Future-Proof Access Denial Systems

Vincent Immler
Central Office for Information Technology in the Security Sector (ZITiS)
GERMANY

vincent+nato@immler.us

Keywords: Anti-Tamper, Tamper-Evident Physical Unclonable Functions, Access Denial System.

ABSTRACT

Manufacturing Integrated Circuits (ICs) is a complex task and highly globalized with many dependencies that cannot be changed easily. This makes it challenging to invent security primitives from the ground-up that protect against all known physical attacks at the same time. While silicon Physical Unclonable Functions (PUFs) were designated to fill that gap w.r.t. improved key storage, they largely failed to meet corresponding expectations. Therefore, systems requiring higher levels of security still require Access Denial Systems (ADSs), e.g., an envelope which completely encloses the device and that actively detects and responds to attempted intrusions, thereby ensuring physical security of multiple-chip embedded systems and preventing loss of Critical Program Information (CPI). For decades, these system-level physical boundaries were actively checked by battery-backed mechanisms. Unfortunately, their crude and low-power monitoring circuits typically rely on fragile knowledge, i.e., once the attacker gathers sufficient information it is possible to defeat the countermeasure. This contradicts open design principles as otherwise followed for cryptographic systems to allow for public scrutiny. In this position paper, we provide a brief assessment of both battery-backed enclosures and previous silicon PUFs. We then summarize current research and outline a way forward based on non-silicon tamper-evident PUFs. Additionally, we explain some of their conceptual benefits over previous solutions. Furthermore, we present a concept how to integrate this in a secure boot process. To encourage further research in this area, we sketch what is still needed to build a future-proof ADS that is capable of resisting attacks within the next two decades.

1.0 INTRODUCTION

A multitude of security certifications, such as FIPS 140-2 [1], Common Criteria (CC) [2], or PCI-PTS [3], demand a physical security boundary for higher certification levels to protect compliant systems against tampering. These boundaries aim at separating the secure and insecure domains of a system, thereby protecting the device against physical attacks, such as drilling, grinding, etching, or (micro-)probing. They can be made from covers, housings, envelopes, etc. and represent a layer in the overall set of countermeasures as part of a layered security approach. Hence, these boundaries are typically complemented by additional sensing circuitry to detect adversarial conditions that cannot be detected or avoided by the physical boundary alone.

In contrast to single-chip devices such as smartcards that can only be protected in silicon, these countermeasures are of particular importance for high-performance cryptographic modules and other applications requiring anti-tamper mechanisms on a Printed Circuit Board (PCB) level. Having such a physical security boundary represents a generic countermeasure that is designated to make a wide range of invasive, semi-invasive, and non-invasive follow-up attacks more difficult to perform, as they typically require unobstructed hardware access which is hindered by the boundary. Especially for devices that are not available on the free market, exploration and exploitation become a challenging task.

One of the formerly widespread Access Denial Systems (ADS) by GORE [4] was based on a cover or envelope with a mesh that encloses the Module Under Protection (MUP). Attempts to physically penetrate the mesh are very likely to destroy its tracks and result in open circuits, i.e., a condition that can be sensed easily by a continuous measurement from the inside. Upon detection of such an event, an alarm is triggered that causes the zeroization of Critical Security Parameters (CSPs), such as cryptographic keys. Hence, this is called a tamper-detection and response mechanism.

However, a battery is required for this continuous monitoring mechanism whenever the supplying carrier system is powered off. Additionally, the CSPs must be stored in a volatile Battery-Backed Random-Access-Memory (BBRAM) to enable instantaneous zeroization upon detection of a physical intruder. Zeroization is typically implemented by a crowbar circuit that rapidly discharges the BBRAM. Hence, this is a highly-critical circuit component that must not fail. Additionally, storing constant values in volatile memory makes them prone to radiation imprinting if not periodically refreshed with their bit complement. Unfortunately, the specifics of such countermeasures are typically not made public.

Moreover, since either cover or envelope are manufactured using specialized technology, there is a risk of single-source supplier problems and minimum order quantities, i.e., there is no free market in addition to trust issues. This approach also has significant practical drawbacks: adding a battery to the system increases bulk and weight, it negatively impacts the device's operating temperature range, prohibits prolonged storage, and increasing complexity of the shipping process as its detection mechanism must be armed and operational at the time. Unfortunately, once the battery is fully discharged, the CSPs are lost and physical integrity can no longer be guaranteed. Clearly, storing a cryptographic key in non-volatile memory is also not an option, as its contents can be extracted while the system is powered off.

