confirmed our observation of this correlation by using Spearman's rank-order correlation measure [28].

We ranked the sensors based on the level of user familiarity, using the same method applied in each category of sensors in Figure 4. Separately, the levels of concern were ranked as well. After applying Spearman's equation, the correlation between the comparative knowledge was $r = 0.48$ and $r = 0.52$ ($p < 0.05$), for the first group and the second group of our participants, respectively. This, together with the results described in [14], suggests that there was a moderate/strong correlation between the general knowledge and perceived risk. These results support that the more the users know about these sensors (before being presented with any information), the more concern they express about the risk of the sensors revealing PINs in general.

5. Apps and Permissions Review

In the final part of the workshop, we asked our participants to review the permissions of some of the pre-installed apps on their devices through the settings. In this section, the participants had the opportunity to go beyond sensor security and investigate access to all sorts of mobile OS resources by apps (Figure 3, left). For the second workshop, this activity was done in two forms: per app vs. per permission, as we explain later.

5.1. Reviewing Permissions Per App

The participants in both workshops picked a wide varieties of apps to investigate the permissions; ranging from system apps, social networking, gaming, banking, shopping, discount apps, etc. In most cases, they could successfully identify the functionality of the app and whether it had reasonable permissions or not. However, in some cases, the participants felt unsure about the permissions. The decision made by the users for either uninstalling the app, limiting its access or leaving it as it was before varied across users and apps for various reasons, as we explain here.

Uninstalling: Some of our participants expressed their willingness to uninstall certain apps since they were over-privileged. In the comment section, the participants explained various reasons including: they don't really need the app, they can replace it by using a web browser, they don't understand the necessity of the permission and/or they are concerned about their security and privacy. For example, after one of our participants discovered the permissions already given to a shopping app (camera, contacts, location, storage and telephone), she expressed: "It does not need those things-uninstalled!". Similarly another participant could easily infer that a discount app should not be able to modify/delete the SD card and decided to remove it. In some cases, the extra permissions without explanation made our participants upset, leading them to remove the app. For example, a participant stated that he did not know about the too many permissions that some of his apps such as a university app had and would uninstall them since he was "not happy with the fact that this app uses contacts". Another participant stated that: "I don't see why the BBC needs access to my location", and he decided to remove it.

Disabling/limiting access: There were cases where participants could identify the risk of extra permissions granted to apps, but instead of uninstalling, they chose to disable certain accesses or limit them to while using the app. For instance, one participant observed that if she disabled the access to contacts, storage and telephone, Spotify would still work. The same approach was taken by another participants when he limited FM Radio's access to microphone and storage and LinkedIn's access to camera, microphone, storage and location, and continued using them. Another participant said that she would occasionally turn off location on Twitter, e.g., if she is on holiday. In another example, one of the participants commented: "[I] would remove photos and camera permissions but still use [Uber] app". Some participants commented that they changed the access to location to while using in some apps such as Google Maps and Trainline.

Leaving as before: In some cases, our participants reviewed the app permissions and found them reasonable and not risky. For example, when one of our participants found out that a parking payment app has access to the camera, she commented: "Camera [is] used to take pictures of payment cards". Another comment was on a massaging app that had a variety of permissions; the user said: "[this app] needs those permissions to fully work". Another participant said his taxi booking app uses location in the while using mode, and he thought it was "secure and functional".

In some other cases, our participants could identify over-privileged apps, but decided to leave the apps and their permissions as before. They expressed various reasons for this decision. For example, one participant chose to continue using a discount app saying that "[I'm] not that concerned that it has access to photos". Another participant said she would not uninstall a sleep monitoring app since "I find it useful for self-tracking. I don't worry about people having access to that particular information [microphone, motion and fitness, mobile data] about me." In another case, while our participant could list the extra permissions of a fitness app, she said she would not uninstall it since: "I am addicted to it". Another participant refused to uninstall a pedometer app expressing: "[I] don't see the need for [access to] contacts and storage, but [I would] still use [it] as other apps ask for the same [permissions]." Another attendee listed camera, contacts and location as Groupon's (extra) permissions and commented: "[The app's] benefits outweigh threats". Another example is when one of our participants spotted that a university app uses location and stated: "I trust it and I frequently need it".

