Thinking Inside the Box: System-Level Failures of Tamper Proofing

Saar Drimer Steven J. Murdoch Ross Anderson
University of Cambridge, Computer Laboratory
15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
http://www.cl.cam.ac.uk/users/{sd410,sjm217,rja14}

Abstract

PIN entry devices (PEDs) are critical security components in EMV smartcard payment systems as they receive a customer's card and PIN. Their approval is subject to an extensive suite of evaluation and certification procedures. In this paper, we demonstrate that the tamper proofing of PEDs is unsatisfactory, as is the certification process. We have implemented practical low-cost attacks on two certified, widely-deployed PEDs – the Ingenico i3300 and the Dione Xtreme. By tapping inadequately protected smartcard communications, an attacker with basic technical skills can expose card details and PINs, leaving cardholders open to fraud. We analyze the anti-tampering mechanisms of the two PEDs and show that, while the specific protection measures mostly work as intended, critical vulnerabilities arise because of the poor integration of cryptographic, physical and procedural protection. As these vulnerabilities illustrate a systematic failure in the design process, we propose a methodology for doing it better in the future. These failures also demonstrate a serious problem with the Common Criteria. So we discuss the incentive structures of the certification process, and show how they can lead to problems of the kind we identified. Finally, we recommend changes to the Common Criteria framework in light of the lessons learned.

1 Introduction

In this paper we examine the definition and application of security boundaries in tamper-proof systems. Our working example is the UK card payment system, 'Chip and PIN', which is an implementation of EMV (the EuroPay, MasterCard and Visa protocol suite) [23]. We show how two models of PEDs fail to protect against tampering and demonstrate real, practical, low-cost attacks. The attacks highlight problems throughout the entire process of specification, design, certification and deployment.

Smartcards are now replacing magnetic strip cards for point of sale and ATM payments in many countries, to resist counterfeiting. The leading system, EMV, has been deployed throughout most of Europe, and is currently being tested in Canada [40]. In EMV, customers authorize a transaction by inserting a bank smartcard and entering a PIN into a PIN entry device (PED); the PIN is verified by the smartcard, which is in turn authenticated to the PED by a public-key certificate. Transactions may be further authenticated online by the card issuer. The move from magnetic strip to chip has reduced the use of counterfeit cards domestically, but fraud abroad has more than compensated. According to APACS, the UK banks' trade association, the first half of 2007 saw £72.3m of fraud due to counterfeit cards, up 37% from the 2006 figure [6]. The inadequacies of the deployed systems have thus impacted many people.

The contributions of this paper are to expose significant vulnerabilities in two of the most widely deployed PEDs in the UK; to discuss the flawed incentive structure of the certification process; and to propose general design principles that would minimize future occurrences of the types of vulnerability we disclose. We also believe it is in the public interest to inform cardholders of the true security of banking systems, in contrast to the banks' frequently overstated claims. This will encourage improved security and better treatment of customers, who are often blamed for fraud.

The remainder of this section surveys anti-tampering technology. Section 2 describes in detail the flaws we have identified; Section 3 discusses some defenses and their limitations; Section 4 presents our methodology for the analysis of tamper-proof systems; Section 5 discusses why these flaws were not prevented by the extensive certification procedures that PEDs must pass; and finally, we suggest how to improve the evaluation process. Additional pictures and discussion of the tamper proofing of the devices we studied are in the extended version of this paper [21].

1.1 Tampering

To prevent unauthorized access, hardware that processes cryptographic keys and other confidential data often incorporates anti-tampering mechanisms, which may be categorized as follows:

Tamper evident seals allow an examiner to determine if protected spaces have been breached. Seals are usually affixed to an enclosure using an adhesive that reacts to being peeled or torn, to solvents, and to extreme temperatures. It is challenging, however, to create tamper-evident seals that cannot be trivially bypassed, and if users are not trained to detect tampered seals their value is extremely limited [28].

Tamper resistant devices physically hinder unauthorized access. Technologies used include locks, metal barriers, and uniquely-shaped screw heads. Electronic circuits may be 'potted' by encasing them in an opaque solid compound that cannot easily be cut, dissolved, drilled or milled, while being able to conduct heat away from enclosed circuitry and dissipate it.

Tamper response means providing sensors to detect tampering, and associated response mechanisms. Sensors monitor environmental and electrical conditions such as connectivity, light, pressure, temperature, radiation, motion, voltage, clock signals, conductivity, and others; Weingart [44] provides a concise list of such sensors. When a breach is detected, a supervisory circuit responds appropriately.

These techniques are often combined to form tamper-proof systems. The IBM 4758 security module, for example, uses a dense multi-layered mesh of non-metallic conductive grids embedded within a potting compound made of a material with similar visual and chemical properties to the conductors, so that identification and separation becomes more difficult [36]. The whole assembly is encased in a hard metal shell to prevent accidental damage and to minimise electromagnetic interference and leakage.

A common response mechanism is *zeroization*, where secret data is deleted. *Passive* zeroization involves disconnecting power to volatile memory such that content is lost, while *active* zeroization overwrites data. Passive zeroization may not be sufficient because of data remanence, where previously stored state remains in RAM cells and other storage media after they have lost power. Ionic contamination, hot-carrier effects, and electromigration can 'imprint' the stored state over time [24, 25], and extreme temperature or voltage may cause RAM content to remain for seconds or even minutes after power is removed [34].

Although very little work has been published on mid-range, relatively cheap security modules, such as PEDs and payment terminals, there is some literature on the more expensive high-end security modules, such as those protecting the bank master keys used for PIN verification. In 1983, Chaum [17] provided design concepts for tamper proofing systems using a layered approach, most of which still remains relevant today, although some of the terminology has changed. To decrease the probability of successful attacks, Chaum suggested that inner-layer sensors be able to also detect tampering of outer layers. In 1990, Weingart *et al.* [45] offered evaluation criteria for security modules, which take into account the environment and value of the protected modules; these criteria later formed the basis for NIST's FIPS 140-1. In 1999, Smith and Weingart [36] described the tamper proofing and the API design of the first FIPS 140 Level-4 approved security module, the IBM 4758. A year later, Weingart surveyed known tamper-proofing techniques and state-of-the-art attacks [44]. Anderson *et al.* [2, 4] surveyed the security of cryptographic processors and the importance of equally robust APIs. Smith [35] discussed the very relevant disconnect in the minds of protocol designers between the assumed and actual security of secret storage in the real world. Both Bowles *et al.* [13] and Yang *et al.* [46] surveyed possible vulnerabilities and protection mechanisms in PEDs in a general sense, but stopped short of studying deployed models to find and demonstrate existing attacks and flaws, especially in the context of EMV and the certification process. And following the deployment of EMV in Britain, Anderson *et al.* [1] discussed security problems associated with its design, including the application of relay attacks to EMV, which were later implemented by Drimer and Murdoch [20] using custom hardware combined with a fake PED.

Our work pushes this forward, first, by considering the intersection of physical security, protocol design and the banking transaction environment; second, by looking at low-cost PEDs that operate in an uncontrolled environment yet must protect information valuable to third parties; third, by showing how individual anti-tampering mechanisms must be considered in the context of the system as a whole; fourth, by discussing the implications for design and assurance of the vulnerabilities we find; and finally, by examining the implications for certification schemes such as the Common Criteria. We did this work as independent researchers not beholden to any external interests.

2 Real world failures in tamper-proofing

For backwards compatibility, cards in the UK have both a chip and magnetic strip; the strip is used in ATMs without chip readers or when the chip is unreadable. Thus a criminal who learns the contents of the magnetic strip and a cardholder's PIN can withdraw cash by causing an ATM to fall back to the older system, or by using a copy of the card in an ATM in a country such as the USA that has not adopted EMV. A copy of the magnetic strip is stored on the chip in its public-key certificate and is sent to terminals (for backward-compatibility reasons), so PEDs must therefore protect not just PINs entered by cardholders but also card details. There may also be symmetric keys, used to protect communication between the PED and the bank, but these are outside the EMV protocol.