Yet another issue is the lack of formal integration into the operating system and application domain, i.e., there is no inherent cryptographic binding that is destroyed when the physical boundary is being attacked, as there is no cryptographic property that could be verified from within the system. This is in contrast to the concept of trusted/measured boot which otherwise makes supply chain attacks more difficult to perform.

Alternatively to the battery-backed approach of key storage, Physical Unclonable Functions (PUFs) [5] could be used to store a key without battery-backed memory. Once the device is running, this security primitive is designed to derive a cryptographic key from the device's inherent manufacturing variations. As long as the device is powered off, extracting these parameters is assumed to be difficult. Unfortunately, most research on PUFs was geared towards minimalistic on-chip primitives in Integrated Circuits (ICs) which makes it impossible to use them as an aftermarket protection for other Commercial-Off-The-Shelf (COTS) components. Furthermore, these silicon PUFs are typically a tiny subcomponent in a chip, i.e., they cannot obstruct physical access to other parts of the chip. Even worse, they typically do not provide the property of tamper-evidence, i.e., their physical primitive was not designed to be affected by physical tampering, e.g., by decapsulation of the chip. Consequently, such PUFs neither can detect attacks that happened prior to power-on nor at runtime of the chip, e.g., attacks that extract values from the data bus of a System on Chip (SoC) by using probing needles and corresponding preparatory steps in advance.

To overcome these issues, it is apparent that more research needs to be done on tamper-evident PUFs that represent a physical boundary that is sensitive to tampering. Once tampered with, its physical properties and resulting measured quantities – otherwise needed to derive the designated key from the PUF – would have been irreversibly changed, thereby achieving an access denying feature as required to build an ADS. Please note that the values derived from this type of PUF-based boundary would primarily be used to detect physical attacks and when blended with on-chip secrets, which in turn could be the output of another PUF, would serve as key-encryption-key. In the following, we briefly iterate over related research, provide a critical assessment, and point out what is needed to obtain a more future-proof solution.

2.0 STATE OF THE ART IN ACCESS DENIAL SYSTEMS

This section very briefly presents background information on two different types of ADSs, namely battery-backed tamper-resistant enclosures and tamper-evident PUFs. As outlined here [6], an ADS is always a trade-off between producibility, usability, and security.

2.1 Battery-Backed Tamper-Respondent Enclosures

A very recent overview is presented in [7] and provides a summary on tamper-respondent enclosures including their pros and cons. Here, we would like to emphasize some aspects more clearly and add missing aspects. Most notably, these tamper-respondent enclosures are not stand-alone solutions and are typically complemented with other sensing circuitry, e.g., light and X-ray detectors to provide a layered approach to security. In addition, one aspect that is not included in the referenced paper is the rapid response of such battery-backed systems. For example, the security policy of the Utimaco HSM CryptoServer Gen2 [8], which is protected by a battery-backed enclosure, states a tamper-response and zeroization time of just 4 ms. Hence, when looking into solutions that aim at a similar security level, not only the physical (im-)possibility of an attack needs to be considered but also the response time of the detection mechanism.

While the craftsmanship put into these solutions is incredible, modern inspection instruments are able to resolve the obfuscated physical patterns of such enclosures, i.e., it can no longer be assumed that the attacker is facing an unknown physical structure. Since defeating tamper-respondent enclosures requires rework at the scale of PCB-like structures only – as opposed to defeating a complex evaluation inside an IC – it is difficult to foresee a new generation of battery-backed enclosures that would be able to keep up with advances on the attacker’s side. Instead, similar to assumptions regarding the computational infeasibility of contemporary cryptographic schemes, it would be preferred to state a minimum complexity in terms of bits for physical attacks.

