

# Can't Touch This: Inertial HSMs Thwart Advanced Physical Attacks

Anonymous Submission

**Abstract.** In this paper, we introduce a novel countermeasure against physical attacks: Inertial hardware security modules (iHSMs). Conventional systems have in common that their security requires the crafting of fine sensor structures that respond to 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. We have built a proof of concept hardware prototype that demonstrates solutions to the concept's main engineering challenges. As part of this proof of concept, we have found that a system using a coarse security mesh made from commercial printed circuit boards and an automotive high g-force accelerometer already provides a useful level of security.

**Keywords:** hardware security · implementation · smart cards · electronic commerce

## 1 Introduction

While information security technology has matured a great deal in the last half century, physical security not kept up with the pace of the remainder of this industry. Given the right skills, physical access to a computer still often allows 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 [14, 6, 11]. 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].

In contrast to TPMs and Smartcards, HSMs rely on an active security barrier usually consisting of a fragile foil with conductive traces. These traces are much larger scale than a smart card IC's microscopic structures, and instead are designed to be very 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

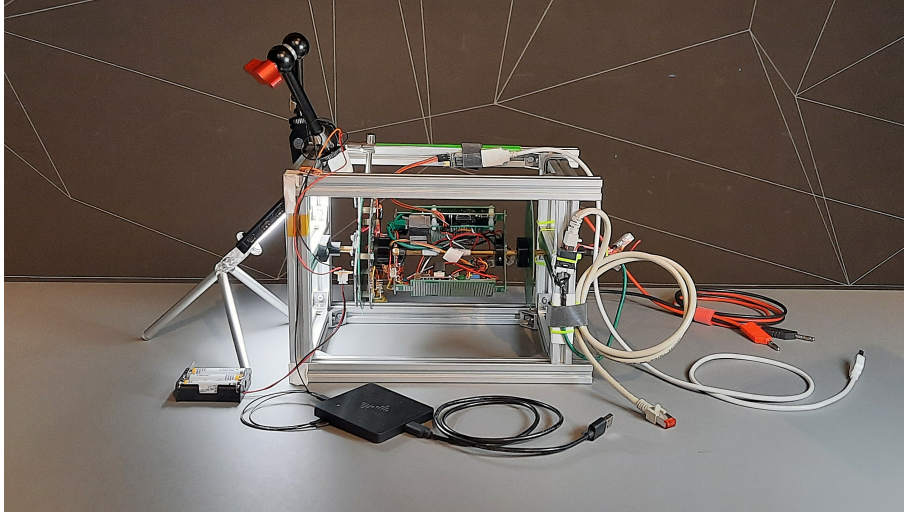


Figure 1: The prototype as we used it to test power transfer and bidirectional communication between stator and rotor. This picture shows the proof of concept prototype’s configuration that we used for accelerometer characterization (Section 6) without the vertical security mesh struts that connect the circular top and bottom outer meshes.

44 is that any cheap but coarse HSM technology can be made much more difficult to attack  
 45 by moving it very quickly.

46 For example, consider an HSM as it is used in online credit card payment processing.  
 47 Its physical security level is set by the structure size of its security mesh. An attack on its  
 48 mesh might involve fine drill bits, needles, wires, glue, solder and lasers [4]. Now consider  
 49 the same HSM mounted on a large flywheel. In addition to its usual defenses, this modified  
 50 HSM is now equipped with an accelerometer that it uses to verify that it is spinning at  
 51 high speed. How would an attacker approach this HSM? They would have to either slow  
 52 down the rotation—which triggers the accelerometer’s monitoring circuit—or they would  
 53 have to attack the HSM in motion. The HSM literally becomes a moving target. At slow  
 54 speeds, rotating the entire attack workbench might be possible—but rotating frames of  
 55 reference quickly become inhospitable to human life (see Section 4.1). Since non-contact  
 56 electromagnetic or optical attacks are more limited in the first place and can be shielded,  
 57 we have effectively forced the attacker to use an “attack robot”.

58 This paper contains the following contributions:

- 59 1. We present the *Inertial HSM* concept. Inertial HSMs enable cost effective, small  
 60 scale production of highly secure HSMs.
- 61 2. We discuss possible tamper sensors for inertial HSMs.
- 62 3. We explore the design space of our inertial HSM concept.
- 63 4. We present our work on a prototype inertial HSM (Figure 1).
- 64 5. We present an analysis on the viability of using commodity MEMS accelerometers  
 65 as braking sensors.

66 In Section 2, we will give an overview of the state of the art in HSM physical security.  
 67 On this basis, in Section 3 we will elaborate the principles of our Inertial HSM approach.  
 68 We will analyze its weaknesses in Section 4. Based on these results we have built a proof  
 69 of concept hardware prototype the design of which we will elaborate in Section 5. In

70 Section 6 we present our characterization of an automotive MEMS accelerometer IC as a  
71 rotation sensor in this proof of concept prototype. We conclude this paper with a general  
72 evaluation of our design in Section 7.

## 73 2 Related work

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

76 HSMs are an old technology that traces back decades in its electronic realization.  
77 Today's common approach of monitoring meandering electrical traces on a fragile foil that  
78 is wrapped around the HSM essentially transforms the security problem into the challenge  
79 to manufacture very fine electrical traces on a flexible foil [10, 8, 2]. There has been some  
80 research on monitoring the HSM's inside using e.g. electromagnetic radiation [21, 13] or  
81 ultrasound [23] but none of this research has found widespread adoption yet.

82 HSMs can be compared to physical seals [2]. Both are tamper evident devices. The  
83 difference is that a HSM continuously monitors itself whereas a physical seal only serves  
84 to record tampering and requires someone to examine it. This examination can be by eye  
85 in the field, but it can also be carried out in a laboratory using complex equipment. An  
86 HSM in principle has to have this examination equipment built-in.

87 Physical seals are used in a wide variety of applications, but the most interesting ones  
88 from a research point of view that are recorded in public literature are those used in  
89 monitoring of nuclear material under the International Atomic Energy Authority (IAEA).  
90 Most of these seals use the same approach that is used in Physically Unclonable Functions  
91 (PUFs), though their development predates that of PUFs by several decades. The seal is  
92 created in a way that intentionally causes large, random device to device variations. These  
93 variations are precisely recorded at deployment. At the end of the seal's lifetime, the seal  
94 is returned from the field to the lab and closely examined to check for any deviations from  
95 the seal's prior recorded state. The type of variation used in these seals includes random  
96 scratches in metal parts and random blobs of solder (IAEA metal cap seal), randomly cut  
97 optical fibers (COBRA seal), the uncontrollably random distribution of glitter particles  
98 in a polymer matrix (COBRA seal prototypes) as well as the precise three-dimensional  
99 surface structure of metal parts at microscopic scales (LMCV) [9].

