COMPUTING
SCIENCE

Title: Making Sense of Sensors:
Mobile sensor security awareness and education.

Names: Maryam Mehrnezhad, Ehsan Toreini, Sami Alajrami

TECHNICAL REPORT SERIES

No. CS-TR- 1510 2017

TECHNICAL REPORT SERIES

No. CS-TR- 1510 Date July 2017

Title: Making Sense of Sensors:
Mobile sensor security awareness and education

Authors: Maryam Mehrnezhad, Ehsan Toreini, Sami Alajrami

Abstract: Mobile sensors have already proved to be helpful to different aspects of people's everyday lives such as fitness, gaming, navigation, etc. However, illegitimate access to these sensors provides 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 security and privacy of mobile sensors. Second, we reflect the results of a workshop which we organized on mobile sensor security. Finally, we provide recommendations for educators, app developers and mobile users to contribute toward awareness and education on this topic.

Printed and published by Newcastle University,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne, NE1 7RU, England.

Bibliographical details

Title and Authors

NEWCASTLE UNIVERSITY
Computing Science. Technical Report Series. CS-TR- 1510

Abstract: Mobile sensors have already proved to be helpful to different aspects of people's everyday lives such as fitness, gaming, navigation, etc. However, illegitimate access to these sensors provides 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 security and privacy of mobile sensors. Second, we reflect the results of a workshop which we organized on mobile sensor security. Finally, we provide recommendations for educators, app developers and mobile users to contribute toward awareness and education on this topic.

About the Authors:

Maryam Mehrnezhad is a Research Fellow in the School of Computing Science, Newcastle University. She received her PhD from Newcastle University. Her research interests include usable security and privacy, mobile sensor security, contactless payment, blockchain technology, and machine learning. Maryam has contributed to W3C specifications and mobile industry based on her research in mobile sensor security.

Ehsan Toreini is a final year PhD student in Newcastle University. His doctoral research is about tamper evident technologies in physical objects and cyber security. His work has been published in different magazines and journals including ACM transaction for privacy and security (TOPS), the Economist and Wall Street Journal. His research interests are Tamper Evident Technologies, End to End Integrity, Side Channel Attacks, Web Security and applied Cryptography.

Sami Alajrami is a software consultant working on continuous delivery and DevOps at Praqma. He received his PhD and MSc from Newcastle University where his research was focused on novel ways for conducting software development in the cloud. Sami has worked at the Cloud & Security Lab in Hewlett Packard Labs as a software intern where he has been involved in the Security Intelligence as a Service (SILAS) and the Situational Awareness as a Service (SAaaS) projects.

Suggested keywords: Mobile sensors, Mobile Security, Security education

Making Sense of Sensors: Mobile sensor security awareness and education

Maryam Mehrnezhad, Ehsan Toreini, Sami Alajrami
{maryam.mehrnezhad, e.toreini, s.h.alajrami }@newcastle.ac.uk
Newcastle University, UK

Abstract—Mobile sensors have already proved to be helpful to different aspects of people's everyday lives such as fitness, gaming, navigation, etc. However, illegitimate access to these sensors provides 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 security and privacy of mobile sensors. Second, we reflect the results of a workshop which we organized on mobile sensor security. Finally, we provide recommendations for educators, app developers and mobile users to contribute toward awareness and education on this topic.

1 Introduction

According to the Economist [7], 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 device vendors are increasingly augmenting their products with different types of sensors such as NFC (near field communication), accelerometer, orientation and motion, which are connected to each other through the Internet of Things (IoT).

Sensors are added to mobile devices to make them "smart": to sense the surrounding environment and infer aspects of the context of use from the sensor data, 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 [3], [6], authorization [16], device pairing [17], and secure contactless payment [19]. However, malicious access to sensor streams provides an installed app running in the background with an exploit path. Researchers have shown that the user's PINs and passwords can be disclosed through sensors such as camera and microphone [25], ambient light [28], and gyroscope [35]. Sensors such as NFC can also be misused to attack financial payments as demonstrated in [18].

In our previous research [20]–[23], we have shown that the sensor management problem is spreading from apps to browsers. We proposed the first JavaScript-based side channel attack revealing user 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, our attack infers the user's touch actions and PIN with an accuracy of over 70% in the first try.

The above research has attracted considerable national and international media coverage (newspaper, radio, tv, online news, social media, etc.) – which reassures the importance of the topic. Examples of the media articles and interviews include: Guardian [12], BBC [24], Telegraph [4], Economic Times (a leading business newspaper) [31], Science Friday (American radio talk show) [8], German public radio Deutschlandfunk [15], Sina (largest Chinese-language web portal) [26], Lavoz (a leading Spanish-language newspaper) [30], etc.

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. The results of our previous research [20], [23] show 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 [23], we discuss how this observation, along with other factors, renders many academic and industry solutions ineffective in managing mobile sensors. In view of all this, we believe that there is a lot of room for more focus on people awareness and education about the privacy and security issues of the mobile and sensor technology.

