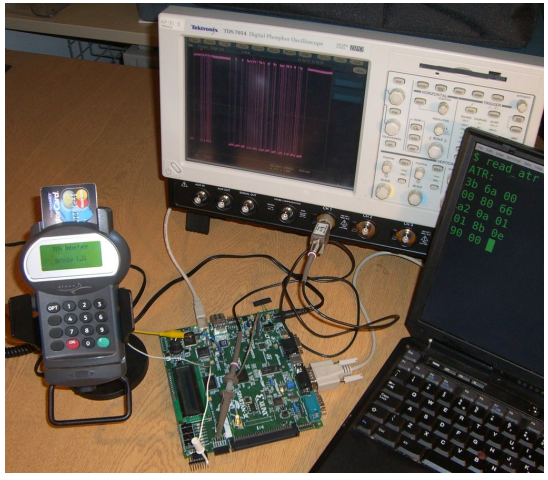
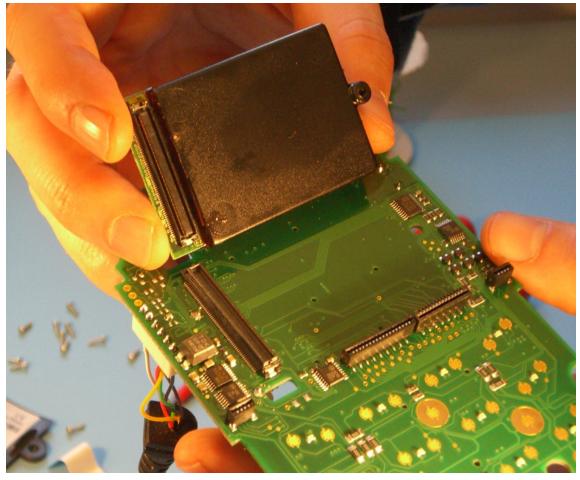
Thinking inside the box: system-level failures of tamper proofing





Saar Drimer Steven J. Murdoch Ross Anderson

www.cl.cam.ac.uk/users/{sd410,sjm217,rja14}

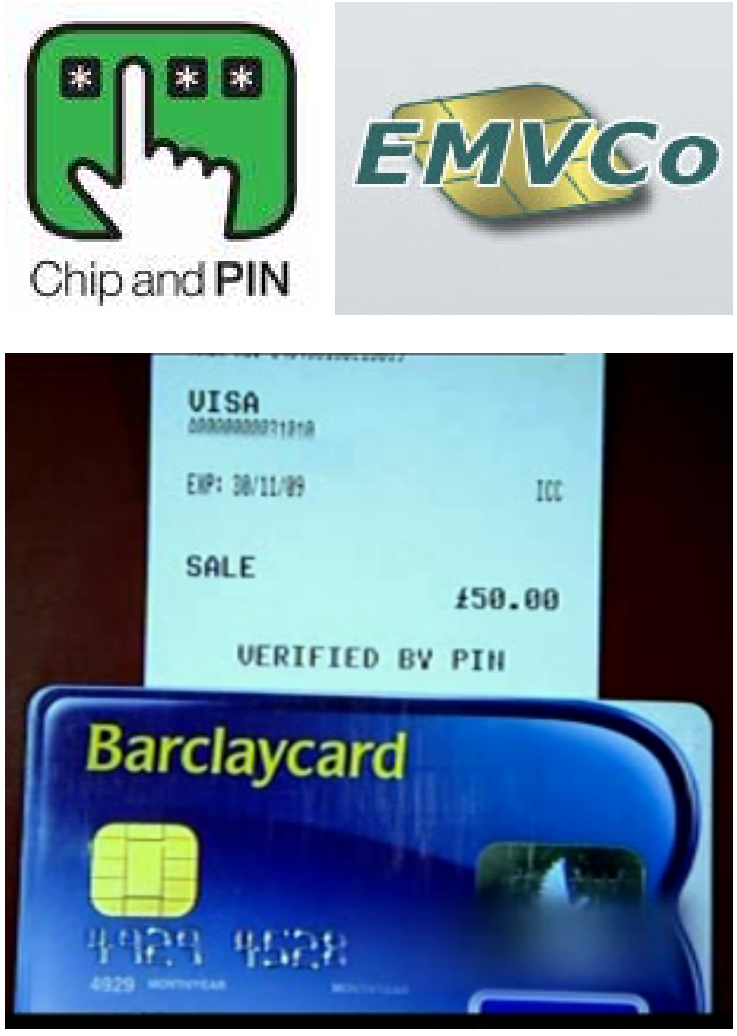
UNIVERSITY OF CAMBRIDGE
Computer Laboratory