Merchants have free access to PEDs (as do corrupt employees); customers sometimes have access for long enough to tamper with them [19]; and fraudsters have impersonated service engineers to gain access [9]. Thus the PED must be assumed to operate in an uncontrolled environment, and must also fulfill its protection goals subject to assumptions about attacker capabilities defined in certification criteria. Currently the most economically important threat is that if the PIN and card details are intercepted when they are sent, unencrypted, between the card and PED, a fake magnetic strip card may be created. As European bank customers do not in general enjoy the consumer protection that Regulation E affords to USA bank customers, they are routinely accused of negligence or even complicity in fraud. This creates a moral hazard in that the PED is purchased by the merchant from a list of devices approved by the banks, yet its role is to protect the cardholder. This makes PED security a matter of public interest, and there are also interesting constraints on PEDs: they must protect valuable secrets in an unsupervised environment, while being cheap enough to be affordable by all merchants.

For analysis, we purchased two each of the Ingenico i3300 [26] and Dione Xtreme [38] (now branded as VeriFone) PEDs, one for reverse engineering and another for implementing the attacks. Each of those was obtained online for under \$20 – thus, in practice, the sale of PEDs is not restricted. What we found validated our suspicion, in that the most widely deployed PEDs in the UK appear to protect bank and merchant secrets well, yet leave customer card details and PINs inadequately protected.

Both terminals have passed the Visa PED evaluation, which requires that the terminal meet one of four alternative requirements (that defeating the tamper-detection would cost over \$25,000 per-PED; or that inserting a PIN-stealing bug would be detected, or take more than ten hours, or cost over \$25,000) [41, p5, A8]. Neither terminal meets any of these requirements. In the case of the APACS PED 'Common Criteria' evaluation (which the Ingenico device also passed), the Protection Profile requires that "The [security function] shall resist physical attacks based on addition of any PIN tapping device to the PIN Entry Device and Card Reader by {selection: providing the capability to detect such attacks with a high probability, automatically responding such that the [security policy] is not violated}" [5, p 32, 5.1.4.4]. Again, the Ingenico device clearly fails. The remainder of this section will show how.

2.1 Anti-tampering mechanisms

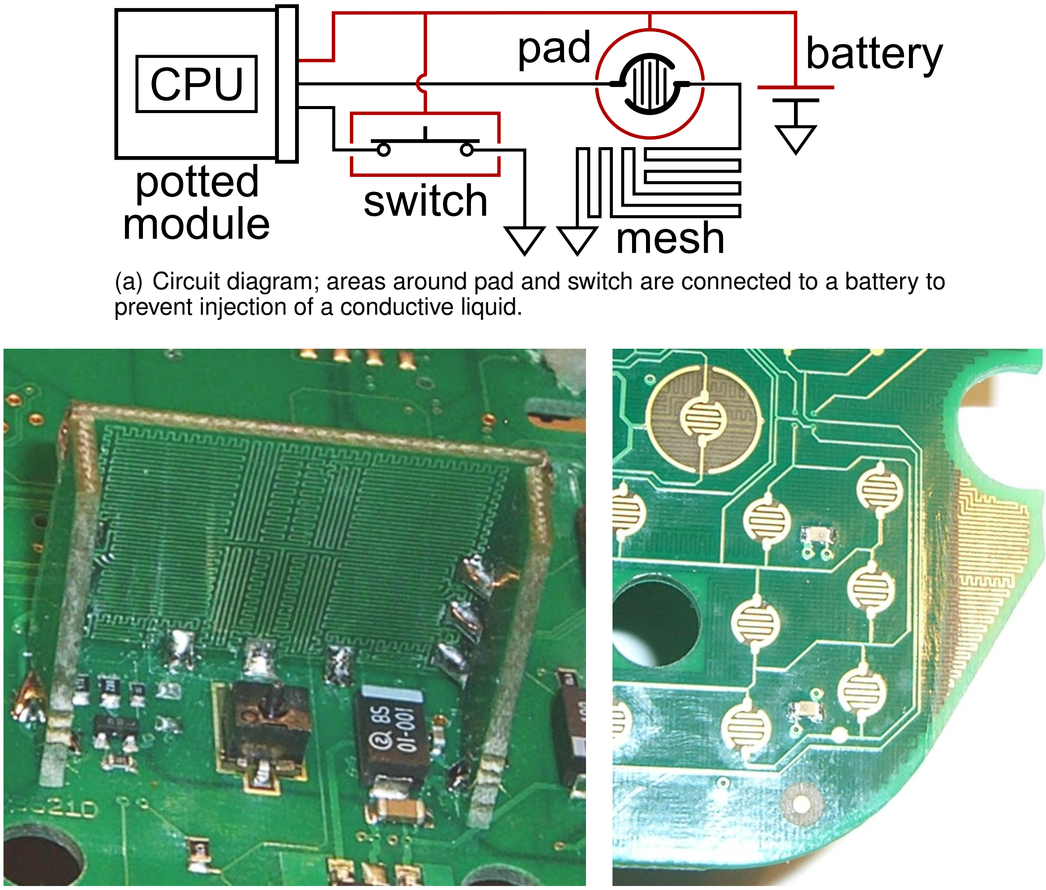
The Ingenico PED's enclosure is made from two plastic shells attached to each other by four 'Torx 6' star-head screws possibly intended to discourage casual opening. A tamper-response switch is released upon opening the shell, and breaks a supervisory circuit, as shown in Figure 1(a). One entire internal circuit board layer is a dense sensor mesh that is intended to detect drilling from the rear of the PED. This sensor mesh extends to a three-sided wall that protects the switch from drilling through a user-accessible compartment (shown in Figure 2(a)). Additionally, four contacts (one of which is shown in Figure 1(b)) are pressed by the enclosure's top shell, so as to alarm if the keypad panel is removed. The contacts are surrounded by a conductive ring connected to the battery supply; this is presumably to prevent the attacker from defeating the mechanism by injecting a conductive liquid. The processing module is gift-wrapped with a coarse sensor mesh and then potted.

The Dione PED is ultrasonically sealed at seven interlocking plastic joints, and has a simple pad shorting a contact to detect opening. Unlike the Ingenico PED, it has no mechanisms to detect drilling from the rear (the designers even provide easily accessible circuit board pads to short the tamper detection mechanism). However, the main processing unit and the keypad are potted together, which makes it harder to capture PIN keystrokes between the keypad and the processor.

In both designs the secure storage for cryptographic keys is fairly well protected. However, in each case it is possible to tap the data line of the PED-smartcard interface. The data exchanged on this line is not encrypted [12]; it yields both the information we need to create a fake magnetic-strip card and the PIN to use with it.

2.2 Signal eavesdropping attack

We defeated the Ingenico PED with a simple 'tapping attack' thanks to a succession of design flaws. Its rear has a user-accessible compartment, shown in Figure 2(a), for the insertion of optional SIM-sized cards to expand its functionality. This space is not intended to be tamper-proof, and when covered it cannot be inspected by the cardholder even if she handles the PED. This compartment gives access to the circuit board and many signals that are routed on its bottom layer, though the sensor mesh layer mentioned earlier prevents the attacker from drilling the PCB to access more sensitive routes, such as the smartcard's data line. Curiously, however, the PED's designers opted to provide the attacker 1 mm diameter holes and other vias through the PCB. The holes are used for positioning optional surface-mount sockets; none of the PEDs we examined had these sockets populated. Other exploitable vias do not seem to serve any obvious electrical purpose. Through one of these holes, a simple metal hook can tap the serial data line. This tap is easy to place between the microprocessor and the card interface chip. We preferred, however, to tap the signal before the interface chip, and found that a 1 mm diameter via, carrying the data signal, is easily accessed using a bent pa-



(a) Circuit diagram; areas around pad and switch are connected to a battery to prevent injection of a conductive liquid.

(b) Actual circuits; tamper response switch with a surrounding protective mesh wall; the whole printed circuit layer is covered with a sensor mesh.