In the past, we had studied the impact of providing the sensors descriptions to mobile users on the perceived risk levels for a particular scenario: stealing PINs via a background app which has access to all sensors [23]. 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 same PIN discovery scenario. We reflect the results of an interactive workshop that we organized on mobile sensor security. This workshop 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 on how to manage the app permissions on different mobile platforms. In Section 3, we present the structure of the workshop in full details.

Category	Sensors
Identity-related (Biometric)	GPS, Camera, Microphone, Fingerprint (TouchID), Touch Screen
Communicational	WiFi, Bluetooth, NFC
Movement	Gyroscope, Accelerometer, Rotation, Orientation, Motion, Sensor Hub
Ambient (Environmental)	Temperature (ambient, device), Humidity, Pressure (Barometer), Light, Proximity, Gravity, Magnetic Field, Hall Sensor

TABLE 1
Categorization of current mobile sensors

Sensor	Android	iOS	W3C
GPS	✓	✓	✓
Camera	✓	✓	✓
Microphone	✓	✓	✓
Fingerprint/ TouchID	✓	✓	NA
Touch Screen	✗	✗	✗
WiFi	✓	✓	✗
Bluetooth	✓	✓	✓
NFC	✗*	Locked	✗
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	✗	✗	NA
Magnetic Field	✗	✗	✗
Hall Sensor	✗	NA	NA

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 in Android for any program to be able to use it.

2 Mobile sensors

As shown in [29], the average number of permissions used by Android apps (installed from Google Play) increases over time, especially for popular apps as well as free apps. These permissions are requested for having access to the OS resources as well as sensors such as GPS, camera, and microphone. This has the potential to make apps over-privileged and unnecessarily increase the attack surface.

Developers can have access to mobile sensors either by 1) writing native code using mobile operating system (OS) APIs [9], 2) recompiling HTML5 code into a native app [14], or 3) using standard APIs provided by the W3C which are accessible through JavaScript code within a mobile browser[1]. As shown in Table 2, both iOS and Android as well as mobile web browsers allow native apps and JavaScript code in web pages to access many of these sensors without any user permission being required.

2.1 Mobile sensors categorization

Here we present a list of different sensors, borrowing it from our previous research [23]. This list was prepared by inspecting the official websites of iPhone 6[2], Nexus 6P[3], and the specifications that W3C[4] and Android [9] provide for developers. We also add some extra sensors (wireless technologies, camera, microphone, touch screen, and GPS) as common sensing mobile hardware. We propose to categorize these sensors into four main groups: identity-related (biometric) sensors, communicational sensors, movement 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 world's first thermal imaging sensor on mobile phones is offered by Cat S60 smartphone[5]. We chose *movement* instead of *motion* for sensors such as accelerometer, gyroscope, etc. on purpose since 'motion' is already taken by W3C specifications for a limited list of sensors in this category [33]. One might argue that GPS belongs to the environmental category, however since it is assigned with people's identities, we propose to keep it in the identity-related category. In Appendix A, we present a brief description of each sensor.

2.2 Sensor management challenges

As it can be seen in Table 2, sensing is 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 discussed in [25], 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, usage of the sensor data is not restricted. Even worse, 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 in operating systems. As it can be seen in Table 2, permission policies for having access to different sensors vary across sensors and platforms [2], [32].

Although the information leakage caused by sensors has been known for years [25], [28], [35], 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 our in-browser-based attacks [20]–[23], we have demonstrated that these measures are ineffective.

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 expected to become more severe. Our previous research suggests 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.

1. w3.org/TR/#tr_Javascript_APIs
2. apple.com/uk/iphone-6/specs/
3. store.google.com/product/nexus_6p
4. w3.org/2009/dap/
5. catphones.com/en-gb/phones/s60-smartphone

3 Workshop

This 90-min workshop entitled *"What Your Sensors Say About You"* [6] was organized as one of the four workshops hosted by the Thinking Digital Women conference in Nov 2016 at Newcastle University. 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"* [34]. The deficit model acknowledges that a lack of available information leads to a lack of popular understanding, which in turn fosters skepticism 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 [27].

We acknowledge the role popularisation of science plays in informing future iterations of research [5], [13]. Indeed our observations of participants interactions serve to inform future technological interventions to support mobile sensor security.

3.2 Participants

Workshop participation was voluntary, with conference attendees selecting among four parallel workshops. We (the first two authors of the paper) presented the workshop to an audience of 27 female, and 3 male participants, aged between 22 to 51. The attendees owned iOS and Android phones for an average of 8 years. Full details of the participants demography is presented in Appendix A. The workshop had more female participants due to the title and remit of the host conference: Thinking Digital Women. We acknowledge that our participant set was less diverse as opposed to our previous studies [23]. However, we believe the bias in the participants would not disprove the results of this work since they are compatible with the results of our previous studies, as we discuss later. The workshop attendees were sitting on tables of 5 or 6 and could interact with each other and the educators during the workshop.