www.torproject.org

IEEE Security & Privacy, 18–21 May, Oakland, CA, US

Chip & PIN is the most widely deployed smartcard payment system worldwide

- Chip & PIN, based on the EMV (EuroPay, Mastercard, Visa) standard, is deployed throughout most of Europe
- Visa is currently rolling out Chip & PIN in Canada
- Supports both credit and debit cards
- Customer inserts contact-smartcard at point of sale, and enters their PIN into a PIN Entry Device (PED)
- PIN is verified by card



Protocol overview (as used in the UK)

$$Card \rightarrow PED$$

- Card details (account number, cardholder name, expiry, etc.)
- Public key certificate and static digital signature
- Copy of the magnetic strip details $*$

$$PED \rightarrow Card$$

- Transaction description (value, currency, type)
- PIN as entered by customer $*$

$$Card \rightarrow PED$$

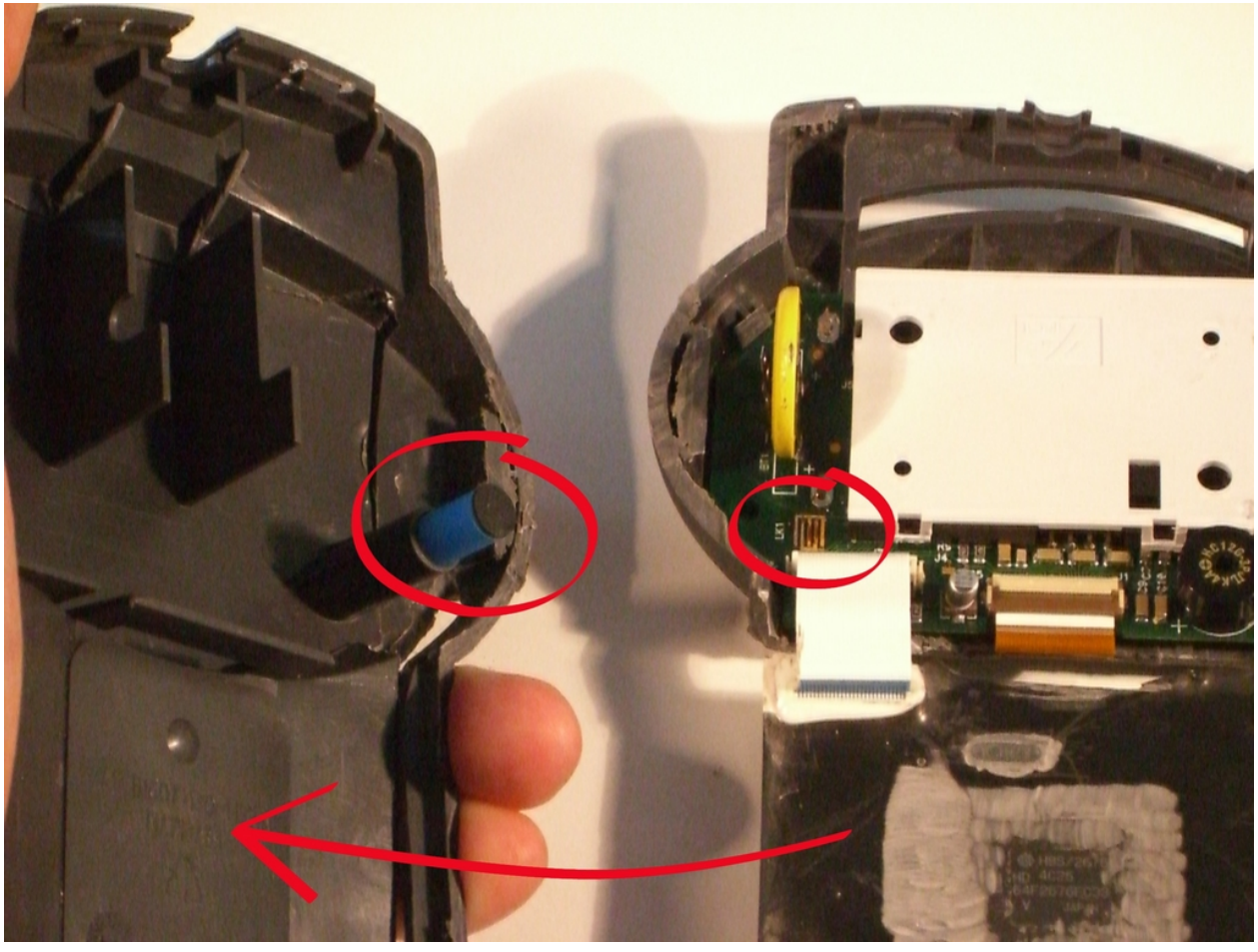
- PIN verification result and authorisation code

