

Tamper Sensing Meshes in Payment Terminals and Beyond

Jan Sebastian Götte^{1,2} and Björn Scheuermann¹

¹ Technische Universität Darmstadt, Darmstadt, Germany

² Yasec, Berlin, Germany

research@jaseg.de, bjoern.scheuermann@tu-darmstadt.de

Abstract. Card Payment Terminals commonly use tamper sensing meshes to deter physical attacks on devices handling sensitive data such as cryptographic keys. Although their use of such meshes is frequently referenced in research literature, the public record contains little research on their construction. Addressing this gap, in this paper we present the first comprehensive security evaluation of Tamper Sensing Meshes (TSMs) across a wide range of payment terminals and other devices such as ATM key pads and a data center HSM. We provide detailed photos of critical features. Based on our observations, we construct a taxonomy of mesh construction techniques and analyze their security properties. Our analysis reveals that most commercial devices use surprisingly simple construction techniques, and their structure size rarely approaches manufacturing limits.

Based on our analysis, we propose a concise set of design recommendations for the construction of secure TSMs. We conclude that designing TSMs that exceed the industrial state of the art is viable even using inexpensive and easily available manufacturing processes. Our design recommendations create a foundation both for practical TSM implementations and for future research into their design.

Keywords: Tamper Sensing Mesh (TSM), Security Mesh, Hardware Security Module, Physical Security

1 Introduction

Both software as well as hardware security have seen rapid advancements throughout the past decades. Despite this progress, there is still no such thing as a perfectly secure computer and practical security always relies on multiple layers of defense in both software and hardware. For the past three decades, Tamper Sensing Meshes (TSMs) have been commonly used as the first line of defense in applications that require a high level of security. TSMs are intentionally fragile conductive structures surrounding the payload to be protected that break when an attacker attempts to physically access the payload. They provide a generic and low-cost way to protect against a wide range of physical attacks and are widely used across application domains from electronic payment terminals to datacenter Hardware Security Module (HSM) appliances. However, despite their widespread use, their concrete construction is rarely detailed in either industry or academic publications.

In this paper, we will start with a brief history of TSMs. Based on this historical analysis, we present the results of a survey of mesh implementation approaches in a wide range of devices. We examine their construction techniques and analyze their security. We conclude with concrete guidelines for the construction of TSMs using low-cost manufacturing processes that lay the groundwork for both defensive and offensive security research. The contributions of this paper are as follows:

- We present a detailed analysis of the security and construction techniques of Tamper Sensing Meshes (TSMs) in a total of 30 devices across application domains (e.g. card payment terminals, ATM key pads, HSMs). Prior to this work, the academic corpus only contained concrete information on a total of three comparable devices.
- We develop a taxonomy of construction techniques covering mesh materials, trace layouts, electrical connections, and three-dimensional assembly.
- We identify recurring design weaknesses in the surveyed devices. We propose concrete structure size, mesh layout and 3D construction targets based on standard manufacturing processes as a baseline model for future research.
- We show that Computed Tomography (CT) can recover security-relevant mesh details and we discuss mitigations.

2 The History of Tamper Sensing Meshes

TSMs offer many degrees of freedom in their design ranging from the precise conductor layout, through the manufacturing technology of the mesh and how it is wrapped around the payload during manufacturing up to their monitoring circuitry. As a result, manufacturers across application domains from datacenter appliance HSMs to card payment terminals have historically used patents on parts of their TSM implementations as a means to prevent copying of their designs [40, 20, 11, 21, 38]. The basic principle of modern TSMs is to reliably detect physical intrusion using an embedded looped conductor to cover a surface. This concept traces back at least as far as 1870 [10, 26], when it was applied to the protection of bank vaults from robbers attempting to dig, drill and saw through the vault’s floor and walls. Even multi-layer, orthogonal TSMs are documented as far back as 1902 [43]. Using printed circuits instead of wires for this purpose occurs in literature as soon as printed circuit technology finds widespread commercial adoption in the 1960s [19]. The history of more HSM-like devices begins in the 1990s with the widespread adoption of cryptography in commercial applications [30, 29, 16, 8, 9, 17, 13, 6, 12, 39] when instead of protecting an entire device it became feasible to create a protected cryptographic coprocessor.

2.1 Military use

According to Boak [5, 4], around World War II, the US became concerned about the security of their ciphering machines. Boak notes that the safes used at the time would not withstand a specialist attack for more than an hour. As a countermeasure, the combination of a tamper-sensing envelope and key zeroization on alarm that is still used today was developed in the 1970ies. Boak notes other ways to penalize an intrusion attempt, including raising a remote alarm or—more exciting—exploding the device.

Predating these developments are Permissive Action Links (PALs), the US term for the tamper-proof ignition part of nuclear weapons. Their tamper response is described to be either locking out the ignition or igniting the weapon in a less harmful way. Carter et al. [7] mention a tamper sensing membrane being used in US PALs.

On the other side of the nuclear arsenal, the International Atomic Energy Agency (IAEA), tasked with monitoring treaty compliance, has reported research on using piezo-electric transducers or optical fibers inside an enclosure’s walls as a tamper sensor to replace passive tamper-indicating enclosures it uses previously. The IAEA’s Electro-Optic Sealing System (EOSS) is reported to use a flexible TSM [27, 44].

2.2 Commercial Use

Commercial use of TSMs has started with datacenter HSMs, initially marketed for finance applications [2]. Over time, their use has spread to include ATM pin pads and card payment terminals.

HSMs are used for highly sensitive operations outside of the financial industry. For example, in this paper, we will analyze a commercial HSM that was used in the key management infrastructure of a premium TV provider. Other applications include mail franking machines, where they are used to protect the credit counter and certain models of key safes used in Germany that are mounted on the outside of buildings to provide keys to emergency services [41, 31]. We found a niche application where a processing unit of a mid-2000s series of slot machines includes a TSM, presumably to prevent modification or cloning. This device will also be analyzed later in this paper.

2.3 Academic Research

Academic research on TSMs found in the field is rare. In their 2008 paper, Drimer, Murdoch, and Anderson [15] show several bypasses of the security of a payment terminal. The bypasses they show are based on insufficient TSM coverage, which we also identify as a common weakness in this survey. Obermaier and Immler [36] in 2018 analyze the TSMs of two datacenter HSMs. They report coarse mesh structure sizes of 300 μm in one case and 1 mm in the other, which we also observe as a common weakness in this paper. In contrast to these prior works, this paper covers a larger range of specimens and focuses on TSM security.

3 Tamper Sensing Mesh Design Principles

The manufacturing technology of a TSM is a critical factor in its security. While in many applications, meshes manufactured from off-the-shelf processes such as Flexible Printed Circuit (FPC) processes are used, these processes tend to be optimized to maximize the robustness of the produced circuits to mechanical stress. In contrast, the ideal TSM is exactly as robust as it needs to be not to be destroyed accidentally during normal handling, but should not be more robust than that. As a result, more secure meshes tend to be manufactured in bespoke manufacturing processes [24, 25, 10, 22, 37, 45, 42].

One more widely cited TSM implementation is a commercial product developed by IBM in collaboration with chemical company W. L. Gore & Associates Inc. This product is used in IBM’s datacenter HSM products up to approximately 2020 [36, 2, 42]. It uses a stack of multiple layers of a clear, flexible plastic substrate on which carbon-based traces are printed. Vias, i.e. contacts between layers, are made by laser cutting small holes into the substrate before the traces are printed. The flexible circuit layers are joined with an opaque black, stretchy glue and are embedded in an elastic opaque resin after installation. The plastic substrate foil is thinner and significantly less resistant to tearing than plastic substrates commonly used in the electronics industry for applications like key pads and circuit boards, which improves its security against tampering. It is clear that both the glue fusing the foil layers together and the resin that the mesh is embedded inside are co-designed with the carbon trace material such that the trace material adheres well to both, leading to the traces being destroyed when either are peeled off.

The design of these IBM/Gore meshes is documented in an extensive list of patents, mostly under IBM’s name. Its basic construction and layout has not changed much since the early 1990s [34, 33].

Concluding this brief history of TSMs, we find that they were initially developed for sensitive military applications, and their use in civil applications is a recent phenomenon. The implementation of tamper sensing meshes in civil applications was likely catalyzed

by two advancements in electronics. First, electronic components became less expensive and more integrated reducing the cost overhead of tamper sensing circuits. Second, the mass-scale adoption of PCB and FPC production processes enabled their use as inexpensive, high-resolution substrates for such meshes.

3.1 Monitoring Circuit Approaches

TSMs are most effective when they are continuously monitored using a backup power supply while the rest of the system is powered off. In practice, the main challenge with continuous monitoring of TSMs is in the design of the monitoring circuit. A large portion of industry attention has been spent on designing low-power monitoring circuits that are sensitive to tampering with the mesh while using little enough power to enable years of operation from a battery. Commonly, one or two cylindrical or large coin cell Lithium primary batteries are used, providing in the order of 10 W h over their lifetime [23]. Broken down to an unpowered storage life of e.g. 5 years, this corresponds to a maximum average power consumption of less than $230 \mu\text{W}$.

To achieve low power consumption, a popular technique known since at least 1902 [43] and still used today [8, 40] is to measure the deviation of the mesh’s end-to-end ohmic resistance from its baseline value. This measurement can be implemented either by directly comparing a mesh trace’s resistance with a reference resistor, or using a Wheatstone bridge. Bridge circuits were already used in early TSM implementations [18, 19, 14] since they make it possible to detect small changes in the mesh’s resistance with little complexity.