Overall, we observed that this activity (app permission review) helped our participants to successfully identity over-privileged apps. However, different users chose to react differently on the matter. It seems that this decision making process was affected by some general mental models such as the ubiquity of the app, the functionality of the app, its advantages vs. the disadvantages, (not) being worried about sharing data, (not) being aware of any real exploitation of these permissions and trusting the app.

Through our discussions with the participants, they stated that they liked this permission review model since they can have an overall picture about each app and its permissions. They also argued that it helped them to keep using certain apps that they enjoy while limiting particular permissions on them.

5.2. Reviewing Apps' Accesses Per Permission

As mentioned before, in the second round of the workshop in 2018, we asked our participants to also review all the apps that have access to certain permissions, e.g., microphone, location, body sensors, etc. Both recent versions of Android and iOS provide the users with this review option (Figure 3 middle and right). Some of our participants were on older versions of Android, which did not support this activity. These participants could use our extra phones to complete this part.

All of our participants found some apps with certain permissions that they did not approve of and decided to stop access. For example, when one of our participants realised that more than 35 of his pre-installed apps had access to location, he stated: "some of these [apps'] accesses do not seem necessary" and decided to disable them. Another participant observed that some of the pre-approved accesses such as Messages' access to heart rate was not reasonable and should be stopped.

A few of our participants stated that via this way of reviewing, they felt that giving permission to too many apps without being aware of it is intrusive and upsetting. For example, a participant decided that he would stop access to the camera on some apps commenting: "e.g., Amazon [uses camera] and I don't like it". Another user said that the fact that too many apps had access to location and the camera was "quite intrusive when not known", and decided to deny some of those permissions.

Some of our participants could not find a good explanation of why they needed to allow certain apps to have certain permissions. For example, one of our participants decided to stop access to body sensors, location and the microphone on some of his apps stating: "some of these apps obviously need [these accesses], but others seem odd [that] they would need these." We observed that when our participants did not realise the reason behind some of the permission requests and were doubtful, most of them chose to deny access. For example, a participant commented: "Unless I am sure of why [any app] needs it (SMS permission), I delete it (disable the access)". Another participant stated: "maybe [it is] risky to give access to camera to so many apps without knowing why?" and decided to disable some of these accesses.

In general, our participant found this way of permission review intuitive. Throughout our discussions with them, they thought that in this way, they could save time by reviewing the permissions that they were most worried about. They also discussed that they could reason better and make a more informed decision since they understood which permissions put them at risk.

6. Recommendations to Different Stakeholders

After we presented the sensor attacks to our participants in the workshops, we observed that they are shocked about the power of motion sensors. However, when completing the app permission review activity, they could not see whether certain apps had access to these sensors or not. For example when reviewing the permissions, one of our participants commented: "why aren't all of the sensors on this list to review?". Hence, even if the mobile users were very well aware of the risk of these sensors to their security and privacy, since mobile apps and websites do not ask for permission for many sensors (see Table 2), users will not have the option to disable the access.

One way to fix this problem, which is commonly suggested by research papers, is to simply ask for permission for all sensors or sensor groups. However, this approach will introduce many usability problems. People already ignore the permission notifications required for sensitive resources such as the camera and microphone. Other solutions such as using artificial intelligence (AI) for sensor management has not been effectively implemented yet. We believe that more research (both technical and human dimensions) in the field of sensor security should be carried out to contribute to this complex usable security problem. This research should be conducted in collaboration with the industry to achieve impactful results. Based on our research, we conclude the following recommendations:

Researchers and educators: Although the amount of technical research conducted on sensor security is considerable, human dimensions of the technology, especially education aspects, have not been addressed very well. When we asked for more comments on improving sensor security at the end of the workshop, one of the participants commented: "better education/information for smartphone users [is needed, eg.] on what app permissions really mean, and how [permission setting] can compromise privacy".

