MAGNETO: Fingerprinting USB Flash Drives via Unintentional Magnetic Emissions

OMAR ADEL IBRAHIM, SAVIO SCIANCALEPORE, GABRIELE OLIGERI, and ROBERTO DI PIETRO, Hamad Bin Khalifa University, Qatar

Universal Serial Bus (USB) Flash Drives are nowadays one of the most convenient and diffused means to transfer files, especially when no Internet connection is available. However, USB flash drives are also one of the most common attack vectors used to gain unauthorized access to host devices. For instance, it is possible to replace a USB drive so that when the USB key is connected, it would install passwords stealing tools, rootkit software, and other disrupting malware. In such a way, an attacker can steal sensitive information via the USB-connected devices, as well as inject any kind of malicious software into the host.

To thwart the above-cited raising threats, we propose MAGNETO, an efficient, non-interactive, and privacy-preserving framework to verify the authenticity of a USB flash drive, rooted in the analysis of its unintentional magnetic emissions. We show that the magnetic emissions radiated during boot operations on a specific host are unique for each device, and sufficient to uniquely fingerprint both the brand and the model of the USB flash drive, or the specific USB device, depending on the used equipment. Our investigation on 59 different USB flash drives—belonging to 17 brands, including the top brands purchased on Amazon in mid-2019—reveals a minimum classification accuracy of 98.2% in the identification of both brand and model, accompanied by a negligible time and computational overhead. MAGNETO can also identify the specific USB Flash drive, with a minimum classification accuracy of 91.2%. Overall, MAGNETO proves that unintentional magnetic emissions can be considered as a viable and reliable means to fingerprint read-only USB flash drives. Finally, future research directions in this domain are also discussed.

CCS Concepts: • **Security and privacy → Embedded systems security**; *Malware and its mitigation*;

Additional Key Words and Phrases: USB, magnetic emissions, hardware security, critical infrastructures protection

ACM Reference format:
Omar Adel Ibrahim, Savio Sciancalepore, Gabriele Oligeri, and Roberto Di Pietro. 2020. MAGNETO: Fingerprinting USB Flash Drives via Unintentional Magnetic Emissions. *ACM Trans. Embed. Comput. Syst.* 20, 1, Article 8 (December 2020), 26 pages.
https://doi.org/10.1145/3422308

This publication was made possible by Awards No. NPRP11S-0109-180242 and No. GSRA6-1-0528-19046, from the QNRF-Qatar National Research Fund, a member of Qatar Foundation. The findings achieved herein are solely the responsibility of the authors.

Authors' address: O. A. Ibrahim, S. Sciancalepore, G. Oligeri, and R. Di Pietro, Hamad Bin Khalifa University, College of Science and Engineering, Qatar; emails: {oaibrahim, ssciancalepore, goligeri, rdipietro}@hbku.edu.qa.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2020 Association for Computing Machinery.

1539-9087/2020/12-ART8 $15.00
https://doi.org/10.1145/3422308

1 INTRODUCTION

The Universal Serial Bus (USB) standard is nowadays the most convenient, cheap, and widespread means to physically connect peripheral devices to workstations and laptops [21]. Over the last years, the Universal Serial Bus (USB) standard replaced a large number of earlier interfaces, including serial and parallel ports, used to supply either power or data connectivity to external devices, thus providing a unique and standardized interface to be used for the connection of any peripheral board. In addition, the ongoing introduction of the USB 3.0 standard specification is further widening the application scenarios where USB connections are suitable, thanks to transfer speeds up to 5 Gbps and a maximum storage capacity of 1 TB [25]. As a result, USB connectivity is more and more used by companies in industrial environments to transfer data between devices, as well as to charge electrical components [35].

The widespread diffusion of USB connections is confirmed by the increasing market size associated with the new wave of USB 3.0 devices. According to Transparency Market Research, the worldwide market for USB 3.0 drives is growing at a Compound Annual Growth Rate (CAGR) of roughly 23.5% over the last years, reaching 3.1 billion US$ in 2020, from 1.1 billion US$ in 2015. At the same time, USB devices are getting cheaper: the average price of a USB drive in China decreased from 6.7 USD/Unit in 2011 to 6.0 USD/Unit in 2016, and a further decreasing trend is expected in the upcoming years [52].

Despite the provided advantages, the USB standard communication interface also poses increasing concerns from the security perspective [30]. Being focused on boosting the availability of connected peripherals and on reducing the latency in accessing remotely stored data, the USB software design paid little attention to security issues. Exploiting such a weak security barrier, many attacks and vulnerabilities emerged over the last few years [28]. Indeed, malicious attackers have been able to modify the firmware of specific (faulty) USB flash drives, turning them into a vector to launch tools for information stealing, host system impairment, Internet traffic redirection, and malware injection, to name a few [27, 29]. As reported by the latest media and newspapers, USB attacks are very likely to happen especially when the target system is not connected to the Internet, such as in the case of ships, remote keyless entry systems, and critical infrastructures [11, 43].

While a few countermeasures have been provided in the literature—mainly based on standard anti-malware software—attackers are still able to escape detection, e.g., by masquerading the malicious USB device as a legitimate one at the time of connection to the host [50]. Even if the forthcoming USB Type-C standard enhanced the security guarantees via digital certificates, installing and verifying such certificates into regular USB 2.0 and 3.0 devices would lead to a complete software and hardware redesign of the interfaces, thus being invasive and hard to be deployed. Especially in industrial companies and critical infrastructure scenarios, the impact of such attacks can be devastating, preventing the daily activities of the company and possibly leading to huge economic losses on the whole country relying on the target critical infrastructure.

To provide an effective tool for the detection of malicious USB devices, in this article, we present MAGNETO, a framework able to identify replaced and faulty USB flash drives connected to a specific host, based on unintentional magnetic emissions radiated by the USB boards, during the execution of the boot procedure. We show that the magnetic emissions radiated at very low frequencies by USB flash drives immediately after the connection to a specific host system are consistent and unique, i.e., they show the same profile over time, and they are specific to the model and version of the analyzed device. Thus, such low-frequencies magnetic emissions can be effectively used to achieve both a method for USB brand and model identification and a physical-layer fingerprinting mechanism for USB devices—hence, providing a powerful tool to spot the replacement or malicious corruption of the authorized USB flash drive.

Our experimental campaign took into consideration 59 different USB devices, including the top brands purchased on Amazon in July 2019, and it revealed impressive performances. When deployed using low-cost Software-defined Radios (SDRs), MAGNETO reaches up to 98.2% of accuracy in correctly identifying the brand and model of the device, after an observation time of only 1.08 s. When the identification of the single USB flash drive is crucial, such as in critical infrastructures, using a wide-band spectrum analyzer MAGNETO can discriminate the specific USB device connected to a given host with a minimum accuracy of the 91.2%. Such outstanding performances require only minor computations on a commercial laptop, further confirming the viability of MAGNETO.

It is worth noting that MAGNETO could be extended also beyond the execution of the boot procedure. In fact, by just extending the time duration of the observation window, it could be possible to monitor the activities of the USB flash drive when it is in the idle state, thus detecting any asynchronous (potentially malicious) activities originated by the USB device.

MAGNETO, though being of general applicability, could benefit those environments interested in strictly protecting the access to sensitive equipment—such as critical infrastructures and industrial companies. Indeed, under the reasonable assumption that only a few (brands of) USB flash drives are authorized (e.g., the ones distributed by the company itself), MAGNETO can be implemented on a reference computing machine, to detect any replacement or modification of the intended USB flash drives, further strengthening the enforcement of security policies.

We highlight that three main elements distinguish MAGNETO from previous contributions. First, MAGNETO is the first solution to exploit the usage of unintentional *magnetic emissions* to address the threats associated with malicious USB drives. Despite this feature could appear just an application of a well-known background notion, it brings new unprecedented challenges. Indeed, differently from other devices analyzed in the scientific literature, USB flash drives cannot be modified (or deeply inspected) by end-users, and they should be analyzed as *black-box*.

Second, we prove that unintentional magnetic emissions occurring during the boot process of a USB flash drive can be used to fingerprint its hardware, without any intervention at either the firmware or the software level, but only requiring to plug-in the USB flash drive. Further, our solution guarantees the full privacy of the device under test, making MAGNETO overall enjoying the properties of being non-invasive, minimal-interactive, and privacy-preserving, and fully compatible with read-only devices. To the best of our knowledge, all these features are not provided by any other competing solution in the literature.

Finally, the open-source code and data of MAGNETO framework are available at Reference [13]. This will allow practitioners, industries, and academia to verify our claims, as well as to extend the adoption of MAGNETO as a ready-to-use basis for their further software development.

The sequel of this article is organized as follows: Section 2 provides a brief background on unintentional RF and magnetic emissions, as well as an overview of USB security-related work; Section 3 highlights the assumed scenarios and the adversary model; Section 4 provides the details of MAGNETO; Section 5 describes the tools and the results achieved by using MAGNETO; Section 6 highlights the advantages and limitations of MAGNETO; and, finally, Section 7 tightens conclusions.

2 BACKGROUND AND RELATED WORK

Despite being assembled in a Printed Circuit Board (PCB) through industrial-grade processes, any embedded device produces even small unintentional magnetic emissions, emanated directly from the integrated circuits.

The source of such emissions is mainly due to the local oscillator, which continuously emits electromagnetic waves at a given fundamental frequency, to provide a unique timing reference for

hardware and software operations executed by the embedded device. Even being narrow-band, the signal emitted by the oscillator creates also several *harmonics*, i.e., components at frequencies many times that of the fundamental tone, characterized by a non-negligible power spectral density. Such harmonics couple with very small integrated wires on the embedded device and create resonating effects, which turn the wires into small antennas, emanating RF power [2]. The physical effects underpinning these phenomena are described by the physics fundamental Maxwell equations, and also specific mathematical models are available in the literature, describing their complex creation [7]. On the one hand, this phenomenon can be the cause of signal interference between devices operating close to each other. For this reason, any embedded device emitting RF signals must be compliant to specific international regulations before being available to the commercial market [17]. On the other hand, unintentional magnetic emissions effectively represent a side-channel for any embedded device, providing useful information about the nature of the device and the specific activities executed at a given time instant [14].

