Tech Report: Inerial HSMs Thwart Advanced Physical Attacks

Jan Sebastian Götte*† Björn Scheuermann*†
*Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG)
†Humboldt-Universität zu Berlin
goette@jaseg.de, scheuermann@informatik.hu-berlin.de

Abstract

In this tech report, we introduce a novel countermeasure against physical attacks: Inertial hardware security modules (iHSMs). Conventional systems have in common that they try to detect attacks by crafting sensors responding to increasingly minute manipulations of the monitored security boundary or volume. Our approach is novel in that we reduce the sensitivity requirement of security meshes and other sensors and increase the complexity of any manipulations by rotating the security mesh or sensor at high speed—thereby presenting a moving target to an attacker. Attempts to stop the rotation are easily monitored with commercial MEMS accelerometers and gyroscopes. Our approach leads to a HSM that can easily be built from off-the-shelf parts by any university electronics lab, yet offers a level of security that is comparable to commercial HSMs.

This tech report is the abridged version of our forthcoming paper.

I. Introduction

While information security technology has matured a great deal in the last half century, physical security has barely changed. Given the right skills, physical access to a computer still often means full compromise. The physical security of modern server hardware hinges on what lock you put on the room it is in.

Currently, servers and other computers are rarely physically secured as a whole. Servers sometimes have a simple lid switch and are put in locked "cages" inside guarded facilities. This usually provides a good compromise between physical security and ease of maintenance. To handle highly sensitive data in applications such as banking or public key infrastructure, general-purpose and low-security servers are augmented with dedicated, physically secure cryptographic co-processors such as trusted platform modules (TPMs) or hardware security modules (HSMs). Using a limited amount of trust in components such as the CPU, the larger system's security can then be reduced to that of its physically secured TPM [10, 4, 8].

Like smartcards, TPMs rely on a modern IC being hard to tamper with. Shrinking things to the nanoscopic level to secure them against tampering is a good engineering solution for some years to come. However, in essence this is a type of security by obscurity: Obscurity here referring to the rarity of the equipment necessary to attack modern ICs [1, 2].

HSMs rely on a fragile foil with much larger-scale conductive traces being hard to remove intact. While we are certain that there still are many insights to be gained in both technologies, we wish to introduce a novel approach to sidestep the manufacturing issues of both and provide radically better security against physical attacks. Our core observation is that any cheap but coarse HSM technology can be made much more difficult to attack by moving it very quickly.

For example, consider an HSM as it is used in online credit card payment processing. Its physical security level is set by the structure size of its security mesh. An attack on its mesh might involve fine drill bits, needles, wires, glue, solder and lasers [3]. Now consider the same HSM mounted on a large flywheel. In addition to its usual defenses the HSM is now equipped with an accelerometer that it uses to verify that it is spinning at high speed. How would an attacker approach this HSM? They would have to either slow down the rotation—which triggers the accelerometer—or they would have to attack the HSM in motion. The HSM literally becomes a moving target. At slow speeds, rotating the entire attack workbench might be possible but rotating frames of reference quickly become inhospitable to human life. Since non-contact electromagnetic or optical attacks are more limited in the first place and can be shielded, we have effectively forced the attacker to use an attack robot.

In Section II, we will give an overview of the state of the art in the physical security of HSMs. On this basis, in Section III we will elaborate the principles of our inertial HSM approach. We conclude this paper with a general evaluation of our concept in Section IV.

II. Related work

In this section, we will briefly explore the history of HSMs and the state of academic research on active tamper detection.

HSMs are an old technology tracing back decades in their electronic realization. Today's common approach of monitoring meandering electrical traces on a fragile foil that is wrapped around the HSM essentially transforms the security problem into the challenge to manufacture very fine electrical traces on a flexible foil [7, 6, 2]. There has been some research on monitoring the HSM's inside using e.g. electromagnetic radiation [15, 9] or ultrasound [16] but none of this research has found widespread adoption yet.

