Fatal Attraction: Identifying Mobile Devices Through Electromagnetic Emissions

Beatrice Perez
University College London
London, UK
beatrice.perez.14@ucl.ac.uk

Mirco Musolesi
The Alan Turing Institute
University College London
London, UK
m.musolesi@ucl.ac.uk

Gianluca Stringhini
Boston University
Boston, MA, USA
gian@bu.edu

ABSTRACT

Smartphones are increasingly augmented with sensors for a variety of purposes. In this paper, we show how magnetic field emissions can be used to fingerprint smartphones. Previous work on identification rely on specific characteristics that vary with the settings and components available on a device. This limits the number of devices on which one approach is effective. By contrast, all electronic devices emit a magnetic field which is accessible either through the API or measured through an external device.

We conducted an in-the-wild study over four months and collected mobile sensor data from 175 devices. In our experiments we observed that the electromagnetic field measured by the magnetometer identifies devices with an accuracy of 98.9%. Furthermore, we show that even if the sensor was removed from the device or access to it was discontinued, identification would still be possible from a secondary device in close proximity to the target. Our findings suggest that the magnetic field emitted by smartphones is unique and fingerprinting devices based on this feature can be performed without the knowledge or cooperation of users.

CCS CONCEPTS

• **Security and privacy → Side-channel analysis and countermeasures**.

KEYWORDS

fingerprint, magnetic field, sensor readings, supervised learning

ACM Reference Format:
Beatrice Perez, Mirco Musolesi, and Gianluca Stringhini. 2019. Fatal Attraction: Identifying Mobile Devices Through Electromagnetic Emissions. In *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3317549.3319726

1 INTRODUCTION

Smartphones are equipped with a wide range of sensors that measure a variety of physical quantities including light, humidity, orientation, acceleration, pressure, proximity, and location [9]. The information collected is used to enhance user experience (e.g., automatic screen brightness adjustment and energy saving mode during phone calls), to improve services (e.g., location-based services like Uber and calendar reminders based on travel time), and also as a commodity that benefits third parties (e.g., the use of microphones in mobile devices to respond to ultrasonic beacons in order to measure the audience of an advertisement [36]). In many instances, identifying a device or a user is trivial and expected (particularly for services that require registration) but for unknown third parties (i.e., secondary data collectors that gain access to the data without users being explicitly aware of their activities) or for applications where the user expects to remain anonymous (e.g., applications for gaming, weather, and the news), many of these sensors potentially expose the user's private information [37].

The magnetometer is the sensor responsible for measuring the magnetic field in the environment of the phone. It is commonly available in all platforms and is usually combined in the same chip with the sensors for linear acceleration and gyration. Apple, with the release of the iPhone 3GS in 2009, added magnetometers to the sensor array available on their devices [11]. The Android operating system opened API support that same year with the release of Cupcake (Version 1.5) [8]. The magnetometer provides a new means to effectively fingerprint mobile devices in a manner that is *transparent* to users. Accessing magnetometer readings requires no permission declaration on either platform and the fact that the magnetic field is radiated means that it can be measured from outside the phone.

In this paper, we show that measurements of the magnetic field can be used for identification. Every electronic device generates a magnetic field. In smartphones, it varies depending on the components active in the phone, the tolerance level of each component, the degradation of the manufacturing materials on the phone, and the topology of the underlying circuit. Each cell phone contains hundreds of thousands of transistors alone and every component in the phone is unique. Previous work shows that two seemingly identical components have unavoidable differences that arise from the manufacturing process [43]. This variability has been leveraged for identification of sensors and other integrated circuits [18, 32]. We present two identification attacks that rely on magnetic fields: a *malware-based* approach that can be carried out by any application installed on a device that contains a magnetometer and a *proximity-based* attack that can identify any device inside the range of the external sensor measuring the magnetic field.

In the malware attack, the device on which the app is installed is both the source and the instrument of collection of the magnetic field. To demonstrate the feasibility of the attack, we released an

WiSec '19, May 15–17, 2019, Miami, FL, USA

ACM ISBN 978-1-4503-6726-4/19/05…$15.00
https://doi.org/10.1145/3317549.3319726

app on the Play Store. Our final dataset comprises 175 devices with a minimum of 10,000 readings per device. The application collects readings from the magnetometer and transmits them back to our servers for analysis. We use these readings to generate *fingerprints* with which we identify devices. We show that selecting 1,000 randomly spaced readings is sufficient to identify one device from a group of 175 with an accuracy of 98.9%. To mitigate the risk to users, we propose adding sensor readings to the permission platform. While this would not directly affect the generation of the fingerprint, it would at least serve as a warning system to users.

However, even after protecting the readings with the new permission, bypassing this safeguard is still possible: we present a second attack where the magnetic field readings are collected from a device in close proximity to the target. Here, the requirements (i.e., the sensor and the software that collects the readings) have shifted to the attacker and the victim has no possible means of detection. The only countermeasure for this attack would be to increase the shielding in the target device and reduce or, alternatively, eliminate all electromagnetic emissions. However, we do not consider this as a viable solution since it will render a device completely unusable.

This work is not the first in considering magnetic field emissions in the context of privacy and security. Previous work shows that electromagnetic leaks can be used to determine the instruction being executed by a processor [20] and to extract data from a system through the manipulation of memory access [27, 44] or through write instructions to the hard drive [15]. However, *this is the first work to use magnetic fields as a way to achieve identification.* There are some *practical* difficulties related to device fingerprinting in general. First, the fingerprinting accuracy attained with a specific set of features is likely dependent on the total number of devices present in the dataset. Second, the market diversity for mobile devices with all the possible vendors, carriers, and designs makes it difficult to find a single universal feature for identification. We conduct a user study with 175 devices over a period of four months using a feature common to all electronics.

We summarize our contributions as follows:

- We investigate and characterize the emission and collection of magnetic fields from a large set of off-the-shelf mobile devices, discussing how the fingerprint can be used for an identification attack.
- We present two identification attacks based on magnetic fields that enable adversaries to track devices remotely due to the lack of permission protection from mobile platforms and the properties inherent to electromagnetic fields. Moreover, these fingerprints can be computed by anyone at any time and they are as of now undetectable.
- We propose a methodology to process sensor readings and through the use of two machine learning algorithms, *k*-Nearest Neighbors (KNN) [22] and Random Forests (RF) [17]. We show that, by means of this approach, we are able to achieve correct identification of the devices with up to 98.9% accuracy in 1,000 readings.
- We discuss countermeasures for each attack and we outline the open research directions in this area.

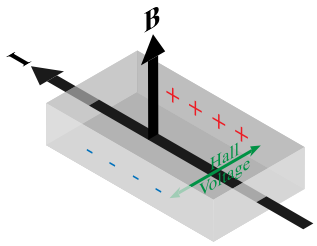


Figure 1: Measuring the Magnetic Field from a MEMS device. The flow of current (I) through a conductor polarizes the material. The resulting voltage between opposite sides is known as the Hall Voltage, from which you can derive the magnetic induction B.