100 The IAEA's equipment portfolio does include electronic seals such as the EOSS. These  
101 devices are intended for remote reading, similar to an HSM. They are constructed from  
102 two components: A cable that is surveilled for tampering, and a monitoring device. The  
103 monitoring device itself is in effect an HSM and uses a security mesh foil such as it is used  
104 in commercial HSMs.

105 In [2], Anderson gives a comprehensive overview on physical security. An example  
106 HSM that they cite is the IBM 4758 HSM whose details are laid out in depth in [19]. This  
107 HSM is an example of an industry-standard construction. Although its turn of the century  
108 design is now a bit dated, the construction techniques of the physical security mechanisms  
109 have not evolved much in the last two decades. Besides some auxiliary temperature and  
110 radiation sensors to guard against attacks on the built-in SRAM memory, the module's  
111 main security barrier uses the traditional construction of a flexible mesh foil wrapped  
112 around the module's core. In [19], the authors state that the module monitors this mesh  
113 for short circuits, open circuits and conductivity. The fundamental approach to tamper  
114 detection and construction is similar to other commercial offerings [16, 4, 2, 10].

115 Shifting our focus from industry use to the academic state of the art, in [8], Immler  
116 et al. describe an HSM based on precise capacitance measurements of a security mesh,  
117 creating a PUF from the mesh. In contrast to traditional meshes, the mesh they use  
118 consists of a large number of individual traces (more than 30 in their example). Their  
119 concept promises a very high degree of protection. The main disadvantages of their concept

120 are a limitation in covered area and component height, as well as the high cost of the  
121 advanced analog circuitry required for monitoring. A core component of their design is  
122 that they propose its use as a PUF to allow for protection even when powered off, similar  
123 to a smart card—but the design is not limited to this use.

124 In [21], Tobisch et al. describe a construction technique for a hardware security module  
125 that is based around commodity WiFi hardware inside a conductive enclosure. In their  
126 design, an RF transmitter transmits a reference signal into the RF cavity formed by the  
127 conductive enclosure. One or more receivers listen for the signal's reflections and use them  
128 to characterize the RF cavity w.r.t. phase and frequency response. Their fundamental  
129 assumption is that the RF behavior of the cavity is inscrutable from the outside, and that  
130 even a small disturbance anywhere within the volume of the cavity will cause a significant  
131 change in its RF response. A core component of the work of Tobisch et al. [21] is that  
132 they use commodity WiFi hardware to reduce the cost of the HSM's sensing circuitry.  
133 The resulting system is likely both much cheaper and capable of protecting a much larger  
134 security envelope than designs using finely patterned foil security meshes such as [8], at  
135 the cost of worse and less predictable security guarantees. Where [21] use electromagnetic  
136 radiation, Vrijaldenhoven in [23] uses ultrasound waves travelling on a surface acoustic  
137 wave (SAW) device to a similar end.

138 While Tobisch et al. [21] approach the sensing frontend cost as their primary opti-  
139 mization target, the prior work of Kreft and Adi [13] considers sensing quality. Their  
140 target is an HSM that envelopes a volume barely larger than a single chip. They theorize  
141 how an array of distributed RF transceivers can measure the physical properties of a  
142 potting compound that has been loaded with RF-reflective grains. In their concept, the  
143 RF response characterized by these transceivers is shaped by the precise three-dimensional  
144 distribution of RF-reflective grains within the potting compound.

145 To the best of our knowledge, we are the the first to propose a mechanically moving  
146 HSM security barrier as part of a hardware security module. Most academic research  
147 concentrates on the issue of creating new, more sensitive security barriers for HSMs [8]  
148 while commercial vendors concentrate on means to certify and cheaply manufacture these  
149 security barriers [4]. Our concept instead focuses on the issue of taking any existing, cheap  
150 low performance security barrier and transforming it into a marginally more expensive but  
151 high performance one. The closest to a mechanical HSM that we were able to find during  
152 our research is an 1988 patent [17] that describes a mechanism to detect tampering along  
153 a communication cable by enclosing the cable inside a conduit filled with pressurized gas.

### 154 3 Inertial HSM construction and operation

155 Mechanical motion has been proposed as a means of making things harder to see with  
156 the human eye [7] and is routinely used in military applications to make things harder to  
157 hit [20] but we seem to be the first to use it in tamper detection.

158 The core questions in the design of an inertial HSM are the following:

- 159 1. What **type of motion** to use, such as rotation, pendulum motion, or linear motion.
- 160 2. How to construct the **tamper detection sensor**.
- 161 3. How to **detect braking** of the IHSM's movement.
- 162 4. The **mechanical layout** of the system.

163 We will approach these questions one by one in the following subsections.

### 164 3.1 Inertial HSM motion

165 First, there are several ways how we can approach motion. Periodic, aperiodic and  
166 continuous motion could serve the purpose. There is also linear motion as well as rotation.  
167 We can also vary the degree of electronic control in this motion. The main constraints we  
168 have on the HSM's motion pattern are that it needs to be (almost) continuous so as to not  
169 expose any weak spots during instantaneous standstill of the HSM. Additionally, for space  
170 efficiency the HSM has to stay within a confined space. This means that linear motion  
171 would have to be periodic, like that of a pendulum. Such periodic linear motion will have  
172 to quickly reverse direction at its apex so the device is not stationary long enough for this  
173 to become a weak spot.

174 In contrast to linear motion, rotation is space efficient and can be continuous if the  
175 axis of rotation is inside the device. In case it has a fixed axis, rotation will expose a  
176 weak spot at the axis of rotation where the surface's tangential velocity is low. Faster  
177 rotation can lessen the security impact of this fact at the expense of power consumption  
178 and mechanical stress, but it can never eliminate it. This effect can be alleviated in two  
179 ways: Either by adding additional tamper protection at the axis, or by having the HSM  
180 perform a compound rotation that has no fixed axis.

181 Large centrifugal acceleration at high speeds poses the engineering challenge of pre-  
182 venting rapid unscheduled disassembly of the device, but it also creates an obstacle to  
183 any attacker trying to manipulate the device in what we call a *swivel chair attack* (see  
184 Section 4.1). An attacker trying to follow the motion would have to rotate around the  
185 same axis. By choosing a suitable rotation frequency we can prevent an attacker from  
186 following the devices motion since doing so would subject them to impractically large  
187 centrifugal forces. Essentially, this limits the approximate maximum size and mass of an  
188 attacker under the an assumption on tolerable centrifugal force.

189 In this paper we focus on rotating IHSMs for simplicity of construction. For our initial  
190 research, we focus on systems with a fixed axis of rotation due to their simple construction  
191 but we do wish to note the challenge of hardening the shaft against tampering that any  
192 production device would have to tackle.

