Electromagnetic Enclosure PUF for Tamper Proofing Commodity Hardware and other Applications

Abstract—In this paper, we introduce a novel approach for verifying the authenticity, integrity and/or physical condition of an item. We examine this construction as a tamper resistance mechanism for computer systems, which are located within an electromagnetic measurable dedicated environment. Our approach forms an Algorithmic Tamper Proof (ATP) to protect secret information, such as keys, without circuit-level sensors, which is a known difficult and imperfect undertaking. The approach also allows tamper evidence for larger structures, e.g., off-the-shelf computers and its periphery. To this end, we build a confined and shielded space around the system of interest, together with an RF measurement system, consisting of antennas and sealing material. The RF channel between the antennas is uniquely influenced by the environment, including computer system and sealing. Channel State Information (CSI), which captures the influence of the physical environment, represents the basis for a digital fingerprint.

CSI is used to extract cryptographic keys that are directly tied to the integrity of the whole system. We use an experimental setup for verifying the applicability of our idea. The setup enables us to demonstrate the three core requirements: uniqueness, sensitivity and reliability. We show how the channel measurements allow constant real-time tests of the integrity and, by analyzing raw CSI values, we demonstrate that the keys can only be recovered if the physical structure remains undisturbed. The derived cryptographic keys can, for example, be used for memory encryption or remote attestation to ensure the integrity and confidentiality of any stored data within the device.

I. INTRODUCTION

Many computer systems, especially within the growing IoT ecosystem, are publicly accessible but contain and process various types of sensitive data, e.g., personal data, access data, cryptographic key material, login data, data containing intellectual property, company-internal data or security-critical data. Still, this information is often not protected appropriately against physical attacks, such as invasive attacks, side channel attacks, and fault induction attacks, cf. [1], because integrated or upgraded protection measures are insufficient, technically not realizable, and/or too expensive. One of the principal reasons for this lies in insecure (key) storage solutions, which are required to protect the Critical Security Parameters (CSPs), such as encryption keys, signing keys, etc. Providing a defense against read-out attacks has been observed as a highly complex problem. Another problem, apart from secure key storage, is adversarial tampering which can lead to successful exploitation of the system.

Motivated by approaches from the research field of Wireless Physical-Layer Security (WPLS) and from Physical Unclonable Functions (PUFs), we present a novel approach for providing data security that tackles both the problems of secure key storage and tamper protection. Our method extends the idea of chip-level or PCB-level protection to a system-level Enclosure PUF, which is able to prove the integrity of larger and arbitrarily shaped structures such as computer systems and which connects the system’s state of integrity to a unique cryptographic key. The construction can be retrofit to typical existing computer casings as well as to new computer systems in a cost-efficient and easy way. Moreover, expensive battery-powered and real-time capable attack-detection circuits or data deletion circuits are not required.

We utilize key extraction mechanisms from the field of WPLS, which build upon the principle that a unique cryptographic key can be extracted from an electromagnetic (EM) transmission channel and, therefore, from the electromagnetic properties of the environment. The key can only be recovered if the integrity of the environment has not been violated and it can essentially be seen as a digital fingerprint of the state of the environment. As an example, the key can be used to prove the authenticity of the system, to establish secure communication with another party or to encrypt stored data within the device.

We term the underlying system Enclosure PUF.

The solution we introduce is envisioned to facilitate a FIPS140-2 Level 4 [2] certification of a computer system (or its dedicated environment), which is the highest non-military physical protection standard for hardware that is required for trustful operation within hostile environments. As a novel feature, the Enclosure PUF offers the possibility of a reinitialization of the protection mechanism which is especially advantageous for systems with frequent maintenance requirements. This means that the system can be reset again after every authorized destruction of the initial integrity and
can be reinitialized with secret key material that is protected under the physical key.