3.2 Other Tamper Sensing Techniques

Besides TSMs, environmental sensors such as temperature or light sensors are frequently used as a secondary line of defense in HSMs and similar devices. By placing such sensors in the device and verifying the device is within its nominal operating environment, tampering can be made less convenient. Modern security standards often mandate the implementation of at least a temperature sensor to prevent cold-boot attacks on a device [1, 28]. A multitude of other sensors have been proposed, including vibration sensors, light sensors, magnetometers, and radiation sensors such as X-ray sensors. While the implementation cost of most sensor types is low, each additional environmental sensor comes with an increased false alarm rate [2].

4 A Survey of Meshes in the Wild

In this section, we will examine a large sample of recent devices that include TSMs to gain an understanding of how they are implemented, and what security level they are targeted towards. Since we were unable to acquire a nuclear weapon for our research, we limited our survey to commercial devices. While we analyzed devices across a broad spectrum of applications, our survey includes a large variety of card payment terminals, which represent the most varied class of device incorporating such meshes.

4.1 Specimen Selection

Given their niche applications and high cost, devices incorporating TSMs tend to be hard to find. For this survey, we chose 30 total devices starting from 23 different models of card payment terminals, and including 7 other devices. All devices were procured from electronic waste. A complete list of our specimens can be found in Table 1. External and internal photos of each device are shown in Figure 1. We sampled devices from these classes:

Table 1: The specimens we dissected in our survey. PED stands for *Pin Entry Device*, the industry term for card payment terminals that have sufficient security to handle credit card PINs. EPP stands for *Encrypting Pin Pad*, the type of keypad used for pin entry on ATMs. HSM stands for Hardware Security Module.

ID	Brand	Device	Year
H01	Verifone	PED VX 570	ca. 2010
H02	Merkur / ADP	Slot machine CPU mod-	ca. 2012
	Gauselmann	ule Sam 12 EC2	
H03	Sagem	EPP USA1315-4240	2014
		R1A	
H04	Sagem	EPP USA1316-5120	2007
		R1A	
H05	Xac	PED xAPT-103	2014
H06	Ingenico	PED iCT250-	2016-17
		11T1860A	
H08	Sagem	PED NOR4100-4220	2012
		R1A	
H09	Hypercom	PED M4230	2010
H10	Worldline	PED YOMANI XR	2016
H11	Banksys	PED C-ZAM Smash	2004
		Portable	
H12	Hypercom	PED Optimum P2100	2010
H13	Ingenico	PED iCT 220-	2016
		11T2938A	
H14	Verifone	PED H5000	2016
H15	Verifone	PED MX 925	2018
H16	Verifone	PED V200c CTLS	2021
H17	Verifone	PED VX 680	2014
H18	Ingenico	PED i7910	2010
H19	Banksys	PED XENTA	2004-2011
H20	Verifone	PED VX 520 3G	2017
H21	Verifone	PED V400m Plus 4G	2018
H22	Ingenico	PED Move 3500	2020
H23	Ingenico	PED iPP 350-	2015
		11T1718A	
H24	Ingenico	PED iWL255-	2016
		01T2117A	
H25	Neopost	Franking Machine IJ-25	ca. 2001
H27	Sumup	PED AIR1E205	2021
H28	NCR	EPP 5814 UEPP	2019
H29	SafeNet	HSM VBD-05	2018
H30	Irdeto (Utimaco)	HSM Mayflower- IDX/C201	2011
H31	SumUp	PED SumUp 3G	2019
H32	SumUp	PED SumUp Air	2022

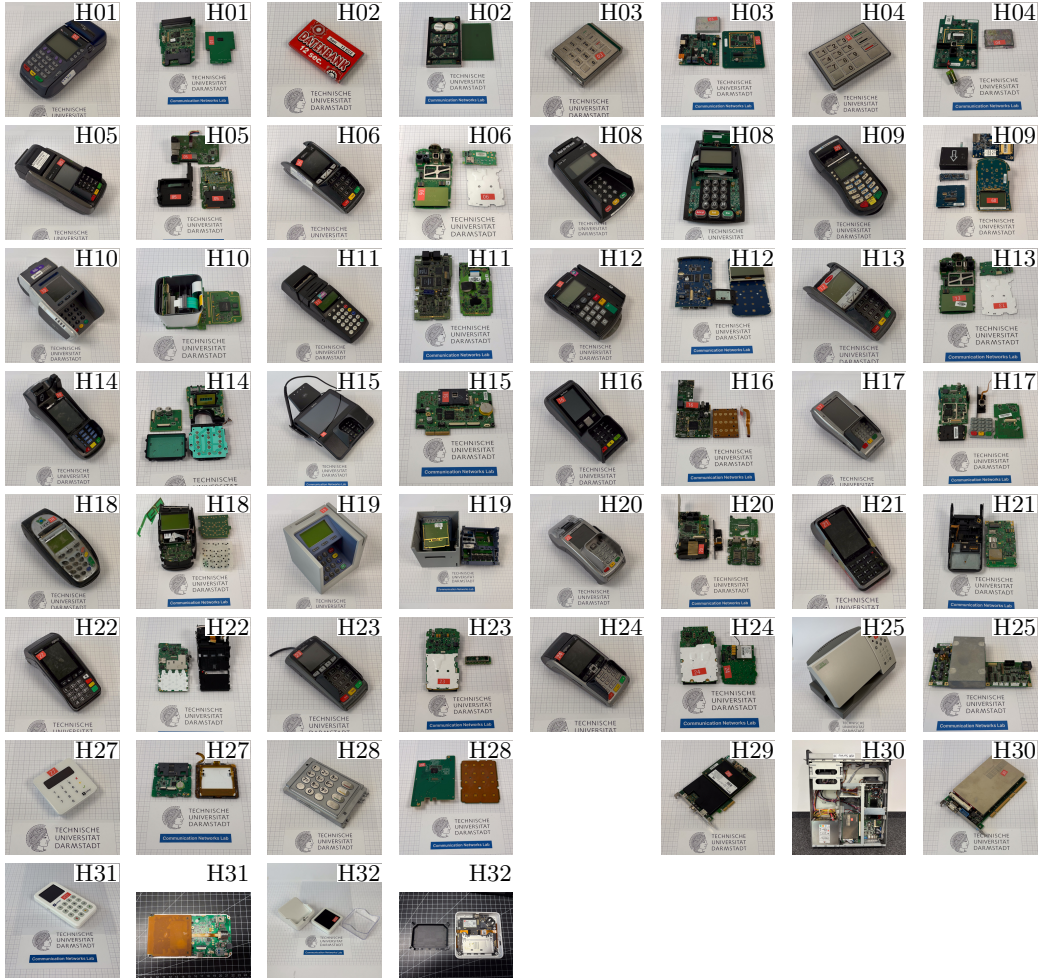


Figure 1: External and internal photos of all survey specimens. For each specimen, the external photo is shown on the left and the internal photo on the right.

Card Payment Terminals. Card payment terminals commonly include advanced tamper sensing features to discourage physical attacks such as skimming that aim to exfiltrate card data and PINs entered by the customer. Payment terminal security is standardized by the Payment Card Industry Security Standards Council (PCI SSC), an association of all major western credit card network operators. Since card payment terminals are widely deployed, many different models from various manufacturers are available. Each manufacturer tends to have their own, patented tamper sensing implementation. Being manufactured at scale, card payment terminals are cost-sensitive devices, which is reflected in the construction of their tamper sensing implementations.

HSM Appliances. HSM appliances are usually standalone rackmount devices designed to handle cryptographic keys in datacenter applications. We were able to procure two such devices, one of which contained a tamper-sensing mesh.

ATM Encrypting Pin Pads (EPPs). ATMs are built in a modular construction approach. Inside the enclosure, the PIN pad acts as a secondary security barrier. ATM pin pads contain a microcontroller that encrypts the customer's PIN [2] before it leaves the PIN pad. The circuit board containing the PIN pad's keyboard matrix and this microcontroller are shielded by a TSM to prevent physical attacks such as the installation of a skimming device that would record and transmit the plaintext PIN.

We acquired three EPPs for analysis: Two designed by Sagem re-sold by Cryptera and Diebold, and one made by NCR. All three devices have robust stainless steel front cases, and are built in a sandwich construction of several layers of steel sheets and PCBs.

Other miscellaneous devices. We acquired two other devices that commonly contain TSMs. We acquired a mail franking machine, a type of device that is used to directly print a code on an envelope that replaces a conventional postage stamp. Since in businesses handling large volumes of mail these devices were routinely charged with large sums of money in postage, such devices have security features ranging from physical seals on their enclosure to full security meshes encasing their CPU modules. While there is online evidence of meshes being used in such devices [35], we found that our older specimen only contained a sturdy, welded cast zinc case with a spring-loaded lid switch. Beyond this device, we found a CPU module from a series of slot machines that included both a TSM as well as a light sensor inside of a sealed sheet metal enclosure.

4.2 Methodology

After disassembling specimens, we photographed each major component. Figure 1 shows a selection of these photos showing the major internal components of the devices. We proceeded with destructive techniques where necessary to understand the devices' use of TSMs. We took microscope photos where we found interesting small structures. PCBs were sectioned using a sanding drum attachment on a Dremel rotary tool. Potted modules were disassembled using milling, cutting and prying, and applying heat from a heat gun as necessary to soften polymer compounds and to break glue joints.