6. tdcwomen.com/workshops/what-your-sensors-say-about-you/

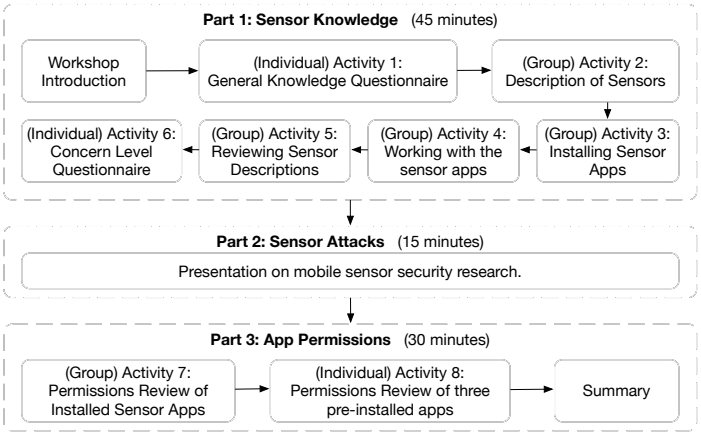

Fig. 1. The workshop structure

3.3 Workshop content

We ran the workshop by presenting a PowerPoint file, which is publicly available via the first author's homepage[7]. 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 group. We also observed them during the workshop to make sure everyone is following the instructions. We explained to the attendees that their feedback during the workshop, through completing a few forms, will be used for a research project.

This workshop was organised in three parts, as shown in Fig. 1. In part one, we went through the current mobile sensors *a)* by providing the participants with a description of sensors, and *b)* working with sensor-enabled apps. In part two, we explained the sensor-based attacks that we have performed on sensitive user information such as touch actions and PINs [20]–[23]. Finally, in part three, we discussed mobile app permission settings.

3.4 Part One: Sensor Knowledge

Activity one (general knowledge questionnaire): 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 25 different sensors listed in Section 2.1 (see Appendix A). We have been consistently using this form in our previous research [23]. In this form, we ask the users to express the level of the general knowledge they have on 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, with the list of sensors was randomly ordered for each user to minimise bias.

Activity two (description of sensors): 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

7. homepages.cs.ncl.ac.uk/m.mehrnezhad/

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

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 senors for gaming, and NFC for contactless payment.

Activity three (installing sensor apps): 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 which visually allow the users to choose different sensors on the screen and see its functionality. For Android users, we recommended the participants to install Sensor Box for Android[8], as shown in Fig. 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 Sensor Kinetics app[9], as shown in Fig. 2, right. In contrast to the Android app, this app mainly supports movement 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 has at least one Android phone. This was a group activity and the attendees could help each other to find the app in the store and install it. We observed that all users were able to install the app, except two cases who had connection and storage problems. We lend the Android phones to these users.

Activities four and five (working with the sensor apps): 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 on the app and sensors as well as helping 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 movement sensor, using the Android app. Through this pair-working activity, we made sure all participants have 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 five), we made sure nobody expressed difficulties in understanding the general functionality of mobile sensors.

Activity six (concern level questionnaire): 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 [23], 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 participants to fill in a questionnaire (see Appendix A) which included five different level 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(optional), first language (optional), mobile device brand, and the duration of owning a smartphone.

3.5 Part two: sensor attacks

After a short break, we presented the work we have done on mobile sensor security [20]–[23]. In particular, we explained the attacks that we have performed on user sensitive information by using motion and orientation sensors via JavaScript. 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 three: app permissions

After another short break, we explained the problem of over-privileged apps to the participants. We showed two examples of such apps: Calorie Counter-MyFitnessPaland Sensor Box for Android (the one that we used in this workshop). Fig. 3 shows the permissions that these apps ask for. As it can be seen, both apps ask for extra permissions e.g. Sensor Box does not need to have access to WiFi and Device ID and call information. Similarly, MyFitnessPal does not need to have access to many of those listed in the picture.

Activity seven: permission review of installed sensor apps. In this group activity, we invited the participants to go to the system settings of their mobile phones (or the