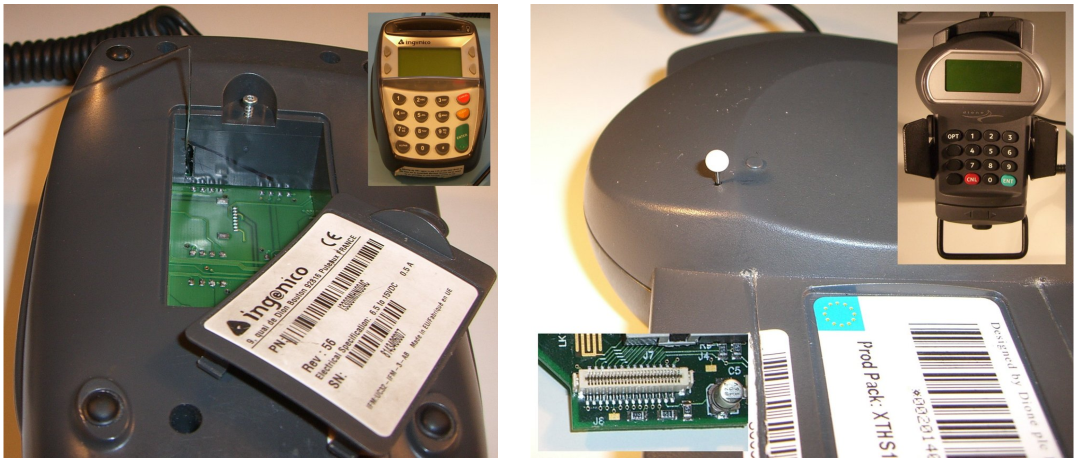
Figure 1. Tamper detection mechanisms of the Ingenico PED.

perclip. This can be inserted through a hole in the plastic surrounding the internal compartment, and does not leave any external marks.

Having tested this attack in the laboratory, we repeated it in the field for the BBC 'Newsnight' programme; we tapped a terminal from a London shop and, during a transaction, extracted the card and PIN details for a journalist's card without triggering the tamper detection system.

The Dione PED does not provide a concealed compartment to hide the wiretap, but is still vulnerable. By drilling a 0.8 mm hole from the rear, we can insert a 4 cm needle into a flat ribbon connector socket shown in Figure 2(b). Figure 3 shows the full Dione attack, with the PED mounted, as it would be in a shop, with a thin wire connected to an FPGA board that translates the data and sends it to a laptop; the scope and laptop screen show an 'answer to reset' (ATR) initial exchange intercepted using the tap.

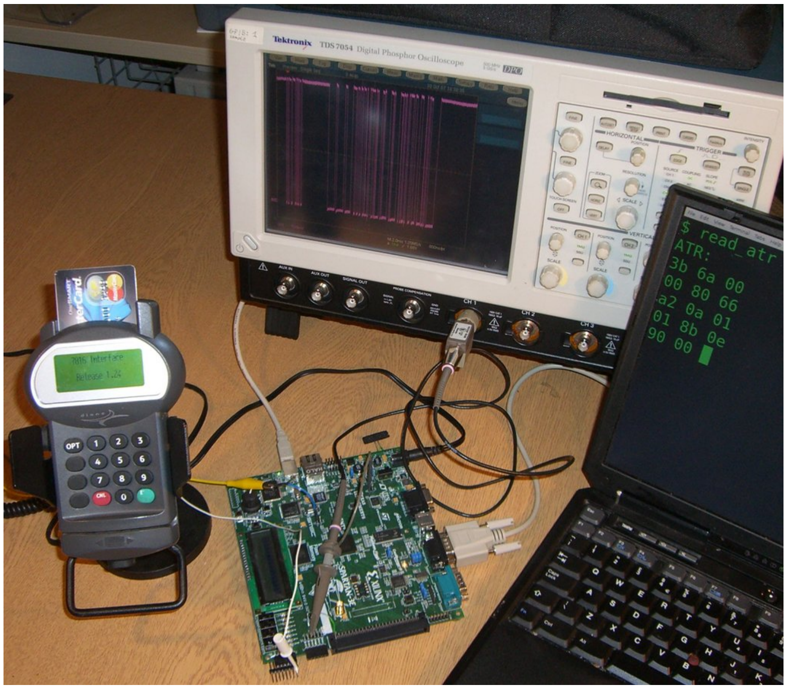
What should have required $25,000 needed just a bent paperclip, a needle, a short length of wire and some creative thinking; attaching them to the data line takes minutes with some practice. A small FPGA or microcontroller board with some non-volatile memory can easily fit inside the Ingenico PED's compartment and record transaction details without the cardholder's knowledge, while a wire routed from the back of a mounted Dione PED to a recorder under the counter will not be detected unless the cardholder conducts a very close inspection – and knows what to look for. The recording circuit can be very small and either battery operated or attached to the PED's power supply; with a full transaction requiring about 1 kB of storage, even a small memory can record thousands of transactions. Detecting such a tap from within the PED is extremely difficult, since high input-impedance probes do not significantly distort signals, and proper termination suppresses reflections; Bond [12] has shown that even without these measures a tap outside the terminal is not detected, while Drimer and Murdoch [20] showed that PEDs can drive 1.5 m cables placed between the card slot and a card.



(a) A paperclip is shown inserted through a hole in the Ingenico's concealed compartment wall to intercept the smartcard's data. The front of the PED is shown on the top right.

(b) A needle is shown inserted through the rear of the Dione PED for data interception, attaching to a ribbon cable connector shown on the bottom left; a mounted PED is in the top right.

Figure 2. Tapping attacks on working Ingenico and Dione PEDs.



```
$ read_atr
ATR:
3b 6a 00
00 80 66
a2 0a 01
01 8b 0e
90 00
```

Figure 3. An implemented attack on a Dione PED. The white wire is connected to the FPGA board, which sends the signals to the laptop via RS232; the ATR message can be seen on the scope and laptop displays. The yellow wire is ground from the power supply.

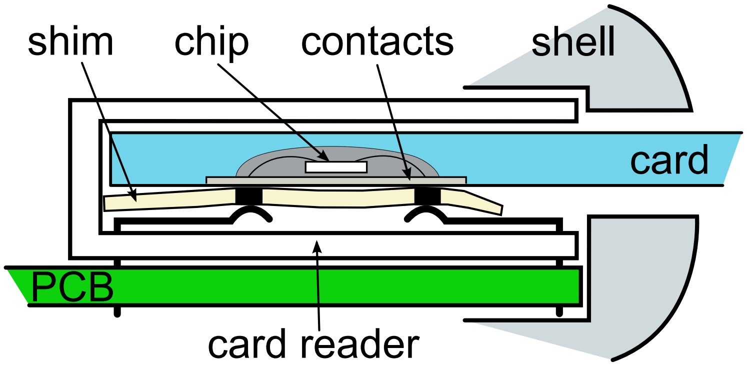


Figure 4. A flexible circuit board placed between the card and card-reader contacts transmits transaction details to a nearby receiver; low profile components in the reader are used to create a simple transmitter.

2.3 Shim-in-the-middle attack

We postulate, but have yet to implement, an attack of inserting a thin, flexible circuit board into the card slot, so that it lodges between the reader and the card's contacts. This 'shim-in-the-middle' attack is illustrated in Figure 4; a very basic circuit that can transmit the signal on the data line to a nearby receiver would not be easily detected by a cursory inspection, because it is within the PED itself. The fraudster can create an 'inserter card' with the shim attached to it so that, when inserted into a particular device, the shim locks into place as the carrier card is removed. A receiver is then placed nearby to record card details and PINs; this receiver could easily include a mobile phone to SMS the proceeds back to the fraudster.