2.2 Tamper-Evident Physical Unclonable Functions

Earliest PUF-like patents on the silicon-level included the idea of tamper-evidence (cf. the seminal work of [9] from 1999) but it needed to be rediscovered in academia by the authors of the Coating PUF [10] in 2006. However, due to the early stage of PUF research at the time – PUFs had been formally introduced in 2002 [11,12] – the Coating PUF had many shortcomings, e.g., no protection of the chip backside, a measurement principle prone to side-channel leakage, insufficient sensitivity of the key derivation process w.r.t. the physical tampering, no dual-check of the coating’s integrity, etc. Hence, while this provided practical evidence that such a solution could be made, it clearly would not have been able to withstand real-world attacks. A similar tamper-evident PUF for smartcards based on optical measurements was attempted in [13].

On the enclosure level, the earliest attempts are the optical waveguide PUF [14,15] and B-TREPID [16] including its follow-up papers [17,18]. Another concept [19] presented at the Chaos Communication Congress was unfortunately never published at a peer-reviewed conference, which makes it difficult to assess the quality of their claims.

This incredibly short list of publications for tamper-evident PUFs is in strong contrast to the many papers on silicon PUFs that lack the property of tamper-evidence. This, in addition to the purely mathematical concept of ‘weak’ and ‘strong’ PUFs as per [20] emphasizes the unfortunate mischaracterization of the PUF technology and its potential benefit for anti-tamper mechanisms, as the property of tamper-evidence was not included in these definitions. In addition, as opposed to some publications such as [20], a PUF cannot be assumed to be a black box that can only be accessed through its designed interface. Instead, any PUF can be directly attacked by physical means as proven, e.g., in [21,22,23]. Therefore, silicon PUFs without the property of tamper-evidence should generally be considered as insecure against physical attacks.

3.0 NEEDS FOR FUTURE-PROOF ACCESS DENIAL SYSTEMS

To obtain a future-proof ADS, it seems apparent that tamper-evident PUFs could be used. Ideally, this would result in a much better trade-off w.r.t. producibility, usability, and security. When assessing previous work [17], their overall architecture can be divided into the following domains: physical, measurement, statistical, and application. In the following, we briefly discuss some of the specifics of these domains.

3.1 Physical Domain

Until recently, we have primarily seen two competing design approaches: I) the physical boundary approach where the ADS is a mesh or otherwise tamper-evident material enclosing the system and II) a backscatter sensing approach where the enclosed volume is scanned by means of either light or electromagnetic waves. On a conceptual level, these fundamentally different choices have complementary properties. For example, while I) has the advantage of a well-defined physical boundary with specified geometry, II) has the disadvantage that due to the complex backscatter behavior, it is difficult to prove full coverage by the chosen measurement principle and uniformity of the sensitivity against attacks. In contrast, II) has the advantage of the ‘economies of scale’, as scaling a backscatter approach is deemed much easier compared to I) where the physical structure itself must be adapted while the size of the attacker’s drill diameter remains the same. Regarding environmental noise, these two distinct approaches are expected to behave differently, too. Of course, a hybrid approach may be feasible, too.

Another important design consideration is the measured quantity. First of all, it needs to take its surrounding into consideration as it is the case, e.g., for electrical or magnetic stray fields. Secondly, in [17] both the nominal and random components of a capacitive-PUF primitive were taken into consideration. However, in the referenced work, the problem is that the nominal component is dominant compared to the random variation. This is due to the chosen physical structure and the standardized manufacturing process. This disproportion leads to a concept that could be called “global” and “local” randomization of the physical quantity, e.g., in [17] sufficient global randomness of the measured quantity, as needed for a proper PUF behavior, was only possible since the nominal component was later canceled out by means of a differential measurement that allowed accumulating the minuscule local variation. While this automatically results in a strong error propagation effect upon destructive physical tampering – the nominal capacitance removed was orders of magnitude larger than the local variation – it cannot prevent attempted repairs so well, since the removed capacitance was mostly the non-random nominal component. This resulted in the requirement to measure the nominal component for further improved tamper detection capabilities. Furthermore, from a practical point of view, it appears beneficial for contact-based probing to keep the variation as small as possible, as this falsifies the measurement result more easily without a tailored measurement circuit.