We did not conduct attack attempts on the specimens for two main reasons. First, since they were obtained from e-waste streams, most specimens were not operational so measuring mesh response through normal operation was not possible. Second, directly contacting the meshes was not generally possible without first successfully attacking the mesh since the meshes' monitoring connections were generally shielded inside the mesh.

Our analysis focuses on physical attacks that inherently are not remotely exploitable and thus do not scale easily. Our specimen selection is focused on older devices sourced

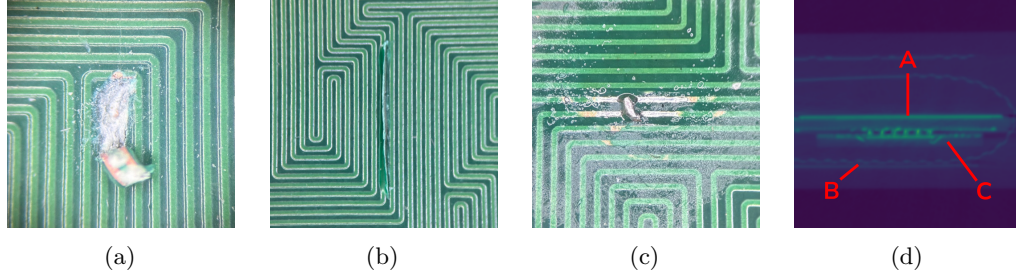


Figure 2: Examples of attacks manipulating a mesh. (a) folding up and (b) slicing and lifting a trace, synthetic mesh, trace pitch $240\text{ }\mu\text{m}$. (c) bridging part of a trace, synthetic mesh, trace pitch $300\text{ }\mu\text{m}$. (d) CT imaging. Labels: A—Cu ground plane, B—Ag mesh traces, C—Cu IC lead frame. Specimen H18, mesh trace pitch $1000\text{ }\mu\text{m}$.

from e-waste streams, and we report aggregate observations so no coordinated disclosure appeared necessary.

4.3 Results

In this section, we will list some observations we made while dissecting our specimens. Across devices and manufacturers, we observe certain common weaknesses, which are summarized in the list below. We assign each weakness an identifier, and we will refer to these weaknesses by their identifier when discussing mesh characteristics in the remainder of this section.

W1 Insufficient Coverage such as gaps at corners or missing sides. An attacker can insert tools or probes through such gaps. Even when gaps are filled with glue or resin, small drills can be used to open access. Furthermore, a sharp probe such as one made from a standard stainless steel hypodermic needle can be inserted through many filler materials by simply applying force.

W2 Mechanical Robustness of the mesh allows an attacker to peel apart layers and to insert probes without disturbing the mesh’s conductivity. This weakness can be mitigated by using fragile substrates and thin conductive layers for the traces. Especially FR-4 substrates with copper traces are prone to separation since the resin is brittle, the embedded fiberglass weave is strong, and the copper traces are malleable and can both bend and stretch. Figures 2a and 2b show two such attacks.

W3 Chemical Robustness and Resistance to Heat of the mesh allows an attacker to chemically remove glue layers, opaque cover layers, or structural components, enabling mechanical access. Where metals are used on heat-resistant substrates, an attacker can directly solder to mesh traces to bridge over parts of the mesh (cf. Figure 2c). These weaknesses can be mitigated by using chemically resistant glues or potting compounds such as epoxy resin, and choosing more sensitive materials for the mesh itself.

W4 Mesh Layout Visibility in optical or X-ray spectra enables an attacker to reconstruct the layout in preparation of an attack. This weakness can be mitigated by using opaque potting compounds, low atomic mass trace materials, and metal shielding layers. Figure 2d illustrates the contrast of copper PCB and silver mesh traces after Computed Tomography (CT) imaging. Silver traces show lower contrast due to their lower thickness in this specimen.

W5 Coarse Feature Size of the mesh enables an attacker to drill holes through gaps between mesh traces using standard industrial drills. For such small holes, a limiting factor is aspect ratio, i.e. at a given diameter, the depth of the hole is limited by the mechanical rigidity of the drill. Particularly structure sizes above $150\text{ }\mu\text{m}$ are susceptible to attack using standard PCB rework tools. Choosing an appropriate manufacturing process and designing the mesh to the process capabilities mitigates this weakness. Spacing layers apart also limits the impact of coarser structure size since drill holes of $d \leq 300\text{ }\mu\text{m}$ diameter are usually limited in depth to $\leq 10d$ due to the mechanical strength of the drill.

W6 Single-Layer Layouts leading to striated gaps between parallel mesh tracks. Long gaps allow the insertion of larger tools by cutting along the gap and tenting upwards of one layer (cf. Figure 2b).

W7 Insufficient Adhesion allows the separation of layers and deforming the mesh to enable mechanical access. To mitigate this issue, the bond between glues or resins and trace material should exceed the internal strength of those trace materials. Figure 3d below shows an extreme example where sandwiched polyimide FPC and FR-4 PCB mesh layers could be separated cleanly.

4.3.1 Mesh materials.

We found meshes constructed from rigid PCBs (e.g. specimens H02, H03 and H08) as well as a number of FPC processes. TSMs constructed from PCBs sometimes used parts of an existing PCB (e.g. specimens H03 and H10), and sometimes additional PCBs only containing a mesh were added (e.g. specimen H02 and H08). In some samples (e.g. specimens H08 and H18), multiple rigid PCB meshes were assembled in a house of cards fashion to enclose a card slot. All flexible meshes that we found with the exception of the Utimaco HSM appliance’s HSM card (specimen H30) were clearly manufactured either entirely or mostly in standard processes. We found printed silver ink (e.g. specimen H12) and printed carbon ink-based foils (e.g. specimen H09) similar to those used for membrane keyboards, as well as conventional photolithographically etched copper/polyimide FPCs (e.g. specimens H03, H04 and H08). Overall, etched PCBs showed better resolution compared to silkscreen-printed meshes. Feature size for both rigid and flexible etched PCB meshes was generally in the order of $100\text{ }\mu\text{m}$ to $200\text{ }\mu\text{m}$, while feature size for screen printed foil meshes was coarser at between $500\text{ }\mu\text{m}$ to $3000\text{ }\mu\text{m}$. In contrast to these standard processes, the Utimaco HSM used a mesh foil that is manufactured in a proprietary, bespoke process by Gore.

Weaknesses. Standard PCB materials are engineered to withstand mechanical stress (W2) and chemical stress (W3). This also often leads to a lack of adhesion (W7), particularly with polyimide substrates. Standard processes often allow layout reconstruction from surface unevenness even when cover lacquers are used (W4). Copper traces are easily visible on X-ray (W4). For non-copper trace materials, we found feature sizes are limited (W5) and meshes are often single-layer (W6).

4.3.2 Mesh layout.

A key goal in tamper sensing mesh design is to avoid any gaps in coverage. In single-layer meshes, gaps between adjacent mesh traces cannot be avoided, and provide an easy approach for an attack. In multi-layer meshes, these structure size-dependent gaps can be mitigated in multiple ways as shown in Figure 3. In the following list, we will address several common structural features that we observed across samples.

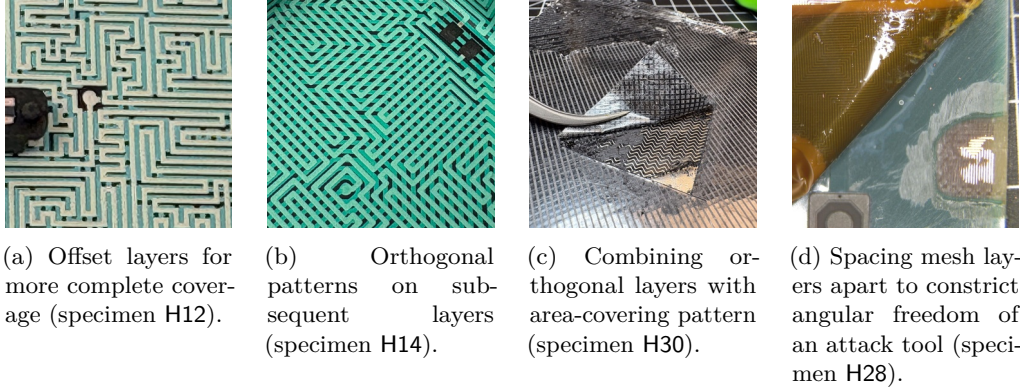


Figure 3: Mesh trace layout approaches for multi-layer meshes.