This attack completely bypasses all tamper protections and does not even require the participation of anyone in the store. None of the PEDs we examined appeared to contain any countermeasures to the shim attack, and it's rather hard to imagine what they might be. If the PED vendor included a LED and a photocell, for example, the shim designer would just use a transparent material. One option is to make the card slot transparent – though this means dumping liability on unsuspecting cardholders. (A better, but not infallible, option is PIN encryption, as we'll discuss later.) Note that a corrupt merchant may also prefer this type of attack, as he can indignantly deny all knowledge of it in the unlikely event that the police find the shim.

2.4 Further attacks and observations

The Visa PED certification criteria [41] insist that an attacker not be able to hijack the display so as to prompt the user to enter a PIN at any other time than intended, or to tap the keypad interface to capture PIN keystrokes. We have not seen any special protection given to those interfaces though the need to access multiple wires would make an attack harder (unless more tamper proofing mechanisms are defeated). The keypad interface on the Dione PED is better protected than Ingenico's because it is potted, though the display interface goes through the same connector we tap for the smartcard's data line. Furthermore, the Dione PED is also a magnetic-strip card reader and a similar tap attack can be made on that interface (though that would not reveal the PIN).

Even if the PED were tamper-proof, pressure sensors in a mat under it may be able to triangulate key-presses [29, p132]. Another risk is that some PEDs don't encrypt the data they send to the bank, so a crooked store employee can get the card data in clear from the local network and observe the PIN using the Mark 1 human eyeball (this attack appears to have been widely used in fuel stations, where CCTV has also been used to capture PINs).

A further possible attack is terminal replacement. Some terminals are handheld devices that communicate via wireless to a base station; yet the shopkeeper has to trust the terminal display as to whether payment has been made. A villain could walk into a jeweler's shop, do a transaction at which he swaps the terminal for an identical one that he's programmed to accept bogus cards too, then send in accomplices with bogus cards to buy expensive goods [30]. (Banks even advise merchants not to look at a PED while the customer is using it.) Other PEDs are connected to stores or even bank counters using a detachable cable, which raises the question of whether a recording device placed between the PED's connector and the cable could do anything creative with the communications.

The primary goal of this research is to protect the cardholder, and our secondary goal is to help merchants make informed purchasing decisions. The publication of this paper by itself should make it harder for banks to blame customers for fraud by claiming systems are secure when they're not. We have successfully performed a live demonstration of the tapping attack and, given our experience, we see no reason why the shim attack would fail or be detected. We also do not think that we are revealing concepts not already known to the bad guys; there have already been attacks using Trojanned terminals [9], and with a price tag of $20 for each PED, all a crook needs is a sense of curiosity and some imagination.

3 Defenses and attack extensions

We analyzed the main products from the market-leading vendors. It may be that newer models are less vulnerable, though the Ingenico PED we examined is still currently offered as standard by Barclaycard. The prompt replacement of insecure devices with more secure models could be prudent; we don't believe that 'patching' these devices is likely to solve the problem. In fact, we just do not believe the interface between smartcard and PED can be protected adequately, so changes in EMV system configuration will be needed. Essentially, the vulnerabilities we exploit are not just a matter of hardware design, but also of the options many banks chose as they implemented EMV.

In our view, EMV is flawed in that it permits unencrypted PIN transfer over the hard-to-defend smartcard interface. Even if cardholders 'take matters into their own hands' by examining PEDs before PIN entry, 'bugs' may be completely concealed in compartments, as with the Ingenico PED, or hidden as shims inside the card slot. Nevertheless, there are some mitigation techniques – although not all are as effective as they might at first appear.

3.1 Encrypted PIN

Our attack reads data as it passes between PED and card 'in the clear'. If both the card and PED support it, EMV permits the PIN to be encrypted under the card's public key. Cards currently issued in the UK do not support this, as banks chose a low-cost EMV option (SDA) where cards do not possess the capability to do asymmetric cryptography. Upgraded cards will prevent a passive eavesdropper from observing the PIN (though card details are still unencrypted). This requires the card be capable of public key operations, so only applies to appropriately configured DDA and CDA cards [23].

However, due to a quirk in the EMV implementation, PIN encryption can sometimes be bypassed. A card advertises its support of encrypted PIN verification by placing an appropriate entry in the cardholder verification method (CVM) list, which is sent at the start of the transaction. In eight out of the 15 cards we examined, the CVM list is not signed, and so may be modified – causing the PIN to be sent unencrypted. This attack can be done by an active tap that selectively alters the communication, forcing a HIGH bit to LOW so that the PED thinks that the card cannot process encrypted PINs, and sends the cardholder's PIN in the clear. Conveniently for the attacker, CVM entries are normally qualified with 0x03, indicating that this applies to all types of transactions, but by flipping a single bit so it becomes 0x01, this entry will be ignored for purchases.

If a full middleman scenario can be implemented, a more sophisticated attack may defeat even signed CVM lists. Here, the attack device impersonates an entirely different card to the PED at the start of the transaction, and presents a CVM list that allows clear PIN entry. Once the customer has entered their PIN and it has been intercepted, the attack device causes the PED to restart the normal transaction. At worst this looks like an intermittent error; in some PED implementations it may be possible to avoid alerting the customer at all.

This attack illustrates that evaluators should consider active attacks too. All of the specifications we have examined appear to consider only passive taps. But there may be some mileage in anti-tampering measures that prevent the communication path from being broken, and where the card or PED checks if the data sent has been corrupted – a more feasible task than detecting passive taps. Protocol defenses are also possible: displaying the cardholder name from the card's certificate on the PIN entry prompt would allow some middleman attacks to be detected.

3.2 iCVV

We mentioned above that all of the information needed to clone a working magnetic-strip card from a chip card is transmitted in clear during a normal EMV transaction. This backward-compatibility feature is known to be a serious factor in the fallback vulnerability. Visa has therefore proposed that the card verification value (CVV), a cryptographic checksum stored on the magnetic strip, be replaced with a different one – the 'iCVV' (CVV for Integrated Circuit Cards) – in the card's certificate [39].

Some systems don't check CVVs, but many appear to, and once iCVV is universal a fraudster wanting to make a correct magnetic-strip card would have to recover the true CVV from the mag strip using a 'swipe and dock' reader, or by swiping the card in a separate reader. We strongly support iCVV deployment as it would also reduce the risk of many of the attacks discussed in this paper. But despite Visa's recommendation being made in 2002, and APACS stating that it is mandatory from January 2008, cards are still being issued in February 2008 that store an exact copy of the magnetic strip on the chip.

3.3 Trusted user interface and 2-channel communication

Even once PIN encryption is mandatory, iCVV introduced, and CVVs checked on all magnetic-strip transactions without exception, there remains a further vulnerability – the relay attack [20]. Here, a bogus terminal in one location forwards transaction data to a bogus card in another. The cardholder tries to pay two pounds to a parking-ticket machine in London, but the machine is run by a crook; when she gets her statement she sees a debit for twenty thousand dollars' worth of casino chips in Macao. There are two ways to block relay attacks: either use a distance bounding protocol, or provide a trustworthy user interface. The latter is likely to be more practical in the short term.

One approach, already being deployed in Britain for Internet banking, is to give customers a pocket-calculator sized card reader and keypad, using the Chip Authentication Program (CAP) protocol. This can operate in several modes, but in the most secure variant, the customer inserts their EMV card into the calculator and types in their PIN, the transaction value and the recipient's account number. The EMV card then computes a code that is shown on the calculator screen and which the customer types into their PC; this is verified online by their bank. CAP keeps the card and PIN within the cardholder's trust boundary, and provides strong authorization of the transaction. However, it may present usability problems even for occasional use in home banking, and is likely to be quite unusable in a fast-moving environment such as a train station or supermarket.

If fraud continues to rise, might customers eventually be asked for a CAP code for high-value retail transactions, such as buying a car? Unfortunately, this doesn't really defeat the bad-terminal problem, as a bogus PED could be programmed to work out a CAP code without the cardholder knowing. The critical problem is the card's lack of a trustworthy user interface.