We understand that the focus of technical research might not be education, hence organizing similar workshops might not be the priority. However, apart from raising public knowledge awareness, holding such workshops for a non-technical audience is a strong medium to disseminate technical research. Part 2 of our workshop was a presentation about our research in sensor security. This part can be replaced with any other research in the field of sensor security, without diminishing the workshop's goal. The feedback from non-technical audiences will lead technical research in an impactful direction.

We have published our workshop slides for other educators and the general public. Other ways of raising public awareness include providing related articles on massive open online courses (MOOCs) and publishing user friendly-videos on YouTube. For example, we have provided two articles entitled: "Is your mobile phone spying on you?" and "Auditing your mobile app permissions" in the Cyber Security: Safety at Home, Online, in Life online course (futurelearn.com/courses/cyber-security), part of Newcastle University's series of MOOCs. Through our second workshop, we also witnessed that publishing research findings via public media has an impact on the general knowledge of the users. We strongly encourage researchers to produce educational materials and report their experiences and findings on other aspects of sensor security.

App and web developers: Throughout our studies over years, we have concluded that the factors that contribute to the users' risk inference about technology in general, and mobile sensors in particular, are complicated. As is known, security and privacy issues are low motivations in the adoption of apps. Therefore, app and web developers have a fundamental role in addressing this problem and delivering more secure apps to the users. As discussed in [29], developers are recommended to secure tools with proven utility. Many mobile apps in app stores are "permission hungry" [21]. These extra permission requests are likely not understood by the majority of developers who copy and paste this code into their applications [30]. This is where app developers end up inserting extra permission requests into their code. We advise developers to not copy code from unreliable sources into their apps. Instead, they should search for stable libraries and APIs to be used in their apps. Accordingly, including minimal permission requests in the app would lead to fewer security decisions to be made by the users when installing and using the app.

Moreover, explaining the reason why the app is asking for certain permissions would improve the user experience. As an example, when one of our participants found out that a discount app has access to location, the participant commented: "Location allows me to find nearby offers- app gives explanation". When we asked for more comments on improving sensor security at the end of the workshop, one of our participants wrote: "let the user know why permission is needed for the app to work and choose which features/permissions are reasonable". Educating app developers about more secure products seems to be vital and is another topic of research on its own.

Android Developer has recently published best practices for app permissions to be followed by programmers (developer.android.com/training/permissions/usage-notes). These best practices include: only use the permissions necessary for your app to work; pay attention to permissions required by libraries; be transparent; and make system accesses explicit. These are all consistent with the expectations that our participants expressed during the two workshops.

End users: As we observed in our studies, mobile users do not know that many apps have access to their mobile OS resources, either without asking for permission or via the permissions that they ignore. In order to keep their devices safer, we advise users to follow the general security practice:

- Some users tend to be lazy and careless in closing apps after finishing working with them. Close background apps and web browser tabs when you are not using them.
- Some users can be greedy in installing multiple apps and keeping them on their devices. This is especially true for free apps. Uninstall apps you no longer need.
- Security patches are being constantly released by the vendors. Keep your phone OS and apps up to date.
- Installing apps from unknown sources might impose security risks. Only install applications from approved app stores where these apps are vetted comprehensively.
- Scrutinise the permission requested by apps before you install them and while using them. You can choose alternative apps with more sensible permissions if needed.
- Try to audit the permissions that apps have on your device regularly via system settings.

Each of the above items can be developed by educators as educational material to be taught to mobile users.

We believe that the problem of sensor security is already beyond mobile phones. The challenges are more serious when smart kitchens, smart homes, smart buildings and smart cities are equipped with multiple sensor-enabled devices sensing people and their environment and broadcasting this information via IoT platforms. As a matter of fact, some of our participants listed a few dedicated IoT apps when they were auditing the app permissions; for example, Hive, which is described in its app description as: “a British Gas innovation that creates connected products designed to give people the control they want for their homes anytime, anywhere.” This app offers a wide range of features enabling the users to control their heating and hot water, home electrical appliances, controlling the doors and windows and reporting if movement is spotted inside the user;s home via, as described, “sophisticated sensors”. One of our participants using this app commented: “It allows me to control my heating/hot water to make it more efficient. I have turned off analytics and location for security. A bit concerned as if someone hacked, they could analyse when I am at home”. We know that the risks of hacking into IoT platforms is beyond knowing whether or not someone is at home. It could be harmful to people’s lives as described in [31]. Hence, we encourage researchers to conduct more studies on human dimensions of sensors in IoT.