A. Contributions

In this paper, we present a method and a practical implementation of read-proof hardware that protects entire computer systems against physical attacks. The method is based on a protective physical unclonable structure and an EM measurable dedicated environment. Our contributions in this work are:

- We introduce the concept of Electromagnetic Enclosure PUFs and explain how these can be used to verify the authenticity, integrity, and/or physical condition of the protected system and how to embed secret data by using the properties of radio channels.
- We provide experimental data to show the feasibility of the system using off-the-shelf software defined radios in a controlled environment. Important points are the estimation of extractable secrecy (key quality), tamper-sensitivity, and the reliability of measurements.
- We discuss attack scenarios and explain the challenges an adversary would have to overcome in order to break the system as well as the challenges in applying our approach to a wide range of devices.

II. BACKGROUND

We begin with a brief overview of physical layer security, which is a new security paradigm that has been brought into the spotlight recently. We summarize important preliminaries of electromagnetic channels, which are a well known description of physical complexities that affect wireless signals traveling through them. Furthermore, we give a brief overview of PUFs and of conventional tamper-protection approaches.

A. Wireless Physical-Layer Security

The investigation in security through applied information theory using physics of electromagnetic properties of devices and its environment is called Wireless Physical-Layer Security (WPLS) [3]. In the past, WPLS was used to complement and improve the communication security of wireless networks by exploiting physical features of wireless channels. A channel can be measured and characterized by the changes a signal takes by traveling through it. Radio waves sent through a physical medium are usually affected by different channel distortions. In particular, the symmetry (channel reciprocity between two antennas), the diversity (complex spatial channel variation) and the inherent randomness (complex shape due to multipath propagation and different channel distortions) of the wireless medium can be utilized to establish a shared secret. The detailed trace of a channel can be virtually infinitely complex, but it mainly depends on the measurement procedure. We refer to literature of Rappaport [4], Goldsmith [5], and Jakes [6] for further details.

This approach is referred to as Channel Reciprocity based Key Extraction (CRKE) and is characterized by three parties A, B, and E which observe a Discrete Memoryless Source (DMS). The observations of A and B are assumed to contain mutual information, which is not or only partly shared with E. Entropy not shared with E is called the secret-key capacity of the DMS. Furthermore, it is assumed that the DMS is not predictable or malleable in a way that E can guess A’s and B’s observations.

In practice, the approach is based on the quasi-simultaneous measurement of the wireless channel by A and B. Afterwards, measurements are post-processed, quantized, and error corrected in order to remove noise and interferences. The resulting entropy is collected and utilized as a shared symmetric key.

If E’s distance to both legitimate nodes is large enough, her observation of the channel is uncorrelated with the observations of A and B and thus an attack is not possible. We refer to literature of Bloch [3] for further details.

B. Physical Unclonable Functions

A PUF performs a mapping of input values or challenges to output values or responses based on its random physical structure. The input-output characteristic is unique for each manufactured device and can therefore be used for identification or authentication.

An important class of PUFs are so called Weak PUFs that are used to derive cryptographic keys which can serve as a root of trust. The main challenges that have to be overcome are the unreliability and limited bit-entropy of the response, which require an error-correction and an entropy extraction step. This can be done by using fuzzy extractors [7]. Especially relevant in the context of this paper is the Coating PUF as introduced by Tuyls et al. [8]. This PUF aims at providing chip-level tamper resistance. For this, capacitance sensors are embedded onto the die of an integrated circuit. Above the sensors, a coating layer that has beneficial chemical properties, is opaque to light over a wide range of wavelengths, and features randomly distributed capacitance values over its surface is applied. The capacitance values can be read out and are transformed via post-processing to form PUF responses which attest the integrity of the integrated circuit and can be used to derive device-specific cryptographic keys.

The use of radio channel properties has been explored for many different security applications. DeJean and Kirovski [9] introduced a system called RF-DNA in which RF fingerprints of so called Certificates of Authenticity (COAs) are utilized. COAs are hardware tags and ideally have PUF properties such as uniqueness, uncloneability and response reproducibility. Their RF fingerprint is evaluated by a custom reader in the near-field which yields superior results in regard to the fingerprint quality compared to far-field measurements. DeJean and Kirovski give a detailed attack scenario in which an adversary has the goal of cloning a hardware tag. They argue that this is fundamentally hard because even the accurate simulation of the RF fingerprint of a given 3D model is computationally infeasible. Given that that the simulation is not possible, the actual manufacturing of a physical clone is supposed to be intractable as well. Lakafosis et al. [10] presented a follow-up.
work, in which the concept is developed further for practical application.