Hence, for follow-up implementations of a mesh- or custom material-based tamper-evident PUF, this problem needs to be investigated more carefully, as a robust error-propagation effect is needed while still ensuring sufficient local damage to counteract attempted repairs. Hopefully, the concept of strong PUFs and more advanced measurement principles with greater inter-dependency could help. At this point though, it remains unclear how these somewhat contradicting requirements could be fulfilled at the same time without some kind of physical avalanche effect, such as a brittle component that cracks upon tampering, thereby causing more severe damage. Clearly, copper tracks as a result from a regular PCB manufacturing process do not provide such a feature.

For a future-proof ADS, yet another design challenge in the physical domain is the material composition being used. On the one hand, it needs to be a “smart but disorderly” material which represents itself as indistinguishable upon inspection in addition to being difficult to probe or tamper with and that behaves the same under varying environmental influence, e.g., having the same and relatively small z-thermal expansion coefficient. On the other hand, it should be easy to produce and follow some kind of systematic to prove its properties when scaled to different sizes and when subject to different types of attacks. Taking all of this into account on its own is already difficult enough. When factoring in future advances on the offensive side, such as a smaller drill diameter of 30 um instead of 300 um, it is quite challenging to select a suitable manufacturing technology that is expected to scale correspondingly.

3.2 Measurement Domain

Once a suitable physical material and structure is found, it is important to tailor the measurement circuit accordingly [24]. One of its aspect is the selection of the type of measurement, e.g., absolute, differential, or a “3-signal” measurement technique. In contrast to some of the existing works, we are of the opinion that a differential measurement primarily helps to extract local variation in the measured quantity, which may not be needed at all, depending on the specifics of the physical parameter being considered and the requirement to neglect certain parasitics that would otherwise invalidate the measurement result.

Furthermore, selection of the measurement principle should take into account the requirements of a compensated measurement, i.e., a type of self-balancing ad-hoc measurement that already ignores substantial amount of environmental noise without any additional helper data or reference structures inside the PUF. Note that circuit noise would still be present in the data and necessitate corresponding error-reduction and error-correction steps to ensure sufficient reliability of the system. In particular, these compensated measurements need to work without impractical characterization and testing of each individual device across the whole range of environmental parameters.

Another aspect of the measurement principle is the possibility to obtain a kind of layout randomization without the need to have physically different designs, as this is deemed too complex for real-world applications. This is achieved by means of suitable configuration of the measurement circuit, e.g., either by dynamically recombining spots of the enclosure as a kind of puzzle [6], or by leveraging non-linearities in the excitation parameters that would lead to unpredictable responses. Please note that while this shares similarity with the concept of a “Strong PUF”, it should be considered a concept on its own as the objective would not be to have an authentication-level strong entropy but instead sufficient entropy to obfuscate the layout or its physical parameters to make physical attacks improbable to succeed. To put this into perspective, for a practically secure layout randomization it may already be enough to have 10 bits of ‘layout randomization’ *in addition* to the extracted cryptographic key entropy which should be much higher.

To further add to the security of the system, having a dual approach to the measurement would be a prudent design principle that appears beneficial. For example, in [17], both the integrity of electrodes could be checked in addition to measuring their capacitance. Alternatively, measurement principles of a different nature could be leveraged to measure the same quantity but with different techniques, thereby making attacks more difficult to perform that would try to work around the specifics of one or the other measurement technique. Especially for tamper-evident PUFs, outperforming the rapid response time of battery-backed enclosures appears to be challenging, given the needed measurement resolution. Considering the dual-approach of measuring values, having a lower sensitivity mode could be a way forward.

Finally, any measurement principle and implemented circuit must be resistant to side-channel observations and against probing of the physical structure, i.e., the physical structure must be sufficiently tamper-evident to be considered as “read-proof” [25]. Hence, for a future-proof ADS, the measurement circuit would not only need to provide a self-balancing compensated measurement that allows neglecting the influence of environmental noise and fulfill other security criteria but also be resistant to attacks on itself.