7. Limitations and Future Work

This research is limited in a few ways, which we plan to address in the future. We acknowledge that our participant set was less diverse as opposed to previous studies [14,17] since the recruitment process was through attending a technical conference, which attracts more tech-friendly people. Note that the first round of the workshop had more female participants due to the title and remit of the host conference in 2016: Thinking Digital Women. More of the second workshop’s participants were male, which is normally the case with Thinking Digital conferences. However, we believe the bias in our participants would not disprove our results since they are compatible with the results of previous papers.

Despite our attempt to choose the most functional sensor apps, the ones that we used in our workshops did not offer the whole range of sensors to the users to experiment with. This might not enable the users to understand fully the functionalities of all available sensors on their smart devices. In the future, we plan to develop our fully-functional sensor app and conduct studies by offering that to our participants.

In the second part of the workshop, our focus was on side channel attacks on users’ sensitive information such as touch actions and PINs via motion sensors. This part was presented before the app permission review activity. There are other types of attacks using motion sensors and/or other sensors, which we have not studied in this paper. Furthermore, we did not observe and measure the behaviour of our participants on disabling permissions and removing apps before and after being presented with these security attacks. This is the case with the concern level before and after knowing the description and working with the sensor apps as well. These choices were made deliberately to keep the workshop length reasonable. Each of these can be a researched on their own, which we leave as future work.

Apart from the above, we would like to study all the sensors available on smart devices in IoT platforms specially in smart homes, e.g., smart kitchen items, smart toys, etc. We would like to know what are the new sensors on other smart devices and what data are they broadcasting about users and their environments. In particular, we are interested in the actual risks of these sensors vs. the perceived risks that the users express for them. This is particularly interesting if studied from a legislation angle, e.g., with regards to General Data Protection Regulations (GDPR). By conducting more research in this area, the academic community and the sensor industry will have a better vision of the human factors of this fast-growing technology with more robust results.

8. Conclusions

In this paper, we reflected on the results of two workshops where we mainly explained the following three items to the mobile users: (i) the data generated by mobile sensors, (ii) how that data might be used to undermine their security and privacy and (iii) what precautionary measures they could and should take. We studied the impact of teaching mobile users about sensors on their perceived risk levels for each sensor. The results showed that teaching about general aspects of sensors might not immediately improve people's ability to perceive the risks, and other factors such as their prior general knowledge had a stronger impact. On the other hand, when we taught the permission reviewing technique as a precautionary measure, our participants could successfully identify over-privileged apps. Users' decision on either modifying the app permissions, uninstalling or keeping it as before varied due to various reasons. We believe this suggests that there is much room for more focus on education about mobile and sensor technology.

Author Contributions: Both authors have contributed during all stages of this paper including conceptualization, methodology, running the workshop, and writing the paper. M.M. has analysed the self-declared forms completed by the participants in the workshop and presented the results in the paper.

Funding: This research received no external funding.

Acknowledgments: We would like to thank Thinking Digital for hosting this workshop for two years and the participants who attended the workshop. We thank Anssi Kostiainen, from Intel and the chair of the W3C Device and Sensors Working Group, for his feedback on Section 2. We would like to thank Matthew Forshaw from Newcastle University for his feedback on Section 3. All of our user studies were approved by Newcastle University's Ethics Committee, and all the data were processed and saved according to the GDPR. This paper is based on *Making Sense of Sensors: Mobile sensor security awareness and education*, by Maryam Mehrnezhad, Ehsan Toreini and Sami Alajrami, which appeared in the Proceedings of the International Workshop on Socio-Technical Aspects in Security and Trust (STAST), 2017.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Mobile Sensors' Description

In the following, we present a brief description of each sensor:

- GPS: identifies the real-world geographic location.
- Camera,microphone: capture pictures/videos and voice, respectively.
- Fingerprint, TouchID: scans the fingerprint.
- FaceID: scans the face.
- Iris scan: scans the eye's iris.
- Heart rate (HR): measures the heart rate.
- Touch screen: enables the user to interact directly with the display by physically touching it.
- Active Edge: enables the user to use certain functionalities by physically pressing the edges.
- Haptic sensor: recreates the sense of touch by applying forces, vibrations or motions to the user.
- Body sensors: provides access to user's health data from certain sensors (e.g., HR).