C. Tamper-Resistant Enclosure and Envelopes

Most approaches to tamper-protection are based on the following ideas:

Sensors, most commonly in the form of switches, are placed in the Environment Under Protection (EUP). These sensors are then connected to a zeroization mechanism that erases all volatile memory once an intrusion is detected (cf. [11]). However, such approaches can be broken by bypassing the switches and drilling through unprotected areas of the encasement. Wrapping the EUP in a protective mesh that detects any breach and also zeroizes the CSP is a widely used strategy. A signal is continuously sent through the mesh and it is verified that the response is as expected. This approach is widely used in a multitude of systems [12]–[14]. However, these meshes also require a constant power supply and often only protect small components (size of a PCI-express card) instead of offering a system wide protection envelope.

Both approaches require an integrated battery in order to provide interruption-free monitoring. Physical access can be denied by placing the system in a protective case whose integrity is assured by sensor readings. The design and manufacturing of such an encasing is a challenging and expensive task. Maintenance procedures such as switching batteries are not feasible when the protective case is irrevocably damaged by any opening attempt, leading to a limited life-time and higher costs. This has been addressed by Immler et al. [15] who introduce a protective envelope that unlike a traditional mesh cannot only be actively monitored but also provides a PUF response. The envelope consists of a grid of capacitors whose capacitance is the raw PUF response. Therefore, an attacker has to make sure that the derived key’s entropy is lost. It must not be guaranteed that a breach of the outer case alters the response material is performed. The detection of such a breach is a necessary but not sufficient condition for the security of the system. As the goal of the system is to derive a cryptographic key from the whole integrity measurement, it has to be possible to brute-force the key from a partially corrupted PUF response. Therefore, an attacker has to make sure that her manipulations are too small to be reflected in the PUF response. For scenario c) she could also try to repair the damage made to the sealing material.

In the attack scenarios a) and b) a breach of the sealing material is performed. The detection of such a breach is a necessary but not sufficient condition for the security of the system. As the goal of the system is to derive a cryptographic key from the whole integrity measurement, it has to be guaranteed that a breach of the outer case alters the response such that the derived key’s entropy is lost. It must not be possible to brute-force the key from a partially corrupted PUF response. Therefore, an attacker has to make sure that her manipulations are too small to be reflected in the PUF response. For scenario b) she could also try to repair the damage made to the sealing material.

Alternatively to the invasive attack scenarios a) and b), an attacker could also pursue the non-invasive scenario c) which aims at simulating the physical system. Firstly, this requires an accurate physical model of the system under attack. In order to acquire this in a non-invasive way, the attacker would have to resort to means such as X-ray imaging. Especially, the sealing material has to be scanned in detail, as the rest of the system could arguably be known by analysis of other devices. If the scanning of the system and sealing material is successfully done, the attacker is still faced with the problem of accurately simulating the EM wave propagation within the sealed device.

IV. PROTOTYPICAL IMPLEMENTATION

In order to support the concept of the Enclosure PUF, as described in the previous sections, we have build a test setup that allows us to examine key principles of the proposed system.
One part of the implementation consists of a measurement device that is able to perform channel measurements. The second part consists of an enclosure for which we opted for aluminum containers that allow a range of experiments.

A. WPLS-based Key Extractor

For extraction of physical complexities from the environment, we utilize common Wi-Fi hardware embedded in a single-board computer which estimates CSI values. For channel measurement, an orthogonal frequency-division multiplexing (OFDM)-based approach is used, which is known from the literature and has been multiple times applied and evaluated for WPLS research testbeds [16]–[18]. OFDM is a widely applied communication technology in practice, e.g., in LTE, WiMAX, and Wi-Fi systems.

With a 3x3 MIMO setup we are able to measure 9 spatial channels, as illustrated in Figure 2. Please note that both transmitter and receiver are embedded in the same device. By placing the antennas at a minimum distance of 0.4\(\lambda\) (2 cm for 6 GHz) from one another, independence between all channels can be achieved [19].