In [2], Anderson gives a comprehensive overview on physical security. An example they cite is the IBM 4758 HSM whose details are laid out in depth in [13]. This HSM is an example of an industry-standard construction. Although its turn of the century design is now a bit dated, the construction techniques of the physical security mechanisms have not evolved much in the last two decades. Besides auxiliary temperature and radiation sensors to guard against attacks on the built-in SRAM memory, the module's main security barrier uses the traditional construction of a flexible mesh wrapped around the module's core. In [13], the authors state the module monitors this mesh for short circuits, open circuits and conductivity. The fundamental approach to tamper detection and construction is similar to other commercial offerings [11, 3, 2, 7].

To the best of our knowledge, we are the the first to propose a mechanically moving HSM security barrier as part of a hardware security module. Most academic research concentrates on the issue of creating new, more sensitive security barriers for HSMs [6] while commercial vendors concentrate on means to certify and cheaply manufacture these security barriers [3]. Our concept instead focuses on the issue of taking any existing, cheap low-performance security barrier and transforming it into a marginally more expensive but high-performance one. The closest to a mechanical HSM that we were able to find during our research is an 1988 patent [12] that describes a mechanism to detect tampering along a communication cable by enclosing the cable inside a conduit filled with pressurized gas.

III. Inertial HSM construction and operation

Mechanical motion has been proposed as a means of making things harder to see with the human eye [5] and is routinely used in military applications to make things harder to hit [14] but we seem to be the first to use it in tamper detection. If we consider different ways of moving an HSM to make it harder to tamper with, we find that making it spin has several advantages.

First, the HSM has to move fairly fast. If any point of the HSM's tamper sensing mesh moves slow enough for a human to follow, it becomes a weak spot. E.g. in a linear pendulum motion, the pendulum becomes stationary at its apex. Second, a spinning HSM is compact compared to alternatives like an HSM on wheels. Finally, rotation leads to easily predictable accelerometer measurements. A beneficial side-effect of spinning the HSM is that if the axis of rotation is within the HSM itself, an attacker trying to follow the motion would have to rotate around the same axis. Their tangential linear velocity would rise linearly with the radius from the axis of rotation, which allows us to limit the approximate maximum size and mass of an attacker using an assumption on tolerable centrifugal force. In this consideration the axis of rotation is a weak spot, but that can be mitigated using multiple nested layers of protection.

In a rotating reference frame, centrifugal force is proportional to the square of angular velocity and proportional to distance from the axis of rotation. We can exploit this fact to create a sensor that detects any disturbance of the rotation by placing a linear accelerometer at some distance from the axis of rotation. During constant rotation, after subtracting gravity both acceleration tangential to the rotation and along the axis of rotation will be zero. Centrifugal acceleration will be constant.

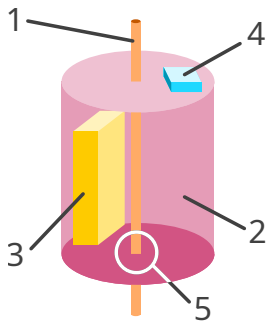

Figure 1: Concept of a simple spinning inertial HSM. 1 - Shaft. 2 - Security mesh. 3 - Payload. 4 - Accelerometer. 5 - Shaft penetrating security mesh.

Large centrifugal acceleration at high speeds poses the engineering challenge of preventing the whole thing from flying apart, but it also creates an obstacle to any attacker trying to manipulate the sensor. We do not need to move the entire contents of the HSM. It suffices if we move the tamper detection barrier around a stationary payload. This reduces the moment of inertia of the moving part and it means we can use cables for payload power and data. Even at moderate speeds above $500\,\mathrm{rpm}$, an attack would have to be carried out using a robot.