1. **Offset patterns.** In a two-sided foil mesh, most of the gaps between adjacent traces can be covered by simply offsetting the pattern by one structure size in both axes between the foil’s top and bottom layers as shown in Figure 3a. Depending on the mesh layout, only a small number of point-shaped gaps remain at corners in mesh traces on one of the layers. The number of these gaps can be reduced by reducing the number of misaligned corners between both layers for instance by choosing a systematic serpentine or spiral trace layout.
2. **Orthogonal patterns.** In some other specimens, the manufacturer chose the opposite approach of keeping the mesh pattern mostly orthogonal on the mesh’s two layers as shown in Figure 3b. While this leads to a larger amount of gaps compared to offset patterns as described above, it also reduces the largest gap size to about one structure size by one structure size.
3. **Combined approaches.** Figure 3c shows the layout of a Gore tamper sensing mesh foil used in a Utimaco HSM. This mesh consists of two foil layers bonded to each other. The outer foil is patterned on both sides with a sparse pattern of thin serpentine traces with the patterns on both layers being orthogonal to each other. Both patterns are oriented at a 45° angle relative to the sides of the rectangular enclosed volume. The inner foil is only patterned on one side, and contains a thicker serpentine trace laid out in a zigzag pattern. The two foil layers are aligned such that no gaps remain between the layers.
4. **Using layer spacing.** Figure 3d shows how an ATM Encrypting Pin Pad (EPP) implemented the mesh on its keypad. Off-the-shelf metal snap dome contacts were used on the surface of a conventional rigid PCB to create the keys. On top of the rigid PCB and contact domes, a two-layer copper/polyimide FPC with an additional polyimide cover layer was glued down. Meshes were placed on both layers of the FPC, as well as on one internal layer of the rigid PCB. The resulting structure had the FPC mesh layers separated from the rigid PCB mesh layer by several hundred micrometers of the rigid PCB’s substrate. The meshes on both the FPC and the rigid PCB used a structure size of $150\mu\text{m}$. The vertical separation between the two meshes was several times that structure size, which limits the possible angles an attack tool could be inserted through both mesh layers.

Weaknesses. Offset patterns partially mitigate coarse feature size (W5) and sometimes make the layout harder to distinguish (W4). Spaced layers of different mesh materials can

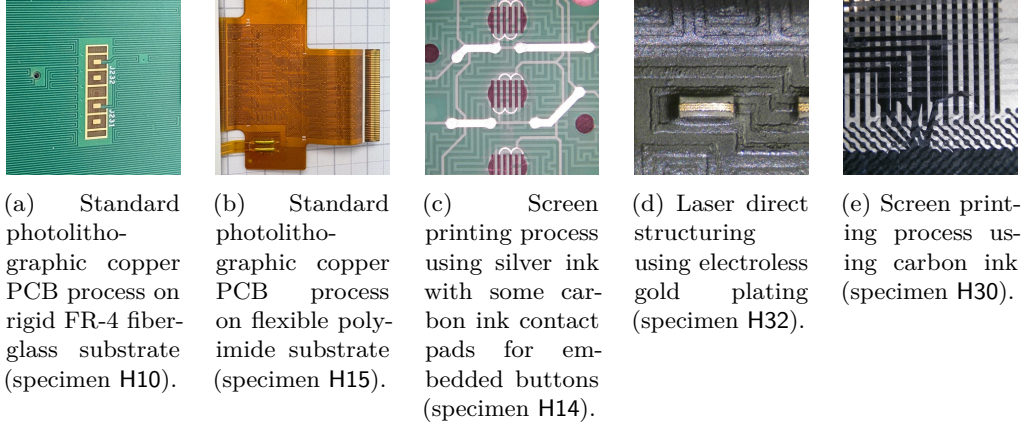


Figure 4: Materials and manufacturing processes used for mesh traces and contacts.

mitigate chemical resistance (W3) if the materials are chosen to be sensitive to a large range of solvents and etchants.

4.3.3 Contact and trace construction.

Regular Printed Circuit Boards are frequently used to implement TSMs as shown in Figure 4a. PCB production is a highly advanced, large-scale industry and PCBs are inexpensive, commodity products. PCBs can be manufactured with many layers, at almost arbitrary total thickness, and offer small structure sizes enabling the creation of fine features down to approximately $100\mu\text{m}$ even on commodity processes. The primary disadvantage of using PCBs to implement TSMs is that PCBs are fundamentally designed to be as robust as possible. The traces on the top of a PCB are etched from a thick (usually $35\mu\text{m}$ on the outer layers) copper foil adhered to the PCB substrate. As a result, the PCB and the traces on its surface are easy to manipulate by hand using tools like knives and techniques like soldering. For a TSM, trace patterns manufactured to be more fragile might be advantageous. Additionally, standard PCBs are made using a rigid FR-4 fiberglass/epoxy substrate. Since a TSM must often enclose all sides of a payload, flexible foils offer benefits over rigid PCBs.

Figure 4b shows an FPC produced in a standard commercial process similar to PCB production. In FPCs, a copper foil adhered to a substrate is etched, but the substrate here usually is a thin foil made from polyimide, an orange, temperature-resistant polymer that survives common reflow (hot air) soldering temperatures. In contrast to rigid PCBs, FPCs are usually limited to no more than four layers before losing flexibility. Flexible PCBs are often used for TSMs that wrap around a payload, but they come with the same limitation as standard PCBs: Due to their robust substrate and thick copper layers, they are easily manipulated by hand.

Figure 4c shows an FPC created in a different process. Here, instead of photolithographically etching a continuous copper foil adhered to a flexible substrate, the pattern is printed onto the substrate using a conductive ink. A variety of printing processes are suitable for this technique. The conductive ink is based on small conductive particles suspended in a hardening binder. Common conductive ink materials are silver (Figure 4c) and carbon (Figure 4e). Silver-based inks offer lower resistance compared to carbon-based inks, but are prone to surface oxidation and as such are not suitable for contacts. As such, they are often combined with a carbon ink used in contact areas. Carbon-based inks have high resistance, and can be used to create embedded resistors. The circuit shown in Figure 4c contains a TSM on a lower layer, and a keypad matrix with carbon contacts on

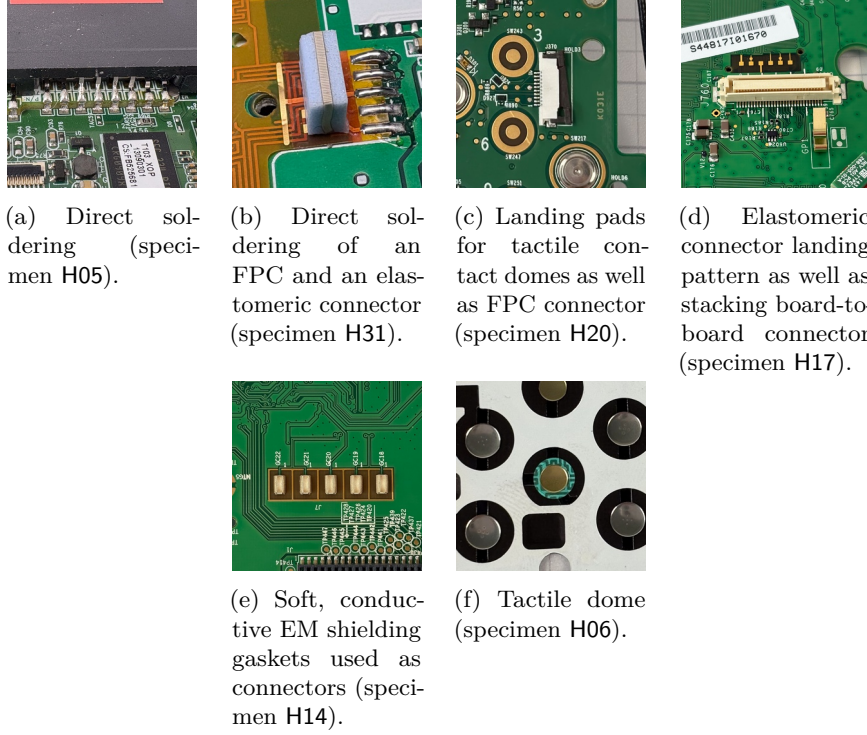


Figure 5: Connecting methods used between TSM assemblies and their base PCBs

its surface.

Figure 4d shows part of a mesh and a contact created using Laser Direct Structuring, an industrial technique combining selective activation of a plastic surface using a scanning laser and electroless gold plating [32]. Where in electroplating electrical current is used to deposit metal atoms on a surface, in electroless plating a series of chemical reactions is used. Electroplating requires all traces to be electrically connected to form a single electrode, while electroless plating can be used on the finished circuit. Laser Direct Structuring allows patterning complex surfaces with fine structures made from metal deposited in a thin layer. In Figure 4d, it is visible how the trace was created using three parallel passes by the laser. The micrograph also shows the rather coarse edge structure created by LDS, which is caused by the rough surface left after pulsed laser ablation. The uneven, thin layer of metallization created by LDS results in mechanically fragile contacts that must be contacted using a soft material, usually an elastomeric connector.

Weaknesses. Copper traces are resistant to solvents, enabling chemical attacks (W3). Copper is also the mechanically most robust trace material, increasing susceptibility to mechanical attacks due to robustness (W2) and lack of adhesion (W7). We found all printed ink trace materials to result in coarse structure size (W5). Meshes produced using Laser Direct Structuring mitigate W3, W5 and W7 well due to the thin and fragile traces, but allow attacks using thin probes inserted between mesh lid and PCB (W1).

4.3.4 Connection methods

In our survey, we found a wide variety of connecting methods used to connect TSM assemblies with their base PCBs with a selection shown in Figure 5. Both rigid PCBs and FPCs can be soldered directly to a PCB using either a Land Grid Array (LGA) technique

where pads on both PCBs are soldered facing each other, or using *castellated* edges, where pads on the base PCB are soldered sideways to holes on the top PCB that have been milled in half as shown in Figure 5a. FPCs can also be soldered by dragging a blob of solder across the contact as shown in Figure 5b, but this technique is only suitable for hand soldering. Hand soldering increases unit cost over mechanized soldering techniques such as wave soldering or reflow soldering.