To provide a few examples in this direction, recently the authors of Reference [9] provided a novel side-channel attack on mixed-signal chips, where digital logic circuits and the radio transceiver are coupled on the same chip. Using information leaked from digital circuits on a Nordic Semiconductor nRF52832 chip, the authors recovered the full AES 128-bit key, up to a distance of 10 meters from the target device. The authors of References [12, 53] identified that the fabrication process of embedded circuits induced variations in the electrical properties of each chip. By using RF emissions from 16 different micro-controllers, they were able to identify uniquely each of them, recurring to imperfections of the fabrication processes. Similarly, the author of Reference [54] focused on the identification of the SCADA sensors and actuators in critical infrastructures and measured the unintentional emissions derived from the execution of a specific piece of code. Another application in this context is discussed in Reference [6], where researchers used the unintentional RF emissions to achieve the classification and verification of IEEE 802.15.4 ZigBee wireless devices that are widely used in critical infrastructure applications. In the context of the IEEE 802.15.4 communication technology, unintentional RF emissions have been also investigated in References [15, 36], to build a system able to reject rogue devices. Concerning generic RF devices, the authors of Reference [47] demonstrated the feasibility of fingerprinting wireless devices by looking at the non-idealities of the emitted RF signals. They showed that each packet emitted by a device has unique distinguishing features, that can be used to identify the transmitting entity. Indeed, we note that this fingerprinting methodology requires the transmission of RF packets, and thus, it cannot be applied to non-RF devices, such as the USB drives. Another use-case was introduced by the authors of Reference [24], where unintentional RF emissions and random noise waveforms were used to actively interrogate target microwave devices, recognize and classify antennas and terminations. Recently, the authors of Reference [10] used the magnetic signals radiated by the CPU to fingerprint heterogeneous devices, including laptops, smartphones, and additional mobile devices. This result has been achieved by precisely controlling the hardware, firmware, and software of the devices under tests, forcing the CPU to execute a stimulation software that enables devices fingerprinting.

A few works in the recent literature investigated the same context tackled by this contribution, i.e., malicious USB Flash Drives, with specific reference to the *BadUSB* attack [4, 49, 50]. For instance, the authors of Reference [50] presented *USBFILTER*, a software solution providing first packet-level access control for USB, and preventing unauthorized interfaces from successfully connecting to the host Operating System (OS). The authors of Reference [18] proposed an innovative approach, forcing the user to interact with the connected USB device before allowing the device to be used, thus ensuring that a real human-interface device is attached. The authors of Reference [4] developed *Cinch*, a countermeasure against malicious peripherals leveraging

Table 1. Qualitative Comparison of MAGNETO Against Competing Solutions

Ref.	No Host Firmware Modification	No Target Modification	Compatible with Read-Only Devices	No Radio Operations
[9]	✓	✗	✗	✓
[53]	✓	✗	✗	✓
[12]	✓	✗	✗	✓
[54]	✓	✗	✗	✓
[6]	✓	✗	✗	✓
[15]	✓	✗	✗	✓
[36]	✓	✗	✗	✓
[47]	✓	✓	✓	✗
[24]	✓	✗	✗	✓
[10]	✓	✗	✗	✓
[50]	✗	✓	✓	✓
[4]	✗	✓	✓	✓
[49]	✗	✓	✓	✓
[18]	✗	✗	✗	✓
[48]	✗	✗	✗	✓
[5]	✗	✗	✗	✓
MAGNETO	✓	✓	✓	✓

virtualization techniques to place the connected hardware in a logically separate machine, as an isolation layer from the main and protected one. This layer depends on security policies configured by the users to reject or accept interaction with connected USB peripherals. The authors of Reference [49] designed and implemented *GoodUSB*, a mediation architecture for the Linux USB Stack. This solution defends against BadUSB attacks by enforcing permissions based on user expectations of device functionality. Recently, the authors of Reference [48] proposed to authenticate individual USB devices using tamper-proof Physical Unclonable Functions (PUFs), combining multiple security technologies available in commodity PCs, e.g., Trusted Platform Module (TPM), customized secure boot, and virtualization support. This is a software solution, that could not help in case the specific USB brand is a regular USB stick, such as in the Scenario described in our article. We also report the interesting work by the authors of Reference [5], where the firmware and software features of the USB protocol stack are used to identify the specific host.

On the one hand, we highlight that such solutions are specifically developed to thwart the BadUSB attack and its behavior [31]. Today, the vendors of the devices used to carry out the BadUSB attack have fixed the vulnerabilities, thus making the BadUSB attack very hard to be realized. On the other hand, attackers are still able to cheat both the above defense measures and the current anti-malware software, e.g., by masquerading the malicious USB device as a legitimate one at the time of connection to the host [50]. Especially in industrial companies and critical infrastructure scenarios, the impact of such attacks can be devastating, preventing the daily activities of the company and possibly leading to huge economic losses on the whole country relying on the target critical infrastructure.

Table 1 summarizes the above contributions, along some reference system requirements.

Table 1 highlights that a novel element characterizing MAGNETO is its application to devices whose firmware and software is read-only, and therefore, not accessible by the verifier. Indeed, all the previous contributions on Radio Frequency (RF) fingerprinting require either the transmission of an RF packet by the device, e.g., an IEEE 802.11a packet References [47, 53], or an identical

sequence of operations on known data packets in Reference [12], or the access to the device under test, that have to execute a specific piece of code, e.g., the Ladder Logic Program (LLP) scan in Reference [54]. The first class of the above-described solutions restricts the application of fingerprinting to only devices featuring a radio. Conversely, the second class implies that the verifier has direct access to the firmware or the software of the device under test, by deploying a firmware/software update to allow for the fingerprinting process. Conversely, our solution exploits the unintentional magnetic emissions of the boot process of a USB flash drive, therefore, enabling the fingerprinting process without requiring access to either the firmware or the software in the device under test—even when the device does not emit any RF signals. Further, our solution guarantees the full privacy of the device under test, making MAGNETO overall enjoying the properties of being non-invasive, minimal-interactive, and privacy-preserving.

3 REFERENCE SCENARIOS AND ADVERSARY MODEL

In the following, we assume two reference scenarios: (i) a private company and (ii) a critical infrastructure.

Scenario #1: Private Company. We consider a private company, interested in maintaining very high levels of security and privacy for its own most important equipment and data. The employees of the company need to use USB flash drives for daily work, e.g., to transfer files between different equipment. Being aware of the vulnerabilities associated with the USB standard specification, the system administrator would like to deploy a solution enabling the connection of authorized USB devices only, i.e., brands and models that are not affected by any known vulnerability. Therefore, the company provides to the employees its own USB flash drives, characterized by a specific brand and model. Only the USB flash drives of this particular brand and model can be used by the employees, while the use of any other brand or model of USB flash drive is not allowed. To enforce such a protection strategy, the IT system administrator deploys a host device on purpose, dedicated to the measurement and testing of specific USB Flash Drives brought into the company by the employees. By connecting the USB Flash Drives to the host, the system administrator could verify that the brand and the model of the USB Flash Drive are effectively the ones authorized by the company. It is worth noting that the physical deployment of such a host device can be optimized to be located within an *electromagnetic safe zone*, where the electromagnetic interference due to other devices is limited.

Scenario #2: Critical Infrastructure. We also consider a digitized Critical Infrastructure, such as the control center of an airport, a smart port, an electricity control station, a smart grid, or a train station, to name a few. Being very sensitive computing centers, the computational units behind these critical infrastructures are usually highly protected, and equipped with minimal interfacing capabilities toward the public Internet. As such, the usage of USB Flash Drives is allowed only for unavoidable tasks, such as the installation of critical updates to the system, or the export of data stored locally. Indeed, such critical infrastructures can be the target of malicious attackers, aiming at compromising the operation of a whole country by shutting down, e.g., its transportation or electricity network. Thus, the computing equipment controlling the operation of these critical infrastructures need to be carefully protected against any hazard, including the usage of malicious USB Flash Drives. To enforce such a protection strategy, we assume that the system administrator would like to use only a specific USB Flash Drive, and reject any other one, even if it is of the same brand and model. To this aim, the system administrator could deploy a dedicated host device for the test of the USB flash drive, and to deploy a system enabling and supporting the unique identification of the specific USB Flash Drive. As for the previous scenario, such a host device can be deployed where electromagnetic interference is minimal, to optimize the overall measurement procedure.

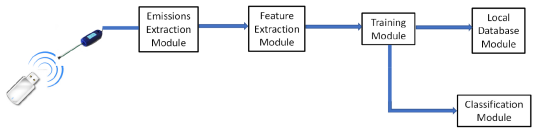

Fig. 1. Logical architecture of the MAGNETO framework.

Adversary Model. We assume an adversary that is interested in compromising the equipment of the company or the Critical Infrastructure, by adopting malicious USB flash drives. The specific aims of the adversary could be manifold, e.g., injecting malware into the ICT infrastructure where the USB flash drives are connected to, redirecting the Internet traffic to malicious websites, or stealing information stored locally in the ICT infrastructure, to name a few.

To this aim, the adversary can replace the regular (allowed) USB flash drive with another USB flash drive, having the same external look and form factor of the previous one, but a different hardware and/or firmware. This USB flash drive is modified on purpose to achieve one of the objectives listed above. In addition, we also assume that the adversary can exploit weaknesses in the USB firmware deployment and replace the legacy firmware of the USB flash drive provided by the company, injecting its malicious version [31]. It is worth noting that in such a scenario, the deployment of regular anti-malware software would not be effective. Indeed, as highlighted by previous contributions [28], attacks exploiting USB external drives can modify the firmware of the component in such a way to appear to host devices as regular USB equipment, e.g., a keyboard. Thus, the anti-malware would recognize the keyboard as a legitimate component and it would grant the related permissions.

We also assume that the adversary does not have access to the source code of the firmware deployed in a specific USB flash drive. This is confirmed by the fact that the firmware on-board of commercial USB flash drives cannot be changed and even cannot be accessed by the end-users after the deployment. All the hacks that are described in technical and unofficial blogs refer to particular firmware versions of specific USB flash drives.[1,2] However, the manufacturers immediately withdrew the affected devices from the market, and they updated the native firmware to fix these weaknesses. Therefore, we believe that in the vast majority of practical cases the native firmware of commercial USB flash drives cannot be modified by end-users.

Even in the unlikely case where an adversary can access the firmware, we consider it extremely hard and impractical to reverse-engineer it to obtain the source code, and to re-deploy it on the same USB flash drive. Generally, the firmware is protected by intellectual property rights, the source code of such firmware is secret, and protected by multiple security layers deployed at manufacturing time, and not available for public download.