### 193 3.2 Tamper detection mesh construction

194 Once we have decided how our IHSM's security barrier should move, what remains is the  
195 actual implementation of that security barrier. There are two movements that we have  
196 observed that are key to our work. On the one hand, there is the widespread industry use  
197 of delicate tamper sensing mesh membranes. The usage of such membranes in systems  
198 deployed in the field for a variety of use cases from low security payment processing devices  
199 to high security certificate management at a minimum tells us that a properly implemented  
200 mesh *can* provide a practical level of security. On the other hand, in contrast to this  
201 industry focus, academic research has largely focused on ways to fabricate enclosures that  
202 embed characteristics of a Physically Uncloneable Function. By using stochastic properties  
203 of the enclosure material to form a PUF, such academic designs effectively leverage signal  
204 processing techniques to improve the system's security level by a significant margin.

205 In our research, we focus on security meshes as our IHSM's tamper sensors. Most of  
206 the cost in commercial security mesh implementations lies in the advanced manufacturing  
207 techniques and special materials necessary to achieve a sensitive mesh at fine structure sizes.  
208 The foundation of an IHSM security is that by moving the mesh even a primitive, coarse  
209 mesh made e.g. from mesh traces on a PCB becomes very hard to attack in practice. This  
210 allows us to use a simple construction made up from low-cost components. Additionally,  
211 the use of a mesh allows us to only spin the mesh itself and its monitoring circuit and keep  
212 the payload inside the mesh stationary. Tamper sensing technologies that use the entire  
213 volume of the HSM such as RF-based systems do not allow for this degree of freedom in

214 their design: They would require the entire IHSM to spin, including its payload, which  
215 would entail costly and complex systems for data and power transfer from the outside to  
216 the payload.

### 217 3.3 Braking detection

218 The security mesh is a critical component in the IHSM's defense against physical attacks,  
219 but its monitoring is only one half of this defense. The other half consists of a reliable  
220 and sensitive braking detection system. This system must be able to quickly detect any  
221 slowdown of the IHSM's rotation. Ideally, a sufficiently sensitive sensor is able to measure  
222 any external force applied to the IHSM's rotor and should already trigger a response at  
223 the first signs of a manipulation attempt.

224 While the obvious choice to monitor rotation would be a tachometer such as a magnetic  
225 or optical sensor attached to the IHSM's shaft, this would be a poor choice for our purposes.  
226 Both optical and magnetic sensors are susceptible to contact-less interference from outside.  
227 A different option would be to use feedback from the motor driver electronics. When using  
228 a BLDC motor, the driver electronics precisely know the rotor's position at all times. The  
229 issue with this approach is that depending on construction, it might invite attacks at the  
230 mechanical interface between mesh and the motor's shaft. If an attacker can decouple  
231 the mesh from the motor e.g. by drilling, laser ablation or electrical discharge machining  
232 (EDM) on the motor's shaft, the motor could keep spinning at its nominal frequency while  
233 the mesh is already standing still.

234 Instead of a stator-side sensor like a magnetic tachometer or feedback from the BLDC  
235 controller, an accelerometer placed inside the spinning mesh monitoring circuit would  
236 be a good component to serve as an IHSM's tamper sensor. Modern, fully integrated  
237 MEMS accelerometers are very precise. By comparing acceleration measurements against  
238 a model of the device's mechanical motion, deviations can quickly be detected. This  
239 limits an attacker's ability to tamper with the device's motion. It may also allow remote  
240 monitoring of the device's mechanical components such as bearings: MEMS accelerometers  
241 are fast enough to capture vibrations, which can be used as an early warning sign of failing  
242 mechanical components [12, 18, 3, 5].

243 In a spinning IHSM, an accelerometer mounted at a known radius with its axis pointing  
244 radially will measure centrifugal acceleration. Centrifugal acceleration rises linearly with  
245 radius, and with the square of frequency:  $a = \omega^2 r$ . For a given target speed of rotation, the  
246 accelerometer's location has to be carefully chosen to maximize dynamic range. A key point  
247 here is that for rotation speeds between 500 and 1000 rpm, centrifugal acceleration already  
248 becomes very large at a radius of just a few cm. At 1000 rpm  $\approx 17$  Hz and at a 10 cm  
249 radius, acceleration already is above  $1000 \text{ m s}^{-1}$  or  $100g$ . While beneficial for security,  
250 this large acceleration leads to two practical constraints. First, off-axis performance of  
251 commercial accelerometers is usually in the order of 1% so this large acceleration will feed  
252 through into all accelerometer axes, even those that are tangential to the rotation. Second,  
253 we either have to place the accelerometer close to the axis or we are limited to a small  
254 selection of high- $g$  accelerometers mostly used in automotive applications.

255 To evaluate the feasibility of accelerometers as tamper sensors we can use a simple  
256 benchmark: Let us assume that an IHSM is spinning at 1000 rpm and that we wish to  
257 detect any attempt to brake it below 500 rpm. The difference in centrifugal acceleration  
258 that our accelerometer will need to detect then is a factor of  $\frac{\omega_2^2}{\omega_1^2} = 4$ . If we choose  
259 our accelerometer's location to maximize its dynamic range, any commercial MEMS  
260 accelerometer should suffice for this degree of accuracy even over long timespans. For  
261 rapid deceleration, commercial accelerometers will be much more sensitive as effects of  
262 long-term drift can be ignored. If we wish to also detect very slow deceleration, we have  
263 to take into account the accelerometer's drift characteristics.

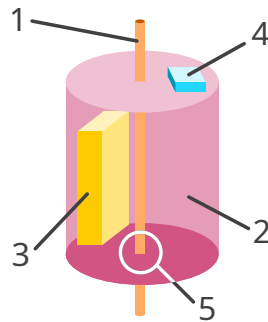


Figure 2: Concept of a simple spinning Inertial HSM. 1 - Shaft. 2 - Security mesh. 3 - Payload. 4 - Accelerometer. 5 - Shaft penetrating security mesh.

264 In Section 6 below, we conduct an empirical evaluation of a commercial automotive  
265 high- $g$  MEMS accelerometer for braking detection in our prototype IHSM.

### 266 3.4 Mechanical layout

267 With our IHSM's components taken care of, what remains to be decided is how to put  
268 together these individual components into a complete device. A basic spinning HSM might  
269 look as shown in Figure 2. Visible are the axis of rotation, an accelerometer on the rotating  
270 part that is used to detect braking, the protected payload and the area covered by the  
271 rotating tamper detection mesh. A key observation is that we only have to move the  
272 tamper protection mesh, not the entire contents of the HSM. The HSM's payload and  
273 with it most of the HSM's mass can be stationary. This reduces the moment of inertia  
274 of the moving part. This basic schema accepts a weak spot at the point where the shaft  
275 penetrates the spinning mesh. This trade-off makes for a simple mechanical construction  
276 and allows power and data connections to the stationary payload through a hollow shaft.