8. play.google.com/store/apps/details?id=imoblife.androidsensorbox&hl=en_GB

9. https://itunes.apple.com/us/app/sensor-kinetics/id579040333?mt=8

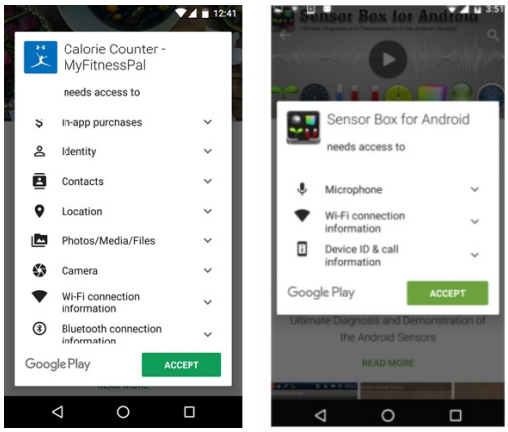

Fig. 3. Examples of over privileged apps

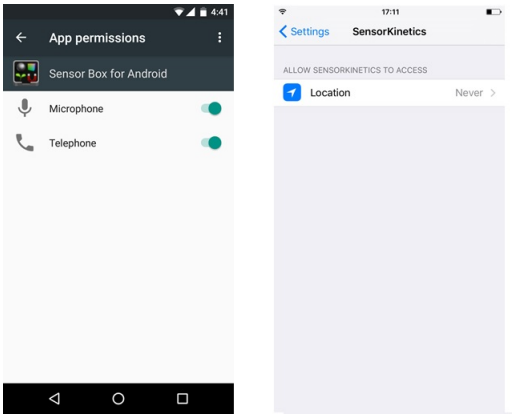

Fig. 4. Sensor apps permissions: Android (left), iOS (right)

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 the pre-granted access to sensors or other OS resources via the system settings, as shown in Fig. 4 [10].

Activity eight: permission review of three pre-installed apps. At this stage, we asked the participants to go through the pre-installed apps on their own devices and chose 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 uninstall it, and why? This form is provided in Appendix A.

At the end of this workshop, we invited the attendees to discuss their opinions on mobile sensor security with their peers and the educators.

4 Results

In this section, we present the results of our analysis on different stages of the workshop.

4.1 General knowledge

Recall that our participants completed the general knowledge form in the beginning of the workshop, before being presented with any information. We present this knowledge level in a stacked bar chart in Fig. 5. As it can be seen, we have categorized these sensors in four groups, as suggested in Section 2.1. In each category, sensors are ordered based on the aggregate percentage of participants declaring they know generally or very well how each sensor works. This aggregate percentage is shown on the right-hand side. In the case of equal percentage, the sensor with a bigger share on being known very well by the participants is shown earlier.

When reading the sensor description page, our participants were generally surprised to hear about some sensors and impressed by the variety. As it can be seen in Fig. 5:

- Our participants knew identity-related sensors (very) well. Although most of these sensors have been available on mobile devices for a longer time, Fingerprint and TouchID came out during 2014 and 2015.
- Apart from NFC (which was extensively adopted by users after the introduction of ApplePay in late 2014), other communicational sensors (WiFi and Bluetooth) were known to the users. When we explained the usage of NFC for contactless payment, our users could recognize it, though its name did not contribute to their knowledge they expressed for it.
- Low-level hardware sensors such as accelerometer and gyroscope seem to be less known to the users in comparison with high-level software ones such as motion, orientation, and rotation, which were named after their functionalities.
- Our participants were generally not familiar with ambient sensors. Some of these sensors, such as ambient light, device temperature, gravity and barometer were better known to the users.

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 picture, unlocking the phone, exchanging files) which users can easily associate with. In contrast, the usage of ambient and movements sensor is not immediately clear to the users. These explicit use cases contribute to a better knowledge people express for the first two categories.

4.2 Perceived risks of sensors

Similar to the above, we present the level of the concern our participants had for each sensor. Following our previous work [23], we limit 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. Note that when our participants completed the concern form, they had not been given with any security knowledge about sensors. This activity was done after they had the description about sensors, and worked with the sensor apps. As it can be seen in Fig. 6:

- Except a few identity-related and communicational sensors, people are generally not concerned, or in some cases only a little concerned, about the risks of sensors to their PINs.
- In the case of the identity-related and communicational sensors, there are only a few sensors which some