2 THE MAGNETOMETER SENSOR

The popularity and use of magnetic sensors have exploded in the last decades and, while there are different technologies capable of measuring magnetic fields, the most common distribution for mobile devices is the Micro-ElectroMechanical Systems (MEMS) [19]. MEMS is the name given to batch fabrication techniques that allow for the combination of miniaturized (typically in the range of micrometers to millimeters) mechanical and electrical systems that generate a response in the macro scale. These silicon-based systems are composed of mechanical structures, sensors, actuators, and electronics all in the same chip [6].

Android classifies, the magnetometer as a position sensor [9]. In most devices it is contained in a 9-axis MEMS chip where, along with the accelerometer and the gyroscope, provides data over 3 axes [4]. MEMS magnetic sensors operate by measuring the potential difference (i.e., voltage) across two sides of a conductive material generated by a current flowing in the presence of a magnetic field. This phenomenon, called Hall Effect, is an established method to measure the intensity of magnetic fields. Figure 1 provides a visualization of the operation of the sensor. In reality, the measure is an approximation: while we are theoretically interested in the value of the magnetic field (H) measured in amperes per meter (A/m), the sensor actually measures the magnetic induction (B) measured in Tesla (T). Equation 1 shows the relationship between the magnetic field and the magnetic induction. The factor μ in the equation corresponds to the magnetic permeability of the material. While this value varies depending on the medium through which the wave propagates, we assume that the medium is similar for all mobile devices (i.e., plastic, air, and other electronics). We assume that the value of μ is constant for all the readings and we use H as a proxy of B [39].

$$B = \mu H \tag{1}$$

The Android Sensor Stack controls the access to the magnetometer [7]. It has seven levels of abstraction that go from the low-level hardware component to the high-level software application. The lower layers are implemented by the hardware manufacturers and include drivers and library interfaces to the sensor. The higher levels are determined by Google and are made available for developers to use through the Application Programming Interface (API). The

Table 1: Starting from the left, column one lists the two types of magnetic field events. The middle columns contain the size and description of the response. Finally, the column on the far right contains the units corresponding to the values reported.

Sensor Call	Response	Description	Units
TYPE_MAGNETIC_FIELD	SensorEvent.values[0]	Geomagnetic field strength: x axis	μT
	SensorEvent.values[1]	Geomagnetic field strength: y axis	
	SensorEvent.values[2]	Geomagnetic field strength: z axis	
TYPE_MAGNETIC_FIELD_UNCALIBRATED	SensorEvent.values[0]	Geomagnetic field strength (without hard iron calibration): x axis	μT
	SensorEvent.values[1]	Geomagnetic field strength(without hard iron calibration): y axis	
	SensorEvent.values[2]	Geomagnetic field strength(without hard iron calibration): z axis	
	SensorEvent.values[3]	Iron bias estimation: x axis	
	SensorEvent.values[4]	Iron bias estimation: y axis	
	SensorEvent.values[5]	Iron bias estimation: z axis	

API allows an application to register a sensor and it can be programmed to collect a response upon a value change event. Table 1 describes the data structure used by Android to represent the readings of the magnetic field. The magnetometer has the ability to output both the raw sensor readings and a measure calibrated for internal interference. The calibrated reading is the combination of the uncalibrated reading and some bias. This bias is the internal magnetic field generated by the phone.

3 OVERVIEW OF THE ATTACKS

We consider an adversary who aims to establish the identity of a device without directly requesting the Unique Device Identifier (UID) provided by the platform. Android protects the UID through the telephony permission, which is classified as a dangerous permission, and the attacker may not want to alert the user as to their intention [12]. The methodology we propose results in a strong component of the identity (with an accuracy of over 90%) being revealed to attackers without the consent of the user. We assume that the adversary can either have an application installed on the target device (*malware attack*) or get a secondary device in close physical proximity to it (*physical proximity attack*). We anticipate the physical proximity attack to be relevant in situations where the phone is likely to remain static for any period of time. This might include wireless charging stations, coffee shops, or workplace environments where an employer could potentially track the movement of employees from the identification and localization of their phones.

3.1 Malware Attack: Identification Through the Analysis of the Bias

We first consider a malware attack where the primary goal of the adversary is to maximize the number of devices to fingerprint. The underlying requirements are that each phone has both a magnetometer and an app that collects the readings and transmits them back to the attacker. The app gets installed on the phone through usual means: social engineering or drive-by downloads.

The magnetic induction (B) reported by the OS is measured in the 3D coordinate plane. The Hardware Abstraction Layer interface (HAL) provided by Android gives developers six values corresponding to the raw sensor readings and the device's internal bias each reported in three dimensions.

In this first attack we use the magnetic field emitted by the phone (i.e., the *bias*) as the input feature to the classifier. Section 5 provides an in-depth analysis of the attack, including a description of our use of each of the fields in Table 1.

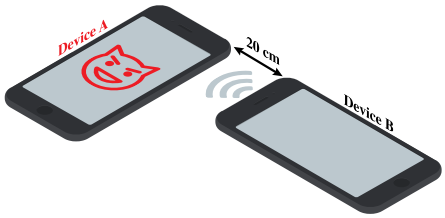


Figure 2: The environmental magnetic readings of one device capture the emissions of proximate devices.

3.2 Physical Proximity Attack: Identification Through External Readings

The first attack is an *internal* software-based attack. The sensor, while present in the device, is not being used to assess the environment in which it operates but rather to report a value that comes as the outcome of a calibration equation. In other words, there is no evaluation of external phenomena, but only of the intrinsic characteristics of the MEMS-based sensor. Instead, in the second attack, the sensor is used to measure the radiation coming from the device to be identified, i.e., it is therefore an *external* attack. Figure 2 presents the second attack scenario. We have two devices: a target or victim and an adversary or attacker. The requirement is that the attacker has a magnetometer and the software with which to collect and process the readings.

The challenge is to extract a set of characteristics that describes the behavior of the signal emitted by the targeted device from the environmental signal collected by the attacker. The deployment of the second attack is described in Section 6 and the features selected for identification are discussed in detail in Section 6.2.

4 DESCRIPTION OF THE IDENTIFICATION MODEL

To show the feasibility of the method we propose, we follow three steps: data collection; feature definition and analysis; and, identification. Each step will be discussed in detail throughout the paper.

To carry out identification, we use supervised classification algorithms. We are interested in two pieces of information: a unique identifier for each device which will be used as ground truth (i.e., the label of each observation) and the measure of the magnetic field emitted by each device (i.e., the separable features).
For each device d_i in our dataset $\mathbf{D}$ of size $|\mathbf{D}| = M$

$$\mathbf{D} = \{d_1, d_2, \ldots, d_i, \ldots, d_M\},$$

we have a set of L independent readings

$$\mathbf{R}^{d_i} = \{\mathbf{r}_1^{d_i}, \mathbf{r}_2^{d_i}, \ldots, \mathbf{r}_j^{d_i}, \ldots, \mathbf{r}_L^{d_i}\},$$

with i being the unique identifier of each device and, therefore, the label assigned to the appropriate reading during classification. Each reading $r_j^{d_i}$ for device d_i is composed of N features on which the classifier is built.

$$\mathbf{F}(\mathbf{R}_j^{d_i}) = \{f_1(\mathbf{R}_j^{d_i}), f_2(\mathbf{R}_j^{d_i}), \ldots, f_k(\mathbf{R}_j^{d_i}), \ldots, f_N(\mathbf{R}_j^{d_i})\}.$$

The model trained on $\mathbf{F}(\mathbf{R}_j^{d_i})$ is then evaluated on unseen unlabeled observations. We use d_{unk} to denote a reading taken from an unknown device. This will be the case for all the testing observations.