Finally, we notice that the two scenarios described above always assume an end-user that could not circumvent the deployed system, e.g., by not testing its USB flash drive before usage. This assumption is consistent with the scenario of a benign employee, not aware of the (possible) replacement of its USB Flash drive with a malicious one.

4 THE MAGNETO FRAMEWORK

MAGNETO consists of five different modules, as depicted in Figure 1.

[1] https://arstechnica.com/information-technology/2014/07/this-thumbdrive-hacks-computers-badusb-exploit-makes-devices-turn-evil/.
[2] https://www.reddit.com/r/netsec/comments/112kuv/reprogram_usb_flash_drive_microprocessors_firmware/.

We identify two modes of operation:

- *Training Mode.* During this phase, a local database is populated with all the profiles of the available USB devices, including the authorized ones.
- *Classification Mode.* This is the online operational mode of MAGNETO, where a new unknown USB device is tested to verify if its profile matches the one already collected during the training mode.

The details of the modules involved in the MAGNETO framework are provided below:

- *Emissions Extraction Module.* The role of this module is to detect, capture, and log unintentional magnetic emissions from a particular device. Specifically, MAGNETO focuses on the analysis of the unintentional magnetic emissions leaked by USB flash drives at boot time, i.e., when the USB device is first connected to the host device and it executes boot operations. Then, the raw data consisting of: (i) a timestamp, (ii) the acquisition frequency, and finally, (iii) the value of the Received Signal Strength (RSS) are passed to the Features Extraction Module. The operations of the Emissions Extraction Module are carried out with particular hardware equipment, able to capture magnetic emissions on the specific operating frequency thanks to a suitable magnetic antenna. More details about the equipment used in our experiments will be provided in Section 5.
- *Features Extraction Module.* Starting from the raw data provided by the Emissions Extraction Module, this module is responsible for generating the features of interest for the particular signal. Specifically, this module operates in three different phases, i.e., *Data Normalization*, *Regions Definitions*, and *Features Computation*.
  - *Data Normalization.* The data acquired by the Emissions Extraction Module are normalized by re-centering them to the minimum value of the dynamic range of the observation, and then, by re-scaling them by the value of their dynamic range. Specifically, assuming x_i is a sample of the distribution, and X_{MIN} and X_{MAX} are the minimum and the maximum value of the dynamic range, the normalized sample $\hat{x_i}$ is computed as: $\hat{x_i} = \frac{x_i - X_{MIN}}{(X_{MAX} - X_{MIN})}$. These operations are crucial to enable cross-comparisons between different measurements, as they contribute to eliminate any small difference in the absolute value of the received power—e.g., due to small misalignment of the measurement setup.
  - *Regions Definition.* Each value of the Received Signal Strength (RSS) reported by the *Emissions Extraction Module* is associated with a given timestamp and a specific frequency. In this phase, the *Features Extraction Module* merges in the same observation vector the measurements within a given time and frequency regions, that can be configured uniquely for any specific investigation. The output of this phase is a matrix, containing for each identified region all the collected RSS values for the particular experiment.
  - *Features Computation.* Starting from the matrix created in the previous phase, the *Features Computation* phase is responsible for computing the features on each observation vector. Assuming now that $X = [x_1, x_2, ..., x_i, ..., x_N]$ is the observation vector containing the normalized intensity of the acquired signal in a given time frame and frequency range, we consider the following statistics: (i) mean; (ii) standard deviation; (iii) variance; (iv) skewness; and finally, (v) kurtosis, to precisely characterize the unintentional radiated emissions from each USB device. Equations (1) and (2) report the formulas for the skewness and kurtosis, respectively, where $(\bar{X})$ is assumed to be the mean value of the observation vector:

$$\gamma = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{X})^3}{\left[\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{X})^2\right]^{3/2}}, \tag{1}$$

$$\kappa = \frac{\sum_{n=1}^{N}\left(x_i - \bar{X}\right)^4}{\frac{1}{N}\left(\sum_{n=1}^{N}\left(x_i - \bar{X}\right)^2\right)^2}. \tag{2}$$

The output of this phase is a new matrix, containing the value of each feature for the reference experiment.

The current matrix containing the values of the features for each time and frequency interval can be passed either to the Training Module or the Classification Module, according to the particular operating mode of MAGNETO.

- *Training Module.* This module, involved only in the Training Mode, is responsible for creating the reference profile of the particular device under investigation, by using the features previously identified by the *Features Extraction Module*. The created profile is then uploaded to the *Local Database Module*.
- *Local Database Module.* The local database stores information about the specific training model associated with each device. When a new (previously unknown) device is registered, the *Training Module* establishes the specific statistical model for this device, that is stored in the *Local Database Module*. At the same time, when the *Classification Module* is executed, the *Local Database module* provides the reference statistical models used for comparison and classification.
- *Classification Module.* This module, involved only in the Classification Mode, is in charge of establishing if the previously stored profiles match the one extracted from the device under test. The comparison is carried out by considering the specific features considered by the *Features Extraction Module*, and by comparing the obtained features with the stored profiles available in the *Local Database Module*. The module outputs a similarity score, representing how much the magnetic emissions collected from the device under test are similar to the stored profile. If such a score is equal or greater than zero, then the device is assumed to be authentic. Otherwise, it is discarded. Among the several possible classifiers available in the literature [44], in this article, we have adopted the one-class Support Vector Machine (SVM) classifier, since it natively fits our objectives. More details will be provided in Section 5.

Using the five modules described above, depending on the scenario and the specific objective, either the brand and the model of the USB Flash Drive or the specific USB device can be uniquely characterized when connected to a host device.

Wrapping up, during the *Training Mode*, the unintentional magnetic emissions leaked by the USB devices are collected via the hardware equipment and the functionalities offered by the *Emissions Extraction Module*. Then, the reference features are extracted from the raw signals by the *Features Extraction Module*, and a reference statistical model is created by the *Training Module* and stored into the *Local Database Module* for future use. The process is performed for a large number of devices, to create a database containing an exhaustive number of products of the same device.

During the *classification mode*, all the USB devices are tested, by connecting them to a reference host device and collecting the unintentional magnetic emissions during the boot procedures via the functionalities offered by the *Emissions Extraction Module*. The reference features are computed from the acquired signal, and then passed to the Classification Module, which provides a similarity score, indicating how much the stored profile matches the provided one. If no correspondence is found (i.e., the similarity score is negative), then the new device is assumed as unauthorized.

Instead, if the profile of the unintentional magnetic emissions is found to be consistent with the allowed class (i.e., the score is equal to 0 or positive), the device will be authorized.

It is worth noting that MAGNETO focuses on the boot procedures of USB devices, because they are strictly required for the normal operations of the USB themselves. Indeed, being loaded in the firmware, the boot procedures associated with the USB device should not be changed by a non-malicious user. Otherwise, any modification to the firmware (either intentional or not) will generate significant changes to the magnetic emissions during the boot procedures, indicating therefore that the USB flash drive has been either tampered with or replaced. Such modifications of the behavior of the USB flash drive during the boot operations can be detected by MAGNETO and can lead to a timely rejection of the device. More details on the specific modifications that can be done when tampering with USB devices are provided in Section 6.

5 EXPERIMENTAL ASSESSMENT

In this section, we provide the details of our experimental campaign, aimed at measuring the performance of MAGNETO for the classification of either the brand and model of USB flash drives, or the specific USB flash drive, according to the scenarios previously introduced in Section 3. Section 5.1 illustrates the equipment used in our experiments, Section 5.2 provides evidence of the consistency among different observations of boot operations on the same USB flash drives, Section 5.3 shows the results achieved by MAGNETO in the classification of different brand and models of USB flash drives, Section 5.4 illustrates how MAGNETO achieves the identification of single USB flash drives using more advanced equipment, Section 5.5 provides the accuracy of MAGNETO when a reduced number of features is selected, Section 5.6 includes some experiments on firmware modification, and finally, Section 5.7 illustrates how the features of the host device impact on the profile of unintentional magnetic emissions radiated by USB flash drives.

The code of MAGNETO, including the source data of our experiments and the tools necessary to reproduce our results, are available for download at Reference [13].

5.1 Tools and Methodology

In our experimental campaign, we used the equipment listed below.

- **USB Devices**. We tested the performance of MAGNETO with a set of total of 59 different USB devices, related to 17 unique models, whose details are reported in Table 2, including the model of the included *Controller Chip*, containing the local oscillator (mainly) responsible for magnetic emissions generation (we notice that the manufacturer SanDisk does not provide any detail about the controller chip). We selected these brands to create a large dataset, considering both the most used models and any possible factor affecting the magnetic emissions of such devices. Specifically, SanDisk, Samsung, and Kingston USB flash drives are the top three brands purchased by users on Amazon—as of July 2019 [3]. At the same time, Juanwe, PNY, HP, and Mosdart are all positioned among the top 10 brands. In addition, we also selected some brands based on the use of the same version of the micro-controller. For instance, we highlight that the micro-controller of the HP (U1), the Kingston (U3), the PNY (U5), the Patriot (U6), the Silicon Power (U13), and the Toshiba (U14) are the same, i.e., they feature the same hardware chip, while the layout of the Printed Circuit Board (PCB) and/or the versions of the firmware are different (e.g., 09-V for the Kingston, 09-26 for the Silicon Power) [33]. Also, it is also worth noticing that we considered different devices having the same brand, model, and firmware: specifically, we considered 15 *SanDisk 16 GB*, 15 *Strontium 16 GB*, and 15 *Klevv Neo C20 16 GB*. All the devices have been analyzed as provided by the manufacturer, without any modification to the legacy firmware. To prove

Table 2. List of USB Brands and Models Adopted in Our Experiments

Device	Controller Chip	Device ID
HPx900w-64GB [20]	PHISON-PS2251-09-V	U1
JUANWE-32GB [22]	FirstChip-FC1179	U2
Kingston Digital 16GB Data Traveler G4 [23]	PHISON-PS2251-09-V	U3
Mosdart-8GB [26]	AlcorMP	U4
PNY Turbo 128GB [34]	PHISON-PS2251-09	U5
Patriot 128GB Supersonic Rage Series [32]	PHISON-PS2251-09-V	U6
Rubber Ducky [19]	Atmel 32UC3B1	U7
Samsung BAR Plus 32GB [37]	Silicon Motion SM3267	U8
SanDisk Ultra 128GB [38]	SanDisk	U9
SanDisk Cruzer 128GB [40]	SanDisk	U10
SanDisk Cruzer 32GB [42]	SanDisk	U11
SanDisk Cruzer 64GB [39]	SanDisk	U12
Silicon Power 32 GB Blaze B30 [45]	PHISON-PS2251-09-26	U13
Toshiba TransMemory 64GB [51]	PHISON-PS2251-11	U14
SanDisk 16 GB [41]	SanDisk	U15
Strontium 16 GB [46]	Strontium	U16
Klevv Neo C20 16GB [16]	Essencore	U17

the effectiveness of our method, we acquired the magnetic emissions by temporarily removing the case of the USB flash drive. Besides, we highlight the presence of a *malicious* device, i.e., a USB Rubber Ducky. This USB Flash drive is a cross-platform keystroke injection tool, able to work effectively with either Windows, Mac, or Linux. It features a 60 MHz 32-bit processor, hidden in the form factor of an ordinary generic USB flash drive. It consists mainly of a CPU chip and a micro SD storage, used to upload malicious payloads to the host device. Once connected to a host machine, the Rubber Ducky is recognized as a keyboard. Thus, the host device accepts its payload, consisting of pre-programmed regular keyboard strokes, up to a maximum rate of 1,000 words per minute [19]. The commands are programmed using a dedicated scripting language, and it is possible to perform a wide range of automated functions, such as password brute-forcing, binaries injection, shell reversing, as well as changing system settings. Nowadays, it is mainly used by professionals, penetration testers, and system administrators.