277 The spinning mesh must be designed to cover the entire surface of the payload, but it  
278 suffices if it sweeps over every part of the payload once per rotation. This means we can  
279 design longitudinal gaps into the mesh that allow outside air to flow through to the payload.  
280 In traditional boundary-sensing HSMs, cooling of the payload processor is a serious issue  
281 since any air duct or heat pipe would have to penetrate the HSM's security boundary.  
282 This problem can only be solved with complex and costly siphon-style constructions, so in  
283 commercial systems heat conduction is used exclusively [10]. This limits the maximum  
284 power dissipation of the payload and thus its processing power. Using longitudinal gaps  
285 in the mesh, our setup allows direct air cooling of regular heatsinks. This unlocks much  
286 more powerful processing capabilities that greatly increase the maximum possible power  
287 dissipation of the payload. In an evolution of our design, the spinning mesh could even be  
288 designed to *be* a cooling fan.

## 289 4 Attacks

290 After outlining the basic mechanical design of an inertial HSM above, in this section we  
291 will detail possible ways to attack it. At the core of an IHSM's defenses is the same security  
292 mesh or other technology as it is used in traditional HSMs. This means that in the end  
293 an attacker will have to perform the same steps they would have to perform to attack a  
294 traditional HSM. However, they will either need to perform these attack steps with a tool  
295 that follows the HSM's rotation at high speed or they will first need to defeat the braking

296 sensor. Attacking the IHSM in motion may require specialized mechanical tools, CNC  
297 actuators or even a contactless attack using a laser, plasma jet or water jet.

#### 298 4.1 The Swivel Chair Attack

299 First we will consider the most basic of all attacks: a human attacker holding a soldering  
300 iron trying to rotate herself along with the mesh using a very fast swivel chair. Let  
301 us pessimistically assume that this co-rotating attacker has their center of mass on the  
302 axis of rotation. The attacker's body is likely on the order of 200 mm wide along its  
303 shortest axis, resulting in a minimum radius from axis of rotation to surface of about  
304 100 mm. Wikipedia lists horizontal g forces in the order of 20 g as the upper end of the  
305 range tolerable by humans for a duration of seconds or above. We thus set our target  
306 acceleration to  $100g \approx 1000 \text{ m/s}^2$ , a safety factor of 5 past that range. Centrifugal  
307 acceleration is  $a = \omega^2 r$ . In our example this results in a minimum angular velocity of  
308  $f_{\min} = \frac{1}{2\pi} \sqrt{\frac{a}{r}} = \frac{1}{2\pi} \sqrt{\frac{1000 \text{ m/s}^2}{100 \text{ mm}}} \approx 16 \text{ Hz} \approx 1000 \text{ rpm}$ . From this we can conclude that even  
309 at moderate speeds of 1000 rpm and above, a manual attack is no longer possible and any  
310 attack would have to be carried out using some kind of mechanical tool.

#### 311 4.2 Mechanical weak spots

312 The tamper defense of an IHSM rests on the security mesh moving too fast to tamper.  
313 Depending on the type of motion used, the mesh's speed may vary by location and over  
314 time. Our example configuration of a rotating mesh can keep moving continuously, so  
315 it does not have any time-dependent weak spots. It does, however, have a weak spot  
316 along its axis of rotation, at the point where the shaft penetrates the mesh. The mesh's  
317 tangential velocity decreases close to the shaft, and the shaft itself may allow an attacker  
318 to insert tools such as probes into the device through the opening it creates. This issue is  
319 related to the issue conventional HSMs also face with their power and data connections. In  
320 conventional HSMs, power and data are routed into the enclosure through the PCB or flat  
321 flex cables sandwiched in between security mesh foil layers [19]. In traditional HSMs this  
322 interface rarely is a mechanical weak spot since they use a thin mesh substrate and create  
323 a meandering path by folding the interconnect substrate/security mesh layers several times.  
324 In inertial HSMs, careful engineering is necessary to achieve the same effect. Figure 3  
325 shows variations of the shaft interface with increasing complexity.

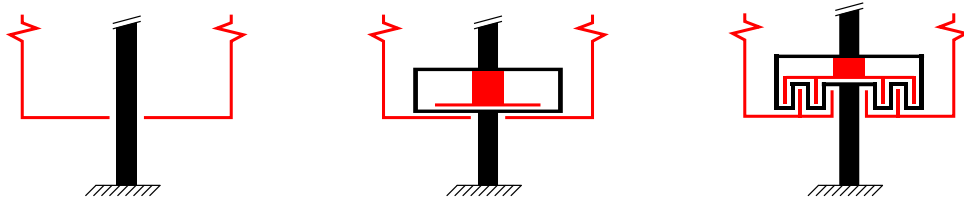
#### 326 4.3 Attacking the mesh in motion

327 To disable the mesh itself, an attacker can choose two paths. One is to attack the  
328 mesh itself, for example by bridging its traces. The other option is to tamper with the  
329 monitoring circuit to prevent a damaged mesh from triggering an alarm [15]. Attacks in  
330 both locations are electronic attacks, i.e. they require electrical contact to parts of the  
331 circuit. Traditionally, this contact is made by soldering a wire or by placing a probe such  
332 as a thin needle. We consider this type of attack hard to perform on an object spinning at  
333 high speed. Possible remaining attack avenues may be to rotate an attack tool in sync  
334 with the mesh, or to use a laser or ion beam fired at the mesh to cut traces or carbonize  
335 parts of the substrate to create electrical connections. Encapsulating the mesh in a potting  
336 compound and shielding it with a metal enclosure as is common in traditional HSMs will  
337 significantly increase the complexity of such attacks.

#### 338 4.4 Attacks on the rotation sensor

339 Instead of attacking the mesh in motion, an attacker may also try to first stop the rotor.  
340 To succeed, they would need to falsify the rotor's MEMS accelerometer measurements. We





(a) Cross-sectional view of the basic configuration with no special protection of the shaft. Red: moving mesh – Black: stationary part.

(b) An internal, independently rotating disc greatly decreases the space available to attackers at the expense of another moving part and a second moving monitoring circuit.

(c) A second moving tamper detection mesh also enables more complex topographies.

Figure 3: Mechanical countermeasures to attacks through or close to the shaft of a fixed-axis rotating IHSM.

341 can disregard electronic attacks on the sensor or the monitoring microcontroller because  
 342 they would be no easier than attacking the mesh traces. What remains would be physical  
 343 attacks of the accelerometer’s sensing mechanism. MEMS accelerometers usually use  
 344 a cantilever design in which a proof mass moves a cantilever whose precise position is  
 345 measured electronically. A topic of recent academic interest have been acoustic attacks  
 346 tampering with these mechanics [22], but such attacks do not yield sufficient control to  
 347 precisely falsify sensor readings. A possible more invasive attack may be to first decapsulate  
 348 the sensor MEMS using laser ablation synchronized with the device’s rotation. Then, a  
 349 fast-setting glue such as a cyanoacrylate could be deposited on the MEMS, locking the  
 350 mechanism in place. This type of attack can be mitigated by mounting the accelerometer  
 351 in a shielded location inside the security envelope and by varying the rate of rotation over  
 352 time.