The outcome of each test $\mathbf{R}_j^{d_{unk}}$ is a conditional probability distribution given by $Pr(d_i|\mathbf{F}(\mathbf{R}_j^{d_{unk}}))$ for each device d_i in $\mathbf{D}$. Finally, we use the optimal decision rule to determine the device $\hat{d}$ to which $\mathbf{R}_j^{d_{unk}}$ belongs to

$$\hat{d} = argmax_{d_i} Pr(d_{unk} = d_i|\mathbf{F}(\mathbf{R}_j^{d_{unk}})).$$

If the predicted device $\hat{d}$ matches the ground truth (i.e., the true label of the reading), which we have for the testing set, we consider the test a success and classify it a *hit*. If, alternatively, the observation is misclassified, then it becomes a *miss*.

To summarize, we can formulate our research question as follows: *given a set of devices, are the differences in the characteristics of the radiated emissions between each device sufficient to uniquely identify each one of them?*

5 MALWARE ATTACK: IDENTIFICATION THROUGH THE BIAS READINGS

The first set of results we present are with respect to the malware attack, i.e., an attacker that wishes to remotely identify devices such as phones and tablets. The main challenge in remotely identifying devices is finding a weakness that can be accessed across all models and all manufacturers. Like for previous studies, the success of the malware attack depends on the device having the appropriate hardware. Given the popularity and widespread use of the magnetometer, we accept this as a reasonable assumption. To collect sensor information, an attacker only requires access to the API. The most natural way for data to be collected and transmitted is through an application. In order to use it they would need to request network access permission to send information. Alternatively, as it was shown in [16], the attacker might gain access to the readings through a browser application and generate a signature that way. In this work, we develop an application to access `TYPE_MAGNETIC_FIELD_UNCALIBRATED` and collect the 3D readings from the phone's magnetometer. From the six readings we obtain from each sensor event (see Table 1), we focus on those that correspond to the internal bias of the phone. The values for the *bias* are constant for a session and we will show that only a few measurements are sufficient to generate a robust signature. Moreover, once generated, we observed that the signature is stable over time and therefore the frequency with which the sensor must be sampled to maintain accuracy is less than once every two months.

One implication of this attack is the ability of service providers (and other interested parties) to track users across multiple devices by linking and distinguishing different devices through log-in events; alternatively, it can be used to recognize the same device when the application has been removed then reinstalled, or to link multiple accounts that connect from the same device.

5.1 Ethics

While we are only identifying devices, the typically exclusive relationship between owner and device (as well as their proximity) implies we are indirectly identifying users. In addition to sensor readings, we collected basic demographic information as well as unique device identifiers that could be traced back to individuals. For these reasons, we submitted this project to our institution's review board and received ethical approval for this work.

Each participant had access to an overview of the project as well as details on the type of data that would be collected throughout the study. Additionally, the information sheet and the informed consent form are available on the project's website as well as withdrawal procedures and a contact email in case of any follow-up questions.

5.2 General Characteristics of the Dataset

To carry out the attack, we developed the app *My Magnetic Field*, distributed through the Google Play Store. In exchange for their participation, users were able to see (i) the value of the sensor; (ii) an electronic compass; and (iii) a heat map showing the intensity of the magnetic field at the locations of the data points.

The app was installed by 315 users in 15 countries. We identified 41 manufacturers with 61% of all devices belonging to the top 5 most popular brands (i.e., Samsung, Xiaomi, Huawei, Motorola, and Lenovo) and a total of 187 distinct models. The magnetometers can all be traced back to 14 vendors, the most popular being Yamaha Corporation. We also found that the same phone manufacturer may have more than one company supplying their sensors.

From the dataset, we discarded all devices for which we had less than 33 minutes 20 seconds of data (the equivalent of 10,000 readings) and all those users that installed the application on phones that did not have a magnetometer. We also deleted entries for which the magnetic field readings were all reported as $0\mu T$. The final dataset contains readings from 175 devices.

5.3 Classification Task

Figure 3 provides a high-level view of the distribution of the magnitude of the magnetic field for 30 sample devices. We observe that the classes are not easily separable: the values are clustered

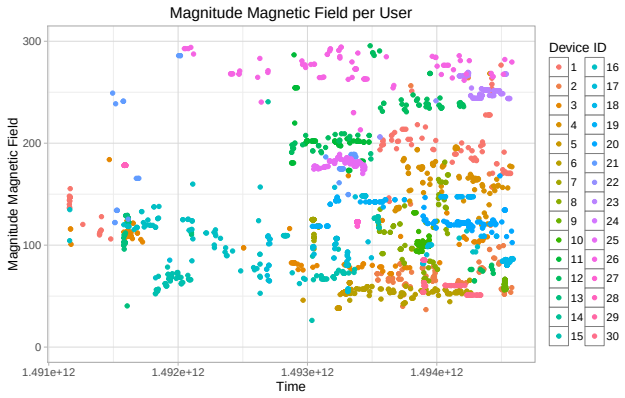


Figure 3: Magnitude of the *bias* for a subset of users.

s	classifier	precision	accuracy
10,000	KNN	0.995 (±0.019)	0.995 (±0.0001)
	RF	0.995 (±0.016)	0.995 (±0.0001)
1,000	KNN	0.989 (±0.002)	0.989 (±0.0004)
	RF	0.988 (±0.002)	0.988 (±0.0003)
100	KNN	0.964 (±0.0005)	0.964 (±0.001)
	RF	0.957 (±0.0004)	0.957 (±0.002)
10	KNN	0.888 (±0.0001)	0.871 (±0.011)
	RF	0.869 (±0.0001)	0.840 (±0.015)

Table 2: Precision and Accuracy for the classification of 175 devices. In the table, *s* denotes the number of readings or samples included in the training set.

together, often overlapping. The behavior displayed suggests that, while the emissions of each device are not random, boundary-based algorithms are not likely to be effective.We chose Random Forests (RF) [17] and *k*-Nearest Neighbors (KNN) [22] for the classification task. We chose RF for its robust behavior in the presence of noise and KNN for its distance-based selection of the predicted class.

In this paper, we use the term model to refer to the evaluation of an algorithm with specific training data (i.e., a classifier with a defined dataset). The values of the parameters required for each algorithm were chosen as a combination of best practices and empirical results through the use of the grid search algorithm in scikit-learn [38]. KNN requires two parameters to be set: the number of neighboring points to be considered in the class assignment of the unlabeled data (i.e., the value of k) and the definition of the distance metric that links any two points. In our KNN models, we use Euclidean distance as the metric between two points as recommended in [42] and $k = 1$ as the optimal value reported by the grid search.