- **Aaronia PBS2 EMC Probe set.** To collect the unintentional magnetic emissions radiated by the USB devices, we used the Aaronia PBS2 EMC Probe set [1]. This equipment allows straightforward pinpointing and measurement of interference in the frequency band from the DC (1Hz) up to 9 GHz in electronic component groups, as well as the execution and monitoring of generic Electro-Magnetic measurement. As a probe, we used a 25 mm magnetic (H) field probe PBS-H3, covered with an insulating layer, thus providing a safe measurement environment for oscillators and mains lines. This probe is connected to the UBBV2 40 dB EMC RF pre-amplifier, allowing for a clear separation between the useful signal and the surrounding noise. The probe is then connected via a low-impedance cable to a Software Defined Radio (SDR).
- **HackRFOne Software Defined Radio.** The HackRFOne SDR has been used to record unintentional magnetic emissions acquired from the Probe Set over a frequency span of 10 MHz, and to convert raw data (in the form of regular I-Q samples) into spectral power density measurements. Specifically, the SDR performs a Fast Fourier Transform (FFT) on

Table 3. Configuration of the HackRFOne Software Defined Radio

Feature	Value
Resolution Bandwidth	976.6 Hz
Center Frequency	5 MHz
Start Frequency	0 MHz
Stop Frequency	10 MHz
Reference Level	−5 dB
FFT Size	8,192 samples

Table 4. Configuration of the Rohde & Schwarz FSW8 Spectrum Analyzer

Feature	Value
Video Bandwidth	3 MHz
Resolution Bandwidth	3 MHz
Center Frequency	100 MHz
Start Frequency	0 MHz
Stop Frequency	200 MHz
Frequency Span	200 MHz
RF Attenuation	10 dB
Reference Level	−5 dB
Sweep time	4.01 ms
Sweep points	4,001

the provided I-Q data and it generates, for each time frame, a tuple containing a reference timestamp (in milliseconds), a frequency (in Hz), and a power level (in dBm). Table 3 provides the details of the configuration of the SDR.

- **Rohde & Schwarz FSW8 Spectrum Analyzer.** The Rohde & Schwarz FSW8 Spectrum Analyzer has been used in place of the HackRFOne to record unintentional magnetic emissions acquired from the Probe Set over a larger frequency span, up to 200 MHz. As with the HackRFOne, the equipment automatically converts raw data into spectral power density measurements, by performing the FFT over the acquired samples, and it provides a tuple for each time frame, containing a timestamp (in milliseconds), a frequency (in Hz), and a power level (in dBm). Table 4 provides the details of the configuration of the spectrum analyzer.
- **Matlab R2020a.** Matlab R2020a has been used to implement the *Features Extraction Module*, the *Training Module*, the *Local Database Module*, and the *Classifier Module*. As the classification algorithm, we used the one-class SVM classifier provided by the Machine Learning Toolbox of Matlab. Specifically, the one-class SVM classifier analyzes each of the USBs as a standalone USB flash drive, by creating a profile that matches the features provided for the particular USB brand (or the specific USB flash drive). When a test set is provided in input for classification, as an output, the one-class SVM classifier provides an *evaluation score* for each input sample. Such evaluation score indicates the likelihood that the specific input sample is consistent with the created model, or not. This approach is particularly useful when the range of possible classes is wide, such as for USB flash drives, and thus a multi-class classification approach is not suitable.

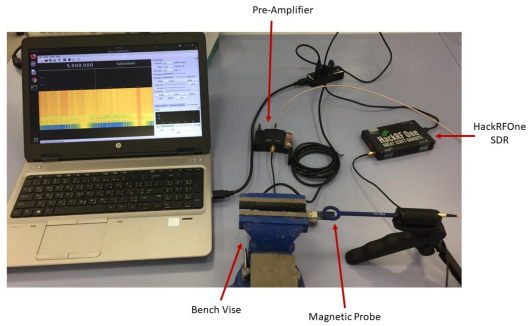

Fig. 2. Measurements setup.

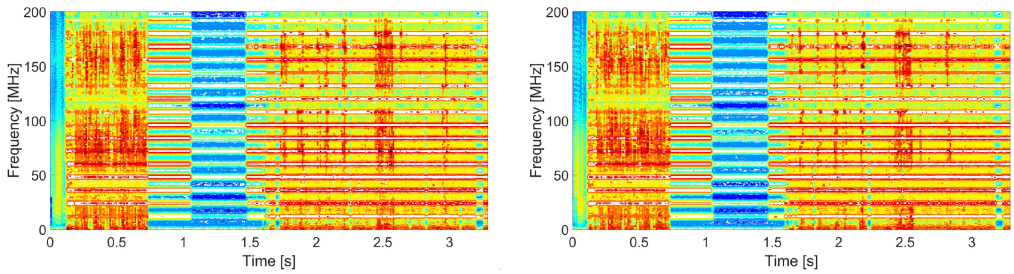

Fig. 3. Profile of the unintentional magnetic emissions of a Rubber Ducky USB flash drive (U7), during two different executions of the boot procedures.

All the experiments described in the following subsection have been conducted by collecting the unintentional magnetic emissions radiated by the target USB devices in regular laboratory conditions, without any effort to reduce the environmental noise. Our measurement setup is shown in Figure 2.

Note that a USB cable extension was placed on a Bench Vise, to physically stabilize the USB device under test. In addition, this setup allows having uniform conditions for emissions collection. The Magnetic Probe has been placed on top of the USB device controller chip, in a way to clearly capture the radiated emissions. For each USB device under test, ten different boot sequences were acquired, where each measurement was at least 3.35 s long.

Finally, for the data processing, we used a Lenovo Ideapad 320 laptop, equipped with an Intel i7-7500 processor running at 2.70 GHz and equipped with 8 GB of RAM.

5.2 Consistency of Unintentional Magnetic Emissions Radiated from USB Devices

Our first investigation aims at establishing the feasibility of uniquely identifying either the brand and model of the USB flash drive or the specific USB device, based on the profile of the unintentional magnetic emissions.

Figure 3 shows two sample measurements acquired at different times, related to the unintentional magnetic emissions radiated from the same Rubber Ducky USB flash drive (U7), during the boot procedures. Because of the normalization phase occurring in the *Features Extraction module*, all the samples corresponding to given times and frequencies have a value between 0 and 1. Specifically, the blue color maps values in the range [0–0.25[, the cyan corresponds to values in the range [0.25–0.5[, the yellow is related to values in the range [0.5–0.75[, while the red color indicates value in the range [0.75–1].

First, we notice that the time duration of our experiments is enough to capture not only the boot phase, where the whole system is powered up and initialized, but also to acquire the following idle state, where the USB device waits for instructions by the target USB device.

By comparing the two figures, it emerges that different recordings have similar normalized power profiles, as per the time and the frequency. Indeed, small differences can be found in the time domain, due to a different delay between the time instant at which the acquisition was started and the time instant where the USB device was connected to the host device, and in the intensity of the unintentional radiation emissions, due to the surrounding noise and minimal displacement between the USB device and the probe. However, even across different measurements, different acquisitions of the unintentional radiated emissions from the same USB device are consistent, confirming that their statistical analysis can be effectively used for discriminating the USB brand and model.

5.3 Scenario #1: Classification of USB flash drives brand and model

The *Scenario #1* described in Section 3 involves the identification of the brand and model of the specific USB Flash Drive under test. As shown in the previous section, different brands of USB Flash Drives are characterized by a very different profile of magnetic emissions. This motivates the use of relatively cheap equipment, i.e., the HackRFOne SDR, as the tool for data acquisition and processing. We recall that the HackRFOne has a maximum acquisition bandwidth of 10 MHz. Thus, this frequency span can be used only to classify USB flash drives brands and models.

To enable cross-comparisons, we considered a fixed observation window of 1.08 s for each of the acquired traces. This time-slot was further divided into a given number of time and frequency regions, leading to a specific number of features characterizing each observation.

To provide sufficient robustness to the classification, we considered a total number of 325 features, computed as follows. We first considered the overall observation interval of 1.08 s, and we computed 5 features, i.e., the mean, standard deviation, variance, skewness, and kurtosis of the samples in the whole interval (see Section 4 for the details of the computation of each feature). This step results in a total of 5 features. Then, we further divided the overall observation interval of 1.08 s in 4 time regions, each region lasting 0.27 s. For each time region, we computed the same 5 features listed above. This step results in a total of 20 features. Then, we further divided each of the 4 time regions into 15 frequency regions, where each frequency region has a bandwidth of 666.67 Hz. For each of the $15 \cdot 4$ regions, we computed the same 5 features listed above. This step results in a total $15 \cdot 4 \cdot 5 = 300$ features. Summing up the three steps, we have a total of $5 + 20 + 300 = 325$ features.