- WiFi: a wireless technology that allows the device to connect to a network.
- Bluetooth: a wireless technology for exchanging data over short distances.
- NFC (Near-Field Communication): a wireless technology for exchanging data over shorter distances (less than 10 cm) for purposes such as contactless payment.
- Proximity: measures the distance of objects from the touch screen.
- Ambient light: measures the light level in the environment of the device.
- Ambient pressure (barometer), ambient humidity and ambient temperature: measure the air pressure, humidity and temperature in the environment of the device, respectively.
- Device temperature: measures the temperature of the device.
- Gravity: measures the force of gravity.
- Magnetic field: reports the ambient magnetic field intensity around the device.
- Hall sensor: produces voltage based on the magnetic field.
- Accelerometer: measures the acceleration of the device movement or vibration.
- Rotation: reports how much and in what direction the device is rotated.
- Gyroscope: estimates the rotation rate of the device.
- Motion: measures the acceleration and the rotation of the device.
- Orientation: reports the physical angle that the device is held at.
- Sensor hub: an activity recognition sensor wit the purpose of monitoring the device's movement.

Appendix B. Workshop Attendees' Demography

Table A1. Participants' self-reported demographics; y indicates the years of owning a smartphone; left: Workshop 1 (2016), right: Workshop 2 (2018).

Sex	Age	Job/Background	y	Sex	Age	Job/Background	y
f	27	Tech communication	7	f	32	Teacher	7
f	43	Service director	8	m	34	Computer scientist	7
f	28	Finance manager	4	m	24	Student	10
f	45	Graphic designer	15	m	21	Student	10
f	23	Designer	6	m	23	Student	9
f	23	Social media	6	m	26	Student	10
f	47	Teacher	9	m	53	Business manager	18
m	32	Manager	6	m	24	Student	9
f	31	Research director	7	m	23	Student	7
f	29	Costumer service manager	7	m	50	Developer	9
f	27	Content strategist	4	m	45	IT	11
f	45	Teacher	10	m	39	Civil servant	9
f	29	Business analyst	7	f	NA	NA	3
f	32	Photographer	13	m	58	Engineer	8
f	46	Management consultant	8	m	37	Technology	11
f	24	Research assistant	10	m	49	Programmer	10
m	32	Student	7	m	28	IT	7
f	51	Development Manager	11	m	23	Student	11
f	28	IT manager	8	m	44	Futuristic	10
f	28	Marketing manager	8	m	42	NA	7
f	31	Digital marketing	7				
f	23	Student	7				
f	33	Test analyst	8				
f	22	HR manager	5				
f	30	Teacher	7				
f	27	NA	16				
m	23	Student	2				
f	39	Trainee solicitor	9				
f	50	Brand consultant	10				
f	44	NA	1				

Appendix C. General Knowledge and Concern Level Questionnaires for Mobile Sensors

Table A2. This form was used for Activity 1.

Sensor	I've Never Heard of This	I've Heard of This But I don't Know What This Is	I Know What This Is But I don't Know How This Works	I Know Generally How This Works	I Know Very Well How This Works
Bluetooth					
FaceID					
Gyroscope					
Iris Scan					
GPS					
Heart Rate					
Sensor Hub					
Body Sensors					
Ambient Temperature					
Active Edge					
Accelerometer					
Magnetic Field					
Haptic Sensor					
Motion					
Fingerprint					
Orientation					
Proximity					
Ambient Pressure					
Hall Sensor					
Rotation					
Touch Screen					
Camera					
TouchID					
Barometer					
Gravity					
Microphone					
Ambient Humidity					
WiFi					
Ambient Light					
NFC					
Device Temperature					

Table A3. This form was used for Activity 6.