Attempts to solve the trusted interface problem include using a second communication channel, such as SMS [31]. Here, after a transaction has been placed, a text message is sent to the customer's registered mobile phone, which contains the transaction amount, recipient and a code that the customer can release to authorize payment. Again, this may work fine in home banking, but could be tiresome in retail if an SMS took more than a few seconds to get through. In addition, many networks send SMSs in the clear, and even when they don't, their encryption can be broken with some effort; so while two-channel may be reasonable for geographically-dispersed home banking transactions, it may be riskier for transactions concentrated at the attacker's shop.

Furthermore, both the CAP and two-channel approaches would mean reprogramming many hundreds of thousands of PEDs and their supporting infrastructure. Perhaps a better alternative, in which only PEDs would need a software upgrade, is for the PED to provide a trusted path from the card to the customer's mobile-phone display using a 2D barcode read by the phone's camera [10, 18]. In fact there are many options for getting data back and forth between cards, PEDs, phones and customers.

But perhaps the simplest way forward is to skip EMV and move instead to RFID-based payment protocols, as the USA seems poised to do. Here, the customer's credit card can become an application in her mobile phone. The trusted-interface problem is solved, and NFC [27] gives a bidirectional high-bandwidth channel between phone and terminal. Some other issues then require thought – from possible NFC middleperson attacks, through the security of the RFID protocols to malware on the phone – but they are outside the scope of this paper.

4 Security boundaries

While the failures we have presented can be exploited with only moderate technology and know-how (as already used by fraudsters in ATM skimmers), the process that led to these vulnerabilities is far from simple. So it is useful to review what circumstances coincided to make the attacks possible. Superficially, the ability to intercept PIN and card details is due to the anti-tampering mechanisms inadequately protecting the smartcard data line. However, the fact that the PIN is transferred unencrypted is due to a conscious choice by the card issuer to save money. Even if PIN encryption were used, if the card personalization center did not sign the CVM list an attacker can still cause the PIN to be sent in the clear. Finally, the fact that a cloned card is useful is due to magnetic-strip fallback being supported by all banks, and by issuers not implementing Visa's iCVV recommendations.

Hence the task of evaluating a PED depends not just on examining the physical layout of anti-tampering mechanisms, but also on a knowledge of the choices made (or to be made in the future) by the issuer of what protocol to use, what fields to get the card personalization software to sign, the electrical transmission behavior, and the configuration of other payment service providers. It is unreasonable to expect one person to be aware of all these issues unless some effort is made to synthesize them into a concise and coherent piece of documentation. In its absence, each designer may hope that the limitations of their choices will be mitigated by someone else's work.

The root cause of protection failure is not the inadequate design of any one feature, but a poor design and evaluation process. It's just impossible to validate that each module enforces the security guarantees that the other parts of the system require of it, as these guarantees aren't made explicit.

Discussions with an industry insider, involved in designing a product closely related to one that we studied, confirmed our suspicions. The design and verification requirements for individual modules met or exceeded industry best practice. However, designers were given no guidance as to how their module fitted into the overall security architecture.

4.1 The need for a security architecture document

The complexity and fragility of EMV mean that designing a robust tamper-proof PED requires a thorough understanding of the whole fielded system. The EMV protocol suite allows banks to design fairly secure systems, or very insecure ones, depending on the options chosen. Yet although the EMV paperwork describes a lot of detail, there is no one architecture document that a component designer can use to understand the interaction of these options and determine whether their module introduces any critical weaknesses into the local system. The sheer quantity of EMV documentation is also a major impediment. The core specifications are 726 pages long, and there are a further 2,126 pages of testing documentation. Even this is not adequate to understand the whole system, as payment network operators may add additional requirements (Visa publishes another 810 pages). And many security-critical decisions are contained only in local documentation specific to individual banks, which is available only under non-disclosure agreement, if at all. The volume of material, and the many inter-module dependencies, leave much room for interpretation and almost inevitably lead to flawed implementations.

EMV is not the only complex evolving system that includes tamper-resistant components, multiple vendors and perverse incentives on a multi-national scale: other examples range from postal and utility meters through digital tachographs to public-key infrastructures. It would clearly be beneficial if we could find a way to distill down the security-critical information from such systems.

In the old days, system design followed the waterfall model (at least in theory): a top-level requirements document was refined into a functional specification and a systems specification, then implemented and tested. The Common Criteria framework implicitly assumes this model in that it provides the companion documents needed to create and maintain the security case: a security policy is refined into a protection profile, and then into a security target against which the product can be evaluated. However, systems as complex as EMV inevitably involve an iterative design process, and as commercial systems move past the spiral model of limited iteration into evolutionary development, we seem to have neglected to create a mechanism that will enable everyone to keep sight of what the system protection is trying to achieve.

We therefore propose that complex systems such as EMV should have a security architecture document that states clearly and succinctly the threats that the system is supposed to cope with and the mechanisms it will use to do so, tracing these to the major system interfaces. This document should, for systems like EMV on which the public must rely, be a public document. Even in classified systems, it must be available to implementers of every critical component, and short enough that they will read it. They are in the best position to understand what their module achieves, and to take action at design time if needed. For example, the engineers implementing the Ingenico tamper mesh should have had a document that clarified the importance of protecting the serial data link from the card to the PED CPU, and make them think twice about how, where and why they route tracks and create holes/vias in the circuit board.

One way of managing complexity in software systems is abstraction, such as in object-oriented programming, where the internal structure of a component is hidden from its users; only the interface it exposes is relevant [8]. This approach is also taken in the design of networks, where firewalls define a security perimeter; while this does not ensure security by itself, it does at least make analysis easier. Tamper-proof boundaries, in systems like EMV PEDs, ought to be treated in the same way. Now given that architecture depends on APIs, this means finding ways to manage the secure evolution of APIs, and to ensure that everyone involved understands the protection assumptions both above and below each API – so that changes don't create havoc. That's why we believe the missing link should be seen as an architecture document – as a system's architecture is defined by its APIs.

Each suite of mechanisms should implement a particular boundary or API, perform some clear security purpose, and also be a convenient object for abstraction. For each boundary, the following assumptions should be clearly and concisely specified:

- The environment the container is in – what assumptions are made about attacker capabilities and what protection is assured by any outer layers;
- What data items are transmitted to, from or through a tamper-proofed component and what guarantees must be enforced on them;
- What guarantees the container reciprocally provides to its content;
- What protections are provided to any further tamper-proofed containers it encloses.

A summary of the security boundaries should be given, showing how they are interconnected and how protected assets flow. Multiple versions of this document or diagram,

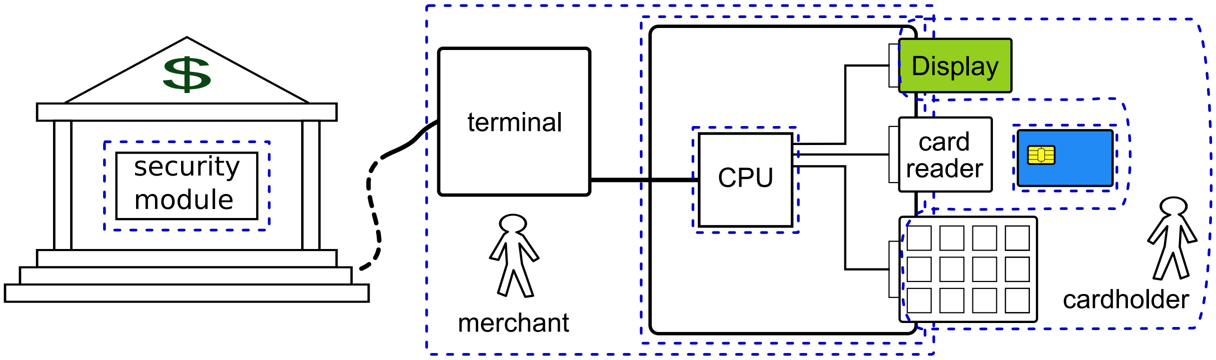


Figure 5. Security boundaries of the payment system environment. The LCD, card reader, keypad and smartcard need to cross boundaries, shown by dotted lines, in order to complete a transaction.

at different levels of detail should be produced for complex systems. At the top level, the documentation of the outermost enclosures are all that is necessary to perform a system evaluation at that level – those boundaries which are completely enclosed by another need not be discussed. However, the detailed documentation for each module should show further depth.