5.4 Feature Generation

The sensor stack introduced in Section 2 provides access to the different sensors (and their corresponding data streams) available in the device. There are two possible values that may be used to access magnetometer readings: `TYPE_MAGNETIC_FIELD` and `TYPE_MAGNETIC_FIELD_UNCALIBRATED`. Equation 2 shows the relationship between observations collected using each of these values. In the equation below, each element is a vector that contains features in three axes: x, y, and z. $\mathbf{R}_{unC}$ contains the raw readings collected from the *uncalibrated* variable and $\mathbf{R}_C$ corresponds to radiation readings external to the phone. The values for $\mathbf{R}_{IB}$ represent the internal bias of the phone, in other words, the magnetic field emitted by the device that is expected to interfere with the environmental measure.

$$\mathbf{R}_{unC} = \mathbf{R}_C + \mathbf{R}_{IB} \tag{2}$$

The physical interpretation of Equation 2 confirms the feasibility of the attack: each device does, in fact, generate a field that is calculated at run-time which interferes with the environmental reading. Essentially, the specification states that the raw sensor readings from `TYPE_MAGNETIC_FIELD_UNCALIBRATED` are the environmental magnetic field as well as the noise introduced by the device itself (i.e., the internal magnetic field of each phone), which they refer to as bias.

The correction formula for each sensor is provided by the device manufacturer. However, we know from the SDK that the bias correction takes into account three factors: the internal temperature of the phone, the internal interference generated by electrical components in the device (i.e., hard-iron calibration), and the internal interference created by any shielding materials contained in the device (i.e., soft-iron calibration) [8]. In a tri-axial MEMS magnetic sensor, the corrections, like the measurements, are reported in three dimensions. Table 1 contains the API's description of the values returned by the sensor and the difference between the calibrated and uncalibrated readings.

In all the experiments presented in this section, we use the values of the *bias* reported in three axes, x, y, and z with respect to each device, as the input features for each of the classifiers. We treat measurements as independent data points (i.e., we do not consider in our analysis the temporal relationship between consecutive measurements). As we will show in the following sections, given the high accuracy of the attack, there was no need for more complex manipulation of the input data. Rather than being detrimental to the proposed idea, its simplicity showcases the effectiveness of the method for identification.

5.5 Results

The magnetic field radiated by each device generates a unique signature that can be accessed through the sensor stack by the bias values reported in `TYPE_MAGNETIC_FIELD_UNCALIBRATED`. In Table 2, the values presented are an aggregation over 60 runs of each model. The left-most column (s) contains the number of measurements per device used to train each model. Figure 4 shows the influence of the number of observations included in the training set for each device. For completeness, we also ran the experiments following a 10-fold cross-validation scheme for each model and found the results to have no significant difference to the ones presented using aggregated randomized sampling. Combined, these results show that the accuracy does not reflect models that are overfitted but rather a true identifier latent in the data.

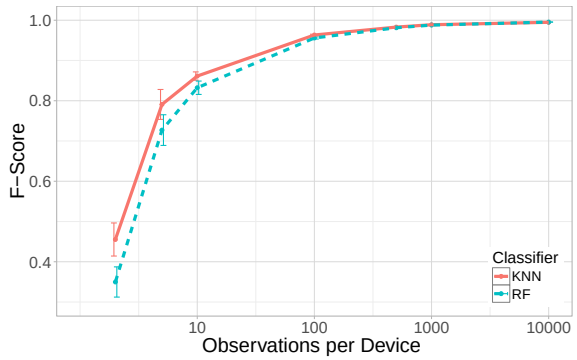


Figure 4: Impact in classification from the number of observations per device for 175 devices.

In terms of the success of the attack, Table 2 shows that for the same number of users, higher accuracy requires an increase in the number of observations per user. In Section 5.2 we discussed that all valid users have at least 10,000 observations. As mentioned above, each experiment was conducted 60 times and the results are an average over all the runs. For each user (in every iteration), all observations (ordered by time) are split into a 70/30 proportion for training and testing data respectively. The observations used in the algorithm are chosen randomly from all data points collected for each user.

5.5.1 Battery Consumption: The Influence of Voltage on Electromagnetic Emissions. Given the results presented in Table 2, one legitimate concern might be that, when measuring the internal magnetic field, the state of the battery is driving the measurement. In other words, the battery status might heavily influence the identification results, making them unreliable. To rule this possibility out, we now look at the influence of battery discharge on the magnetic emission of the device.

As discussed in Section 2, the magnetic field emitted by the phone is a byproduct of the current flowing through a device at any given time. However, measuring the current is not trivial and prone to error. To test the effect of battery discharge, we performed a controlled experiment on 10 phones where we measured both the battery levels and the radiation emitted by the phone. All of the measurements were collected at the same location and similar circumstances. Each device was set to stream an 8-hour video with the screen brightness and volume at maximum settings. Each experiment took on average 5 hours.

Figures 5a and 5b show an example of the typical behavior observed. In Figure 5a the magnetic field is presented as a function of the battery percentage. Comparing these readings to those presented in Section 6.1, we can see that battery depletion serves as a proxy for time and, as evidenced by the trendlines shown in red, the two variables are nearly independent. In contrast, Figure 5b shows that the voltage and the battery depletion have a very strong correlation with a coefficient of approximately 0.9994. The physical explanation for this is that, as the battery of the phone is used, the voltage in the battery falls. Once the voltage is not sufficient to sustain the current that is required for the operation of the device, the phone shuts down with the battery depleted. The relationship between voltage, current and resistance is given by Ohm's Law as $V = IR$ where V is the voltage, I is the current, and R the resistance. Both the empirical evidence and the physical explanation attest to the fact that in using magnetic field readings, we are not identifying the battery level of the phone.

5.5.2 Unique-in-a-line: Differentiating Between Devices in Semi-Controlled Environments. The dataset described in Section 5.2 contains readings from devices of the same brand and indeed the same model. However, given that we do not achieve perfect classification, it is important to understand whether the values provided by the API are the same for all devices of the same model or whether they are unique to a device. Moreover, from Section 5.5.1 we learned that the magnetic field depends also on the resources in use, and therefore, it would be equally as important to determine whether we can distinguish between devices executing the same task.

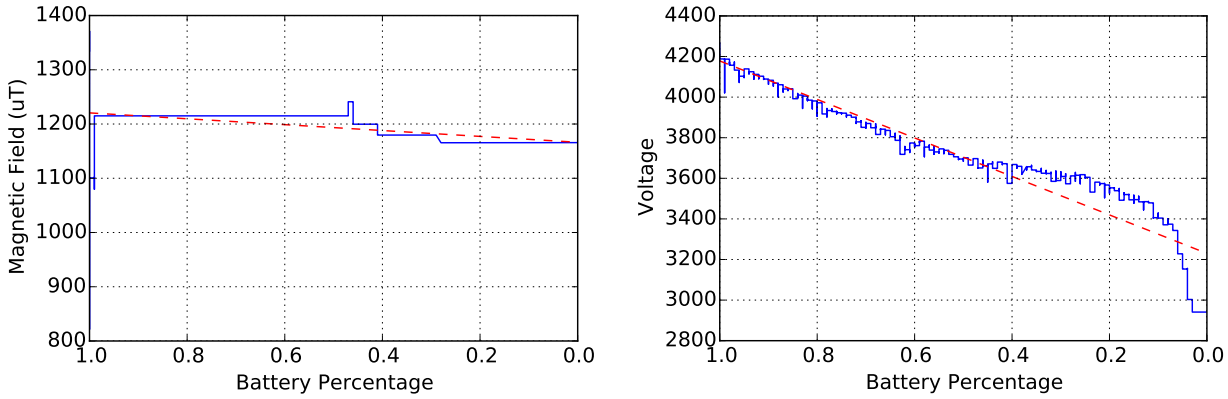
To test both these scenarios we created a second application that triggers a predefined sequence of tasks over the span of 45 seconds. This sequence includes playing a video from the phone's internal memory, a controlled-step increase and decrease of the screen's brightness, and the calculation of two Fibonacci numbers. Our aim was to standardize the behavior of the phone when collecting measurements. We tested this on four Nexus6 devices purchased at the same time, running the application simultaneously, at the same location. We ran the application 10 times on each phone and computed a leave-one-session-out cross validation scheme where we train on nine iterations and test on the remaining one (for each phone). We repeat this 10 times, leaving a different session out each time, then aggregate the results.