Specifically, the detection of authorized devices against not-authorized ones has been performed resorting to the one-class SVM classifier (see Section 4 for more details). For the Scenario # 1, we considered 17 different models of USB Flash Drives (classes), i.e., $\{U1, \ldots, U17\}$, and we performed 10 observations (measurements) for each class, for a total of 170 observations. Moreover, we adopted the 10-fold cross-validation where, in each fold, 90% of the observations (from each class) have been selected for the training process. Then, we test the remaining observations (10%) against the models created for each USB flash drive (disjoint from the test set and therefore not containing any testing sample), and we evaluate the accuracy of the model through a *similarity score*. Note that we have 17 *similarity scores* for each testing sample, i.e., the score resulting from the evaluation of the testing sample against each of the 17 classes (USB flash drives). Therefore, this strategy leads to a set of 17 similarity scores for each testing sample, and a total number of $17 \cdot 170 = 2{,}890$ *similarity scores*.

Figure 4 shows the computed similarity scores as a function of the 17 considered classes $\{U1, \ldots, U17\}$. For each class (USB device), we reported as green circles (10 samples per class) the

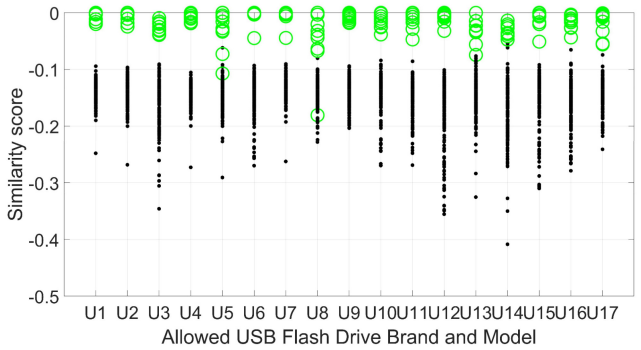

Fig. 4. Classification performance of MAGNETO. Each column refers to a set of 170 experiments where just one USB flash drive model is assumed to be authorized. Green circles report the value of the similarity score of the classifier for the authorized device, while black dots report similarity score for the unauthorized USB brands.

observations coming from the authorized device, while we considered the black dots (160 samples) for the non-authorized ones.

It is worth noting that, in the vast majority of the experiments, the authorized USB flash drives report values that are very close to 0 and less than the value of -0.01, while the unauthorized ones report lower scores. Overall, given that the model of each USB flash drive is trained and validated on its own, we should select a threshold value for each USB brand, and decide to *accept* it as authorized if the evaluation score is higher than the threshold. As a worst-case, we notice that selecting a general threshold $T = -0.075$ guarantees True Positives Ratio (TPR) 0.982 (i.e., 98% of the authorized brands are correctly recognized), and a False Positives Ratio (FPR) of only 0.001 (i.e., only 0.01% of the unauthorized brands are erroneously recognized as authorized). However, a threshold can be selected for each USB flash drive. For instance, focusing on the USB Flash Drive $U7$, the threshold value $T_7 = -0.0365$ provides TPR 1 and FPR 0, i.e., the best possible result.

We remark that the above results show that MAGNETO can distinguish the brand and the model of the USB flash drive, even if the brands share the same controller chip version and same PCB layout. For instance, we can distinguish the specific USB flash drive model among the HPx900w-64 GB, the Kingston Digital 16 GB Data Traveler G4, and the Patriot 128 GB Supersonic Rage Series, despite these three models share the same controller chip and PCB layout, i.e., the PHISON-PS2251-09-V.

The above results suggested that, to some extent, MAGNETO can identify not only the specific hardware chip but also the code that is executed during the boot. Indeed, MAGNETO can discriminate also between the HP, Kingston, PNY, Patriot, Silicon Power, and Toshiba USB flash drives, even if they are based on the same hardware chip. Indeed, we recall that their PCB and/or the version of the firmware is different, and this leads to a different profile in the unintentional magnetic emissions at lower frequencies during the boot operations. More details on the impact of the firmware running on a particular chip will be provided in Section 5.6.

We also investigated the time required by MAGNETO to provide the decision. Using 325 features, over a set of 2,890 experiments, MAGNETO requires 11.5 ms on average, with a lower confidence interval of 10.27 ms and higher confidence interval of 12.72 ms.

Finally, we notice that, in principle, any Machine Learning (ML) and Deep Learning (DL) classification tool can be used to precisely classify the magnetic emissions radiated by the tested USB Flash Drives. However, we highlight that the scope of our article is not to find the best classification tool for this problem, but to show that unintentional magnetic emissions can be used to

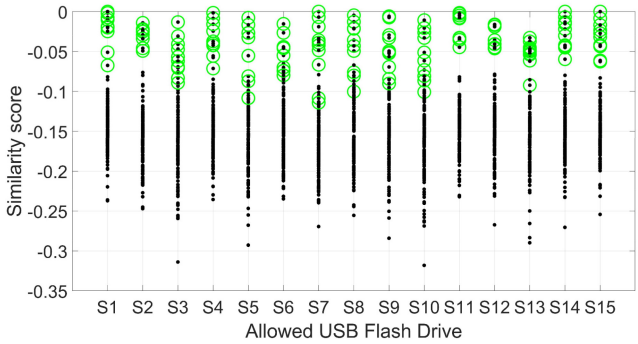

Fig. 5. Classification accuracy of MAGNETO considering 15 SanDisk 16 GB USB Flash Drives.

fingerprint the brand and the model of commodity USB Flash Drives. The data acquired from the tested USB Flash Drives have been released as open-source, to give to interested researchers the opportunity to test additional ML or DL classification tools and further boost the performance of MAGNETO [13].

5.4 Scenario 2: Identifying the specific USB Flash Drive

In the context of the *Scenario #2*, it is of crucial importance to uniquely identify the specific USB flash drive, to protect the Critical Infrastructure against malicious software injection. As shown in Section 5.2, identifying uniquely a USB Flash Drive involves discriminating very subtle differences in the profile of the unintentional magnetic emissions, possibly spanning a wide spectrum. To this aim, more powerful equipment should be used, characterized by a wider real-time bandwidth resolution, such as the *Rohde & Schwarz FSW8* Spectrum Analyzer, leading to an increased number of features, that could be processed by a more powerful processing unit.

To investigate the feasibility of this setup of MAGNETO to uniquely identify USB Flash Drives, we considered USB Flash Drives of the same brand and model, and we applied MAGNETO to identify them uniquely. We considered a fixed observation window of 3.35 s for each of the acquired traces, and the same number of features (325), derived as previously explained. Note that the methodology to test the performance of MAGNETO is still the same previously described: in each experiment, we assumed a selected USB Flash Drive to be the allowed one, while the others were assumed to be rejected, and we used the 10-fold cross-validation, where in each fold, 90% of the recordings were used in the *Training Mode*, and the remaining 10% were used to test the *Classification Mode*.

We considered three different USB Flash Drive brands: the SanDisk 16 GB (U15), the Strontium 16 GB (U16), and the Klevv Neo C20 16 GB (U17), where 15 USB flash drives were available for each experimentation. The results are reported in Figures 5, 6, and 7 for the SanDisk, the Strontium and the Klevv Neo C20, respectively. Note that, now, each column contains $15 \cdot 10 = 150$ experiments, where 10 experiments refer to the authorized USB flash drive and 140 experiments refer to the unauthorized drives.

Figures 5–7 show that most of the (authorized) green circles are characterized by evaluation scores higher than the black (unauthorized) dots. Generally speaking, the selection of the threshold is a key component to determine the accuracy of the devised brands classification method. Low values of the threshold guarantee zero false positives, i.e., no unauthorized brands are erroneously recognized as authorized, but it also implies an increased number of false negatives, i.e., authorized brands erroneously recognized as unauthorized, and thus experiencing a reduced number of

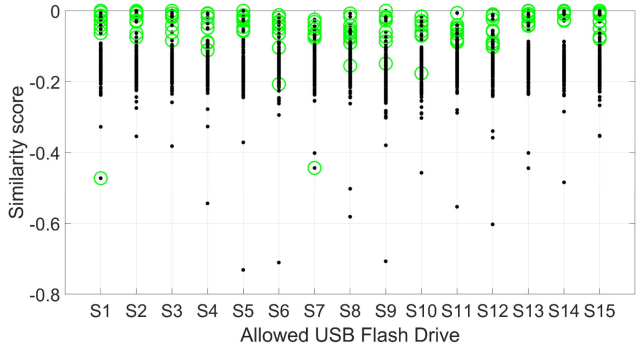

Fig. 6. Classification accuracy of MAGNETO considering 15 Strontium 16 GB USB Flash Drives.

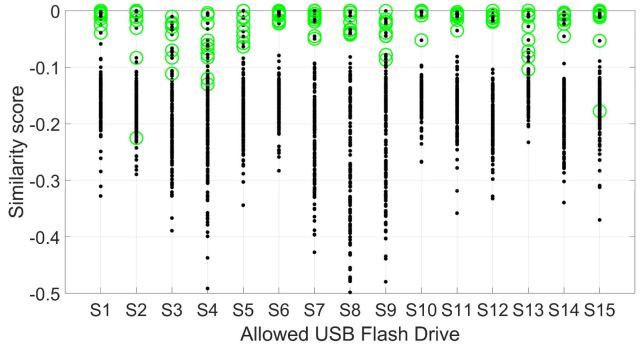

Fig. 7. Classification accuracy of MAGNETO considering 15 Klevv Neo C20 16 GB USB Flash Drives.

True Positives (correctly authorized brands). As a worst-case, we notice that selecting a common threshold $T = -0.09$ for all the SanDisk, the Strontium, and the Klevv Neo, it is possible to guarantee a TPR of 0.946, 0.913, and 0.963, and a FPR of 0.019, 0.027, and 0.012, respectively. We notice that this is the worst-case, as a threshold can be selected appropriately for each single USB Flash Drive. As an example, with the Strontium USB flash drive, an appropriate choice of the thresholds for each flash drive (that can be done looking at Figure 6) can provide up to TPR 0.94 and FPR 0.005. Overall, based on the specific USB flash drive, the network administrator can setup MAGNETO in a way to achieve the best trade-off between the TPR and the FPR, to minimize the false positives. In addition, the administrator can also suggest a specific brand to be used for authentication, based on the achievable ratio between the TPR and the FPR.