Figure 5 gives an example for the EMV systems we have inspected, and includes the major security boundaries. We have included both conventional anti-tampering measures, such as tamper meshes and lid-switches that protect the CPU and case; we have also included the personal space of the customer and merchant – in the sense that they will not permit unauthorized interference with the card or terminal while it remains under their control.

4.2 Security analysis

Given the above information, security analysis becomes more straightforward. For each asset transmitted, it is easy to find all the boundaries it crosses, which provides a systematic way of working through the possibilities to establish whether those boundaries provide adequate protection. For each container, it is possible to see if the anti-tampering mechanism properly protects both data within it, and any enclosed tamper proof boundaries.

This still does not make the analysis trivial, because it requires detailed work to establish which assets need to be protected against which threats, and whether an individual anti-tampering measure meets its requirements. However, these steps permit experts in individual module design to establish the requirements for their component. This does not eliminate the need for system level analysis, but instead it assists the process – it points penetration testers at possible soft spots.

4.3 Design constraints

If the documentation is more than a few pages long, the likelihood of a flawed system increases. It is not reasonable to expect component designers to faithfully implement a complex set of security rules when they also have to deal with other manufacturing issues, such as cost, aesthetics and reliability. A length limit is a very reasonable requirement – constraining the complexity of the security mechanism greatly increases its chance of success.

Also, where several protocol options affect the data items to be protected, all possible combinations should be set out. This will provide a list of scenarios that designers must check, and by making explicit the combinational complexity of options, help push back on their proliferation. Protocol options, and their negotiation procedures, are a significant factor behind the system flaws we found. (Similar problems have been found in other security applications, such as the cipher-suite and version negotiation of SSL [43].) Even though the EMV specification finds compact ways to describe the plethora of options, a security evaluation must consider every relevant combination.

4.4 Analysis of PED security

Given the above methodology, we now present an example of applying it to EMV PED security, by constraining our analysis to the suite of options used in the UK: no PIN encryption, ubiquitous magnetic strip fallback and no iCVV option. There are four top-level tamper-proof boundaries, shown in Figure 5: the merchant, the PED, the card and the customer. We do not need to discuss the CPU protection, since that is wholly enclosed by the PED, and the bank HSM is outside the scope of this paper. The assets to be protected are as follows:

Card details: Stored by card, sent from card to PED;

PIN: Stored by card, entered by customer into PED and sent from PED to card;
Item value: Displayed on PED screen, for customer.

With the card details and PIN, a fake magnetic-strip card can be produced, so the confidentiality of these must be maintained. Also, if the value displayed on the PED screen does not match that processed by the card, the customer may be defrauded. Here, we only cover the system issues that result from information crossing tamper boundaries. We do not discuss issues such as protecting PED code or root-certificate integrity, since they are internal to the PED system and would be discussed in its documentation.

Given these definitions, it becomes clear where the flaws in EMV lie. The PIN is protected by the smartcard; given a tamper-resistant chip which will lock up after too many incorrect attempts, it cannot be directly retrieved from the card. But the PIN and card details are transmitted through the PED, which may or may not protect one or both of them. Card and PIN data may leak at the card–PED interface, and card data may also leak if the PED–bank link isn't encrypted. Finally, since the customer cannot trust the terminal display, she is vulnerable to relay attacks.

We can also examine defenses. If encrypted PIN verification is used, and unencrypted transmission cannot be forced, we can drop the requirement that the card–PED interface physically protect PIN confidentiality. And if magnetic-strip fallback is not permitted, or the iCVV option is used, the interface need no longer protect card details. But if some banks don't use encrypted PIN and iCVV, then either PEDs have to be robust against shims (perhaps using a full metal enclosure and card-handling machinery, like ATMs) or their customers should be indemnified against the costs of the resulting fraud. And regardless of whether physical or cryptographic security protects the card data and PIN, the trusted interface problem remains. Some combination of technical measures and indemnity must be used to deal with relay attacks.

5 The certification process

The exercise described in this paper has been particularly instructive in teaching us about the weaknesses of Common Criteria evaluations.

Until about a year ago, it was possible for market forces to exercise some discipline on vendors. For example, in 2006, Shell withdrew EMV terminals from its UK fuel stations following a fraud that involved PED tampering, and fell back for some months on magnetic-strip processing [9]. Their PED vendor, Trintech, sold its terminal business to VeriFone and left the market [37]. But since then there has been rapid consolidation, with Ingenico and VeriFone now appearing to control most of the market. In addition, all but the largest merchants tend to get their terminals from their bank; many banks only offer one make of terminal; and the banks have been found guilty in both 1989 and 2005 of insufficient competition on the provision of credit card services to merchants [32, 33].

So customers, and now also merchants, depend critically on the certification of terminals, PEDs, smartcards and other system components used in the EMV system. Some certification schemes merely ensure compatibility, such as EMV Level 1 [22], but there are also extensive security evaluations. Both PEDs we examined are certified under the Visa PED approval scheme [42], and the Ingenico PED passed the APACS PED 'Common Criteria' Evaluation [7] despite the vulnerabilities we identified.

The survey of Yang *et al.* [46], apparently done mostly in 2005, identified the classes of vulnerabilities we have found and also suggested physical mitigation techniques. We found it surprising since their paper acknowledges the co-operation of Ingenico engineers, yet these flaws still exist. But while they talk about points of failure in the abstract, we have shown that these and other failures do exist, can break EMV as deployed, and are easy to find in real PEDs, including Ingenico's. What does that tell us about the evaluation and certification process?

5.1 Why evaluations fail

A security failure in an evaluated product can have a number of causes. The Common Criteria (or other framework) might be defective; the protection profile might not specify adequate protection; the evaluator might miss attacks, or estimate their cost and complexity as too high.

One known problem with the Common Criteria is the proliferation of protection profiles. Anyone can propose a protection profile for any purpose and get a lab to evaluate it. The result is a large number of profiles giving little assurance of anything: for example, the profile for ATMs is written in management-speak, complete with clip art, states that it 'has elected not to include any security policy' and misses many of the problems that were well known when it was written in 1999. Indeed it states that it relies on the developer to document vulnerabilities and includes the vague statement that 'the evaluator shall determine that the [Target of Evaluation] is resistant to penetration attacks performed by an attacker possessing a moderate attack potential' [16].

A deeper problem in the security evaluation process is the economics involved. Since the demise of the philosophy behind the Orange Book [14], evaluation is now performed by a laboratory selected and paid by the device manufacturer. The vendor will naturally select the lab that will give his product the easiest ride and charge the least money. What's more, the same process applies to the protection profiles against which the product is evaluated.

Market competition may help reduce evaluation costs, but it promotes a race to the bottom between the labs. To mitigate this, approved labs must be used, selected by Visa in the case of PED approval, or by a national body such as NIST in the USA or GCHQ in Britain for the Common Criteria. In principle, this might provide some quality control, but in practice the agencies appear never to have de-approved a licensed lab, for fear of undermining confidence in 'the system'. Government agencies may also feel reluctant to drive evaluation work abroad. These concerns were expressed by Anderson [3] who describes a number of cases in the 1990s of clearly mistaken evaluations. The vulnerabilities described in this paper provide a further such case. Was this evaluation failure systemic, or the fault of an individual evaluator?