FPCs are suitable for use with standard FPC connectors as shown in Figure 5c. These connectors mate directly to a contact area on the FPC, called *gold fingers* in industry terms. Both FPCs and rigid PCBs can be used with standard board-to-board stacking connectors such as the one visible in the center of Figure 5d, but their use on FPCs requires a stiffener on the FPC’s back side to ensure the solder joints don’t break from mechanical stress when connecting or disconnecting.

In our survey, we frequently found elastomeric connectors used to connect to both flexible and rigid TSM assemblies. Elastomeric connectors such as the one shown in the center of Figure 5b are usually used in LCD construction to contact a PCB to the LCD’s Indium Tin Oxide (ITO)-coated conductive glass, but they can be used between any two parallel, conductive surfaces [3]. Elastomeric connectors consist of two insulating elastic polymer layers on the outside, with a thin strip of fine, alternating conductive and insulating elastic polymer layers sandwiched in between. In Figure 5b the outer insulating layers are the blue polymer, and the alternating pattern can be seen embedded in their middle. The fine alternating pattern mates to much larger pads on the two contact surfaces, ensuring that adjacent contacts are electrically insulated. In TSM applications, elastomeric connectors provide an intrinsic disassembly detection since they require continuous pressure to maintain electrical contact. In the top part of Figure 5d, a land pattern for an elastomeric connector is visible.

Elastomeric connectors are elegant and allow for multiple contacts to be made in a small area using a single elastomeric connector strip, but they are not off-the-shelf components and are always custom made to order. We found several instances where other, off-the-shelf technologies were used instead to create a pressure-sensitive connection. Figure 5e shows a connection made using conductive gaskets intended for creating gapless connections between PCBs and enclosures to shield Electromagnetic Emissions (EMI). Unlike elastomeric connectors, they are not anisotropic and thus they must be cut into pieces to maintain isolation between adjacent pads. This results in a much larger contact pitch compared to other solutions.

Figure 5f shows another technique, here used to connect the mesh layer embedded into a key pad to a base PCB. Here, a tactile metal dome intended to be used for creating buttons in low-profile keypads is used to connect the mesh to the base PCB.

Weaknesses. Soldered connections are mechanically (W2) and chemically robust (W3) and limited in feature size (W5). Elastomeric connectors and tactile domes are limited in structure size (W5) but provide an inherent mitigation against disassembly, mechanical deformation (W2) or layer separation (W7).

4.3.5 3D construction.

While practical meshes are almost always manufactured in planar processes first, their applications usually require at least partially covering a three-dimensional volume. In our survey, we saw a number of methods being used to create three-dimensional structures from planar meshes. Figure 6 a–e show the major construction styles we saw among our samples. Figure 6a and Figure 6b have meshes produced as flexible printed circuits, in Figure 6a using a standard photolithographic copper/polyimide FPC process usually used for flexible PCBs, and in Figure 6b using a standard silver ink screenprinting process. The choice in Figure 6b not to overlap the mesh in the corner is likely caused by manufacturing

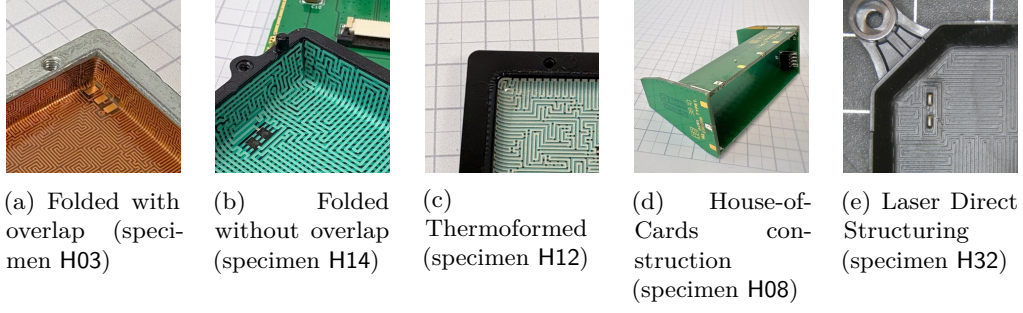


Figure 6: Construction styles used to fit TSMs into 3D envelopes. Grids in the background are 10 mm, subdivisions are 5 mm.

considerations, since it might be difficult to ensure proper folding of a small foil tab with adhesive pre-applied.

Figure 6c shows a sample of a flexible circuit manufactured in a screenprinted silver-ink process thermoformed into a three-dimensional shape [46]. The flexible circuit mesh is first produced in a standard planar printing process. After printing and curing, the resulting foil is then heated to soften it, and forced into a three-dimensional shape using a mold. Depending on the process, one or two molds, and vacuum or pressured air can be used to shape the foil. The process requires a screenprinted flexible circuit, and would not work with copper/polyimide flexible PCBs since their copper layer is too thick to plastically deform without tearing, and because polyimide is not sufficiently thermoplastic at low temperatures.

Thermoforming is a cheap standard process, but has its limitations. Only 2.5-dimensional structures can be created since the input is a flat foil. The foil must be mostly unbroken to keep tension during forming. Lastly, our samples show a maximum depth of 2 mm or less. We expect deeper forming would lead to tears in the mesh traces since the particle-based conductive inks used on flexible substrates are inelastic. Among our samples, we saw two instances of thermoformed meshes. First, all recent Ingenico terminals (specimens H06, H13, H23 and H24) integrated an ink printed mesh with thermoformed cavities into their key pad overlay to protect their main cryptographic processor. Their key pads are made using tactile domes with contacts patterned on their main PCBs' surface. These domes are commonly placed on an adhesive sheet that is die cut to size so that the whole sheet can be placed on the PCB in one assembly step, instead of individually placing each dome. In these samples, the mesh was integrated into this adhesive sheet using a silver ink printing process, and two additional domes were used to provide contact between this integrated mesh and the main PCB.

Figure 7 shows the mesh of specimen H24 before and after removing the black opaque cover lacquer using a cotton swab and acetone. Figure 7b shows mesh detail around the cavities, likely intended to reduce the risk of a break during the forming process. The notable increase in structure size at the cavity edges compromises the mesh's security level, especially considering that the cavity edges are a convenient location for probe access.

Specimen H12 in Figure 6c displays another design defect. Its mesh does not extend to the edges of its plastic carrier. The resulting gap between the bottom edge of the mesh and the PCB surface allows insertion of probes.

A similar design defect was mitigated in the specimens manufactured by Sagem (terminal H08 and EPPs H03 and H04). These specimens all have a polyimide/copper FPC mesh glued to the inside of a cast zinc lid that sits on top of their base PCB. In specimen H03, the gap between mesh and PCB was mitigated by milling a slot into the base PCB for the mesh to sit inside. In specimen H04, the payload circuit was placed on a soldered-down

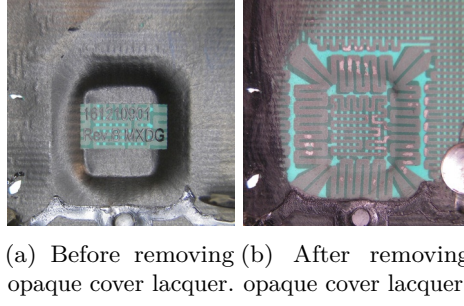


Figure 7: Formed cavities in printed foil mesh in specimen H24.

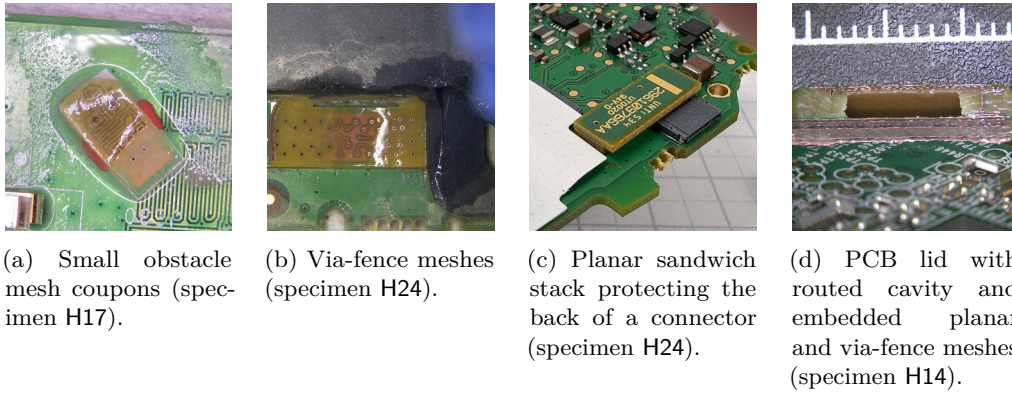


Figure 8: Construction styles used to cover 3D volumes using sandwich-style construction.

daughterboard sitting inside the lid. In specimen H08, metal ring was soldered to the base PCB inside the mesh to mechanically shield its edge.

Figure 6e shows the result of Laser Direct Structuring (LDS), a process that avoids some of the limitations of thermoformed planar meshes. In LDS, conductive traces are placed on a plastic part using laser patterning and chemical process steps. LDS allows covering complex 3D shapes as long as all parts of the pattern have some line of sight to the outside. LDS is commonly used to create complex antenna shapes on the surface of internal structural plastic parts for smartphones, but is more costly compared to printing processes due to its complexity. It is limited to a single trace layer.