Tamper proofing is required to protect customers' PINs and banks' keys

- Various standard bodies require that PEDs be tamper proofed: Visa, EMV, PCI (Payment Card Industry), APACS (UK bank industry body)
- Evaluations are performed to well-established standards (Common Criteria)
- Visa requirement states that defeating tamper-detection would take more than 10 hours or cost over **USD $25,000 per PED**

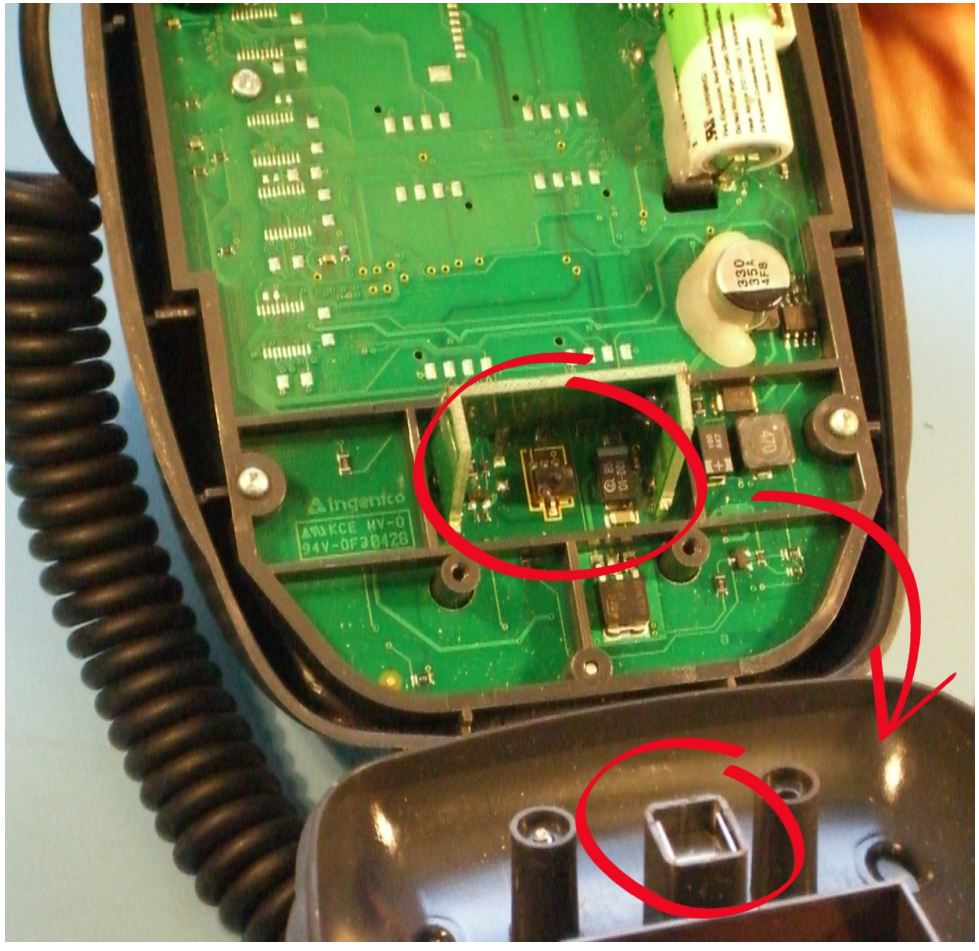
Do they work in practice?