![Diagram of Channel Measurement Using 3x3 MIMO](image)

**Fig. 2**: Channel measurement using 3x3 MIMO.

The CSI of the corresponding channel is represented by a vector with the length of 128 elements or bins. Each frequency bin represents 1/128-th of the bandwidth (40 MHz/128 = 312.5 kHz) at the corresponding frequency band. We apply the channel measurements on 5.275 to 5.835 GHz, which is a license free radio band for industrial, scientific and medical (ISM) applications.

The IEEE 802.11n-conform OFDM standard uses, for a bandwidth of 40 MHz, 12 (band-edge) null subcarriers which are not suitable for channel measurement. A FFT with 128 bins is used where the first 6 bins, the center bin and the last 7 bins are nulled. Therefore, the meaningful part of the CSI per channel is represented by a complex vector of length 114.

In total, we measure 12 frequency channels over 9 spatial channels, results in a PUF response of a total of 12,312 frequency bins. In this work, we only use raw amplitude information of each bin.

B. Device Under Test

We chose aluminum containers from the food industry which offers a cheap and flexible solution for running different kinds of experiments. The containers have a size of 32cm x 25cm x 6cm and offer a complete enclosure of our measurement system. Due to the thinness of the aluminum, it is easy to dent the container. Therefore, no physical stress should be applied on the container during static measurements. Apart from microscopic differences, different instances of the container differ notably along the edges where the aluminum creases.

V. PUF Analysis Results

PUF constructions must fulfill several key requirements. PUF responses must be reproducible. This is important because PUF responses are essentially analog measurements and are subject to (electronic) noise and environmental factors such as temperature. Furthermore, responses must be unique for each device. In the context of the Enclosure PUF, it is also important that the PUF response is sensitive to physical manipulations.

A. Intra-Inter Distance Analysis

In order to analyze the reproducibility and uniqueness of PUF responses, one usually compares intra and inter distances. Intra distances are computed by applying a metric to repeated measurements of the same PUF instance. Conversely, inter distances are the distances between responses of different PUFs. Comparing the distribution of intra and inter distances directly gives an indication of how much between-device variation is captured by the response generation mechanism in relation to the amount of measurement noise. We ran an experiment with ten different aluminum containers, each equipped with their own single-board computer as the measurement equipment. This population of Enclosure PUFs was placed in a lab room with approximately constant temperature and without further disturbing influences. From each PUF we collected 200 responses over a period of 24 hours. Based on these results we computed an intra and an inter distribution. We use the Euclidean distance as the metric for all following results. For the intra distribution, we exhaustively computed the complete list of all combinations of pairs of measurements for each PUF. The maximum number of inter distances is much larger than than the number of intra distances. Therefore, we opted to randomly sample the inter distances, collecting as many samples for the inter distribution as for the intra distribution. The histograms of both sampled distributions is given in Figure 3a. It can be clearly seen that both distributions are separated. The intra distribution, however, features a tail towards the inter distribution. The reason for this can be seen in Figure 3a in which the intra distribution of two PUFs are shown individually. One of the shown PUFs apparently has a starkly different noise structure and a much larger variance in its intra distribution. In the complete population of ten PUFs, we noticed the outlying intra distances for two PUFs. Please note that these two PUFs do not dominate the inter distribution as the majority of inter distances is sampled from pairs of PUFs that have a low-variance intra distribution.

B. Enclosure Manipulation

As a next step, we examined the influence of a breach of the enclosure on the PUF response. To this end we used an
The long tail of the intra distribution is explained by two outlier PUFs. One of the outlier PUFs is shown in (b) together with a more typical PUF. Despite the increased measurement error, a clear separation between intra and inter distance is still given.