A. *Mechanical layout*

Thinking about the concrete construction of our mechanical HSM, the first challenge is mounting both mesh and payload on a single shaft. The simplest way we found to mount a stationary payload inside of a spinning security mesh is a hollow shaft. The payload can be mounted on a fixed rod threaded through this hollow shaft along with wires for power and data. The shaft is a weak spot of the system, but this weak spot can be alleviated through either careful construction or a second layer of rotating meshes with a different axis of rotation. Configurations that do not use a hollow-shaft motor are possible, but may require additional bearings to keep the stator from vibrating.

The next design choice we have to make is the physical structure of the security mesh. The spinning mesh must be designed to cover the entire surface of the payload, but compared to a traditional HSM it suffices if it sweeps over every part of the payload once per rotation. This means we can design longitudinal gaps into the mesh that allow outside air to flow through to the payload. In traditional boundary-sensing HSMs, cooling of the payload processor is a serious issue since any air duct or heat pipe would have to penetrate the HSM's security boundary. This problem can only be solved

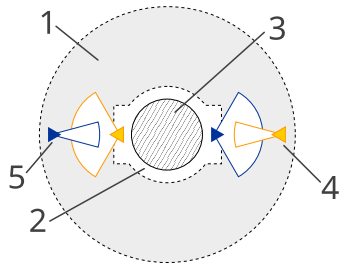

Figure 2: Example of a bidirectional IR communication link between rotor and stator, view along axis of rotation. 1 - Rotor base plate. 2 - Stator base plate. 3 - Motor. 4 - receiver PIN photodiode. 5 - transmitter IR LED.

with complex and costly siphon-style constructions, so in commercial systems heat conduction is used exclusively [7]. This limits the maximum power dissipation of the payload and thus its processing power. Our setup allows direct air cooling of regular heatsinks. This greatly increases the maximum possible power dissipation of the payload and unlocks much more powerful processing capabilities. In an evolution of our design, the spinning mesh could even be designed to *be* a cooling fan.

B. Spinning mesh power and data transmission

On the electrical side, the idea of a security mesh spinning at more than $500\,\mathrm{rpm}$ leaves us with a few implementation challenges. Since the spinning mesh must be monitored for breaks or short circuits continuously, we need both a power supply for the spinning monitoring circuit and a data link to the stator.

We think that a bright lamp shining at a rotating solar panel is a good starting point. In contrast to e.g. slip rings, this setup is mechanically durable at high speeds and it also provides reasonable output power. A battery may not provide a useful lifetime without power-optimization. Likewise, an energy harvesting setup may not provide enough current to supply peak demand.

Since the monitoring circuit uses little current, power transfer efficiency is not important. On the other hand, cost may be a concern in a production device. Here it may prove worthwhile to replace the solar cell setup with an extra winding on the rotor of the BLDC motor driving the spinning mesh. This motor is likely to be a custom part, so adding an extra winding is unlikely to increase cost significantly. More traditional inductive power transfer may also be an option if it can be integrated into the mechanical design.

Besides power, the data link between spinning mesh and payload is critical to the HSM's design. This link is used to transmit the occassional status report along with a low-latency alarm trigger ("heartbeat") signal from mesh to payload. A simple infrared optical link as shown in Figure 2 may be a good solution for this purpose.

IV. Conclusion

To conclude, in this tech report we introduced inertial hardware security modules (iHSMs), a novel concept for the construction of highly secure hardware security modules from inexpensive, commonly available parts. We elaborated the engineering considerations underlying a practical implementation of this concept.

Inertial HSMs offer a high level of security beyond what traditional techniques can offer. They allow the construction of devices secure against a wide range of practical attacks at prototype quantities and without specialized tools. We hope that this simple construction will stimulate academic research into secure hardware.

References

[1] Nils Albartus et al. "DANA Universal Dataflow Analysis for Gate-Level Netlist Reverse Engineering". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2020.4 (2020), pp. 309–336. DOI: 10.13154/tches.v2020.i4.309-336.

[2] Ross Anderson. *Security Engineering*. Sept. 16, 2020. ISBN: 978-1-119-64281-7.