#### 353 4.5 Attacks on the alarm circuit

354 Besides trying to deactivate the tamper detection mesh, an electronic attack could also  
 355 target the alarm circuitry inside the stationary payload, or the communication link between  
 356 rotor and payload. The link can be secured using a cryptographically secured protocol  
 357 like one would use for wireless radio links along with a high-frequency heartbeat message.  
 358 The alarm circuitry has to be designed such that it is entirely contained within the HSM’s  
 359 security envelope. Like in conventional HSMs, it has to be built to either tolerate or detect  
 360 environmental attacks using sensors for temperature, ionizing radiation, laser radiation,  
 361 supply voltage variations, ultrasound or other vibration and gases or liquids. If a wireless  
 362 link is used between the IHSM’s rotor and stator, this link must be cryptographically  
 363 secured. To prevent replay attacks link latency must continuously be measured, so this  
 364 link must be bidirectional.

#### 365 4.6 Fast and violent attacks

366 A variation of the above attacks on the alarm circuitry is to simply destroy the part of  
 367 the HSM that erases data in response to tampering before it can perform its job using a  
 368 tool such as a large hammer or a gun. To mitigate this type of attack, the HSM must be  
 369 engineered to be either tough or brittle: Tough enough that the tamper response circuitry  
 370 will reliably withstand any attack for long enough to carry out its function or brittle in a

371 way that during any attack, the payload is reliably destroyed before the tamper response  
372 circuitry.

## 373 **5 Proof of Concept Prototype implementation**

374 As we elaborated above, the mechanical component of an IHSM significantly increases  
375 the complexity of any attack even when implemented using only common, off-the-shelf  
376 parts. In view of this amplification of design security we have decided to validate our  
377 theoretical studies by implementing a proof of concept prototype IHSM (Figure 1). The  
378 main engineering challenges we set out to solve in this proof of concept prototype were:

- 379 1. A mechanical design suitable for rapid prototyping that can withstand at least  
380 500 rpm.
- 381 2. The automatic generation of security mesh PCB layouts for quick adaption to new  
382 form factors.
- 383 3. Non-contact power transmission from stator to rotor.
- 384 4. Non-contact bidirectional data communication between stator and rotor.

385 We will outline our findings on these challenges one by one in the following paragraphs.

### 386 **5.1 Mechanical design**

387 We sized our proof of concept prototype to have sufficient payload space for up to two  
388 full-size Raspberry Pi boards to approximate a traditional HSM's processing capabilities.  
389 We use printed circuit boards as the main structural material for the rotating part, and  
390 2020 aluminium extrusion for its mounting frame. Figure 4 shows the rotor's mechanical  
391 PCB designs. The design uses a 6 mm brass tube as its shaft, which is already sufficiently  
392 narrow to pose a challenge to an attacker. The rotor is driven by a small hobby quadcopter  
393 motor. Our prototype incorporates a functional PCB security mesh. As we observed  
394 previously, this mesh only needs to cover every part of the system once per revolution, so  
395 we designed the longitudinal PCBs as narrow strips to save weight.

### 396 **5.2 PCB security mesh generation**

397 Our proof-of-concept security mesh covers a total of five interlocking mesh PCBs (Figure 5b).  
398 A sixth PCB contains the monitoring circuit and connects to these mesh PCBs. To speed  
399 up design iterations, we automated the generation of this security mesh through a plugin  
400 for the KiCAD EDA suite<sup>1</sup>. Figure 5a visualizes the mesh generation process. First,  
401 the target area is overlaid with a grid. Then, the algorithm produces a randomized tree  
402 covering the grid. Finally, individual mesh traces are traced according to a depth-first  
403 search through this tree. We consider the quality of the plugin's output sufficient for  
404 practical applications. Together with FreeCAD's KiCAD StepUp plugin, this results in an  
405 efficient toolchain from mechanical CAD design to production-ready PCB files.

### 406 **5.3 Power transmission from stator to rotor**

407 The spinning mesh has its own autonomous monitoring circuit. This spinning monitoring  
408 circuit needs both power and data connectivity to the stator. To design the power link, we  
409 first need to estimate the monitoring circuit's power consumption. We base our calculation

<sup>1</sup> [Author information removed for double-blind peer review]

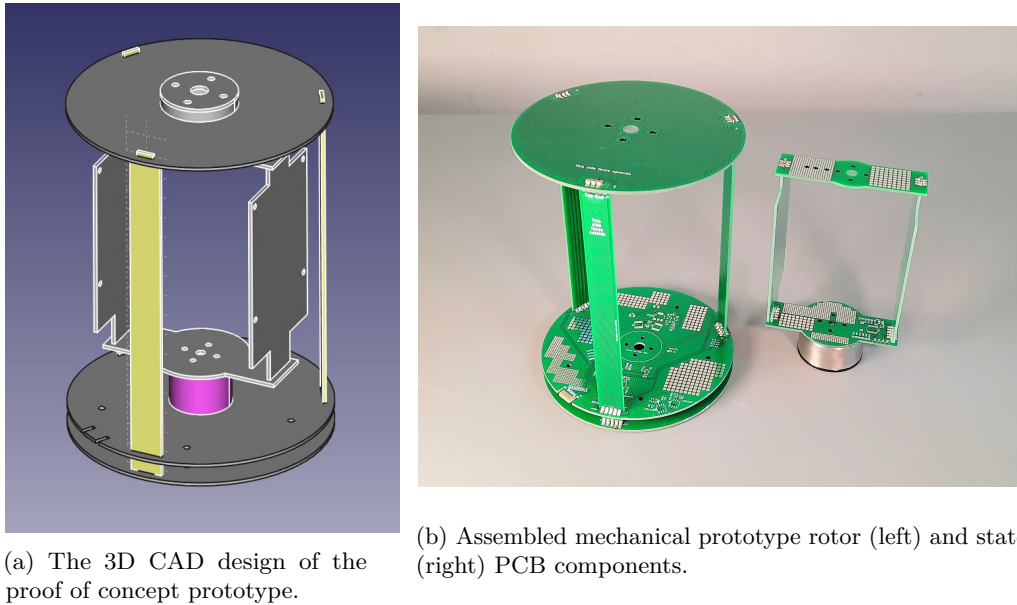
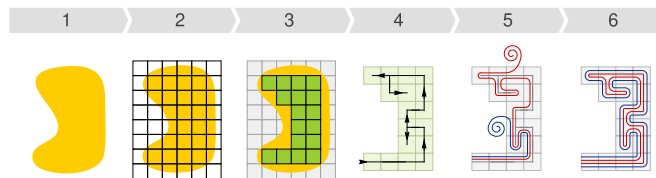
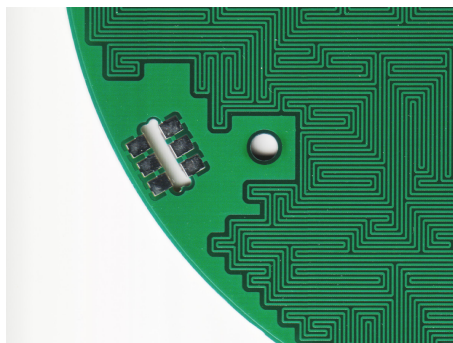


Figure 4: Our proof of concept prototype IHSM's PCB security mesh design



(a) Overview of the automatic security mesh generation process. 1 - Example target area. 2 - Grid overlay. 3 - Grid cells outside of the target area are removed. 4 - A random tree covering the remaining cells is generated. 5 - The mesh traces are traced along a depth-first walk of the tree. 6 - Result.