10. The option of limiting the access to *While Using the App* was discussed with iPhone users.

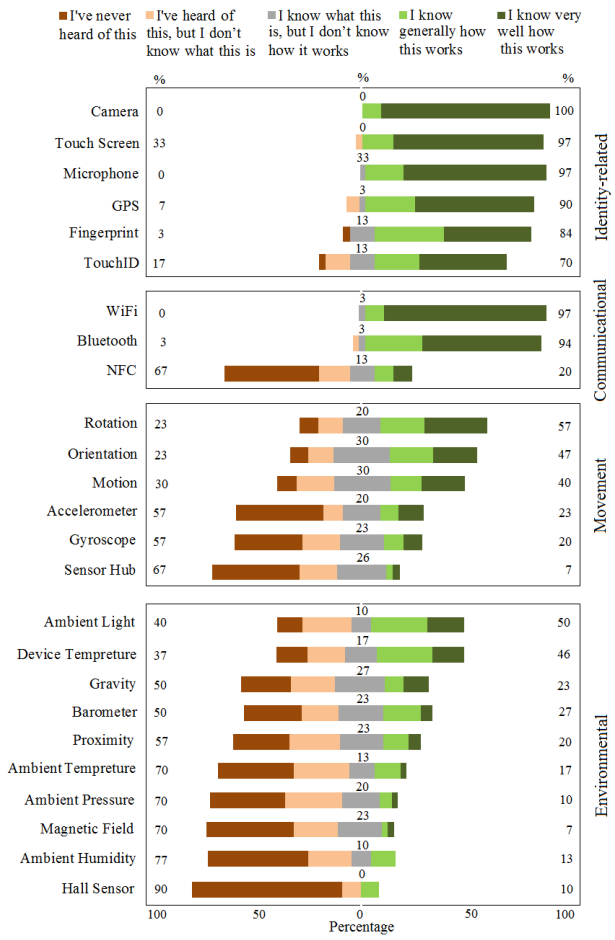

Fig. 5. Self-declared knowledge level of sensors

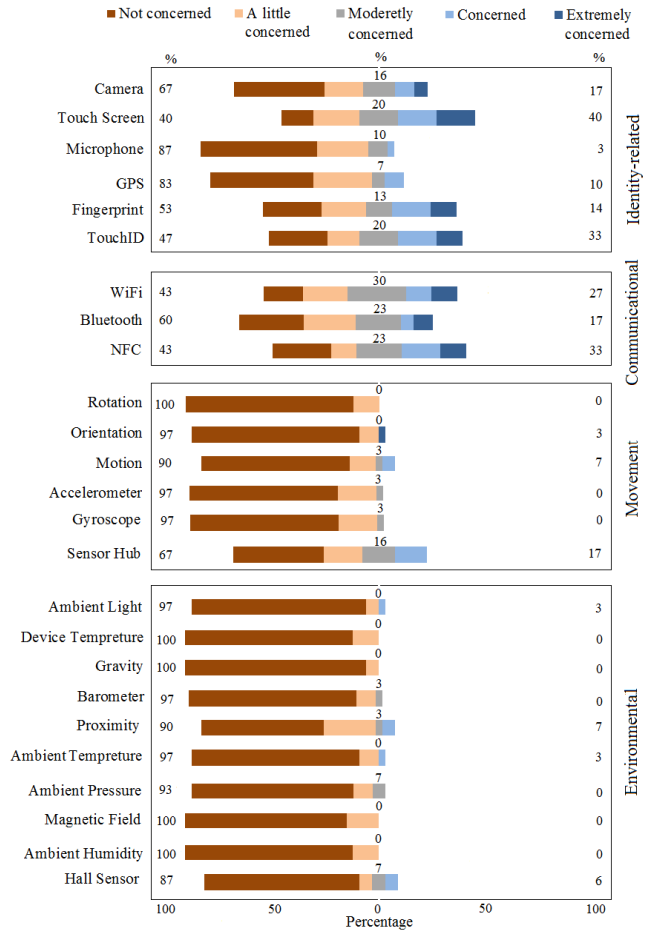

Fig. 6. Self-declared perceived risk of sensors

of our participants were (extremely) concerned regards to their PIN being compromised. These sensors include Camera, Touch screen, Fingerprint, TouchID, WiFi, Bluetooth, and NFC.

- There is a considerable gap between the level of the expressed concern in this study in comparison to the studies we have done in the past [23]. Our participants expressed less concern when they knew the sensor description and worked with sensor apps in the workshop in comparison to when they only knew the description of the sensors via individual interviews [23].

We concluded in our previous work that providing only the description of mobile sensors, would not effect 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, our participants became more concerned after they knew about the sensor description. In this study however, the concern level is lower than what we examined before. This could be due to the confidence that our participants gained about mobile sensors during group activities and via working with sensor apps in the workshop. However, this general knowledge about sensors did not contribute to their inference of possible attacks by sensors on their PINs.

4.3 General knowledge vs risk perception

Figs. 5 and 6 suggest that there may be a correlation between the relative level of knowledge users have about sensors and the relative level of risk they perceive from them. We confirm our observation of correlation using Spearman's rank-order correlation measure [11].

We rank the sensors based on the level of user familiarity, using the same method applied in each category of sensors in Fig. 5. Separately, the levels of concern are ranked too. After applying the Spearman's equation, the correlation between the comparative knowledge (median: "I know what this is, but I don't know how this works", Interquartile range (IQR): "I've never heard of this"-"I know very well how this works") and the perceived risk about different sensors (median: "Not concerned", IQR: "Not concerned"-"A little concerned") is $r = 0.48$ ($p<0.05$). This together with the results we have from [23], suggest that there is 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 (after knowing the sensor description and working with the sensor app).

4.4 App permissions review

In the final part of the workshop, we asked our participants to review the permissions of three pre-installed apps on their devices through the system settings. In this section, the participant had the opportunity to go beyond sensor security and investigate access to all sort of mobile OS resources by apps.

The participants chose a very wide varieties of apps to investigate the permissions; ranging from social networking, banking, shopping, discount apps, etc. In most cases, our participants could successfully identify the functionality of the chosen app and whether it has reasonable permissions or not. 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. Full detail of these completed app permission review forms is available via the first author's homepage.