	Risk to PIN				
Sensor	**Not Concerned**	**A Little Concerned**	**Moderately Concerned**	**Concerned**	**Extremely Concerned**
Bluetooth					
FaceID					
Gyroscope					
Iris Scan					
GPS					
Heart Rate					
Sensor Hub					
Body Sensors					
Ambient Temperature					
Active Edge					
Accelerometer					
Magnetic Field					
Haptic Sensor					
Motion					
Fingerprint					
Orientation					
Proximity					
Ambient Pressure					
Hall Sensor					
Rotation					
Touch Screen					
Camera					
TouchID					
Barometer					
Gravity					
Microphone					
Ambient Humidity					
WiFi					
Ambient Light					
NFC					
Device Temperature					

Appendix D. App Permissions' Audit Forms

Table A4. This form was used for Activity 8.

No.	**App Name**	**Purpose**	**(Extra) Permissions**	**Would you Uninstall?**	**Why?**
1					
2					
3					

Table A5. This form was used for Activity 8 (only for the second workshop).

No.	Permission Name	Purpose	Apps Sing It	Would You Stop Access?	Why?
1					
2					
3					

References

1. Planet of the Phones. From the Print Edition by The Economist, 2015. Available online: http://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones (accessed on 30 November 2018).
2. De Luca, A.; Hang, A.; Brudy, F.; Lindner, C.; Hussmann, H. Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns. In Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems, CHI 2012, Austin, Texas, 5–10 May 2012.
3. Bo, C.; Zhang, L.; Li, X.Y.; Huang, Q.; Wang, Y. SilentSense: Silent User Identification via Touch and Movement Behavioral Biometrics. In Proceedings of the 19th ACM Annual International Conference on Mobile Computing and Networking, MobiCom 2013, Miami, FL, USA, 30 September–4 October 2013.
4. Li, H.; Ma, D.; Saxena, N.; Shrestha, B.; Zhu, Y. Tap-Wave-Rub: Lightweight Malware Prevention for Smartphones Using Intuitive Human Gestures. In Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2013, Nanjing, China, 13–15 October 2013.
5. Mayrhofer, R.; Gellersen, H. Shake Well Before Use: Authentication Based on Accelerometer Data. In *Pervasive Computing*; Springer: Berlin/Heidelberg, Germany, 2007.
6. Mehrnezhad, M.; Hao, F.; Shahandashti, S. Tap-Tap and Pay (TTP): Preventing the Mafia Attack in NFC Payment. In Proceedings of the Second International Conference on Research in Security Standardisation, SSR 2015, San Juan, PR, USA, 18–22 June 2015.
7. Simon, L.; Anderson, R. PIN Skimmer: Inferring PINs Through the Camera and Microphone. In Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones Mobile Devices, SPSM 2013, Atlanta, GA, USA, 9–14 June 2013; pp. 67–78.
8. Spreitzer, R. PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices. In Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones Mobile Devices, SPSM 2014, Scottsdale, AZ, USA, 3–7 November 2014.
9. Xu, Z.; Bai, K.; Zhu, S. TapLogger: Inferring User Inputs on Smartphone Touchscreens Using On-board Motion Sensors. In Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC 2012, Paphos, Cyprus, 28–30 November 2012.
10. Mehrnezhad, M.; Ali, M.; Hao, F.; van Moorsel, A. NFC Payment Spy: Privacy attacks on contactless payments using NFC-enabled mobile. In Proceedings of Third International Conference on Research in Security Standardisation, SSR 2016, San Diego, CA, USA, 16–20 July 2016.
11. Mehrnezhad, M.; Toreini, E.; Shahandashti, S.; Hao, F. TouchSignatures: Identification of user touch actions and PINs based on mobile sensor data via JavaScript. *J. Inf. Secur. Appl.* **2016**, *26*, 23–38. [CrossRef]
12. Mehrnezhad, M.; Toreini, E.; Shahandashti, S.; Hao, F. TouchSignatures: Identification of User Touch Actions Based on Mobile Sensors via JavaScript. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS 2015, Singapore, 14–17 April 2015.
13. Mehrnezhad, M.; Toreini, E.; Shahandashti, Siamakand Hao, F. Stealing PINs via Mobile Sensors: Actual Risk versus User Perception. In Proceedings of the 1st European Workshop on Usable Security, EuroUSEC 2016, Darmstadt, Germany, 18 July 2016.
14. Mehrnezhad, M.; Toreini, E.; Shahandashti, S.F.; Hao, F. Stealing PINs via mobile sensors: Actual risk versus user perception. *Int. J. Inf. Secur.* **2017**, 1–23. [CrossRef]
15. Hern, A. Tilted Device Could Pinpoint PIN Number for Hackers, Study Claims, 2017. Available online: http://www.theguardian.com/technology/2017/apr/11/tilted-device-could-pinpoint-pin-number-for-hackers-study-claims (accessed on 30 November 2018).