In this experiment we achieved perfect classification. Every test value was assigned to the correct device in every iteration. The magnetic field emitted by a phone is not hard-coded into all devices of the same model and while it varies with the level of activity of a phone, different devices exhibit different values.

5.5.3 Impact of Geography: Understanding the Spatial Sensitivity of the Measurements. Another external factor that may influence results is the location of the device at the time of the measurement. In attempting to identify each device, we may be inadvertently fixating on its environment. One form of environmental noise is the presence of significant sources of radiation (e.g., transmission lines, electric substations, thunder storms, etc.) close to the measurement device [5, 34].

Magnetic fields that result from natural events are in the range of micro(μ) and milli(m) Tesla (T). For human-generated emissions, the World Health Organization suggests a maximum dose of 2 T with a recommended occupational exposure of no more than 200 mT [1]. Each country has its own regulations but, as the values we find are in the range of μT, both natural and man-made events have the potential of affecting our results. We define geographic independence as the ability to correctly classify a device using readings from a previously unobserved location.

To test for geographic independence we used the application described in Section 5.5.2 and collected readings at 10 different locations in London. Locations include public transport (buses and subways), coffee shops, university laboratories, restaurants, stores,



(a) Magnetic field as a function of battery consumption for a Motorola Nexus 6.

(b) Voltage as a function of battery consumption for a Motorola Nexus 6.

Figure 5: Influence of battery state on the generated magnetic field

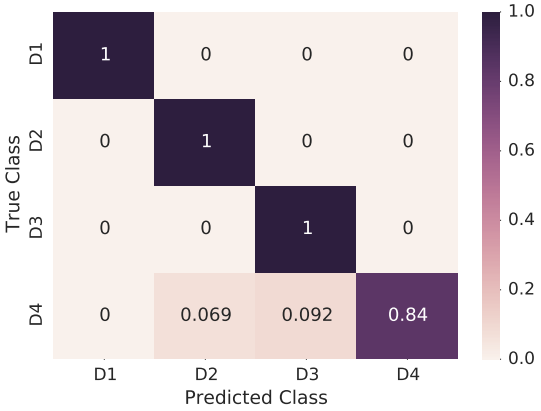


Figure 6: Confusion matrix for the identification of each phone at different locations through the city.

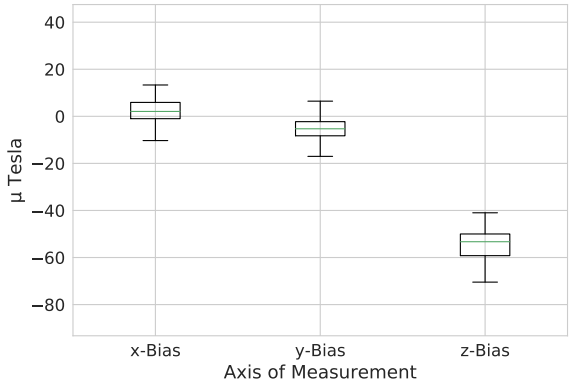


Figure 7: Distribution of the values of the *bias* for each axis.

residential buildings, etc. We aggregate these results in a leave-a-place-out cross validation scheme where we used 9 locations in the training set and the remaining location for testing. This is repeated until every location has been used for testing. With an accuracy of 96%, the results in Figure 6 show that the internal bias of the phones is not determined by its environment.

5.5.4 Robustness Over Time: Exploring the Stability of the Output Values. Finally, we provide results to support the claim for the robustness of the method over time. We investigate the temporal validity of the signature of a device, i.e., the time interval during which the model can be used for the classification task after its initial training.

Using the application described in Section 5.5.2 we present measurements from a single device at intervals of 12 hours over a period of 77 days. The boxplots shown in Figure 7 show that while the values are not identical, the variance within each axis is low. With these results we are confident that the signature of a device will remain constant over the period of at least two months.

5.6 Limitations and Countermeasures

The primary limitation of this attack is that the *bias* can only be accessed from within each device. As there are no permissions for the magnetometer, any (malicious) app can access sensor readings to generate a fingerprint. Removing the magnetometer from devices is not a viable solution. One alternative is having the sensor available but under the responsibility of the user, is a good compromise and it is in agreement with the precedent set by the different platforms [2, 3, 24].

In the next section we will discuss how, by placing a secondary device (i.e., an external measurement instrument) within range of the target, identification remains feasible even when internal access to the sensor is not possible.

6 PHYSICAL PROXIMITY ATTACK: IDENTIFYING ONE DEVICE FROM ANOTHER

Successful attacks are contingent on access to the target system. In many cases, network connectivity is enough to gain access, execute the exploit, and retrieve the response. It also allows for an increase

in the number of potential targets and offers some measure of protection for the attacker. However, the lack of physical presence also translates into diminished control. The results presented in Section 5.5 place the hardware and software constraints on the targets and require users to install an application (or another form of malware) on a phone that has the appropriate sensor. Once the application is running successfully, an attacker can collect information and identify devices simultaneously. However, the novelty of our attack is not that we identify devices through sensor readings (as if to imply that the sensors are the source of the signature) instead, what we propose is that each device emits magnetic radiation that can be collected by a magnetometer and used to generate a unique signature. In this second attack, we shift hardware and software requirements to the attacker and accept physical proximity as the limiting constraint. The implication is that now any electronic device is identifiable; all that is necessary is for the attacker to provide a magnetometer-enabled device with the corresponding software to conduct the attack. In this section we present the identification results for the attack illustrated in Figure 2.

6.1 Experiment Setup and Data Collection

In this scenario we have an adversary (d_A) who collects readings from a victim (d_V), the target of the identification attack. This second dataset was all collected in the same location over a period of two weeks from a group of voluntary participants selected through convenience sampling. Each participant interacted with their own device and the collection device was the same for all measurements. The parameters of the collection were more restrictive than those in the first attack, for instance, for the duration of the collection, participants were (mostly) stationary and their devices were continuously in use. Each participant was briefed at the beginning of the session with the procedure and objectives. The participants were told that the content of their data was not the object of the study, only the emissions of their device. They were each told that the distance between the two devices should never exceed a palm width (approximately 20 cm) and that d_A should remain immobile in a flat surface (i.e., resting on a table). After giving each of them some time to answer questions, they received no further input from the researcher. In practical terms, this means that there is a fair expectation of noise in the collected readings. The participants had no restrictions on the applications being used. They were told that they should maintain continuous interaction (i.e., their task was to use their phone without allowing it to enter standby mode). Participants responded in different ways, some watched videos, others listened to music, responded to emails, used chat applications, played games, read e-books, etc. We assume that the data collected reflects the range of resource consumption and behavior that would be normally associated with each device. All measurements were completed with the same instance of d_A and the settings of the device were adjusted to the highest resolution available (i.e., a sampling rate of 10 Hz).