engraving laser to cut an increasingly larger hole into the aluminum container of one PUF instance. Due to the low thickness of the aluminum sheets, this cutting process requires only little effort. As a side-effect, it can be observed that the heat from the laser cutting leads physical stress and deformation around the hole. Therefore, we note that the manipulation is not localized to the hole itself but affects a larger area that is hard to quantify. The result of our experiment is shown in Figure 4. Before starting the laser cutting, we first collected 10 reference measurements which enable us to estimate the intra distance for this PUF instance and which are used as a reference to compare later measurements against. Then, we started cutting square holes in the middle of the container, starting with an edge length of 0.5mm and ending with a length of 10mm. After each cut, we collected 5 measurements. Each of these groups of measurements is compared against the set of reference measurements. It can be seen that the PUF response decorrelates with an increase of the hole size. This effect is compounded of several factors. Debris from cutting falls into the enclosure, an effect which could arguably be suppressed by an attacker. Apart from this, the hole leads to a larger influence to path components from outside the enclosure on the channel estimation, i.e., the surroundings of the enclosure become a more dominant part of the PUF response. Ideally, the PUF enclosure is perfectly shielded and acts as as barrier that separates the measured wireless channels from the outside. In our case, this is, due to the choice of aluminum container, only approximately the case. Nevertheless, the cut hole is assumed to weaken the shielding considerably. A third effect of the manipulation, is the previously mentioned deformation during the cutting process. In this experiment, we are not able to quantify the contribution of each single effect to the magnitude of deviation of the PUF response. However, it still gives an impression of the sensitivity of our prototypical implementation to manipulations. Furthermore, it is a basis for a host of further experiments that are geared towards more realistic attack scenarios and for the search for dedicated sealing material.

VI. CONCLUSION, OPEN QUESTIONS, AND FUTURE WORK

Upgrading tamper protection mechanisms from the chip-level to the system-level is expensive and often not applicable at all, due to costs or requirements such as maintenance. As a compromise between cost and benefit, readings from various sensors are typically used to detect intrusion and initiate the subsequent deletion of sensitive data. This requires constant monitoring and real-time self-destruction capabilities.

We introduce the concept of Electromagnetic Enclosure PUFs and show that they are suitable for protection of sensitive data without additional detection or data deleting circuits. Key material is extracted from the physical complexity of a dedicated environment using electromagnetic measurements. The key material is presumed to be sufficiently destroyed if unauthorized activities occur. Due to its intrinsic concept and offline ability it is suited for cost-effectively retrofitting unprotected computer systems.

We evaluate the repeatability and uniqueness of a prototypical Enclosure PUF implementation. For this, we employ a
measurement testbed, which is based on commodity hardware. This is enclosed by an aluminum container which acts as a protective boundary. We are able to show a proof-of-concept of the uniqueness by comparing intra and inter distances. Furthermore, we examine the tamper-sensitivity of our setup with laser-based manipulations of the enclosure.

Our experiments show the general applicability and set the stage for multiple further research questions that need to be answered. The choice of sealing material is a trade-off between durability and sensitivity to attacks. Based on our laser attacks, we suggest that a good sealing material should amplify the effect of a local breach to a larger area for easier detection. At the same time, the system must be able to withstand a range of regular environmental conditions. Changes, for example in temperature or pressure, and aging processes should not distort the PUF response greatly. Physical stress such as vibrations or rough treatment during transport should ideally keep the sealing intact. Connected with the choice of sealing material is the question of entropy estimation and fuzzy extractor parameter search. Empiric estimation of entropy poses an obstacle due to the large effort required for building a large sample of enclosures. A mathematical model that translates distributions of physical quantities in the sealing material to PUF measurements would be a useful tool to support entropy estimation. Related to the general problem of entropy estimation is the question of accurate physical attack simulation. Setting the amount of physical damage of the sealing in relation to thereby occurring loss of key material is a non-trivial problem. Individual segments of the PUF response do not directly map to distinct parts of the sealing, which is rather beneficial for the system but complicates model building. A comprehensive experimental setup is required that allows to study the effects of intrusions into the sealing by different means such as drills or lasers. Additionally to physical attacks, one also has to further look at the (im-)possibility of simulating PUF responses based on the examination of the physical structure of the PUF.

In this work, we focused on the Weak PUF setting. However, it would also be possible to add a challenge-generating mechanism to the system, for example, a set of motors with mounted mirrors. This extension of the system to the Strong PUF scenario would open new fields of application but would also require the study of new attack vectors, such as machine-learning modeling attacks.

REFERENCES