Protection measures: tamper switches



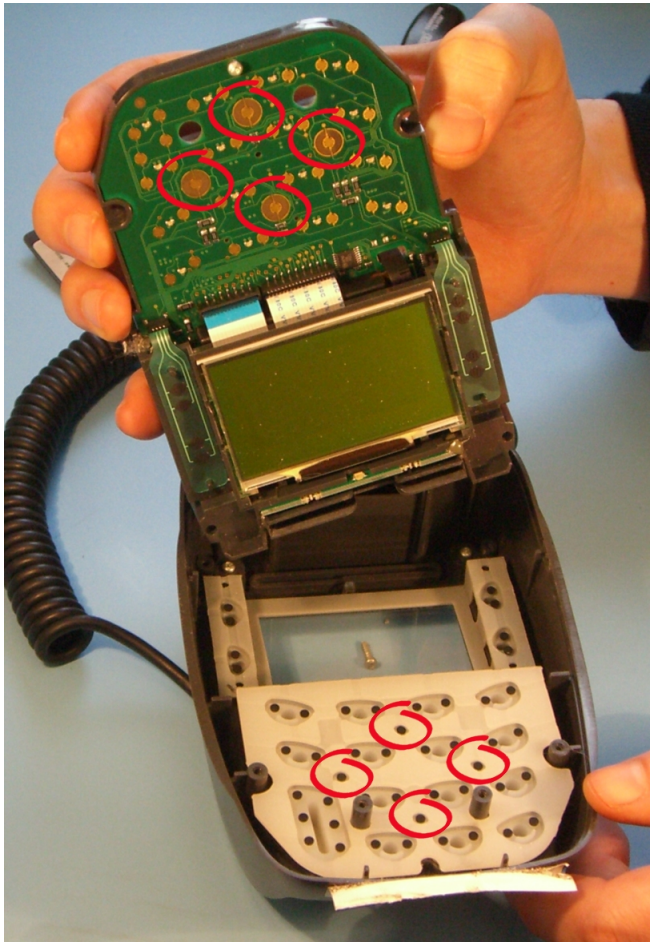
Dione Xtreme

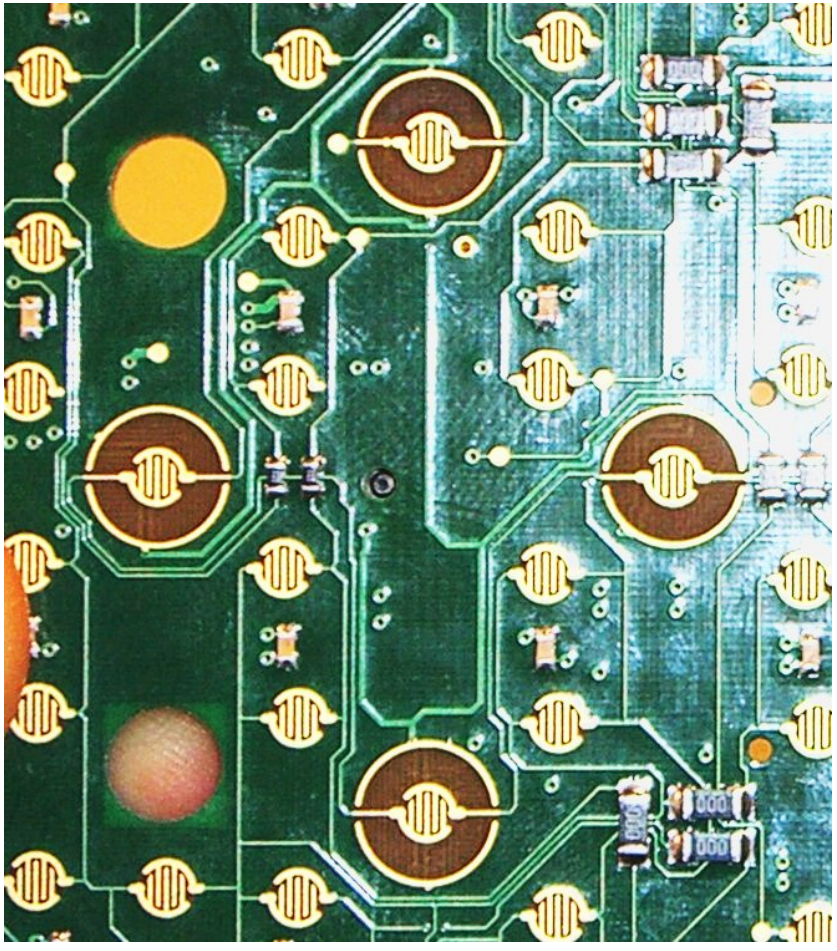