(b) Detail of a PCB produced with a generated mesh.

Figure 5: Our automatic security mesh generation process

410 on the (conservative) assumption that the spinning mesh sensor should send its tamper  
 411 status to the static monitoring circuit at least once every  $T_{tx} = 10$  ms. At 100 kBd, a  
 412 transmission of a one-byte message in standard UART framing would take 100  $\mu$ s and yield  
 413 an 1 % duty cycle. If we assume an optical or RF transmitter that requires 10 mA of active  
 414 current, this yields an average operating current of 100  $\mu$ A. Reserving another 100  $\mu$ A for  
 415 the monitoring circuit itself we arrive at an energy consumption of 1.7 A h per year.

416 This annual energy consumption is close to the capacity of a single CR123A lithium  
 417 primary cell. Thus, by either using several such cells or by optimizing power consumption  
 418 several years of battery life could easily be reached. In our proof of concept prototype we  
 419 decided against using a battery to reduce rotor mass and balancing issues.

420 We also decided against mechanically complex solutions such as slip rings or elec-  
 421 tronically complex ones such as inductive power transfer. Instead, we chose a simple  
 422 setup consisting of a stationary lamp pointing at several solar cells on the rotor. At the  
 423 monitoring circuit's low power consumption power transfer efficiency is irrelevant, so this  
 424 solution is practical. Our system uses six series-connected solar cells mounted on the end  
 425 of the cylindrical rotor that are fed into a large 33  $\mu$ F ceramic buffer capacitor through a  
 426 Schottky diode. This solution provides around 3.0 V at several tens of mA to the payload  
 427 when illuminated using either a 60 W incandescent light bulb or a flicker-free LED studio  
 428 light of similar brightness<sup>2</sup>.

## 429 5.4 Data transmission between stator and rotor

430 Besides power transfer from stator to rotor, we need a reliable, bidirectional data link  
 431 to transmit mesh status and a low-latency heartbeat signal. We chose to transport an  
 432 115 kBd UART signal through a simple IR link for a quick and robust solution. The link's  
 433 transmitter directly drives a standard narrow viewing angle IR led through a transistor.  
 434 The receiver has an IR PIN photodiode reverse-biased at  $\frac{1}{2}V_{CC}$  feeding into an MCP6494  
 435 general purpose opamp configured as an 100 k $\Omega$  transimpedance amplifier. As shown in  
 436 Figure 6b, the output of this TIA is amplified one more time before being squared up  
 437 by a comparator. Our design trades off stator-side power consumption for a reduction in  
 438 rotor-side power consumption by using a narrow-angle IR led and photodiode on the rotor,  
 439 and wide-angle components at a higher LED current on the stator. Figure 6a shows the  
 440 physical arrangement of both links. The links face opposite one another and are shielded  
 441 from one another by the motor's body in the center of the PCB.

## 442 5.5 Evaluation

443 The proof-of-concept hardware worked as intended. Both rotating power and data links  
 444 performed well. As we expected, the mechanical design vibrated at higher speeds but  
 445 despite these unintended vibrations we were able reach speeds in excess of 1000 rpm by  
 446 clamping the device to the workbench. Even at high speeds, both the power link and the  
 447 data links continued to function without issue.

## 448 6 Using MEMS accelerometers for braking detection

449 Using the proof of concept prototype from the previous section, we performed an evaluation  
 450 of an AIS1120 commercial automotive MEMS accelerometer as a braking sensor. The  
 451 device is mounted inside our prototype at a radius of 55 mm from the axis of rotation to

---

<sup>2</sup>LED lights intended for room lighting exhibit significant flicker that can cause the monitoring circuit to reset. Incandescent lighting requires some care in shielding the data link from the light bulb's considerable infrared output.

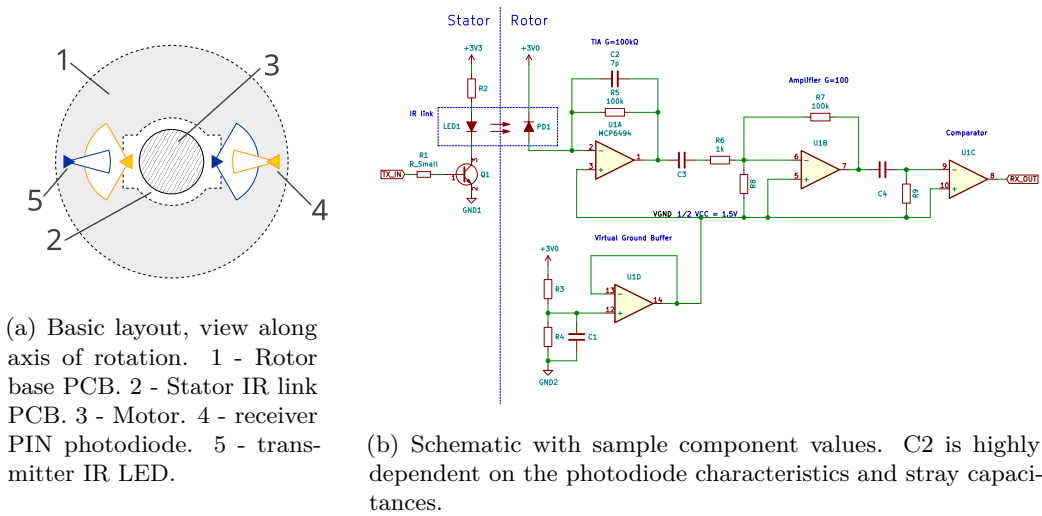


Figure 6: IR data link implementation

452 the center of the device’s package. The AIS1120 provides a measurement range of  $\pm 120 g$ .  
 453 At its 14-bit resolution, one LSB corresponds to 15 mg.

