POSTER: MAG-PUF - Authenticating IoT Devices via Magnetic Physical Unclonable Functions

Omar Adel Ibrahim
Division of Information and Computing Technology
College of Science and Engineering, Hamad Bin Khalifa University
Doha, Qatar

Savio Sciancalepore
Eindhoven University of Technology (TU/e)
Eindhoven, The Netherlands

Roberto Di Pietro
Division of Information and Computing Technology
College of Science and Engineering, Hamad Bin Khalifa University
Doha, Qatar

ABSTRACT

Authenticating Internet of Things (IoT) devices is still a defiant task, despite the remarkable technological advancement achieved in the last few years. The issue is especially challenging in scenarios involving low-cost constrained nodes, hardly supporting dynamic re-keying algorithms. To provide a viable general-purpose solution, we propose MAG-PUF: a novel and lightweight authentication scheme using unintentional magnetic emissions produced by IoT devices to implement Physical Unclonable Functions (PUFs). Our extensive experimental campaign, involving 25 Arduino boards and four example reference functions, unveiled an outstanding authentication accuracy of over 99%, proving the feasibility of using code-driven magnetic emissions as a lightweight, efficient, and robust PUF for IoT deployments.

ACM Reference Format:
Omar Adel Ibrahim, Savio Sciancalepore, and Roberto Di Pietro. 2022. POSTER: MAG-PUF - Authenticating IoT Devices via Magnetic Physical Unclonable Functions. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22), May 16–19, 2022, San Antonio, TX, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3507657.3529656

1 INTRODUCTION

Internet of Things (IoT) devices are nowadays increasingly deployed in a variety of application domains, serving even more safety-critical functions in homes, offices, medical, electricity, and transportation domains, to name a few [1].

Unfortunately, as acknowledged by several sources [2], security issues are still one of the most critical concerns, preventing the unleashing of the full potential behind the IoT. On the one hand, IoT is often applied in natively-insecure environments, being the ideal target of various attacks. On the other hand, the used devices are usually so constrained from the processing, memory, and energy perspective that they cannot support Public Key Infrastructure (PKI) and symmetric key cryptography techniques. At the same time, where IoT devices do support cryptography operations, many deployments use hard-coded keys, stored in the Non-Volatile Random Access Memory (NVRAM) of the devices, making them an easy target for the attackers [3].

Contribution. To address the above-described issues, we design *MAG-PUF*, a novel lightweight Physical Unclonable Function exploiting the unique randomness of unintentional magnetic emissions produced by IoT devices when computing specific functions [4],[5]. Specifically, *MAG-PUF* allows the system administrator of the IoT domain to choose a theoretically-unlimited number of reference functions to be used for authentication purposes. The profile of the magnetic emissions released by the specific devices when executing the reference functions is first acquired by the system administrator before deployment, and then checked at run-time, to verify their consistency. To this aim, as novel feature in the PUF domain, *MAG-PUF* also integrates Machine Learning (ML)-based classification tools, used to extract the model of the magnetic emissions and to check for the match of a specific acquisition with the expected profile. Our extensive experimental performance assessment, performed over 25 Arduino IoT devices and four reference functions, reported an outstanding classification accuracy of over 99%, as well as PUF-related metrics almost coincidental with the optimal values (Intra-PUF Distance of 0.02 and Inter-PUF Distance of 0.51). In the following sections, we provide some details about the architecture of *MAG-PUF* and experimental results.

2 PROPOSED FRAMEWORK

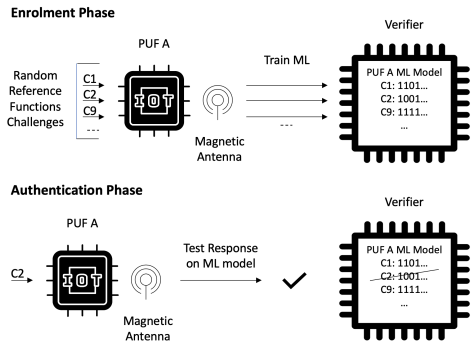


Figure 1: Overview of *MAG-PUF*.

Figure 1 provides an overview of *MAG-PUF*. Overall, *MAG-PUF* allows a verifier (e.g., the local system administrator or another device on its behalf) to authenticate a prover (an IoT device), leveraging the profile of the unintentional magnetic emissions generated

Permission to make digital or hard copies of part or all 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 third-party components of this work must be honored. For all other uses, contact the owner/author(s).
WiSec '22, May 16–19, 2022, San Antonio, TX, USA
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9216-7/22/05.
https://doi.org/10.1145/3507657.3529656

by the prover device while executing a given *reference function*, i.e, a sequence of operations selected appropriately by the verifier.