5.2 Government and industry response

We therefore wrote to GCHQ, Visa, APACS, Ingenico and VeriFone (Dione) in November 2007 with an early draft of this paper and asked them for comments. In February 2008, the BBC's 'Newsnight' programme filmed our research, including an attack that we conducted on a real terminal in a real store and that yielded a journalist's card details and PIN (this was done with consent of both the store owner and the journalist). The imminent broadcast of the programme (26 February 2008) prompted responses from GCHQ, APACS and VeriFone. Ingenico did not respond to our questions and Visa did not even acknowledge receipt of our original disclosure three months earlier (although they did download our paper following our email to them, and one evaluation lab downloaded it from the URL we supplied to Visa). We asked for copies of the evaluation reports, why these reports weren't public, whether the insecure PEDs would be decertified, whether the labs that negligently certified them as secure would lose their licenses, and whether the evaluation system should be changed.

VeriFone's response was evasive, pushing responsibility to APACS, Visa and GCHQ, but the reply from APACS and GCHQ were more instructive. APACS, the bankers' trade association, claimed that previous evaluations *"did not identify any specific vulnerabilities in the devices that required additional mitigation"*; they denied that the evaluations were defective; they said that the devices would not be withdrawn from use as they disagreed with our risk assessment – they said that the attack was harder than we described, and that there were simpler fraud methods.

APACS claimed that *"The numbers of PED compromise that have taken place in the UK are minimal, however, and the banking industry's standard fraud prevention measures have meant that these frauds and their location were detected quickly."* (In two current criminal cases of which we are aware, defendants are accused of stealing eight-figure sums using tampered PEDs.) APACS refused to name the evaluation labs and insisted that the evaluations had to be carried out under non-disclosure agreements. They said, *"we are not aware of any widely recognised and credible evaluation methodology process, in security or otherwise, which makes evaluation reports publicly available."*

GCHQ's response was equally uncompromising but totally different. They informed us that evaluation reports for Common Criteria certified devices must be made public, as a condition of the mutual recognition arrangement. It transpired that the Ingenico device was merely 'evaluated' under Common Criteria, not 'certified' and hence not subject to oversight by GCHQ or any other country's Certification Body (CB). All certified products are listed on the Common Criteria Portal [15], although under the confusingly titled "List of evaluated products". As of February 2008 no PEDs are present on this list.

In fact, the certification for the Ingenico PED was performed by APACS, on the basis of a secret report by an undisclosed laboratory. This laboratory is licensed by a CB to perform certifications, but APACS refused to identify the country in which the lab was registered, and hence which CB was responsible. Had the devices been through certification, it would have been the CB's job to ensure that the security target was appropriate and that proper testing had been carried out. APACS said that the decision of whether the laboratory's license is to be revoked is responsibility of the CB that registered it. But since the PED evaluation was done outside the Common Criteria system, and as far as we know without knowledge of any CB, it is unclear how the errant lab could be disciplined.

As a Certification Body, GCHQ does not object to anyone calling any device 'Common Criteria Evaluated', and will merely object if a false claim is made that a device is 'Common Criteria Certified'. This undermines their brand; it enables organisations such as APACS to free-ride by exploiting the 'Common Criteria' name without either evaluating their products rigorously or publishing the results. GCHQ admits that as the licensing authority it has an interest: *"The CB then has a direct involvement in maintaining the quality of each of the individual evaluations for certification. These mechanisms counter any tendency for such a 'race to the bottom'."* Regrettably, their confidence is not consistent with the research reported in this paper.

For both of these devices, the proximate cause of evaluation failure was that the equipment just didn't meet the protection goals set out in either the Visa certification requirements or the APACS 'Common Criteria' protection profile. A deeper cause was that these requirements were unrealistic; given the shim attack, it's just not clear that any compact low-cost device can be constructed that meets either of them, and so the labs may have been faced with an impossible task. We'd argue that the protection profile should never have assumed that the card–PED interface could be protected at all.

The banks clearly had an incentive to pretend that it could be; by using cheap SDA cards rather than the more expensive DDA/CDA cards, they saved perhaps $1 per card over 70 million accounts. The failure of the CC CB to protect its brand gave them the opportunity to describe insecure terminals as 'Common Criteria Evaluated' without legal penalty. (Indeed one of us has seen banking industry expert witnesses relying on the fact that a terminal was 'certified' in testimony in a case currently before the courts.)

The failure of EMV was multi-factorial: too many protocol options, liability dumping, an over-optimistic protection profile, 'evaluations' funded by vendors, and failures of both markets and regulation at a number of levels. What should be done about it?

5.3 Fixing the evaluation process

Unfortunately, Common Criteria evaluations seem to be most prevalent where incentives are skewed – where one principal operates a system but others bear the costs of failure. This tempts the operator to be careless – a phenomenon known to economists as 'moral hazard'. It's now well known that moral hazard is a major cause of security failure; and evaluation may be sought as a way of avoiding blame for failures by demonstrating due diligence [3].

We believe that the certification process should be re-engineered to take heed of incentives and accountability. In an ideal world, evaluations would be conducted by representatives of the end users. But here, the cardholders and small merchants are not in a position to act collectively. Where evaluation by the relying party is impractical, the next best option might be a hostile laboratory. The closest we often get to this ideal is an evaluation by academics, such as the one in this paper. But the quantity and timeliness of these evaluations falls far short of the optimum: over 200 types of PEDs have been offered for sale in Europe, and this paper is the first open evaluation. Why weren't the other products looked at years ago?

Our experience discussed in this paper, and similar experiences in previous projects, could offer an explanation. The industry's attitude towards independent evaluation is at best unhelpful and at worst actively obstructive. Most importantly, merchants fear that if they are discovered to have assisted in the confirmation of security vulnerabilities, they might face retribution from their bankers. Our co-operation with merchants and other insiders has only been possible when we could protect their identity. In many ways, criminals are in a better position as they can easily set up fake merchant accounts, take higher risks, and be more anonymous than an independent researcher cooperating with a legitimate merchant.

One possible solution is to use markets. People who find vulnerabilities in operating system platforms can sell them into a thriving market: companies such as iDefense and Tipping Point buy and sell such information [11]. The problem for PED evaluations is where the money would come from. Who would be the buyers of PED vulnerabilities?

It does rather look like a certification body of some kind is inescapable in some circumstances. However, if the Common Criteria are to provide the framework, then that brand must be better protected. The certification bodies should register 'Common Criteria' as a trademark, and protect it as vigorously as the banks do theirs. Anyone claiming that a device is 'Common Criteria Evaluated' when it has not been through the full certification process should face having their website taken down for trademark infringement.

Furthermore, given the very strong incentives for vendors to shop around for the easiest evaluation lab, the resulting race to the bottom among labs, and the lack of institutional incentives for the CB to exercise proper discipline, we propose that evaluations of equipment on which the public is forced to rely should in future come with a sufficient reward to motivate independent evaluation. For an evaluation at level EAL3 we propose a mandatory reward of $10,000 for each vulnerability, while for EAL4 the reward should be $100,000.

The introduction of real money will call forth a more socially optimal level of attack effort; while the conditioning of the rewards on responsible disclosure could control any increase in exposure. What's more, we propose that the rewards be paid not by the vendors, nor even by the evaluation labs, but by the certification bodies that license the labs. That way, careless evaluators cost their regulators real money, and are more likely to be disciplined. (The CBs might in turn require vendors to post performance bonds.)

6 Conclusions

Smartcard payments depend on the anti-tampering measures in PIN entry devices. We examined the market-leading products and have found them quite inadequate to protect cardholders. We've shown that it's not enough to concentrate on the design of anti-tampering features. PED designers put a lot of effort into protecting the wrong assets; they appear to have misunderstood the system aspects of attacks. This raises serious questions on the design of tamper-proof systems.

We have therefore proposed an improved design methodology: in particular, complex systems should have a security architecture document to inform all the participants in the design and evaluation process, and protection properties need to be traced across boundaries and interfaces to ensure they don't slip away there. Systems engineering – and indeed computer science – are increasingly about managing complexity; this will be a growing concern of security engineers, and EMV may provide a good case study.

But the failure here was not limited to the technical aspects of the security engineering. Claims that terminals were 'Common Criteria Evaluated' turned out to be almost meaningless; the devices in question were not Common Criteria Certified, and the certification body was not interested in protecting its brand. If the Common Criteria brand is to have any value in the future, other than as a marketing slogan that will be progressively discredited by works such as this paper, the incentives need to be fixed.