454 Our prototype IHSM uses a motor controller intended for use in RC quadcopters. In  
 455 our experimental setup, we manually control this motor controller through an RC servo  
 456 tester. In our experiments we externally measured the device’s speed of rotation using a  
 457 magnet fixed to the rotor and a reed switch held close. The reed switch output is digitized  
 458 using an USB logic analyzer at a sample rate of 100 MHz. We calculate rotation frequency  
 459 as a 1 s running average over debounced interval lengths of this captured signal<sup>3</sup>.

460 The accelerometer is controlled from the STM32 microcontroller on the rotor of our  
 461 IHSM prototype platform. Timed by an external quartz, the microcontroller samples  
 462 accelerometer readings at 10 Hz. Readings are accumulated in a small memory buffer,  
 463 which is continuously transmitted out through the prototype platform’s infrared link. Data  
 464 is packetized with a sequence number indicating the buffer’s position in the data stream  
 465 and a CRC-32 checksum for error detection. On the host, a Python script stores all packets  
 466 received with a valid checksum in an SQLite database.

467 Data analysis is done separately from data capture. An analysis IPython notebook  
 468 reads captured packets and reassembles the continuous sample stream based on the packets’  
 469 sequence numbers. The low 10 Hz sample rate and high 115 kBd transmission speed lead  
 470 to a large degree of redundancy with gaps in the data stream being rare. This allowed us  
 471 to avoid writing retransmission logic or data interpolation.

472 Figure 8a shows an entire run of the experiment. During this run, we started with the  
 473 rotor at standstill, then manually increased its speed of rotation in steps. Areas shaded gray  
 474 are intervals where we manually adjust the rotors speed. The unshaded areas in between  
 475 are intervals when the rotor speed is steady. Figure 8b shows a magnified view of these  
 476 periods of steady rotor speed. In both graphs, orange lines indicate centrifugal acceleration  
 477 as calculated from rotor speed measurements. Visually, we can see that measurements  
 478 and theory closely match. Our frequency measurements are accurate and the main source  
 479 of error are the accelerometer’s intrinsic errors as well as error in its placement due to  
 480 construction tolerances.

481 The accelerometer’s primary intrinsic errors are offset error and scale error. Offset

<sup>3</sup>A regular frequency counter or commercial tachometer would have been easier, but neither was available in our limited COVID-19 home office lab.

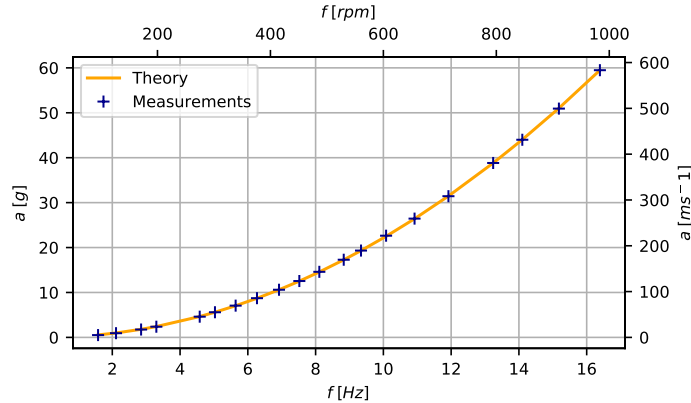


Figure 7: Centrifugal acceleration versus angular frequency in theory and in our experiments. Experimental measurements are shown after correction for device-specific offset and scale error. Our measurements showed good agreement with our theoretical results. Above 300 rpm, the relative acceleration error was consistently below 0.5%. Below 300 rpm, the residual offset error that remains after our first-order corrections has a strong impact (0.05 g absolute or 8% relative at 95 rpm.)

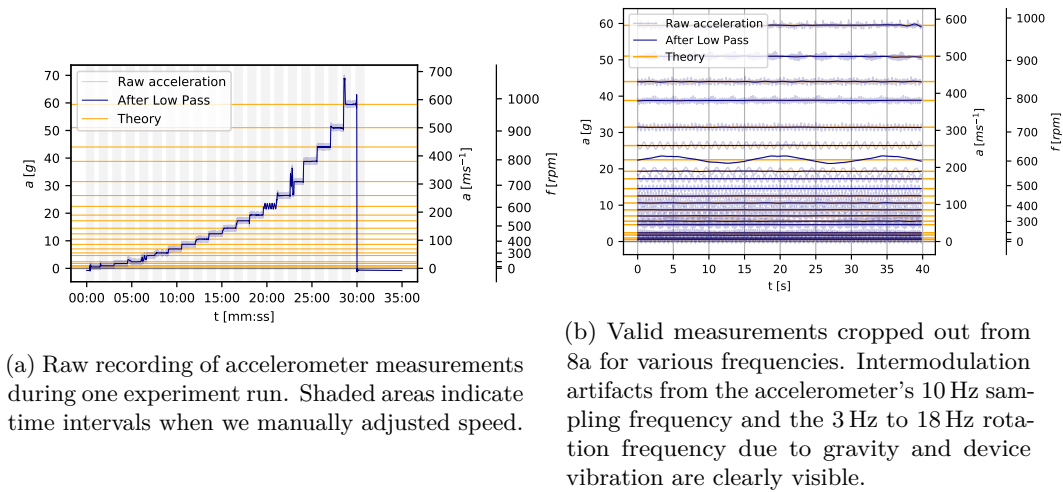
482 error is a fixed additive offset to all measurements. Scale error is an error proportional  
 483 to a measurements value that results from a deviation between the device’s specified and  
 484 actual sensitivity. We correct for both errors by first extracting all stable intervals from  
 485 the time series, then fitting a linear function to the measured data. Offset error is this  
 486 linear function’s intercept, and scale error is its slope. We then apply this correction to  
 487 all captured data before plotting and later analysis. Despite its simplicity, this approach  
 488 already leads to a good match of measurements and theory modulo a small part of the  
 489 device’s offset remaining. At high speeds of rotation this remaining offset does not have  
 490 an appreciable impact, but due to the quadratic nature of centrifugal acceleration at low  
 491 speeds it causes a large relative error of up to 10% at 95 rpm.

492 After offset and scale correction, we applied a low-pass filter to our data. The graphs  
 493 show both raw and filtered data. Raw data contains significant harmonic content. This  
 494 content is due to vibrations in our prototype as well as gravity since we tested our proof of  
 495 concept prototype lying down, with its shaft pointing sideways. FFT analysis shows that  
 496 this harmonic content is a clean intermodulation product of the accelerometers sample  
 497 rate and the speed of rotation with no other visible artifacts.

498 Figure 7 shows a plot of our measurement results against frequency. Data points are  
 499 shown in dark blue, and theoretical behavior is shown in orange. From our measurements  
 500 we can conclude that an accelerometer is a good choice for an IHSM’s braking sensor. A  
 501 simple threshold set according to the sensor’s calculated expected centrifugal force should  
 502 be sufficient to reliably detect manipulation attempts without resulting in false positives.  
 503 Periodic controlled changes in the IHSM’s speed of rotation allow an offset and scale  
 504 calibration of the accelerometer on the fly, without stopping the rotor.