3.3 Statistical Domain

In both [10] and [16,17], the resulting distribution from which entropy was extracted was a Gaussian distribution. Since [26,18] demonstrated that an equidistant quantization is beneficial to improve tamper-sensitivity, there is the problem that a Gaussian distribution only has one peak – hence, no matter how finegrained the measurement circuit and quantization are, the most probable values remain those closest to the peak of the Gaussian distribution. Therefore, in [17], a bimodal or multimodal distribution was suggested as a possible way forward. Here, the attacker faces a practical decision problem since all of the peaks would be designed to be equally probable. Of course, this is based on the rather strong assumption that an attacker would be able to tamper with the values in a meaningful way. Additionally, by allowing for a different shape of the distribution from which entropy is extracted, it is expected that other aspects such as statistical normalization and measurement compensation could be carried out in an improved manner such that it benefits tamper-sensitivity overall. Hence, it is necessary to develop a more advanced understanding of the most desired shape of distribution and how it affects the overall data processing. In addition, 'layout and parameter randomization' similar to a strong PUF and their statistical effects need to be investigated.

3.4 Application Domain

The strong advantage of battery-backed tamper-respondent enclosures is that their security mechanism is never powered off. Bootstrapping and establishing trust in the device can therefore be done once at the time of manufacturing the device in a trusted facility. Unfortunately, since devices protected by a tamper-evident PUF are powered-off and they are deployed in the field, the process of re-establishing trust in these device is much more complex.

In general, device software must not be trusted to make the decision of re-establishing trust in a device. Instead, software must be physically read from devices and compared with the expected and therefore trusted reference. Unfortunately, tamper protection systems impede this process, since legitimate access to a memory chip is denied the same way it is for a physical intruder. Hence, dumping the memory to compare its contents to a known reference is no longer possible. Even worse, any software interface offering the same functionality could have been compromised to behave as expected while still allowing for a backdoored access. Hence, a proper bootstrap concept is needed for constructing a cryptographically verifiable device state while taking into account different trust levels for the assembly/manufacturing factories.

Our attempt to partially solve this problem is based on the Device Identified Composition Engine (DICE) [27], more specifically, we construct a Compound Device Identifier (CDI) from the measurement of the first mutable code on the platform, the ROM stages of the system, and a Unique Device Secret (UDS). By following this approach, we obtain a software root of trust (the processor boot ROM) and a hardware root of trust (the PUF secret) that is combined to a system root of trust which must be used for verification instead of physical evaluation. With this boot architecture for the application domain, we could perform a full verification based on the TPM quote attestation type [28], and a limited verification based on [29]. Once the CDI is established, it can be extended to include additional software stages, e.g., from the TrustZone, Linux Kernel, or arbitrary software IP.

For factory initialization, we added a (split) manufacturing trapdoor function, i.e., a function that takes as input an unprotected device and the encrypted firmware package, containing the firmware itself and all requires secrets, and then outputs a protected device with all parts of the firmware package decrypted and stored on the device. After this process, it is no longer possible to access the device by means of low level interfaces that would otherwise allow to re-program or dump the firmware.

Especially for the scenario of tamper-protected devices, schemes are needed that would allow for an easy pen and paper verification, while still providing full assurance that the software/hardware inside is as expected. Hence, a future-proof ADS would allow for systematically controlling the levels of trust as part of the manufacturing process in addition to enabling an easy in the field verification procedure to re-establish trust in the device once it was left unattended.

4.0 CONCLUSION

Considering the previous work and the assessment provided in this paper, we identified several needs for future-proof access denial systems. This is particularly true for low to mid-volume products, e.g., in the range of up to 100 000 devices that would make the development of a security-hardened ASIC for a single product infeasible. Products with relatively small quantity and very-high security needs will continue to exist in the future and their need to be protected from physical tampering will be even more prevalent considering the rapid rise in unattended and/or unmanned systems, operating without user or operator intervention, e.g., Unmanned Arial Vehicles (UAVs) as part of swarming or other military applications.

REFERENCES

[1] National Institute of Standards and Technology (NIST), FIPS PUB 140-2: Security Requirements for Cryptographic Modules. NIST.

[2] The Common Criteria Recognition Agreement Members, “Common Criteria for Information Technology Security Evaluation.”

[3] Payment Card Industry Security Standards Council, Payment Card Industry PTS POI Modular Derived Test Requirements, v4.0. PCI.

[4] H. MacPherson, “Security enclosure manufacture,” patent US 5 539 379A.

[5] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial,” vol. 102, no. 8, pp. 1126–1141.

[6] V. C. Immler, “Higher-order alphabet physical unclonable functions,” Dissertation, Technische Universität München, München, 2019.