Figure 6d shows an assembly of several rigid PCBs assembled into a three-dimensional structure to protect a card slot. Solder connections between large pads are used to mechanically and electrically join the boards. While the rigid PCBs used in such a structure can be produced in a highly inexpensive, standard process, this style of construction requires manual assembly leading to increased labor cost. Furthermore, the construction leaves large gaps at edges and corners, which is not a problem for card slot protection in payment applications but which would be a flaw in a more standard HSM application.

Besides the house of cards construction style shown in Figure 6d where PCBs are hand-assembled into a 3D shape, rigid PCBs are also often soldered planar on top of other PCBs to serve as meshes. Figure 8 shows examples of such sandwich-style constructions. Figure 8a and Figure 8b show a widely used construction technique where a small mesh PCB coupon is soldered using a Land Grid Array (LGA)-technique on top of a larger base PCB containing circuitry. The goal in this technique is to project a small part of the mesh into the space above the base PCB. While this does not prevent targeted drilling as the small coupon is easy to avoid, it does prevent an attacker from sawing or laser-cutting into

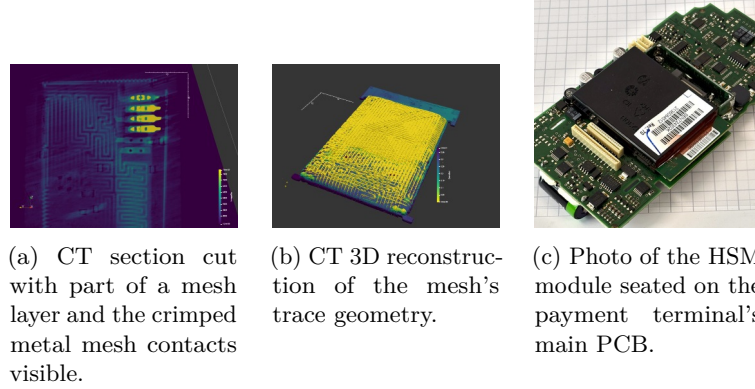


Figure 9: Optical photograph and CT pictures of a potted HSM module (specimen H18).

the side of the device parallel to the base PCB. In the implementation shown in Figure 8a, the coupon simply contains a small mesh embedded in an inner layer. Figure 8b shows a different technique, where the mesh inside the coupon is not primarily laid out in the PCB plane, but instead a large number of vias is used to create a three-dimensional zig-zag trace structure. While due to structure size limitations this via structure is much coarser than a planar mesh like that in Figure 8a would be, it increases the fraction of the vertical space inside the coupon that is covered by the mesh.

Figure 8c shows a variation of this coupon technique where two such coupons are stacked to create a small overhang, here attempting to protect the back side of a magnetic stripe reader contact in a payment terminal. While a similar result could also be achieved by milling a slot into the side of a single custom-thickness PCB, the economics of PCB manufacturing are such that it may be more cost-effective to bond two standard-thickness PCBs on top of one another instead.

Figure 8d shows an advanced construction technique that uses a custom PCB with a large indent milled into its underside soldered on top of a base PCB to create a protected cavity on top of the base PCB. This PCB lid shows a complex internal structure. It is built up in a custom stackup with a total of six layers: A ground plane filling the top layer, then two orthogonal planar mesh layers covering the inside of the lid above the cavity. Below this standard mesh stackup are two more layers that are used to create a via fence structure similar to that shown in Figure 8b in an attempt to protect the sides around the central cavity. Below these two via fence layers, at the bottom of the PCB is one more layer containing the pads connecting it to the base PCB.

Weaknesses. We found that thermoformed meshes and those created with Laser Direct Structuring always sit on the PCB like a lid, which allows an attacker to insert thin needle probes between the mesh lid and the PCB (W1, insufficient coverage and W2, mechanical robustness). Thermoformed meshes additionally often lack in coverage at corners (W1) and lack in structure size in areas of deformation (W5). Laser Direct Structuring meshes are limited to single-layer layouts (W6), which is only mitigated by their fine structure size and fragile traces. Folded construction styles require careful consideration to avoid coverage gaps at corners, at contact areas between mesh and PCBs, and along edges (W1). Mesh materials that can be folded during assembly usually are mechanically robust enough to allow manipulation by an attacker (W2).

4.3.6 CT Imaging

Hardware manufacturers implementing security meshes often attempt to keep the meshes' layouts hidden as a way of security by obscurity. In practice, this can take the form of opaque potting compounds (cf. Figure 9c), opaque cover layers (cf. Figure 4d), and burying the mesh beneath other features such as PCB ground planes (cf. Figure 8d, e.g. specimens H03, H17 and H32). To circumvent such attempts, an obvious attack vector is to use radiographical imaging techniques such as X-ray or CT imaging. To evaluate CT imaging as an attack method, we experimentally imaged the potted HSM module of specimen H18, an Ingenico payment terminal, using an industrial CT. Figure 9 shows the module we analyzed and two images exported from the resulting CT scan data. Figure 9a shows a horizontal cut across part of the module. In this cut, we can clearly identify a mesh layer with multiple traces, four solid metal contacts crimped to the mesh foil, and two unused contact pads and mesh traces in the lower part of the picture. An attacker would be able to use this information to target the metal contacts with a tool like a needle probe. From the CT scan we were able to measure that the mesh of the device has a pitch of 1.0 mm. Thus, even inserting a thin needle probe right through one of the mesh's traces should be possible without breaking the trace.

Figure 9b shows a 3D reconstruction of the mesh's conductor layout. While the reconstruction is slightly noisy due to the limited scan time available, it contains ample detail to reconstruct the mesh's layout and conductor count, and even to derive conductor dimensions in order to calculate resistance and other electronic parameters. The mesh's foil is wrapped around the circuit board forming a pillow shape, which is clearly reflected in the reconstructed 3D mesh geometry. This information could be used to guide a CNC milling machine to selectively ablate the device's potting precisely down to the mesh's conductors to enable direct patching attacks on the mesh.

4.3.7 Results summary

A table representing which features discussed in the sections above we found in which of our samples can be found in Table 2. Overall, we commonly found a combination of a rigid PCB mesh in the specimen's main PCB and flexible meshes formed into a lid structure above its main PCB. The mesh inside the rigid PCB would protect the payload components soldered to the top surface of the PCB such as pin pad buttons or cryptographic coprocessors from probing from underneath, while the flexible mesh lid would protect them from attacks from above or from the side. We only found two specimens that wrapped an entire payload PCB inside of a mesh, the Utimaco datacenter HSM appliance (H30) and an older Ingenico payment terminal (H18). Only the datacenter HSM carried this approach through, its manufacturer going to some length to carefully fold the mesh around corners and the entry point of its Flat Flex Cable (FFC) connections to the outside world to avoid possible weak points there. The payment terminal module had weak points at the corners of the wrapped mesh, and its wrapping pattern only covered five of the six sides of a cuboid, with the remaining side left open to allow for the payload PCB to pass out of the mesh for its external connections.

We found an approximately even split between copper/polyimide FPCs and silver ink printing processes being used for flexible meshes. Printed carbon ink processes were less popular, presumably because they offer no significant cost savings but the resulting mesh has a much higher electrical resistance, limiting possible mesh length.

We found potting was only infrequently used across our sample. We found conductive ink printed meshes commonly used opaque base foils and opaque lacquer cover layers to obscure their features. We found these lacquers to be removable using acetone. In almost all instances the trace structure was easily recognizable from the mesh traces' thickness showing through to the surface of the opaque cover lacquer. In practice it served as

Table 2: Feature matrix of all specimens analyzed. Dots indicate presence of a feature. The figures column lists which figures above contain examples of a particular feature.

Feature	Fig.	Specimen																															
		1	2	3	4	5	6	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	27	28	29	30	31	32		
Mesh Contacts																																	
Elastomeric	5b, 5d	•	•	•	•			•		•		•	•	•		•	•		•		•	•					•	•				•	•
Soldered	5a	•				•	•			•		•				•	•	•			•	•	•	•								•	
Stacking	5d							•									•																
Tactile Dome	5f, 5c						•					•							•		•		•	•									
FPC Connector	5c					•				•	•			•	•	•	•			•		•							•				
Mesh EMI Gasket	5e													•																			
Mesh Material																																	
Rigid PCB	4a	•	•	•		•	•	•	•		•	•	•	•	•		•	•	•		•	•	•	•	•		•	•				•	•
Copper FPC	4b				•	•				•			•	•	•	•		•		•			•	•	•	•		•	•				•
Printed silver ink	4c					•				•				•	•	•			•				•	•	•	•							
Printed carbon ink	4e	•							•																								
Gold	4d																																•
3D Construction																																	
Folded mesh	6a, 6b	•		•	•	•		•	•	•	•		•	•	•		•	•	•		•		•	•	•		•		•				•
House of cards	6d	•						•		•							•																
Laser Direct Structuring	6e																																•
Thermoformed	6c, 7						•					•	•										•	•									
Planar obstacle	8a, 8b	•				•	•						•	•			•	•					•	•									
Complex planar	8c, 8d					•								•									•										
Obscurity Features																																	
Metal enclosure	6a		•	•	•			•								•				•						•		•					
Potting	9c					•											•											•	•				
Opaque foil	5f					•	•		•	•			•				•		•		•		•	•				•					
Opaque lacquer	7					•	•					•				•		•		•		•	•	•				•					•
Other Features																																	
Integrated tactile domes	5f					•	•					•				•				•	•	•				•							•
Integrated contact pads	5c												•			•			•		•					•							

electrical insulation, but did not convey meaningful protection against reverse engineering.