[3] Saar Drimer, Steven J Murdoch, and Ross Anderson. "Thinking inside the box: system-level failures of tamper proofing". In: *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE. 2008, pp. 281–295.

[4] Jessie Frazelle. "Securing the Boot Process: The hardware root of trust". In: *ACM Queue* (Dec. 1, 2019). DOI: 10.1145/3380774.3382016.

[5] Lester Haines. *US outfit patents 'invisible' UAV: Stealth through persistence of vision*. Ed. by The Register. Sept. 25, 2006. URL: https://www.theregister.com/2006/09/25/phantom_sentinel/ (visited on 09/17/2020).

[6] Vincent Immler et al. "Secure Physical Enclosures from Covers with Tamper-Resistance". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019). ISSN: 2569-2925. DOI: 10.13154/tches.v2019.i1.51-96.

[7] Phil Isaacs et al. *Tamper proof, tamper evident encryption technology*. Tech. rep. Surface Mount Technology Association, 2013.

[8] Scott Johnson et al. "Titan: enabling a transparent silicon root of trust for Cloud". In: *Hot Chips: A Symposium on High Performance Chips*. 2018.

[9] Heinz Kreft and Wael Adi. "Cocoon-PUF, a novel mechatronic secure element technology". In: *2012 NASA/ESA Conference on Adaptive Hardware and Systems (AHS)* (2012). DOI: 10.1109/ahs.2012.6268655.

[10] Lily Hay Newman. *Apple's T2 Security Chip Has an Unfixable Flaw*. Wired Magazine. Oct. 6, 2020. URL: https://www.wired.com/story/apple-t2-chip-unfixable-flaw-jailbreak-mac/.

[11] Johannes Obermaier and Vincent Immler. "The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond". In: *Journal of Hardware and Systems Security* 2 (2018), pp. 289–296. ISSN: 2509-3428. DOI: 10.1007/s41635-018-0045-2.

[12] Mujib Rahman. “Optical fiber cable with tampering detecting means”. US Patent US4859024A. Mar. 10, 1988.

[13] Sean Smith and Steve Weingart. *Building a High-Performance, Programmable Secure Coprocessor*. Tech. rep. IBM T.J. Watson Research Center, Feb. 19, 1998.

[14] Daniel Terdiman. *Aboard America’s Doomsday command and control plane*. cnet.com. July 23, 2013. URL: https : / / www . cnet . com / news / aboard - americas - doomsday-command-and-control-plane.

[15] Johannes Tobisch, Christian Zenger, and Christof Paar. “Electromagnetic Enclosure PUF for Tamper Proofing Commodity Hardware and otherApplications”. In: *TRUDEVICE 2020: 9th Workshop on Trustworthy Manufacturing and Utilization of Secure Devices* (Mar. 13, 2020).

[16] Serge Vrijaldenhoven. “Acoustical Physical Uncloneable Functions”. MA thesis. Technische Universiteit Eindhoven, Oct. 1, 2004.

APPENDIX

A. Patents and licensing

During development, we performed several hours of research on prior art for the inertial HSM concept. Yet, we could not find any mentions of similar concepts either in academic literature or in patents. Thus, we are likely the inventors of this idea and we are fairly sure it is not covered by any patents or other restrictions at this point in time.

Since the concept is primarily attractive for small-scale production and since cheaper mass-production alternatives are already commercially available, we have decided against applying for a patent and we wish to make it available to the general public without any restrictions on its use. This paper itself is licensed CC-BY-SA (see below). As for the inertial HSM concept, we invite you to use it as you wish and to base your own work on our publications without any fees or commercial restrictions. Where possible, we ask you to cite this paper and attribute the inertial HSM concept to its authors.

This is version `v1.4-2-ga361f09-dirty` generated on January 14, 2021. Once the full paper has been published, this project’s git repository will be available at:

https://git.jaseg.de/rotohsm.git