Uninstalling. Some of our participants expressed their willingness to uninstall certain apps since they were over-privileged. In the comment section, the participants explained that they don't really need these apps, or they can replace it by using a web browser, or they are concerned about their security and privacy. For example, after one of our participants discovered the permissions they have already given to Zara app (camera, contacts, location, storage, and telephone), the participant expressed: "It does not need those things-uninstalled!". Similarly another participant could easily infer that a discount app (Meerkat movies) should not be able to modify/delete SD card, and decided to remove it.

Disabling/limiting access. There were cases where participants could identify the risky extra permissions granted to apps, but instead of uninstalling the app, they chose to disable certain accesses, or limit them to while using the app. For instance, one participant observed that if they disable the access to contacts, storage, and telephone, Spotify would still work. Another participant said that they would occasionally turn off location on Twitter e.g. if they are on holiday. In another example, one of the participants commented: "[I] would remove photos and camera permissions but still use [Uber] app". Another participant commented that they changed the access to location to *while using* in Google Maps.

Leaving as before. In some cases, our participants reviewed the app permissions and did not find them risky. For example, when one of our participants found out that Pay by Phone app has access to camera, the participant commented: "Camera [is] used to take pictures of payment cards".

In some other cases, our participants could identify the over-privileged app, but decided to leave the app and its permissions as before. They expressed various reasons for this decision. For example, one participant chose to continue using Unidays (a discount app) saying that "[I'm] not that concerned that it has access to photos". Another participant said they would not uninstall the Sleep Cycle 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 permissions of MyFitnessPal, they said they would not uninstall it since: "I am addicted to it". Another participant refused to uninstall 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".

Overall, we observe that this activity (app permission review) has 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, and (not) being aware of any real exploit of these permissions.

5 Discussions

5.1 Replicating studies and experiments

Some parts of this paper are presented as report of replicating previously published studies and experiments [23]. We have changed the method of studying people for their general knowledge and concern about sensors on a new set of participants. Previously [23], we had interviewed our participants individually. In contrast, in this paper, we organized a workshop for all participants to sit together and interact. In addition in the past, for assessing the concern level, we only provided our participants with a brief description of sensors. However in this study, on top of the sensor description, we also offered our participants to work with a few sensor apps.

The user general knowledge of sensors reported in this paper confirms our previous results. The level of concern expressed by our participants in this paper is lower than what we observed in [23]. This means that working with sensor apps has decreased the perceived risk level. This is despite the fact that the workshop description contained some security words (please see Section 3). While the level of concern in this study has generally decreased for sensors compared to [23], for movement sensors, this concern reduction is bigger (except sensor hub). We suspect that it is because working with sensor apps makes users more confident about these sensors. On the other hand, the potential threats to the user security posed by an unauthorized access to the movement sensors are not immediately clear. Hence, working with these apps convince the users that these sensors are benign.

We encourage other researchers to replicate studies and experiments of this paper as well as those presented in [23]. In this way, the academic community and the sensor industry will have a better vision on human factors of this emerging technology with more robust results.

5.2 Recommendations to different stakeholders

After we presented the demonstrated attacks [20]–[23] to our participants in the workshop, we observed that they are very shocked about the power of these movement sensors. However, when completing the app permission review activity, they could not see whether certain apps have access to these sensors or not. Hence, even if the mobile users are very well aware of the risk of these sensors to their security and privacy, since mobile apps and websites don't ask for permission for these sensors, users won't have the option to disable their access.

One way to fix this problem, which is commonly suggested by research papers, is to simply ask for permission for all

sensors. However, it will introduce a lot of usability problems. People are already ignoring the permission notifications required for sensors such as camera and microphone. Hence it is a complex usable security problem. We believe that more research (both technical and human dimensions) in the field of sensor security should be carried out by academia. This research should be conducted in collaboration with the industry to achieve impactful results. Based on our research, we conclude the following recommendations:

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 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 to a non-technical audience is a strong medium to disseminate technical research. Part two of our workshop was a presentation on our technical research in Newcastle University. This part can be replaced with any other research in the field of sensor security, without diminishing the workshop goal. The feedback from non-technical audiences will lead a technical research to an impactful direction.

We have published our workshop slides in order to make them available for use by educators and the general public. In addition, 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[11], part of Newcastle University's series of massive open online courses (MOOCs). We strongly encourage researchers/educators to produce educational materials and report their experiences on other methods of sensor security education.

App and web developers. The fact that working with sensor apps did not contribute to the users' risk inference is worrying. Nevertheless, security and privacy issues are very low motivations in the adoption of apps. Hence, App and web developers have a fundamental role in addressing this problem. As discussed in [1], developers are recommended to secure tools with proved utility. Many mobile apps in app stores are *"permission hungry"* [29]. These extra permission requests are likely not understood by the majority of developers who copy and paste this code into their applications, similar to what is discussed in [10]. This is where app developers end up inserting extra permission requests into their code. We advise developers to not copy code from unreliable sources to 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 few 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 O2 priority (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 the participants wrote: *"let the user know why permission is needed for the app to work and choose which features/permissions are reasonable"*.