Finally, the lessons we learned are not limited to banking. Other fields, such as voting machines, suffer from the same combination of stupid mistakes, sham evaluations and obstructive authorities. Technology alone won't be enough. We need regulatory reform too.

Acknowledgments

We are grateful to Markus Kuhn for providing equipment, and to Richard Clayton and Mike Bond for proofreading and comments. Saar Drimer is funded by Xilinx Inc. Steven Murdoch is funded by the Tor Project and employed part-time by Cronto Ltd.

References

[1] R. Anderson, M. Bond, and S. J. Murdoch. Chip and spin, March 2005. http://www.chipandspin.co.uk/spin.pdf.

[2] R. Anderson and M. Kuhn. Tamper resistance – a cautionary note. In *USENIX Workshop on Electronic Commerce*, pages 1–11, Oakland, California, November 1996.

[3] R. J. Anderson. *Security engineering: A guide to building dependable distributed systems*. John Wiley & Sons, Inc., New York, NY, USA, 2001.

[4] R. J. Anderson, M. Bond, J. Clulow, and S. P. Skorobogatov. Cryptographic processors – a survey. Technical Report UCAM-CL-TR-641, University of Cambridge, Computer Laboratory, August 2005.

[5] APACS. PIN entry device protection profile, July 2003. http://www.commoncriteriaportal.org/public/files/ppfiles/PED_PPv1_37.pdf.

[6] APACS. Fraud abroad drives up card fraud losses. Press release, October 2007. http://www.apacs.org.uk/media_centre/press/03.10.07.html.

[7] APACS: The UK payments association. PIN entry device protection profile common criteria evaluation, September 2007. http://www.apacs.org.uk/payment_options/PINEntryDevices.html.

[8] D. J. Armstrong. The quarks of object-oriented development. *Communications of the ACM*, 49(2):123–128, February 2006.

[9] J. Bale. Shell halts Chip-and-PIN after fraud. The Times, May 2006. http://business.timesonline.co.uk/tol/business/law/article714402.ece.

[10] L. Bauer, S. Garriss, J. M. McCune, M. K. Reiter, J. Rouse, and P. Rutenbar. Device-enabled authorization in the Grey system. In J. Zhou, J. Lopez, R. H. Deng, and F. Bao, editors, *Information Security, 8th International Conference*, volume 3650 of *LNCS*, pages 431–445, Singapore, September 2005. Springer.

[11] R. Böhme. Vulnerability markets. In *Chaos Communication Congress (23C3)*, Berlin, Germany, December 2006. CCC.

[12] M. Bond. Chip & PIN (EMV) interceptor, March 2006. http://www.cl.cam.ac.uk/research/security/banking/interceptor/.

[13] S. Bowles, B. Cuthbert, and W. Stewart. Typical attack techniques for compromising point of sale PIN entry devices. Technical report, Payment Assurance Lab EWA-Canada, September 2005. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper04.pdf.

[14] S. L. Brand. *DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria (Orange Book)*. National Computer Security Center, December 1985.

[15] Brightsight. Common Criteria portal, February 2008. http://www.commoncriteriaportal.org/.

[16] Bull, Dassault, Diebold, NCR, Siemens Nixdorf and Wang Global. *Protection Profile: Automatic Cash Dispensers / Teller Machines*, 1999.

[17] D. Chaum. Design concepts for tamper responding systems. In *Advances in Cryptology (CRYPTO '83)*, pages 387–392. Plenum Press, 1983.

[18] Cronto mobile phone client. http://www.cronto.com/.

[19] S. Drimer. Keep your keypads close, September 2007. http://www.lightbluetouchpaper.org/2007/09/15/keep-your-keypads-close/.

[20] S. Drimer and S. J. Murdoch. Keep your enemies close: Distance bounding against smartcard relay attacks. In *USENIX Security Symposium*, August 2007.

[21] S. Drimer, S. J. Murdoch, and R. Anderson. Thinking inside the box: system-level failures of tamper proofing. Technical Report UCAM-CL-TR-711, University of Cambridge, Computer Laboratory, February 2008.

[22] EMVCo, LLC. *EMVCo Type Approval Terminal Level 1 Test Cases*, December 2002. http://www.emvco.com/.

[23] EMVCo, LLC. *EMV 4.1*, June 2004. http://www.emvco.com/.

[24] P. Gutmann. Secure deletion of data from magnetic and solid-state memory. In *USENIX Workshop on Smartcard Technology*, pages 77–89, San Jose, California, July 1996.

[25] P. Gutmann. Data remanence in semiconductor devices. *USENIX Security Symposium*, pages 39–54, August 2001.

[26] Ingenico. i3300 Keypad, September 2007. http://www.ingenico.com/i3300-i3300_28.html?lg=UK&productId=14#0.

[27] International Organization for Standardization. *ISO/IEC 18092:2004 Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)*, 1st edition, January 2007.

[28] R. G. Johnston, A. R. Garcia, and A. N. Pacheco. Efficacy of tamper-indicating devices. *Journal of Homeland Security*, April 2002.

[29] M. G. Kuhn. Compromising emanations: eavesdropping risks of computer displays. Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003.

[30] M. W. Tobias, personal communication, October 2007.

[31] Masabi. Two factor authentication (2FA) – opportunity and pitfalls, September 2007. `http://blog.masabi.com/2007/09/two-factor-authentication-2fa.html`.

[32] Monopolies and Mergers Commission. Credit card services: A report on the supply of credit card services in the United Kingdom, 1989. `http://www.mmc.gov.uk/rep_pub/reports/1989/255creditcard.htm`.

[33] Office of Fair Trading, UK. Mastercard agreement anti-competitive, rules OFT, September 2005. `http://www.oft.gov.uk/news/press/2005/168-05`.

[34] S. P. Skorobogatov. Low temperature data remanence in static RAM. Technical Report UCAM-CL-TR-536, University of Cambridge, Computer Laboratory, June 2002.

[35] S. W. Smith. Fairy dust, secrets, and the real world. *IEEE Security and Privacy*, 1(1):89–93, 2003.

[36] S. W. Smith and S. H. Weingart. Building a high-performance, programmable secure coprocessor. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 31(9):831–860, April 1999.

[37] Trintech. VeriFone to acquire Trintech's payment systems business, August 2006. `http://www.trintech.com/verifone-to-acquire-trintechs-payment-systems-business/`.

[38] VeriFone. Xtreme Keypad, September 2007. `http://www.verifone.com/products/devices/countertop/xtreme.html`.

[39] Visa. Chip terms explained, November 2002. `http://www.visa-asia.com/ap/center/merchants/productstech/includes/uploads/CTENov02.pdf`.

[40] Visa Canada. Visa chip card information for cardholders, October 2007. `http://www.visa.ca/chip/cardholders.cfm`.

[41] Visa International Service Association. PIN entry device security requirements manual, March 2004. `https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=35`.

[42] Visa International Service Association. Approved PIN entry devices, October 2007. `http://partnernetwork.visa.com/dv/pin/pedapprovallist.jsp`.

[43] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. In D. Tygar, editor, *2nd USENIX Workshop on Electronic Commerce*. USENIX, November 1996.

[44] S. H. Weingart. Physical security devices for computer subsystems: a survey of attacks and defences. In *Cryptographic Hardware and Embedded Systems Workshop*, volume 1965 of *LNCS*, pages 302–317, London, UK, August 2000. Springer-Verlag.

[45] S. H. Weingart, S. R. White, W. C. Arnold, and G. P. Double. An evaluation system for the physical security of computing systems. In *Computer Security Applications Conference*, pages 232–243, December 1990.

[46] C. Yang, G. Tian, and S. Ward. Security systems of point-of-sales devices. In *The International Journal of Advanced Manufacturing Technology*, volume 34, pages 799–815, London, October 2007. Springer.