Finally, we remark that discriminating against the specific USB device requires more powerful equipment than a simple SDR. Specifically, the equipment to be used should be characterized by a wide real-time resolution bandwidth, of about 200 MHz. Despite in our experimental assessment using the *Rohde & Schwarz FSW8* spectrum analyzer, other cheaper devices are available, characterized by a similar bandwidth range, with a price starting from as low as 500 USD.

5.5 Considerations on Features Reduction

As previously highlighted, MAGNETO requires a total number of 325 features to achieve the reported performances. The reported number of features could appear high, with the risk of incurring in the curse of dimensionality and subsequent model overfitting.

Table 5. True Positive Ratio (TPR) and False Positive Ratio (FPR) of MAGNETO for the Scenario 1 (Brand and Model Identification), Using an Increasing Number of Pre-dominant Features, Obtained with the FEAST Toolbox

No. of Features	Threshold Value	TPR	FPR
10	T = −0.015	0.770	0.0003
20	T = −0.015	0.935	0.0014
50	T = −0.06	0.929	0.0018
100	T = −0.07	0.911	0.0025
200	T = −0.07	0.947	0.0029
300	T = −0.078	0.976	0.0051
325	T = −0.078	0.982	0.0022

Table 6. True Positive Ratio (TPR) and False Positive Ratio (FPR) of MAGNETO for the Scenario 2 (USB Authentication), in the Case of 15 Strontium USB Flash Drives, Using an Increasing Number of Predominant Features, Obtained with the FEAST Toolbox

No. of Features	Threshold Value	TPR	FPR
10	T = −0.8	0.753	0.040
20	T = −0.9	0.78	0.026
50	T = −0.9	0.78	0.026
100	T = −0.9	0.893	0.041
200	T = −0.93	0.893	0.028
300	T = −0.93	0.913	0.027
325	T = −0.93	0.913	0.027

First, we highlight that the methodology adopted by MAGNETO is based on the split of the whole data set into multiple disjoint training and test sets. Specifically, for each test, the model of each USB Flash Drive is trained on nine samples and tested on the remaining one. This approach is then iterated, by testing each available sample as a test set (while the others serve as a training set). It is worth noting that the model has not been updated after the testing, and we did not refine the hyper-parameters of the one-class SVM classifier (being these two among the common sources of overfitting). Therefore, we can reasonably exclude the hypothesis of overfitting.

However, to provide further insights, we investigated the effectiveness of MAGNETO using a reduced number of features, both for Scenario 1 and a reference example for Scenario 2. To determine the critical features, we rank them with the help of the FEAST toolbox, which is a commonly used feature ranking tool in machine learning [8]. This toolbox has been used also recently by the authors of Reference [10], to reduce the dimensionality of the features in the context of unintentional magnetic emissions. Tables 5 and 6 show the results of our investigation with a different number of pre-dominant features, assuming the Scenario 1 (brand and model identification) and the worst-case of Scenario 2 (USB authentication, 15 Strontium USB Flash Drives), respectively. In the tables, we also report the correspondent selection of the threshold value (worst-case), set up to achieve the reported results.

We notice that the fluctuations of the results by increasing the number of features is limited. For the Scenario 1, the most representative 20 features are enough to obtain a TPR of 0.93, with

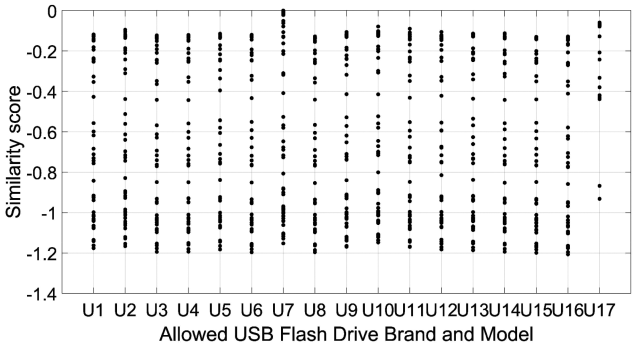

Fig. 8. Classification accuracy of MAGNETO considering 6 modified versions of the boot firmware of the Rubber Ducky USB Flash Drive (U7).

a negligible fraction of false positive (FPR 0.0014). At the same time, for the case of Scenario 2, assuming to work with the Strontium USB Flash Drives, 100 features are enough to obtain a TPR of 0.893, and including more features has only a slight impact on the performance accuracy.

Based on the above considerations and results, we believe that we are both avoiding the curse of dimensionality, and not overfitting the model.

5.6 Discussion on Firmware Modifications

As highlighted in Section 3, the firmware of commercial USB flash drives is usually protected by multiple security layers, and cannot be modified. Despite several tutorials are available on media and technical blogs regarding firmware modification of commercial USB flash drives, this is possible only due to vulnerabilities affecting specific versions of the firmware of the USB flash drive. As a direct consequence, the aforementioned vulnerabilities are usually (and immediately) fixed by the vendor.

However, there are specific USB flash drives, such as the Rubber Ducky, whose firmware is specifically designed to be modified to achieve several tasks. These tasks can include benign operations, such as the opening of a file, or malicious activities, such as the disabling of anti-virus software on the host, or the activation of passwords stealing tool.

To provide more insights on the performance of MAGNETO to identify modified firmware versions, we investigated the effectiveness of our solution considering seven different firmware versions of the Rubber Ducky (U7):

- F1. Baseline default firmware used in Section 5.3, injecting an empty payload;
- F2. Firmware that opens a text file and types a single *Hello World* line;
- F3. Firmware that opens a text file and types 100 *Hello World* lines;
- F4. Firmware that opens a text file and types 200 *Hello World* lines;
- F5. Firmware that disables Windows Defender;
- F6. Firmware that inserts a delay of approximately 750 ms;
- F7. Firmware that steals browser-stored passwords.

First, we investigated the performance of MAGNETO to identify the above firmware modifications, without any previous knowledge of their existence. To this aim, we used the models created for the tests in Section 5.3, while the test set consisted of 10 acquisitions for the firmware versions $\{F2, \ldots, F7\}$. The results are reported in Figure 8. Note that all the markers are now black dots, as the whole test set samples are considered to be *unauthorized*. First, we notice that for all the

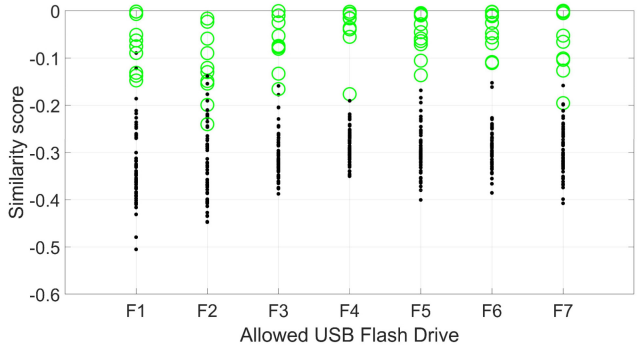

Fig. 9. Classification accuracy of MAGNETO considering 6 modified versions of the boot firmware of the Rubber Ducky USB Flash Drive (U7), assuming to train on the modified firmware versions.

experiments that assume as *authorized* a USB flash drive that is different than the *U7*, report values that are lower than -0.01. Considering the configuration of the threshold discussed in Section 5.3, these experiments all provide correct *True Negative* outputs. Considering the USB flash drive $U7$, we notice that, out of 50 experiments, 13 report values that exceed the local threshold $T = -0.0365$, i.e., the local threshold value obtained from the experiments in Section 5.3, providing FPR 0. These experiments correspond to the firmware $F2$ (8 experiments) and $F5$ (5 experiments). Therefore, in the absence of any training on the modified firmware versions, MAGNETO can discriminate a modified firmware only if the profile of the corresponding EM emanations is consistently different from the *trained* one. When the modifications are very little, such as for $F2$ and $F5$, the accuracy of MAGNETO decreases.

However, we notice that the accuracy of MAGNETO can be significantly enhanced by training on the modified firmware versions. When this is possible (as for the Rubber Ducky), Figure 9 provides the results of such a scenario, using the same procedure used for the previous sections. It is worth noting that selecting the previously adopted threshold value, i.e., $T = -0.07$, MAGNETO achieves FPR 0, i.e., it does not mislead any of the firmware versions with the native firmware version $F1$ for the USB flash drive $U7$.

5.7 Host Device (Verifier) Configuration and Its Impact on MAGNETO

The analysis and results reported in the previous sections have been obtained using a single host device, as detailed in Section 5.1. This is consistent with the two scenarios and the system model assumed in our work. Indeed, both in a company (Scenario #1) and in a critical infrastructure (Scenario #2), it is reasonable to assume that the system administrator has full control of the verifier, i.e., the system used to acquire the fingerprints of the legitimate USB devices and to test new USB devices. Moreover, it is reasonable and convenient for the system administrator that such a system uses the same Operating System of the system(s) used within the site.

To provide further insights about the fingerprinting process, in this subsection, we extend our analysis, investigating the consistency of the fingerprinting process when the hardware and the software of the host devices change.

As a reference example, we investigated the consistency of the magnetic emissions radiated during the boot process by a USB flash drive when different versions of the same OS are used on the same machine. To this aim, we collected the unintentional magnetic emissions radiated during the boot of a sample USB flash drive, i.e., the SanDisk Cruzer 128 GB drive (U10), when connected to the same machine used for the previous tests, operating with the Windows 7 and the Windows

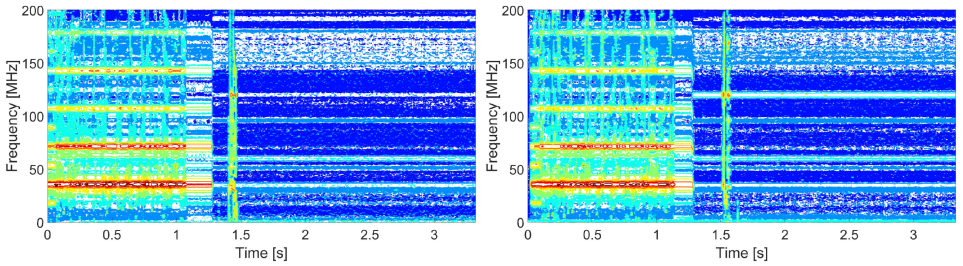

Fig. 10. Magnetic emissions of a USB flash drive (SanDisk Cruzer 128 GB, U10) on (a) Windows 10 OS and (b) Windows 7 OS.

10 OS. The former includes the version 6.1.7601.1910 of the USB driver, dating back to June 2006, while the latter mounts the latest available version at the time of this writing, i.e., the version 10.0.18362.1 of the USB driver (March 2019). The profiles are shown in Figure 10.