Each of the participants used their device continuously providing us data for a period of 30 min. Overall we collected data from 30 participants that resulted in 4 different mobile platforms (i.e., Android, Apple, Blackberry, Windows), 7 brands, and 22 distinct models.

6.2 Feature Generation

We have already shown that the internal magnetic field can be used for identification. The next task is to determine whether the unique internal field identified in Section 5 can be extracted from the environmental magnetic field collected from a secondary device. Different from the analysis conducted in Section 5.5 the measurements collected by d_A do not consist solely of the magnetic field of d_V. Instead, the values represent the magnetic field around d_A, which *includes* the emissions of d_V. A second major difference is that while in Section 5.5 the magnetic field was measured in three orthogonal axes of fixed position and orientation with respect to the device. When we look at the environmental magnetic field, the frame of reference is variable and the axes with respect to the Earth are constantly changing. Hence, for a valid comparison, we transform the three-dimensional readings into a single value through the magnitude (norm) of the readings.

Extracting a specific signature from the environmental magnetic field is a challenging problem. Any environmental reading will contain at least one source of white noise, our planet's naturally occurring magnetic field. If the measurement is recorded in an urban setting, then additional sources of noise are any ferromagnetic materials in the vicinity of the device [21]. This noise is variable and in the order of μT, well within our range of interest. However, given the pervasiveness of the noise any identification attack must, in order to be successful, overcome these challenges and find the signature of a device.

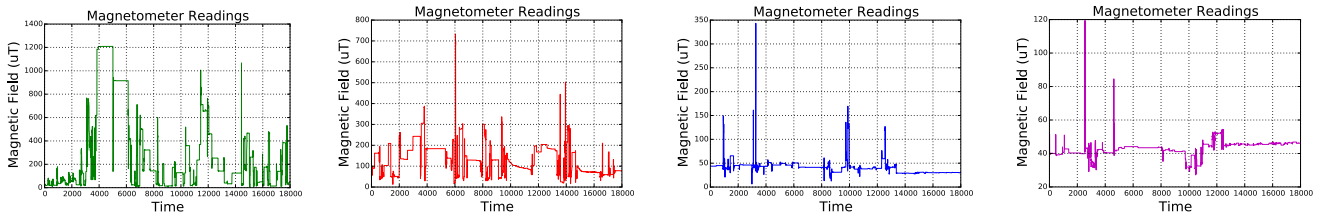
Figures 8a, 8b, 8c, and 8d show the signal collected from four instances of d_V. Each graph corresponds to a different device, the first two represent the same model (an iPhone SE), and the last two are both Samsung devices, one low-range (Galaxy Core Prime) and the other comparatively high-range (Galaxy S5). As evidenced by the figure, for the second dataset, in addition to Android we collected measurements from Apple, Blackberry and Microsoft devices and the results we present include them as well. We would also like to underline another difference: whereas in the previous attack we consider each reading as a discrete signal, now we interpret these observations as time series. Indeed, in the malware attack, we had direct access to the phone's magnetic field. This is no longer the case. Now, we must extract the phone's field from the environmental measurements and in order to achieve this we include in our analysis the relationship between adjacent observations.

We extract features in the temporal and frequency domain and following the recommendation in [33], we rank the features according to the accuracy exhibited in each classifier and build the models in accordance with the rank. Each signal is divided in two: the first 20 minutes are used for training and the remaining 10 for testing.

6.3 Results

The signal of interest is the magnitude of the magnetic field as measured in the environment of d_A. For each device we considered a signal sampled at 10 Hz comprised of 18,000 measurements (i.e., 10 measures per second for 30 minutes). For each device, we sampled the signal for different time-spans and computed the features described in Section 6.2.

Figure 9 summarizes the main results. From all the features tested, using the signal's minimum, maximum, and median values and a



(a) iPhone SE. (b) iPhone SE. (c) Galaxy S5. (d) Galaxy Core Prime.

Figure 8: Magnetic field associated with four smartphones.

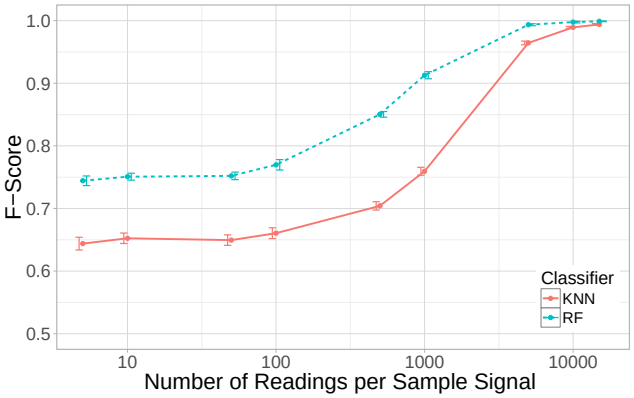


Figure 9: Classification F-Score for increasing duration of training signal.

training signal duration of 16.7 *min* we achieve 99.9% accuracy with RF and 99.0% with KNN. Overall, the attack is viable and results in accurate identification. If however, we reduce the period for data collection, we observe that training time is approximately halved to 8.3 *min* and, at the same time, we are still able to achieve 99.4% for RF and 96.7% for KNN. It is worth underlining that the random baseline for classification is around 3% for both methods.

6.4 Limitations and Countermeasures

The primary limitation of this attack is the proximity required between d_A and d_V. This limits the number of devices that can be identified at any time and it puts physical demands on the attacker that are simply not there in the malware attack. For these experiments we were using Hall Effect Sensors to measure magnetic field. A more sensitive sensor, for instance a fluxgate magnetometer, would undoubtedly increase the spatial range of the measurements. However, the resources available for this project did not allow us to empirically test the range of the fluxgate sensor.

With respect to potential countermeasures, legislation already regulates the emissions from a device to prevent, among other things, interference across devices. Manufacturers already incorporate shielding into their electronics' designs.

While the magnetic field is a single physical (vectorial) quantity measured by one sensor, it is actually the result of an intricate interaction of components, material degradation, and user behavior just to name a few. An effective countermeasure for this attack would be a cover that offers full shielding for the device. This level of shielding however would make the (communication) device unusable: along with the magnetic field, the shielding would filter the network signal and wireless network capabilities.

7 RELATED WORK

Previous work on device fingerprinting can be grouped into two main areas: identification through content and identification through physical characteristics of a device.

7.1 Content-Based Identification

Given the personal nature of devices, we expect the user-specific content of a phone (e.g., photos, applications, contacts, music) to be significantly different to most if not all others. In [40] Quattrone et al. present an interesting approach combining both content (i.e., system settings, language settings, etc.) and physical descriptions (i.e., internal and external memory size, device manufacturer and model) to generate their signature. Using similar types of auxiliary information in [31] and [45] the authors expose a series of information leaks from the operation of the device. One reveals the identity of the user through the monitoring of network data usage statistics of some key applications; the other, the identity of the device from the most recent songs played. One shortcoming of their approach is that, while fingerprinting is possible (and accurate), it is also based on user behavior, which changes over time.