5 Discussion

In our survey, we have seen the technological state of the art to which TSMS have evolved since the earliest designs evidenced in patents from 150 years ago. While mesh manufacturing technology has experienced some advancements from historical wire-wound meshes to modern meshes always being constructed in printed circuit processes, mesh monitoring approaches have received surprisingly little attention through the centuries and even in recent, state-of-the-art systems, a simple comparator monitoring a mesh arranged in a bridge configuration is still considered sufficient in high-security applications [36].

5.1 Mesh construction techniques

We found that in almost all cases, practical TSMS are constructed using standard manufacturing processes. In some card payment terminals, we found meshes that used slightly customized standard processes and e.g. integrated a mesh layer produced in a carbon printing process into a membrane keypad, but customizations were minimal. We only found one mesh manufactured in a bespoke process in the datacenter HSM appliance we examined, and that bespoke process turns out to be a turnkey solution used by at least two HSM vendors. Underscoring stagnating development in the field, this particular mesh manufacturing process seems to have seen only minimal changes since the first patents covering it were published in the late 1990s [33, 34, 36].

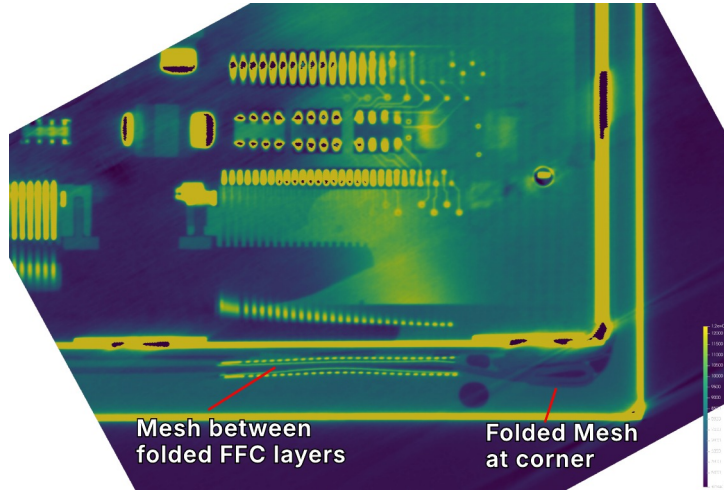


Figure 10: Computed Tomography (CT) scan of a corner of the PCIe HSM module from a Utimaco rackmount HSM appliance (specimen H30). Visible are several capacitors, the edge of a large IC, and a large Flat Flexible Cable (FFC) connector. Two layers of metal enclosures with resin potting in between are visible, and the security mesh can be seen folded between layers of the folded FFC cable connecting to the outside.

We found that pressure-sensitive connectors such as tactile domes or elastomeric connectors are effective in providing an inherent protection against disassembly.

5.2 Mesh monitoring circuits

We observed that in general, academic research leads before patent literature, which is ahead of actual implementations in the field. Practical monitoring circuitry seems basic. Particularly the datacenter HSM appliance we examined (specimen H30) showed a contrast between a mesh manufactured in a bespoke process combined with an unsophisticated, discrete monitoring circuit based around a number of voltage comparators [36].

5.3 Computed Tomography Imaging

CT imaging presents a serious threat to any HSM design that relies on its mesh layout remaining secret. For instance, the Gore TSM product used in IBM and Utimaco HSMs includes a feature where after production, small vias are lasered into a specially prepared area on the mesh foil to randomize the connection pattern of the mesh on a unit-by-unit basis. CT imaging could be used to discern this type of customization. Furthermore, CT imaging can be used to provide sub-millimeter accurate positioning for an attack, even if the specimen to be attacked has large production tolerances. We found that CT imaging can be made more difficult using three complementary techniques.

Low-contrast trace materials. CT imaging can be made more difficult by manufacturing the mesh with very thin conductive traces, and using a trace material that has low atomic number, corresponding to low X-ray absorption. For instance, the Gore mesh specimen used a carbon-based ink that judging by structure size was screen-printed, which leads to an economical yet relatively secure solution [2, 42].

Use of X-ray attenuating materials. We found that placing any highly X-ray attenuating material in the HSM makes CT imaging more difficult. Figure 10 shows a CT image taken

from a Utimaco HSM. The device has two thick metal layers with a potting resin and the TSM in between, so high-energy X-rays were necessary to penetrate both metal layers and image the device. As a result, the contrast on X-ray-transparent features like polymers is low. In comparison, the Ingenico specimen was easy to image since it consisted of a PCB wrapped with a mesh foil and encased in resin inside of an injection-molded plastic enclosure. Thus, we were able to image it at a low X-ray energy and we were able to easily reconstruct detail on both the mesh's layout and the PCB's circuitry. To apply X-ray dense materials for defense in a practical design, a sheet made from elementary tin or a tin alloy would be a suitable choice for such an X-ray absorbing feature since tin is cheap, non-hazardous and absorbs X-rays almost as well as lead. Alternatively to a sheet-metal enclosure, an X-ray absorbing material could also be incorporated into a potting compound as a powder.

Size. Finally, we found that a larger module size makes CT imaging more difficult simply due to the thickness of material that the X-rays need to penetrate. Ideally, an HSM should aim for a cuboid form factor, as the common flat construction style is easily penetrated by X-rays along at least one axis.

Radiation sensors. Besides engineering techniques making CT imaging harder, in battery-powered devices with active tamper sensing, CT imaging can be actively detected to trigger a tamper alarm. During CT imaging, a large amount of high-energy X-ray images are taken. X-ray radiation can be reliably detected using off-the-shelf sensors that usually consist of a large-area photodiode coupled to a scintillator crystal converting X-ray photons to visible light.

6 Conclusion

In this survey, we have analyzed Tamper Sensing Mesh (TSM) construction techniques in a wide range of payment terminals as well as some other devices. Meshes are commonly implemented as part of both rigid (PCB) and flexible (FPC) circuit boards, either standalone, or embedded into PCBs carrying other components. Silver or carbon trace patterning techniques that are normally used for membrane keyboards are also used in some meshes, but are limited in their structure size. The meshes we found in the wild almost never push the boundaries of achievable structure size for a given process.

The strongest systems we found used potted meshes where removing the potting destroyed the mesh's traces. Ink printed circuits like they are used for keyboard matrices performed well in this regard but are limited in structure size. Copper FPCs are commonly used for meshes, and perform less well in this aspect. From our observations, we derive the following set of design recommendations that we propose as a baseline for mesh development and security evaluation:

1. Use a standard lithographic FPC process without soldermask.
2. Use opaque potting compounds and adhesives that adhere strongly to mesh traces.
3. Design to the smallest manufacturable structure size, no more than 100 μ m.
4. Use at least two mesh layers with offset patterns.
5. Aim for $\geq 20\times$ structure size spacing between mesh layers, and between payload and mesh.
6. Cover all sides and ingress points. Overlap meshes at corners and edges.

Our core finding across real-world devices is that for academic research on mesh manufacturing, monitoring or attacks on meshes, realistic tamper sensing mesh samples can easily be created using commercial manufacturing processes. We observe that across application domains, TSMs often use basic construction techniques for both the mesh itself and for its monitoring circuit.

Acknowledgements

We thank Heidi Schweitzer, Holger Hoche and Prof. Matthias Oechsner from MPA-IfW for capturing and providing CT data of the HSM samples.

References

- [1] (US) National Institute of Standards and Technology. *Security Requirements for Cryptographic Modules*. Federal Information Processing Standard (FIPS) 140-3. U.S. Department of Commerce, 2019-03-22. DOI: [10.6028/NIST.FIPS.140-3](https://doi.org/10.6028/NIST.FIPS.140-3) (cit. on p. 4).
- [2] Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed. Wiley, 2020-12-22. DOI: [10.1002/9781119644682](https://doi.org/10.1002/9781119644682) (cit. on pp. 3, 4, 7, 19).
- [3] Davide Andrea. *The Electronic Connector Book*. 1st ed. 2022. ISBN: 978-1-300-09248-3 (cit. on p. 13).
- [4] David G. Boak. *A History of U.S. Communications Security (The David G. Boak Lectures), Volume I*. (US) National Security Agency, 1973 (cit. on p. 2).
- [5] David G. Boak. *A History of U.S. Communications Security (The David G. Boak Lectures), Volume II*. (US) National Security Agency, 1981 (cit. on p. 2).
- [6] William L. Brodsky et al. “Circuit Layouts of Tamper-Respondent Sensors”. U.S. pat. 10136519B2. International Business Machines Corp. 2018-11-20 (cit. on p. 2).
- [7] Ashton Carter et al., eds. *Managing Nuclear Operations*. Washington, D.C: Brookings Institution, 1987. 751 pp. ISBN: 978-0-8157-1313-5 978-0-8157-1314-2 (cit. on p. 2).
- [8] Mario Cesana and Roberto Zavatti. “Tamper Resistant Card Enclosure with Improved Intrusion Detection Circuit”. U.S. pat. 20010056542A1. International Business Machines Corp. 2001-12-27 (cit. on pp. 2, 4).
- [9] Mario L. Cesana, Donald S. Farquhar, and Martino Taddei. “Security Cloth Design and Assembly”. U.S. pat. 6982642B1. International Business Machines Corp. 2006-01-03 (cit. on p. 2).
- [10] Charles T. Chester. “Improvement in Protecting Safes and Vaults from Burglars”. U.S. pat. 106324A. 1870-08-16 (cit. on pp. 2, 3).
- [11] Douglas A. Clark. “Tamper Detection System for Securing Data”. U.S. pat. 6895509B1. Pitney Bowes Inc. 2005-05-17 (cit. on p. 2).
- [12] Corneliu P. Cobianu, Ion Georgescu, and Viorel-Georgel Dumitru. “Large Area Distributed Sensor”. U.S. pat. 20080001741A1. Honeywell International Inc. 2008-01-03 (cit. on p. 2).
- [13] Timothy E. Cook and Gerald Thomas Wardrop Jr. “Tamper Detection Circuit Assemblies and Related Manufacturing Processes”. U.S. pat. 10579833B1. Thales eSecurity Inc. 2020-03-03 (cit. on p. 2).