Mobile users. As we observed in this workshop, mobile users don't 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 mobile devices safer, we advise mobile users to follow the general security practice:

- Some users tend to be lazy 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. 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 vet comprehensively.
- Scrutinise the permission requested by apps before you install them and choose alternatives with more sensible permissions if needed.
- Try to regularly audit the permissions that apps have on your device via system settings.

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

6 Conclusion

In this paper, we reflected the results of a workshop where we mainly explained these three to the 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 measure 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 show that teaching about general aspects of sensors would not immediately improve people's ability to perceive the risks. 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 suggest that there is a lot of room for more focus on education about mobile and sensor technology.

Acknowledgement

We would like to thank Thinking Digital Women for hosting this workshop and the participants who attended the workshop. We would like to thank Dr. Feng Hao, Prof. Aad van Moorsel, Prof. Brian Randell from Newcastle University, and Dr. Siamak F. Shahandashti from York University, UK for their constructive feedback on this paper. All of our user studies were approved by Newcastle University's Ethics Committee.

11. futurelearn.com/courses/cyber-security

References

[1] Ruba Abu-Salma, Anastasia Danilova, M Angela Sasse, Alena Naiakshina, Joseph Bonneau, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *Proceedings of the 38th IEEE Symposium on Security and Privacy*, IEEE S&P '17, 2017.

[2] Android sensors. Available at http://developer.android.com/guide/topics/sensors/sensors_overview.html.

[3] Cheng Bo, Lan Zhang, Xiang-Yang Li, Qiuyuan Huang, and Yu Wang. Silentsense: Silent user identification via touch and movement behavioral biometrics. In *Proceedings of the 19th Annual International Conference on Mobile Computing and Networking*, MobiCom 2013. ACM, 2013.

[4] Henry Bodkin. How the way you hold your smartphone could allow hackers to steal your bank details, 2017. Available online at http://www.bbc.co.uk/newsbeat/article/39565372/the-way-people-tilt-their-smartphonecan-give-away-passwords-and-pins.

[5] Massimiano Bucchi. Science and the Media. 1998.

[6] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. Touch me once and i know it's you!: Implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI 2012. ACM, 2012.

[7] Planet of the phones. From the print edition by The Economist, 2015. Available online at http://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones.

[8] Science Friday. Sensing steps, and perhaps your pin, 2017. Available online at http://www.sciencefriday.com/segments/sensing-steps-and-perhaps-your-pin/.

[9] Location and Sensors APIs. Available at: developer.android.com/guide/topics/sensors/index.html.

[10] Matthew Green and Matthew Smith. Developers are not the enemy!: The need for usable security apis. *IEEE Security and Privacy*, 14(5):40–46, September 2016.

[11] Jan Hauke and Tomasz Kossowski. Comparison of values of pearson's and spearman's correlation coefficients... 2011.

[12] Alex Hern. Tilted device could pinpoint pin number for hackers, study claims, 2017. Available online at http://www.theguardian.com/technology/2017/apr/11/tilted-device-could-pinpoint-pin-number-for- hackers-study-claims.

[13] Stephen Hilgartner. The dominant view of popularization: conceptual problems, political uses. *Social studies of science*, 20(3):519–539, 1990.

[14] Xing Jin, Xunchao Hu, Kailiang Ying, Wenliang Du, Heng Yin, and Gautam Nagesh Peri. Code injection attacks on html5-based mobile apps: Characterization, detection and mitigation. In *Proccedings of 21th ACM Conference on Computer and Communications Security*, CCS 2014. ACM, 2014.

[15] Manfred Kloiber. Swenn die sensoren zum sicherheitsrisiko werden (when the sensors become a safety risk), 2017. Available online at http://www.deutschlandfunk.de/smartphones-wenn-die-sensoren-zum-sicherheitsrisiko- werden.684.de.html?dram:article_id=383916.

[16] Haoyu Li, Di Ma, Nitesh Saxena, Babins Shrestha, and Yan Zhu. 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. ACM, 2013.

[17] Rene Mayrhofer and Hans Gellersen. Shake well before use: Authentication based on accelerometer data. In *Pervasive Computing*. Springer Berlin Heidelberg, 2007.

[18] Maryam Mehrnezhad, Mohammed Ali, Feng Hao, and Aad van Moorsel. Nfc payment spy: Privacy attacks on contactless payments using NFC-enabled mobile. In *Proccedings of Third International Conference on Research in Security Standardisation*, SSR 2016. Springer International Publishing, 2016.