In brief, *MAG-PUF* consists of two phases, i.e., the *enrolment Phase* and the *Authentication Phase*. The former is executed upon manufacture, by supplying to the prover several *reference functions*, extracting the corresponding unintentional magnetic emissions generated by the device, and creating the corresponding *reference models*, via ML algorithms. At run-time, when the verifier requires authentication of the IoT device(s), it chooses at random one or more of the available *reference functions*. Then, the verifier acquires the corresponding unintentional magnetic emissions and checks if the corresponding real-time profile of the unintentional magnetic emissions matches the one available for the prover, via ML-based classification tools. If a match is found, the prover IoT device is authenticated successfully; otherwise, authentication fails.

3 EXPERIMENTAL RESULTS

We first evaluated the profile of unintended magnetic emissions generated by an Arduino IoT device when running different reference functions. To this aim, we defined four exemplary atomic operations: (A1) empty loop; (A2) first encrypt, later decrypt a 128-bit long message, using AES128, Block Cipher Mode (CBC); (A3) comparison of the similarity between two strings 11-bytes long; and, (A4) reading of input data from a DHT11 temperature and humidity sensor. Figure 2 shows the spectral power density of the unintentional magnetic emissions of the four reference functions.

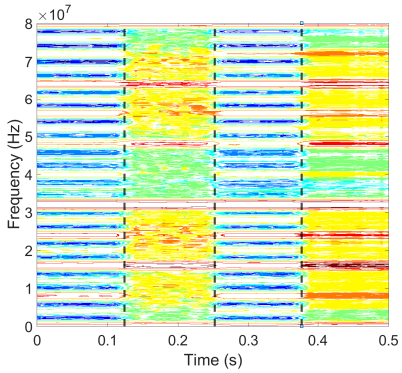


Figure 2: Unintentional magnetic emissions of 120 ms of the four reference functions, separated by dashed line.

For the verifier to authenticate the prover, we use the one-class cubic Support Vector Machine (SVM) ML model available in Matlab. We consider the functions above described, each run separately inside a *For* loop on each of the 25 IoT boards. We divide each collected trace into 120ms segments with 20 MHz acquisition bandwidth, and compute 95 statistical features for each segment. Overall, we consider a total of 1,200 samples of each function running on each individual IoT board. We divided those 1,200 samples into 80% (960 samples) for training of the ML model, and the remaining 20% (240 samples) for testing the trained model. For each IoT board, green circles (240 samples per class) identify data from the authentic IoT device, while the black dots (5,760 samples) represent the non-authentic ones. In most experiments, the authentic IoT devices report values very close to 0.

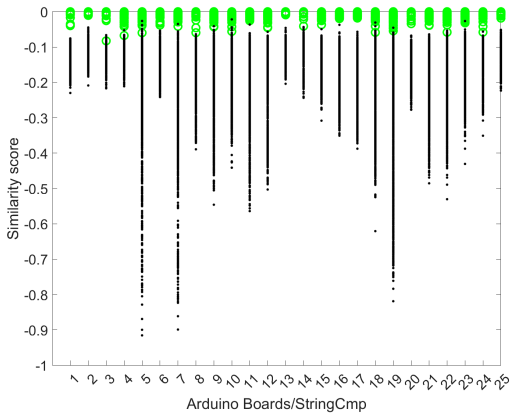


Figure 3: Classification results of (A3) on 25 IoT devices

Figure 3 shows the scores generated by the SVM model, produced by the 25 IoT boards' classes, considering the function (A3), reporting 99.7% accuracy. We obtained similar results also for the other functions, demonstrating the exciting potential of our solution.

4 CONCLUSIONS

In this contribution, we proposed *MAG-PUF*, a novel and lightweight authentication solution for resource-constrained IoT devices. *MAG-PUF* authenticates IoT devices using the uniqueness of the unintentional magnetic emissions radiated by the devices when executing specific functions. Our conceptual framework is supported by a preliminary experimental campaign. Using 25 Arduino IoT boards and four reference functions to test our solution, we revealed an outstanding classification accuracy (over 99%), high flexibility, robustness, and very limited overhead. At the same time, our investigation shows the robustness of using magnetic emissions for PUFs, with relevant metrics very close to the ideal values.

ACKNOWLEDGEMENTS

This publication was partially supported by award GSRA6-1-0528-19046, from the QNRF-Qatar National Research Fund, a member of The Qatar Foundation. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the QNRF.

REFERENCES

[1] Siow, E. et al., "Analytics for the Internet of Things: A Survey," *ACM computing surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.
[2] Semiconductor Eng., "IoT Device Security Makes Slow Progress," https://semiengineering.com/iot-device-security-makes-slow-progress/, 2019, (Accessed: 31-3-2022).
[3] Camurati, G. et al., "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," in *ACM CCS*, 2018, p. 163–177.
[4] McGrath, T. et al., "A PUF Taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, p. 011303, 2019.
[5] Ibrahim, O. et al., "MAGNETO: Fingerprinting USB Flash Drives via Unintentional Magnetic Emissions," *ACM Trans. on Emb. Comp. Sys.*, vol. 20, no. 1, pp. 1–26, 2020.