- [14] Claude Société Civile S. P. I. D. Dalphin. “Enceinte Protégée Avec Interrupteur Électrique et Son Application”. European pat. 0231549A1. Telecommunications Radio-electriques et Telephoniques SA TRT, Philips Gloeilampenfabrieken NV, Koninklijke Philips Electronics NV. 1987-08-12 (cit. on p. 4).
- [15] 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 (cit. on p. 3).
- [16] Hartmut Droege et al. “Sicherheitsmodul Mit Einteiliger Sicherheitsfolie”. German pat. 19600769A1. International Business Machines Corp. 1997-07-17 (cit. on p. 2).
- [17] Arcadi Elbert and Alvin Diep. “Secure Circuit Assembly”. U.S. pat. 20060259788A1. Individual. 2006-11-16 (cit. on p. 2).
- [18] “Elektrische Sicherheitseinrichtung Zum Schutze von Geldschraenken u. Dgl”. German pat. 559905C. Individual. 1932-09-26 (cit. on p. 4).
- [19] Conrad S. Ham and Elwood R. Horwinski. “Printed-Circuit Type Security Apparatus for Protecting Areas”. U.S. pat. 3594770A. Lewis Engineering Co. 1971-07-20 (cit. on pp. 2, 4).
- [20] Kjell Heitmann, Douglas Clark, and Paul Perreault. “Tamper Barrier for Electronic Device”. U.S. pat. 20050161253A1. Pitney Bowes Inc. 2005-07-28 (cit. on p. 2).
- [21] Kjell A. Heitmann, Douglas A. Clark, and Paul G. Perreault. “Method of Making Tamper Detection Circuit for an Electronic Device”. U.S. pat. 7475474B2. Pitney Bowes Inc. 2009-01-13 (cit. on p. 2).
- [22] Maxim Hennig et al. “Apparatus and Method Comprising a Carrier with Circuit Structures”. U.S. pat. 14867889. Fraunhofer Gesellschaft zur Foerderung der Angewandten Forschung eV. 2020-03-17 (cit. on p. 3).
- [23] Paul Horowitz and Winfield Hill. *The Art of Electronics*. Third edition, 21st printing with corrections. Cambridge, New York: Cambridge University Press, 2024. 1230 pp. ISBN: 978-0-521-80926-9 (cit. on p. 4).
- [24] Vincent Immler et al. “B-TREPID: Batteryless Tamper-Resistant Envelope with a PUF and Integrity Detection”. In: International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2018-04, pp. 49–56. DOI: [10.1109/HST.2018.8383890](https://doi.org/10.1109/HST.2018.8383890) (cit. on p. 3).
- [25] Vincent Immler et al. “Secure Physical Enclosures from Covers with Tamper-Resistance”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018-11-09), pp. 51–96. DOI: [10.46586/tches.v2019.i1.51-96](https://doi.org/10.46586/tches.v2019.i1.51-96) (cit. on p. 3).
- [26] “Improvement in Electro-Magnetic Envelopes for Safes, Vaults”. U.S. pat. 110362A. 1870-12-20 (cit. on p. 2).
- [27] International Atomic Energy Agency. *Safeguards, Techniques and Equipment*. Vol. 1. International Nuclear Verification Series. 2011. ISBN: 978-92-0-118910-3 (cit. on p. 2).
- [28] *ISO/IEC 19790:2025*. ISO. URL: <https://www.iso.org/standard/82423.html> (visited on 05/15/2025) (cit. on p. 4).
- [29] Richard J. Joyce and Allan R. Kramer. “Method to Detect Penetration of a Surface and Apparatus Implementing Same”. U.S. pat. 5568124A. Hughes Aircraft Co. 1996-10-22 (cit. on p. 2).
- [30] Theodoor A. Kleijne. “Security Device for the Secure Storage of Sensitive Data”. U.S. pat. 4593384A. NCR Corp. 1986-06-03 (cit. on p. 2).

- [31] Kruse Sicherheitssysteme. *Datenblatt KRUSE FW-Schlüsseldepot Basic*. 2018-12. URL: https://kruse-shop.de/media/pdf/e3/c0/6c/MA-KRUSE-FW-Schluesseeldepot-FSD-D-E_Rev1-3-20-12-18.pdf (visited on 10/30/2025) (cit. on p. 3).
- [32] LPKF Laser & Electronics AG. *LPKF LDS: Laser Direct Structuring for 3D Molded Interconnect Devices*. 2014. URL: https://www.lpkf.com/fileadmin/mediafiles/user_upload/products/pdf/EQ/3D-MID-LDS/brochure_lpkf_laser_direct_structuring_en.pdf (visited on 11/07/2025) (cit. on p. 12).
- [33] Hugh MacPherson. “Tamper Respondent Enclosure”. U.S. pat. 5858500A. WL Gore and Associates Inc. 1999-01-12 (cit. on pp. 3, 18).
- [34] Hugh Macpherson. “Improvements in Security Enclosures”. European pat. 0540139A2. WL Gore and Associates UK Ltd. 1993-05-05 (cit. on pp. 3, 18).
- [35] mikeselectricstuff. *Neopost Postal Franking Machines*. 2023-10-03. URL: <https://www.youtube.com/watch?v=e07AoHI2Tpk> (visited on 02/17/2025) (cit. on p. 7).
- [36] 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. DOI: [10.1007/s41635-018-0045-2](https://doi.org/10.1007/s41635-018-0045-2) (cit. on pp. 3, 18, 19).
- [37] Johannes Obermaier, Vincent Immler, and Robert Hesselbarth. “PUF-film and Method for Producing the Same”. U.S. pat. 11586780B2. Fraunhofer Gesellschaft zur Foerderung der Angewandten Forschung eV. 2023-02-21 (cit. on p. 3).
- [38] Paul Perreault, Douglas Clark, and Kjell Heitmann. “System and Method for Installing a Tamper Barrier Wrap in a PCB Assembly, Including a PCB Assembly Having Improved Heat Sinking”. U.S. pat. 20050160702A1. Pitney Bowes Inc. 2005-07-28 (cit. on p. 2).
- [39] Cuong V. Pham et al. “Anti-Tamper Mesh”. U.S. pat. 7947911B1. Teledyne Technologies Inc. 2011-05-24 (cit. on p. 2).
- [40] Mani Razaghi. “Circuit Board to Hold Connector Pieces for Tamper Detection Circuit”. U.S. pat. 10251260B1. Square Inc. 2019-04-02 (cit. on pp. 2, 4).
- [41] Securitas Technology GmbH. *SD-04203RB25-D5*. Setec Sicherheitstechnik. 2019. URL: <https://setec-security.de/wp-content/uploads/2019/11/SD-04203RB25-D5.pdf> (visited on 10/30/2025) (cit. on p. 3).
- [42] Sean W Smith and Steve Weingart. “Building a High-Performance, Programmable Secure Coprocessor”. In: *Computer Networks* 31.8 (1999-04), pp. 831–860. DOI: [10.1016/S1389-1286\(98\)00019-X](https://doi.org/10.1016/S1389-1286(98)00019-X) (cit. on pp. 3, 19).
- [43] Henry M. Sutton, Walter L. Steele, and Michael Coerver. “Electrically-Protected Structure”. U.S. pat. 708093A. Individual. 1902-09-02 (cit. on pp. 2, 4).
- [44] Keith Tolk et al. “Safeguards Sensors and Systems: Past, Present, and Future”. In: *Journal of Nuclear Materials Management* 35.4 (2007-07-01), pp. 101–110. ISSN: 0893-6188 (cit. on p. 2).
- [45] Daniel-Ciprian Vasile and Paul Svasta. “Protecting the Secrets: Advanced Technique for Active Tamper Detection Systems”. In: 25th International Symposium for Design and Technology in Electronic Packaging (SIITME). IEEE, 2019-10, pp. 212–215. DOI: [10.1109/SIITME47687.2019.8990877](https://doi.org/10.1109/SIITME47687.2019.8990877) (cit. on p. 3).
- [46] Karl Weidner and Anton Wimmer. “Hardwareschutz in Form von zu Halbschalen tiefgezogenen Leiterplatten”. Pat. WO2007003227A1 (WO). Siemens Aktiengesellschaft. 2007-01-11 (cit. on p. 14).