[19] Maryam Mehrnezhad, Feng Hao, and Siamak Shahandashti. Tap-Tap and Pay (TTP): Preventing the mafia attack in NFC payment. In *Proccedings of Second International Conference on Research in Security Standardisation*, SSR 2015. Springer International Publishing, 2015.

[20] Maryam Mehrnezhad, Ehsan Toreini, and Feng Shahandashti, Siamakand Hao. Stealing pins via mobile sensors: Actual risk versus user perception. In *The 1st European Workshop on Usable Security*, EuroUSEC 2016, 2016.

[21] Maryam Mehrnezhad, Ehsan Toreini, Siamak Shahandashti, and Feng Hao. 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. ACM, 2015.

[22] Maryam Mehrnezhad, Ehsan Toreini, Siamak Shahandashti, and Feng Hao. Touchsignatures: Identification of user touch actions and PINs based on mobile sensor data via javascript. *Journal of Information Security and Applications*, 26:23–38, 2016.

[23] Maryam Mehrnezhad, Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao. Stealing pins via mobile sensors: actual risk versus user perception. *International Journal of Information Security*, pages 1–23, 2017.

[24] BBC Newsbeat. The way people tilt their smartphone can give away passwords and pins, 2017. Available online at http://www.bbc.co.uk/newsbeat/article/39565372/the-way-people-tilt-their-smartphone-can-give-away-passwords-and-pins.

[25] Laurent Simon and Ross Anderson. 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, pages 67–78. ACM, 2013.

[26] Sina. Phone gyroscope or spoiler information look at the tilt angle to guess the password, 2017. Available online at http://www.tech.sina.com.cn/it/2017-04-13/doc-ifyeimqc3202830.shtml.

[27] Sergio Sismondo. *An introduction to science and technology studies*, volume 1. Wiley-Blackwell Chichester, 2010.

[28] Raphael Spreitzer. 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. ACM, 2014.

[29] Vincent F. Taylor and Ivan Martinovic. A longitudinal study of app permission usage across the google play store. 2016. Technical report available at http://arxiv.org/abs/1606.01708.

[30] Agencia Telam. Dificil pero no imposible: el modo en que se inclina el celular al usarlo puede revelar contrasenas (difficult but not impossible: the way the cellphone is tilted when using it can reveal passwords), 2017. Available online at http://www.lavoz.com.ar/tecnologia/dificil-pero-no-imposible-el-modo-en-que-se-inclina-el-celular-al-usarlo- puede-revelar-co.

[31] The Economic Times. The way you type on your smartphone can help hackers steal your bank details, 2017. Available online at http://www.economictimes.indiatimes.com/magazines/panache/the-way-you-type-on-your-smartphone-can- help-hackers-steal-your-bank-details/articleshow/58125226.cms.

[32] Device and sensors working group, 2016. Available online at https://www.w3.org/2009/dap/.

[33] W3C Working Draft Document on Device Orientation Event. Available at http://www.w3.org/TR/orientation-event/.

[34] Brian Wynne. Misunderstood misunderstanding: Social identities and public uptake of science. *Public understanding of science*, 2016.

[35] Zhi Xu, Kun Bai, and Sencun Zhu. 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. ACM, 2012.

Appendix

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.
- Touch Screen: enables the user to interact directly with the display by physically touching it.
- WiFi: is a wireless technology that allows the device to connect to a network.

Sex	Age	Job/Background	Mobile (y)
f	27	Tech communication	7
f	43	Service director	8
f	28	Finance manager	4
f	45	Graphic designer	15
f	23	Designer	6
f	23	Social media	6
f	47	Teacher	9
m	32	Manager	6
f	31	Research director	7
f	29	Costumer service manager	7
f	27	Content strategist	4
f	45	Teacher	10
f	29	Business analyst	7
f	32	Photographer	13
f	46	Management consultant	8
f	24	Research assistant	10
m	32	Student	7
f	51	Development Manager	11
f	28	IT manager	8
f	28	Marketing manager	8
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

TABLE 3
Participants' self-reported demographics in the two studies, (y) indicates the years of owning a smartphone

- Bluetooth: is a wireless technology for exchanging data over short distances.
- NFC (Near Filed Communication): is a wireless technology for exchanging data over shorter distances (less than 10 cm) for purposes such as contacless 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 in.
- Sensor Hub: is an activity recognition sensor and its purpose is to monitor the device's movement.

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					
Gyroscope					
GPS					
Sensor Hub					
Ambient Temperature					
Accelerometer					
Magnetic Field					
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 4
This form was used for activity one

	Risk to PIN				
Sensor	Not Concerned	A little Concerned	Moderately Concerned	Concerned	Extremely Concerned
Bluetooth					
Gyroscope					
GPS					
Sensor Hub					
Ambient Temperature					
Accelerometer					
Magnetic Field					
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 5
This form was used for activity six

No.	App name	Purpose	(Extra) permissions	Would you uninstall?	Why?
1					
2					
3					

TABLE 6
This form was used for activity eight