Other studies focus on the identification of devices using lists of applications installed on the phones. Both [10] and [26] find that the list of applications installed is highly discriminative in terms of devices and that even if, instead of app names, the classification was based on the app categories, it would still reveal some partial information about the user.

Finally, in [29] the authors combine a set of descriptors from the browser, system, and hardware attributes as well as some behavioral characteristics of the user. The paper is originally intended to corroborate the standardized settings of web-browser. The authors also find that combining different attributes fingerprinting is still possible. In contrast, as we showed in Section 5, our work only looks at user behavior indirectly (as it reflects the resource consumption of the phone) and never at content.

7.2 Hardware-Based Identification

This concept of manufacturing variability has been presented before in its application as a means for identification and authentication. From a theoretical point of view, in [43] the authors present the properties and applications of silicon-based physically unclonable

functions (PUFs). These rules are then used in [32] where the authors present a system that utilizes the timing delays of transistors and wires in individual circuit boards to compute private cryptographic keys using PUFs. In [18] the silicon-based imperfections of network interface cards are used to identify devices through the passive analysis of the radio signals they transmit.

The array of sensors available in mobile devices gives an important added perspective. It not only allows the exploitation of internal differences for identification, but it also adds a dimension in the form of environmental interactions. In [16] they present two approaches for identification. The authors show that combining microphone and speaker systems and computing the distortion of a control signal results in accurate classification of the device; however, for this approach they need to request two permissions, namely `RECORD_AUDIO` and `MODIFY_AUDIO_SETTINGS`. In the same paper, they introduce a second attack: identification through the calibration error of the accelerometer. Similar to our work, they require no permissions to collect readings from the sensor. They create a web application and ask participants to leave their devices stationary and facing up while the data collection takes place. The authors find that it is possible to identify all devices with an accuracy of 58.7%. To this respect, our results correspond to those presented in this paper, imperfections introduced in the manufacturing process make each device unique; moreover, this uniqueness can be quantified and used for identification. However, there are several notable differences with respect to our work. They rely on all users performing the same task and they propose two methods to reduce the usefulness of their attack: the calibration of each sensor at production time to eliminate the variability in the readings and the introduction of some random value to prevent the recognition of a baseline state in the device. These proposals do not invalidate our work. On one hand, the magnetometer has a dynamic internal calibration that is applied to each reading to compensate for the iron bias in the device and on the other, there already are sources of noise in the readings. The first attack presented (i.e., the malware attack) uses the magnetic field generated by each device (as reported by the sensor's calibration) to identify each phone. In the second attack (i.e., the proximity attack) we collect the signal emitted by the device as well as all the environmental noise and run successful identification tests on them.

Other projects have also looked at identification from sensor imperfections and biases. In [25] the authors present results using the manufacturing imperfections in the accelerometer for identification. Similarly, in [13] the authors use the imperfections found in the magnetometer to identify devices. These two papers rely on identifying one state in the device and finding the difference between the known state and the measurement to compute the influence of the imperfection thereby identifying each phone. Kohno et al. show that remote identification is possible without permissions or modifications to the target device. They rely on clock skews to generate fingerprints but, in their approach, there needs to be an established connection between attacker and target [30]. This requires some access to the target device which might not be feasible. Similarly, physical imperfections have been used to generate fingerprints for other types of devices as is the case for radio transceivers [23], computers (through their USB ports) [14], and wireless devices in a network [28, 41] though in general their use and application is different from the ones proposed.

The body of work presented in this subsection is closer to our approach to identification in that it is based on the analysis of a physical quantity. Similar to the work on accelerometers and audio systems we show that unique physical features in devices exist and can be measured. However, in contrast with the identification work on accelerometer, electromagnetic radiation can be accessed externally and cannot be hidden. In [25] the authors show that adding noise to the data is an effective countermeasure to their identification scheme. In our work, (magnetic field) noise is already part of the signal. Presented differently, most papers that use manufacturing imperfections aim to measure the imperfection, whilst in our work, we assume the imperfection is there and measure a quantity that is necessary for the operation of the device and which is influenced by the imperfection itself. In this sense, the method we propose is more robust than any of those presented in the literature.

7.3 Side Channel Attack: Using Magnetic Fields to Extract Information

Finally, magnetic fields have been exploited for side channel attacks [15, 20, 27, 44]. Most recently, in [35] the authors record magnetic leaks to capture the data being written to a laptop's hard drive. Most of the proposed attacks require dedicated software on the target and the mobile device is used only as a measurement instrument. To the best of our knowledge, this paper is the first to leverage electromagnetic radiation for the purpose of identification.

8 CONCLUSIONS

We have proposed a method for identifying phones from the magnetic field they emit. We considered two types of attack, one internal, based on the magnetic field reported by the Android API, and one external, based on readings collected from a secondary device.

With respect to the internal attack, we have discussed the classification results using two supervised learning algorithms, KNN and RF, over two different datasets and we have shown that we are able to identify one device in a group of 175 and approximately 1.6 minutes of data with a precision of 98.9% This holds an advantage of approximately 165 times over the precision exhibited by the random classification baseline where the probability of success is around 0.6%. Even if this internal attack is limited to those devices that have a magnetometer and which have the data collection application installed, the lack of permissions associated to collecting readings from the sensor makes this attack invisible to users.

As far as the external (proximity) attack is concerned, we have shown that from a distance of approximately 20 *cm* a Hall Effect sensor is sufficient to collect the signal from the victim and generate the fingerprint. Using three features in the temporal domain, we have achieved a maximum accuracy of 99.9% by using a 16 minute signal for training.

ACKNOWLEDGMENTS

This work was supported through the EPSRC grant EP/P016278/1 at UCL and by The Alan Turing Institute under the EPSRC grant EP/N510129/1

REFERENCES

[1] 2016. Electromagnetic fields and public health. http://www.who.int/peh-emf/publications/facts/fs299/en/. Accessed: 2018-11-10.

[2] 2018. Activity Manager: Android Developers. https://developer.android.com/reference/android/app/ActivityManager.html. Accessed: 2018-11-10.

[3] 2018. Best Practices for App Permissions: Android Developers. https://developer.android.com/training/articles/user-data-permissions.html. Accessed: 2018-11-10.

[4] 2018. HAL Interface: Android Open Source Project. https://source.android.com/devices/sensors/hal-interface. Accessed: 2018-11-10.

[5] 2018. Measuring Earth's Magnetism. https://earthobservatory.nasa.gov/images/84266/measuring-earths-magnetism. Accessed: 2018-11-10.

[6] 2018. PRIME Faraday Technology Watch 2002: An Introduction to MEMS. http://www.lboro.ac.uk/microsites/mechman/research/ipm-ktn/pdf/Technology_review/an-introduction-to-mems.pdf. Accessed: 2018-11-10.

[7] 2018. Sensor Stack: Android Open Source Project. https://source.android.com/devices/sensors/sensor-stack. Accessed: 2018-11-10.