[7] J. Obermaier and V. Immler, “The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond,” pp. 1–8.

[8] UTIMACO, “UTIMACO CryptoServer Se-Series Gen2 Security Policy (compliant to FIPS 140-2 level 3).”

[9] O. Kömmerling and F. Kömmerling, “Anti tamper encapsulation for an integrated circuit,” patent US 7 005 733B2.

[10] P. Tuyls, G.-J. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters, “Read-Proof Hardware from Protective Coatings,” in Cryptographic Hardware and Embedded Systems - CHES 2006, ser. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, pp. 369–383.

[11] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, “Silicon Physical Random Functions,” in Proceedings of the 9th ACM Conference on Computer and Communications Security. ACM, pp. 148–160.

[12] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical One-Way Functions,” vol. 297, no. 5589, pp. 2026–2030.

[13] T. Esbach, W. Fumy, O. Kulikovska, D. Merli, D. Schuster, and F. Stumpf, “A New Security Architecture for Smartcards Utilizing PUFs,” in ISSE Conference.

[14] M. Vai, B. Nahill, J. Kramer, M. Geis, D. Utin, D. Whelihan, and R. Khazan, “Secure architecture for embedded systems,” in 2015 IEEE High Performance Extreme Computing Conference (HPEC), pp. 1–5.

[15] V. Immler, J. Obermaier, M. König, M. Hiller, and G. Sigl, “B-TREPID: Batteryless tamper- resistant envelope with a PUF and integrity detection,” in IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 49–56.

[16] V. Immler, J. Obermaier, M. König, M. Hiller, and G. Sigl, “B-TREPID: Batteryless tamper- resistant envelope with a PUF and integrity detection,” in IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 49–56.

[17] V. Immler, J. Obermaier, K. K. Ng, F. X. Ke, J. Lee, Y. P. Lim, W. K. Oh, K. H. Wee, and G. Sigl, “Secure Physical Enclosures from Covers with Tamper-Resistance,” pp. 51–96.

[18] V. Immler and K. Uppund, “New Insights to Key Derivation for Tamper Evident Physical Unclonable Functions.”

[19] C. Zenger, D. Holin, and L. Steinschulte, “Enclosure PUF – Tamper Proofing Commodity Hardware and other Applications,” in 35th Chaos Communication Congress (35c3).

[20] U. Rührmair, J. Sölter, and F. Sehnke, “On the Foundations of Physical Unclonable Functions,” vol. 2009, p. 277.

[21] S. Tajik, On the Physical Security of Physically Unclonable Functions, ser. T-Labs Series in Telecommunication Services. Springer International Publishing.

[22] L. Tebelmann, M. Pehl, and V. Immler, “Side-Channel Analysis of the TERO PUF,” in Constructive Side-Channel Analysis and Secure Design - 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3-5, 2019, pp. 43–60.

[23] D. Merli, D. Schuster, F. Stumpf, and G. Sigl, “Semi-invasive EM Attack on FPGA RO PUFs and Countermeasures,” in Proceedings of the Workshop on Embedded Systems Security, ser. WESS ’11. ACM, pp. 2:1–2:9.

[24] J. Obermaier, V. Immler, M. Hiller, and G. Sigl, “A Measurement System for Capacitive PUF-based Security Enclosures,” in Proceedings of the 55th Annual Design Automation Conference, ser. DAC ’18. ACM, pp. 64:1–64:6.

[25] R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali, and T. Rabin, “Algorithmic Tamper-Proof (ATP) Security: Theoretical Foundations for Security against Hardware Tampering,” in Theory of Cryptography Conference (TCC), M. Naor, Ed.

[26] V. Immler, M. Hennig, L. Kürzinger, and G. Sigl, “Practical Aspects of Quantization and Tamper-Sensitivity for Physically Obfuscated Keys,” in Proceedings of the Third Workshop on Cryptography and Security in Computing Systems, ser. CS2 ’16. ACM, pp. 13–18.

[27] Trusted Computing Group, “Trusted Platform Architecture Hardware Requirements for a Device Identifier Composition Engine.”

[28] ——, “TPM Library Specification.”

[29] M. Garrett. Anti Evil Maid 2 Turbo Edition. [Online]. Available: https://mjg59.dreamwidth.org/35742.html