16. Newsbeat, B. The Way People Tilt Their Smartphone Can Give Away Passwords and PINs, 2017. Available online: http://www.bbc.co.uk/newsbeat/article/39565372/the-way-people-tilt-their-smartphone-can-give-away-passwords-and-pins (accessed on 30 November 2018).
17. Crager, K.; Maiti, A.; Jadliwala, M.; He, J. Information Leakage through Mobile Motion Sensors: User Awareness and Concerns. In Proceedings of the EuroUSEC'17, Paris, France, 29 April 2017.
18. Location and Sensors APIs. Available online: developer.android.com/guide/topics/sensors/index.htmlt (accessed on 30 November 2018).
19. Core Motion. Available online: developer.apple.com/documentation/coremotion (accessed on 30 November 2018).
20. Jin, X.; Hu, X.; Ying, K.; Du, W.; Yin, H.; Nagesh Peri, G. Code Injection Attacks on HTML5-based Mobile Apps: Characterization, Detection and Mitigation. In Proceedings of the 21th ACM Conference on Computer and Communications Security, CCS 2014, Scottsdale, AZ, USA, 3–7 November 2014.
21. Taylor, V.F.; Martinovic, I. A Longitudinal Study of App Permission Usage Across the Google Play Store. Technical Report. 2016. Available online: http://arxiv.org/abs/1606.01708 (accessed on 30 November 2018).
22. Device and Sensors Working Group. 2016. Available online: https://www.w3.org/2009/dap/ (accessed on 30 November 2018).
23. Android Sensors. Available online: http://developer.android.com/guide/topics/sensors/\sensors_overview.html (accessed on 30 November 2018).
24. Wynne, B. Misunderstood misunderstanding: Social identities and public uptake of science. *Public Underst. Sci.* **2016**. [CrossRef]
25. Sismondo, S. *An Introduction to Science and Technology Studies*; Wiley-Blackwell Chichester: Hoboken, NJ, USA, 2010; Volume 1.
26. Hilgartner, S. The dominant view of popularization: Conceptual problems, political uses. *Soc. Stud. Sci.* **1990**, *20*, 519–539. [CrossRef]
27. Bucchi, M. *Science and the Media: Alternative Routes to Scientific Communications;* Routledge; London, UK, 2014.
28. Hauke, J.; Kossowski, T. Comparison of Values of Pearson's and Spearman's Correlation Coefficients. *Quaest. Geogr.* **2011**, *30*, 87–93. [CrossRef]
29. Abu-Salma, R.; Danilova, A.; Sasse, M.A.; Naiakshina, A.; Bonneau, J.; Smith, M. Obstacles to the adoption of secure communication tools. In Proceedings of the 38th IEEE Symposium on Security and Privacy, IEEE S&P '17, San Jose, CA, USA, 22–26 May 2017.
30. Green, M.; Smith, M. Developers Are Not the Enemy! The Need for Usable Security APIs. *IEEE Secur. Priv.* **2016**, *14*, 40–46. [CrossRef]
31. Ronen, E.; O'Flynn, C.; Shamir, A.; Weingarten, A.O. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. Cryptology ePrint Archive, Report 2016/1047, 2016. Available online: http://eprint.iacr.org/2016/1047 (accessed on 30 November 2018).