## 505 7 Conclusion

506 In this paper we introduced Inertial Hardware Security Modules (iHSMs), a novel concept  
 507 for the construction of advanced hardware security modules from simple components. We  
 508 analyzed the concept for its security properties and highlighted its ability to significantly  
 509 strengthen otherwise weak tamper detection barriers. We validated our design by creating



(a) Raw recording of accelerometer measurements during one experiment run. Shaded areas indicate time intervals when we manually adjusted speed.

(b) Valid measurements cropped out from 8a for various frequencies. Intermodulation artifacts from the accelerometer’s 10 Hz sampling frequency and the 3 Hz to 18 Hz rotation frequency due to gravity and device vibration are clearly visible.

Figure 8: Traces of acceleration measurements during one experiment run.

510 a proof of concept hardware prototype. In this prototype we have demonstrated practical  
 511 solutions to the major electronics design challenges: Data and power transfer through  
 512 a rotating joint, and mechanized mesh generation. We have used our prototype to  
 513 perform several experiments to validate the rotary power and data links and the onboard  
 514 accelerometer. Our measurements have shown that our proof-of-concept solar cell power  
 515 link works well and that our simple IR data link already is sufficiently reliable for telemetry.  
 516 Our experiments with an AIS1120 automotive MEMS accelerometer showed that this part  
 517 is well-suited for braking detection in the range of rotation speed relevant to the IHSM  
 518 scenario.

519 Overall, our findings validate the viability of IHSMs as an evolutionary step beyond  
 520 traditional HSM technology. IHSMs offer a high level of security beyond what traditional  
 521 techniques can offer even when built from simple components. They allow the construction  
 522 of devices secure against a wide range of practical attacks in small quantities and without  
 523 specialized tools. The rotating mesh allows longitudinal gaps, which enables new applica-  
 524 tions that are impossible with traditional HSMs. Such gaps can be used to integrate a fan  
 525 for air cooling into the HSM, allowing the use of powerful computing hardware inside the  
 526 HSM. We hope that this simple construction will stimulate academic research into (more)  
 527 secure hardware.

## 528 References

- 529 [1] Nils Albartus et al. “DANA Universal Dataflow Analysis for Gate-Level Netlist Re-  
 530 verse Engineering”. In: *IACR Transactions on Cryptographic Hardware and Embedded*  
 531 *Systems* 2020.4 (2020), pp. 309–336. DOI: 10.13154/tches.v2020.i4.309-336.
- 532 [2] Ross Anderson. *Security Engineering*. Sept. 16, 2020. ISBN: 978-1-119-64281-7.
- 533 [3] Bertrand Campagnie. *Choose the Right Accelerometer for Predictive Maintenance*.  
 534 Tech. rep. Analog Devices, 2019.
- 535 [4] Saar Drimer, Steven J Murdoch, and Ross Anderson. “Thinking inside the box:  
 536 system-level failures of tamper proofing”. In: *2008 IEEE Symposium on Security*  
 537 *and Privacy (sp 2008)*. IEEE. 2008, pp. 281–295.

- 538 [5] Maged Elsaid Elnady. “On-Shaft Vibration Measurement Using a MEMS Accelerometer for Faults Diagnosis in Rotating Machines”. PhD thesis. University of Manchester, 2013.  
539  
540
- 541 [6] Jessie Frazelle. “Securing the Boot Process: The hardware root of trust”. In: *ACM Queue* (Dec. 1, 2019). DOI: 10.1145/3380774.3382016.  
542
- 543 [7] 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/](https://www.theregister.com/2006/09/25/phantom_sentinel/) (visited on 09/17/2020).  
544  
545
- 546 [8] 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.  
547  
548
- 549 [9] International Atomic Energy Agency. *Safeguards, techniques and equipmen*. Vol. 1. International Nuclear Verification Series. 2011. ISBN: 978-92-0-118910-3.  
550
- 551 [10] Phil Isaacs et al. *Tamper proof, tamper evident encryption technology*. Tech. rep. Surface Mount Technology Association, 2013.  
552
- 553 [11] Scott Johnson et al. “Titan: enabling a transparent silicon root of trust for Cloud”. In: *Hot Chips: A Symposium on High Performance Chips*. 2018.  
554
- 555 [12] Ivar Koene, Raine Viitala, and Petri Kuosmanen. “Internet of Things Based Monitoring of Large Rotor Vibration With a Microelectromechanical Systems Accelerometer”. In: *IEEE Access* (2019). DOI: <https://doi.org/10.1109/ACCESS.2019.2927793>.  
556  
557
- 558 [13] 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.  
559  
560
- 561 [14] 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/>.  
562  
563
- 564 [15] Karsten Nohl, Fabian Bräunlein, and dexter. *Shopshifting: The potential for payment system abuse*. 32C3 Chaos Communication Congress. Dec. 27, 2015. URL: <https://media.ccc.de/v/32c3-7368-shopshifting#t=2452>.  
565  
566
- 567 [16] 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.  
568  
569  
570
- 571 [17] Mujib Rahman. “Optical fiber cable with tampering detecting means”. US Patent US4859024A. Mar. 10, 1988.  
572
- 573 [18] Maruthi G. S. and Vishwanath Hegde. “Application of MEMS Accelerometer for Detection and Diagnosis of Multiple Faults in the Roller Element Bearings of Three Phase Induction Motor”. In: *IEEE Sensors Journal* 16 (1 2016). ISSN: 1558-1748. DOI: <https://doi.org/10.1109/JSEN.2015.2476561>.  
574  
575  
576
- 577 [19] Sean Smith and Steve Weingart. “Building a High-Performance, Programmable Secure Coprocessor”. In: *Computer Networks* 31 (8 1999).  
578
- 579 [20] 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>.  
580  
581
- 582 [21] Johannes Tobisch, Christian Zenger, and Christof Paar. “Electromagnetic Enclosure PUF for Tamper Proofing Commodity Hardware and other Applications”. In: *TRUDEVICE 2020: 9th Workshop on Trustworthy Manufacturing and Utilization of Secure Devices* (Mar. 13, 2020).  
583  
584  
585



586 [22] Timothy Trippel et al. “WALNUT: Waging doubt on the integrity of MEMS ac-  
587 celerometers with acoustic injection attacks”. In: *2017 IEEE European symposium*  
588 *on security and privacy*. IEEE. 2017, pp. 3–18.

589 [23] Serge Vrijaldenhoven. “Acoustical Physical Uncloneable Functions”. MA thesis.  
590 Technische Universiteit Eindhoven, Oct. 1, 2004.

591 This is version v2.0-draft5-0-g6c93ccf of this paper, generated on April 16, 2021. The  
592 git repository can be found at:

593  [Author information removed for double-blind peer review]