Comparing the two figures, some small differences are noticeable, especially in the duration of the different phases of the boot sequence. We remark that, while we report the figures only for the $U10$ flash drive, the above-described behavior is common to all the USB flash drives analyzed in our work.

Overall, these findings suggest that the construction of the Local Database (i.e., the training process) and the Classification (i.e., the testing process) required by MAGNETO should be carried out on the same system, guaranteeing both hardware and software consistency. When at least one of these features changes, differences arise that, especially in the case of Scenario # 2, could lead to undesired mismatches. Conversely, when the system administrator only requires the verification of the brand and the model of the USB flash drive (Scenario # 1), fingerprints can be acquired and tested by using different systems or different OSs.

We highlight that these findings are consistent with other related work on unintentional magnetic emissions. Indeed, small modifications to the hardware and software features of involved devices lead to different fingerprints.

Overall, our analysis demonstrates that the profile of the unintentional magnetic emissions radiated during the boot procedure is mainly caused by the combination of four main elements: (i) the memory readings/writings of the USB flash drive; (ii) the software instructions executed by the microcontroller chip of the USB flash drive; (iii) the layout of the PCB of the USB flash drive; and (iv) the hardware and software features of the host device. This is confirmed by several findings. Considering the same micro-controller chip on a specific host, we have recorded completely different profiles of unintentional magnetic emissions when considering different USB flash drives, characterized by different layout of the PCB. This can be verified by looking at the profile of the unintentional emissions of the devices HP (U1), Kingston (U3), PNY (U5), Patriot (U6), Silicon Power (U13), and Toshiba (U14), sharing the same micro-controller chip but a different layout of the PCB.

In addition, as demonstrated by the above analysis, changing the hardware and the software of the host device has a small yet noticeable impact on the fingerprints. When only the software of the host changes, differences in the fingerprint of the same USB flash drive become more pronounced due to a different interaction of the OS with the USB flash drive, affecting the final part of the boot procedure. Considering different hardware (USB flash drive) on the same physical machine, we also experienced small differences in the final part of the boot.

The discussion reported above highlights the effect of the hardware and the software of the host device on the overall recorded fingerprint. However, we remark that the peculiarities associated with the magnetic emissions are both out of the scope of our work and technically hard to achieve

when working with System-on-Chip (SoC), such as the USB flash drives. Indeed, matching the effect of every single electronic component to the fingerprint would require isolating the effect of each of them on the PCB of the specific USB flash drive. This is very hard to achieve both via hardware and software. As for the hardware, disconnecting its components turns out to be very difficult to achieve, in particular when working with SoC, such as the USB flash drives, where all the electronic components are integrated on the same PCB. Disabling the components via software, instead, would require having strict control over the firmware and the software of the USB flash drive. However, they are not accessible by end-users and protected against source code reverse-engineering by multiple security layers.

Overall, we can conclude that the differences among the brands and the devices of the same brand are due to small circuits differences, as well as inaccuracies and imperfections in the manufacturing process. On the one hand, the underlying process behind MAGNETO can be brought back to a specific use-case of the Electro-Magnetic emanations of embedded circuits. On the other hand, we would like to recall that our work aims to identify either the brand and the model or the specific USB device, including all the interacting components, as a unique device. Thus, analyzing the effect of each component of the leakage is out of scope for our work. We also remark that MAGNETO is novel compared to other related work as, to the best of the authors' knowledge, it is the first solution that can fingerprint USB flash drives in a non-interactive, minimal-invasive, and privacy-preserving fashion, not requiring any intervention or modification on the devices under test.

We also highlight that MAGNETO can be further extended to interact with the host OS, to instruct the sampling of the unintended magnetic emissions radiated by a connected USB flash drive asynchronously, e.g., when a suspected activity is recorded by the host OS via software. In such a scenario, it could be possible to compare the recorded profile of the specific USB flash drive in regular operating conditions with the actual one, to identify eventual deviations. However, this extension is left as future work. Finally, we highlight that our methodology, i.e., fingerprinting the device as a whole, without considering the effect of the single components, is consistent with all the related work investigating physical-layer fingerprinting and unintentional Electro-Magnetic emissions, including [6, 9, 10, 12, 14, 15, 24, 36, 47, 53, 54]. The physical effects underpinning these phenomena are described by the physics fundamental Maxwell equations, and also specific mathematical models are available in the literature, describing their complex creation [7].

6 DISCUSSION AND LIMITATIONS

The results presented in Section 5 clearly showed the effectiveness of MAGNETO. We showed that, considering a specific host device, the unintentional magnetic emissions radiated at low frequencies during the boot by a USB flash drive are: (i) very similar for devices of the same brands, (ii) unique for each device, and (iii) consistent in time, thus being a viable and effective tool for USB brand and device fingerprinting. For instance, assuming the reference scenario of a company, such as the *Scenario # 1* discussed in Section 3, the system administrator can enforce the use of only specific brands and models of USB flash drive, eventually provided by the company itself. To this aim, the system administrator can deploy MAGNETO on a dedicated machine, acquiring the profile of the unintentional magnetic emissions of the selected USB flash drives, before their use. Then, in the case of a company, on a selected period (e.g., once a day), every time a USB flash drive needs to be used, the system administrator can plug the device into a dedicated laptop, connected to the proposed MAGNETO system. Then, if the magnetic emissions at low frequencies during the boot operations match the stored profile for the particular brand and model, then the use of the particular USB flash drive could be authorized; otherwise, it will not. Similarly, in a critical infrastructure, such as in the *Scenario # 2* discussed in Section 3, it is possible to deploy

MAGNETO by using powerful equipment, able to acquire the profile of the magnetic emissions on a wider frequency span. As shown in Section 5.4, using such an increased frequency span can enhance the capabilities of MAGNETO, to provide the identification of the specific USB drive.

Another feature of MAGNETO is its *linear overhead*, independent of the amount of USB flash drives on the market. Indeed, the system administrator needs only to generate the profile (according to the procedure detailed in the article) of the USB he/she wants to add to the whitelist of the authorized USB drives. Once the process committed, any USB drive that is screened requires just the collection of the drive's magnetic profile and its comparison against the profiles in the whitelist. The operation has a cost that is linear in the size of the whitelist.

It is worth noting that the setup of MAGNETO is only aimed at protecting and ensuring the authenticity of the boot procedures. This choice allows timely detection of a malicious adversary that: (i) replaces the regular USB flash drive with another one having the same external look and form factor, but a different hardware and (possibly malicious) firmware, and (ii) can replace the firmware of a legacy USB device with a brand new one, by inserting its own code. Such strategies are common to the vast majority of USB attacks known today, as they are based on the complete replacement of the hardware or the firmware of a regular USB device [28].

USB firmware tampering. Despite some USB flash drives being certified according to FIPS 140-2 Levels 2 and 3 standards, USB flash drives cannot be considered as protected against tampering. As demonstrated in Section 5.6, the strength of MAGNETO lies in the inherent capability to detect the tampering, as long as the modified firmware causes a profile of the unintended magnetic emissions sufficiently different from the recorded one.

Indeed, the adversary might replace the firmware of the USB flash drive with a malicious one, where just the minimum amount of lines have been modified to trigger a specific malware. Despite MAGNETO dealing with these modifications by training on the modified firmware versions, we highlight that both the executable file and the source code of the firmware on-board of commercial USB flash drives are usually not modifiable and not accessible by the end-users after the deployment. Even in the unlikely case where an adversary can obtain the file of the compiled firmware, it is hard and impractical to reverse-engineer it to obtain the source code. Indeed, being always protected by intellectual property rights, the source code of such firmware is also secret, protected by multiple security layers deployed at manufacturing time, and not available for public download. Thus, it is unfeasible to obtain it and to deploy the aforementioned attack.

Similarly, another adversarial strategy could consist in smartly modifying the firmware of the legacy USB device, inserting just a code line that postpones the injection of the malicious code after the execution of the boot, i.e., when the USB drive goes in the idle state, waiting for instructions by the host. Despite the considerations previously done for the legacy firmware modifications are still applicable to this attack, we also observe that MAGNETO can be extended to detect the previously mentioned attack. By simply widening the observation window of the *Emissions Extraction Module* and recording the unintentional magnetic emissions when the USB device is in the idle state, MAGNETO can detect any anomalous operations initiated by the USB device, raising an immediate alarm. Thus, MAGNETO can be extended to guarantee the safe usage of any USB flash drive over an arbitrarily large time after the USB device has been connected to the host system.

More powerful adversaries could adopt more sophisticated strategies. For instance, they could tie the execution of the malicious code to a file transfer operation on the particular USB flash drive. When a file is transferred to (or from) the drive, the malicious code is triggered. The effectiveness of MAGNETO against this attack could still be achieved by fingerprinting also a file transfer operation, assuming that a file transfer of a given size leads to the same profile of the unintended radiated emission. To neutralize our countermeasure, the adversary could always trigger the execution of the malicious code in a way to be tied to the size of the file to be transferred (e.g., greater

than 10 MB). In this case, MAGNETO would be effective only if the profile of the unintentional magnetic emissions for the specific file transfer operation has been recorded and profiled before, during the *Training Mode*. It follows that fingerprinting all these operations would affect also the latency and the usability of MAGNETO, increasing the testing time and the overall size of MAGNETO. However, if the attack is triggered only when a specific file stored on the USB is opened, then MAGNETO cannot be effective without any previous fingerprinting process on that specific file.

7 CONCLUSION

In this article, we proposed MAGNETO, a framework able to enhance the security level in the usage of USB flash drives. Depending on the used equipment, MAGNETO can uniquely identify either the brand and the model of commercial USB flash drives, or the specific USB flash drive, by analyzing unintentional magnetic emissions radiated by the target USB devices during the execution of the boot procedure. Through extensive experimental measurements on 59 different USB drives—belonging to 17 brands, including the top brands purchased on Amazon in mid-2019—we demonstrated that a USB flash drive can be fingerprinted by only looking at the magnetic emissions unintentionally radiated during the boot procedure on a given host. When coupled with a commercial low-cost Software Defined Radio such as the HackRFOne, MAGNETO can identify the specific brand and model of the USB flash drive with a minimum classification accuracy of the 98.2%, guaranteeing, at the same time, only 0.01% of false positives. When coupled with more expensive equipment, characterized by a wide analysis bandwidth of at least 200 MHz, MAGNETO can also identify the specific USB flash drive with a minimum classification accuracy of 91.3%. All the results above can be obtained in almost real-time, analyzing a time-frame of at most 3.35 s and requiring a negligible processing time (always less than 1 s on a standard laptop).