[8] 2018. Sensor Types: Android Open Source Project. https://source.android.com/devices/sensors/sensor-types. Accessed: 2018-11-10.

[9] 2018. Sensors Overview: Android Open Source Project. https://developer.android.com/guide/topics/sensors/sensors_overview.html. Accessed: 2018-11-10.

[10] Jagdish Prasad Achara, Gergely Acs, and Claude Castelluccia. 2015. On the Unicity of Smartphone Applications. In *WPES '15*.

[11] Alasdair Allan. 2011. *Basic sensors in IOS: Programming the accelerometer, gyroscope, and more*. O'Reilly Media.

[12] Panagiotis Andriotis, Martina Angela Sasse, and Ginaluca Stringhini. 2016. Permissions snapshots: Assessing users' adaptation to the Android runtime permission model. In *WIFS'16*.

[13] Gianmarco Baldini, Franc Dimc, Roman Kamnik, Gary Steri, Raimondo Giuliani, and Claudio Gentile. 2017. Identification of mobile phones using the built-in magnetometers stimulated by motion patterns. *Sensors* 17, 4 (2017), 783.

[14] Adam M Bates, Ryan Leonard, Hannah Pruse, Daniel Lowd, and Kevin RB Butler. 2014. Leveraging USB to Establish Host Identity Using Commodity Devices.. In *NDSS '14*.

[15] Sebastian Biedermann, Stefan Katzenbeisser, and Jakub Szefer. 2015. *Hard Drive Side-Channel Attacks Using Smartphone Magnetic Field Sensors*. Springer Berlin Heidelberg, Berlin, Heidelberg, 489–496. https://doi.org/10.1007/978-3-662-47854-7_30

[16] Hristo Bojinov, Yan Michalevsky, Gabi Nakibly, and Dan Boneh. 2014. Mobile device identification via sensor fingerprinting. *arXiv preprint arXiv:1408.1416* (2014).

[17] Leo Breiman. 2001. Random Forests. *Machine Learning* 45, 1 (2001), 5–32.

[18] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh. 2008. Wireless Device Identification with Radiometric Signatures. In *MobiCom'08*.

[19] Yongyao Cai, Yang Zhao, Xianfeng Ding, and James Fennelly. 2012. *Magnetometer basics for mobile phone applications*. Technical Report. MEMSIC.

[20] R. Callan, A. Zajic, and M. Prvulovic. 2014. A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events. In *MICRO'14*.

[21] Jaewoo Chung, Matt Donahoe, Chris Schmandt, Ig-Jae Kim, Pedram Razavai, and Micaela Wiseman. 2011. Indoor location sensing using geo-magnetism. In *MobiSys'11*.

[22] T. Cover and P. Hart. 1967. Nearest neighbor pattern classification. *IEEE Transactions on Information Theory* 13, 1 (January 1967), 21–27. https://doi.org/10.1109/TIT.1967.1053964

[23] Boris Danev and Srdjan Capkun. 2009. Transient-based Identification of Wireless Sensor Nodes. In *IPSN '09*.

[24] Anupam Das, Nikita Borisov, and Matthew Caesar. 2016. Tracking Mobile Web Users Through Motion Sensors: Attacks and Defenses. In *NDSS'16*.

[25] Sanorita Dey, Nirupam Roy, Wenyuan Xu, Romit Roy Choudhury, and Srihari Nelakuditi. 2014. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable. In *NDSS'14*.

[26] Remo Manuel Frey, Runhua Xu, and Alexander Ilic. 2016. A lightweight user tracking method for app providers. In *CF'16*.

[27] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. 2015. GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies. In *USENIX'15*.

[28] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong. 2018. Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information. In *IEEE INFOCOM '18*.

[29] Thomas Hupperich, Davide Maiorca, Marc Kührer, Thorsten Holz, and Giorgio Giacinto. 2015. On the Robustness of Mobile Device Fingerprinting: Can Mobile Users Escape Modern Web-Tracking Mechanisms?. In *ACSAC'15*.

[30] T. Kohno, A. Broido, and K. C. Claffy. 2005. Remote physical device fingerprinting. *IEEE Transactions on Dependable and Secure Computing* 2, 2 (April 2005), 93–108.

[31] Andreas Kurtz, Hugo Gascon, Tobias Becker, Konrad Rieck, and Felix Freiling. 2016. Fingerprinting mobile devices using personalized configurations. *Proceedings on Privacy Enhancing Technologies* (2016), 4–19.

[32] J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas. 2004. A technique to build a secret key in integrated circuits for identification and authentication applications. In *VLSI'04*.

[33] Huan Liu and Lei Yu. 2005. Toward integrating feature selection algorithms for classification and clustering. *IEEE Transactions on Knowledge and Data Engineering* 17, 4 (2005), 491–502.

[34] Jeffrey J. Love, Greg M. Lucas, Anna Kelbert, and Paul A. Bedrosian. 2018. Geoelectric Hazard Maps for the Mid-Atlantic United States: 100 Year Extreme Values and the 1989 Magnetic Storm. *Geophysical Research Letters* 45, 1 (2018), 5–14.

[35] Nikolay Matyunin, Jakub Szefer, Sebastian Biedermann, and Stefan Katzenbeisser. 2016. Covert channels using mobile device's magnetic field sensors. In *ASP-DAC'16*.

[36] Vasilios Mavroudis, Shuang Hao, Yanick Fratantonio, Federico Maggi, Christopher Kruegel, and Giovanni Vigna. 2017. On the Privacy and Security of the Ultrasound Ecosystem. *Proceedings on Privacy Enhancing Technologies* 2017, 2 (2017), 95–112.

[37] Lukasz Olejnik. 2016. Report on Sensors APIs: privacy and transparency perspective. W3C Invited Expert.

[38] Fabian Pedregosa, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, et al. 2011. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research* 12, Oct (2011), 2825–2830.

[39] Anne Perrin and Martine Souques. 2013. *Electromagnetic Fields, Environment and Health*. Springer Science & Business Media.

[40] Anthony Quattrone, Tanusri Bhattacharya, Lars Kulik, Egemen Tanin, and James Bailey. 2014. Is This You?: Identifying a Mobile User Using Only Diagnostic Features. In *MUM'14*.

[41] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah. 2015. GTID: A Technique for Physical Device and Device Type Fingerprinting. *IEEE Transactions on Dependable and Secure Computing* 12, 5 (2015), 519–532.

[42] Stuart J. Russell and Peter Norvig. 2016. *Artificial Intelligence: A Modern Approach* (3 ed.). Pearson Education.

[43] Ingrid Verbauwhede and Roel Maes. 2011. Physically Unclonable Functions: Manufacturing Variability As an Unclonable Device Identifier. In *GLSVLSI'11*.

[44] Alenka Zajic and Milos Prvulovic. 2014. Experimental demonstration of electromagnetic information leakage from modern processor-memory systems. *IEEE Transactions on Electromagnetic Compatibility* 56, 4 (2014), 885–893.

[45] Xiaoyong Zhou, Soteris Demetriou, Dongjing He, Muhammad Naveed, Xiaorui Pan, XiaoFeng Wang, Carl A. Gunter, and Klara Nahrstedt. 2013. Identity, Location, Disease and More: Inferring Your Secrets from Android Public Resources. In *CCS'13*.