Thanks to the reported outstanding performance, MAGNETO emerges as a viable option to strengthen the security of any sensitive computing equipment exposed to the threats posed by USB drives, such as the one in a telco-backbone or a power plant, and in general contributing to the security of critical infrastructure systems.

ACKNOWLEDGMENTS

The authors thank the anonymous reviewers who helped to improve the quality of the manuscript.

REFERENCES

[1] Aaronia. 2020. *PBS2 EMC Probe*. Retrieved from http://tinyurl.com/y4jojj9j.
[2] S. P. Acharya and I. G. Guardiola. 2013. Detection of RF devices based on their unintended electromagnetic emissions using Principal Components Analysis. In *Proceedings of the Wireless Telecommunications Symposium*. 1–5.
[3] Amazon. 2020. *Best Sellers in USB Flash Drives*. Retrieved from https://tinyurl.com/y6sq85sc.
[4] S. Angel, R. Wahby, M. Howald, J. Leners, M. Spilo, Z. Sun, A. Blumberg, and M. Walfish. 2016. Defending against malicious peripherals with Cinch. In *Proceedings of the 25th USENIX Security Symposium*. 397–414.
[5] A. Bates, R. Leonard, H. Pruse, D. Lowd, and K. Butler. 2014. Leveraging USB to establish host identity using commodity devices. In *Proceedings of the Network and Distributed System Security Symposium (NDSS'14)*.
[6] T. J. Bihl, K. Bauer, and M. Temple. 2016. Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions. *IEEE Trans. Info. Forens. Secur.* 11, 8 (2016), 1862–1874.
[7] K. Bole, J. McGraw, F. Ryan, T. Hawley, M. Davis, and T. Van. 2009. Integrated passive electronic signature modeling. In *Proceedings of Atmospheric Propagation VI*, Vol. 7324.
[8] G. Brown, A. Pocock, M. Zhao, and M. Luján. 2012. Conditional likelihood maximisation: A unifying framework for information theoretic feature selection. *J. Mach. Learn. Res.* 13, 1 (2012), 27–66.
[9] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon. 2018. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the ACM Conference on Computer and Communications Security*. 163–177.

[10] Y. Cheng, X. Ji, J. Zhang, W. Xu, and Y. Chen. 2019. DeMiCPU: Device fingerprinting with magnetic signals radiated by CPU. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 1149–1170.
[11] C. Cimpanu. 2019. Ships infected with ransomware, USB malware, worms. Retrieved from https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/.
[12] William E. Cobb, Eric W. Garcia, Michael A. Temple, Rusty O. Baldwin, and Yong C. Kim. 2010. Physical layer identification of embedded devices using RF-DNA fingerprinting. In *Proceedings of the Military Communications Conference*. 2168–2173.
[13] CRI-Lab. 2019. MAGNETO source code and data. Retrieved from https://cri-lab.net/usb-fingerprinting.
[14] G. DeJean and D. Kirovski. 2007. RF-DNA: Radio-frequency certificates of authenticity. In *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 346–363.
[15] C. K. Dubendorfer, B. W. Ramsey, and M. A. Temple. 2012. An RF-DNA verification process for ZigBee networks. In *Proceedings of the IEEE Military Communications Conference*. 1–6.
[16] Essencore. 2020. *Klevv Neo C20 16GB*. Retrieved from https://tinyurl.com/ya6v9avv.
[17] Federal Communications Commission (FCC). 2019. Code of Federal Regulations, Title 47 2009. Retrieved from https://www.fcc.gov/wireless/bureau-divisions/technologies-systems-and-innovation-division/rules-regulations-title-47.
[18] F. Griscioli, M. Pizzonia, and M. Sacchetti. 2016. USBCheckIn: Preventing BadUSB attacks by forcing human-device interaction. In *Proceedings of the Annual Conference on Privacy, Security and Trust (PST'16)*. 493–496.
[19] Hack5. 2020. *Rubber Ducky*. Retrieved from https://shop.hak5.org/products/usb-rubber-ducky-deluxe.
[20] HP. 2020. *HP 64GB x900w*. Retrieved from https://tinyurl.com/y3sbtutn.
[21] HP, Intel, Microsoft, NEC, ST-NXP, Texas Instruments. 2018. Universal Serial Bus 3.0 Specifications—Revision 1.0. Retrieved from https://www.usb3.com/whitepapers/USB%203%200%20(11132008)-final.pdf.
[22] JUANWE. 2020. *JUANWE 32GB*. Retrieved from https://tinyurl.com/y6myw3vq.
[23] Kingston. 2020. *Kingston Data Traveler*. Retrieved from https://tinyurl.com/y46vehoh.
[24] M. Lukacs, A. Zeqolari, P. Collins, and M. Temple. 2015. RF-DNA fingerprinting for antenna classification. *Antenn. Wireless Prop. Lett. IEEE* 14 (2015), 1455–1458.
[25] C. Lyu, J. Peng, W. Zhou, S. Yang, and Y. Liu. 2016. Design of a high speed 360-degree panoramic video acquisition system based on FPGA and USB 3.0. *IEEE Sensors J.* (2016), 1–1. DOI: 10.1109/JSEN.2016.2628240
[26] MOSDART. 2020. *MOSDART 8GB*. Retrieved from https://tinyurl.com/y6o29fv2.
[27] C. Mulliner and B. Michéle. 2012. Read it twice! A mass-storage-based TOCTTOU attack. In *Proceedings of the Workshop on Offensive Technologies (WOOT'12)*. 105–112.
[28] N. Nissim, R. Yahalom, and Y. Elovici. 2017. USB-based attacks. *Comput. Secur.* 70 (2017), 675–688.
[29] K. Nohl and J. Lell. 2014. BadUSB—On accessories that turn evil. In *Black Hat USA*.
[30] D. Noyes, H. Liu, and P. Fortier. 2016. Security analysis and improvement of USB technology. In *Proceedings of the IEEE Symposium on Technologies for Homeland Security (HST'16)*. 1–3.
[31] Null Byte. 2015. Make Your Own Bad USB. Retrieved from https://null-byte.wonderhowto.com/how-to/make-your-own-bad-usb-0165419/.
[32] Patriot. 2020. *Patriot 128GB Supersonic Rage Series*. Retrieved from https://tinyurl.com/yxuvjsnm.
[33] Phison. 2019. Phison Consumer Solutions. Retrieved from https://www.phison.com/en/solutions/consumer/removable/usb/53-usb-flash-drive/78-ps2251-70.
[34] PNY. 2020. *PNY Turbo 128GB*. Retrieved from https://tinyurl.com/y249c4dd.
[35] R. Przesmycki and L. Nowosielski. 2016. USB 3.0 interface in the process of electromagnetic infiltration. In *Proceedings of the Progress in Electromagnetic Research Symposium (PIERS'16)*. 1019–1023.
[36] B. Ramsey, M. Temple, and B. Mullins. 2012. PHY foundation for multi-factor ZigBee node authentication. In *Proceedings of the Global Communications Conference (GLOBECOM'12)*. IEEE, 795–800.
[37] Samsung. 2020. *Samsung BAR*. Retrieved from https://tinyurl.com/y3dxrfl2.
[38] SanDisk. 2020. *SanDisk 128GB Ultra Fit*. Retrieved from https://tinyurl.com/y2p6y3jy.
[39] SanDisk. 2020. *SanDisk Cruzer*. Retrieved from https://tinyurl.com/y4gs24ha.
[40] SanDisk. 2020. *SanDisk Cruzer 128GB*. Retrieved from https://tinyurl.com/y6ghcray.
[41] SanDisk. 2020. *SanDisk Cruzer Glide 16 GB*. Retrieved from https://tinyurl.com/ydhtuo3c.
[42] SanDisk. 2020. *SanDisk Cruzer Glide CZ60*. Retrieved from https://tinyurl.com/y2q669zm.
[43] SearchSecurity. 2019. USB attacks: Big threats to ICS from small devices. Retrieved from https://searchsecurity.techtarget.com/feature/USB-attacks-Big-threats-to-ICS-from-small-devices.
[44] A. Shabtai, R. Moskovitch, Y. Elovici, and C. Glezer. 2009. Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. *Info. Secur. Techn. Rep.* 14, 1 (2009), 16–29.
[45] Silicon Power. 2020. *Silicon Power Blaze B30*. Retrieved from https://tinyurl.com/y6gvtxfg.
[46] Strontium. 2020. *Strontium Pollex Flash Drive*. Retrieved from https://tinyurl.com/y86z8rys.

[47] W. Suski, M. Temple, M. Mendenhall, and R. Mills. 2008. Radio frequency fingerprinting commercial communication devices to enhance electronic security. *Int. J. Electron. Secur. Digit. Forensic* 1, 3 (Oct. 2008), 301–322.
[48] K. Suzaki, Y. Hori, K. Kobara, and M. Mannan. 2019. DeviceVeil: Robust authentication for individual USB devices using physical unclonable functions. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'19)*. 302–314.
[49] D. J. Tian, A. Bates, and K. Butler. 2015. Defending against malicious USB firmware with GoodUSB. In *Proceedings of the 31st Annual Computer Security Applications Conference*. 261–270.
[50] Dave Jing Tian, Nolen Scaife, and Adam Bates. 2016. Making USB great again with USBFILTER. In *Proceedings of the 25th USENIX Security Symposium*.
[51] Toshiba. 2020. *Toshiba 64GB TransMemory*. Retrieved from https://tinyurl.com/y4r6wg4w.
[52] Transparency Market Research. 2017. Global USB 3.0 Flash Drives Market. Retrieved from https://www.transparencymarketresearch.com/pressrelease/global-usb-flash-drives-market-size.htm.
[53] W. Cobb, E. Laspe, R. Baldwin, et al. 2012. Intrinsic physical-layer authentication of integrated circuits. *IEEE Trans. Info. Forens. Secur.* 7, 1 (Feb. 2012), 14–24.
[54] B. Wright. 2014. *PLC Hardware Discrimination using RF-DNA Fingerprinting*. Technical Report. Air Force Institute of Technology, Wright-Patterson Air Force Base.

Received February 2020; revised July 2020; accepted September 2020