Protection measures: tamper switches



Ingenico i3300

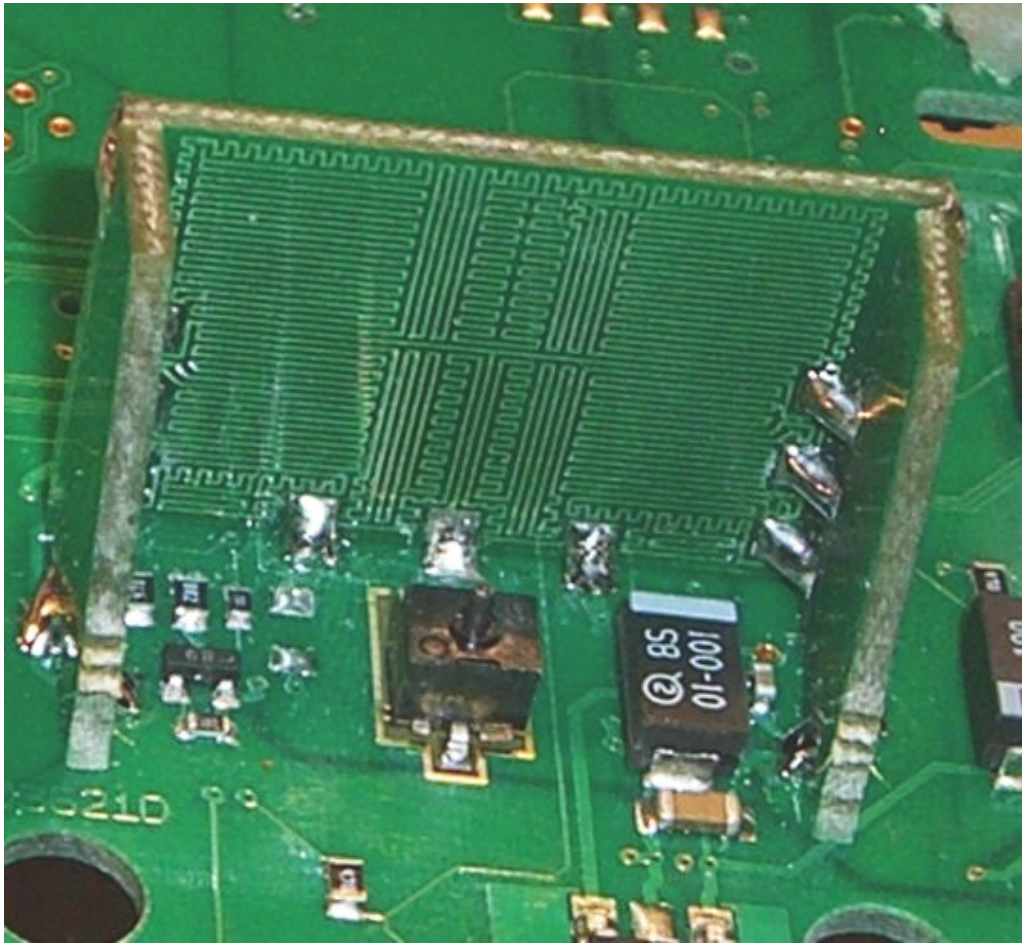
Protection measures: tamper switches

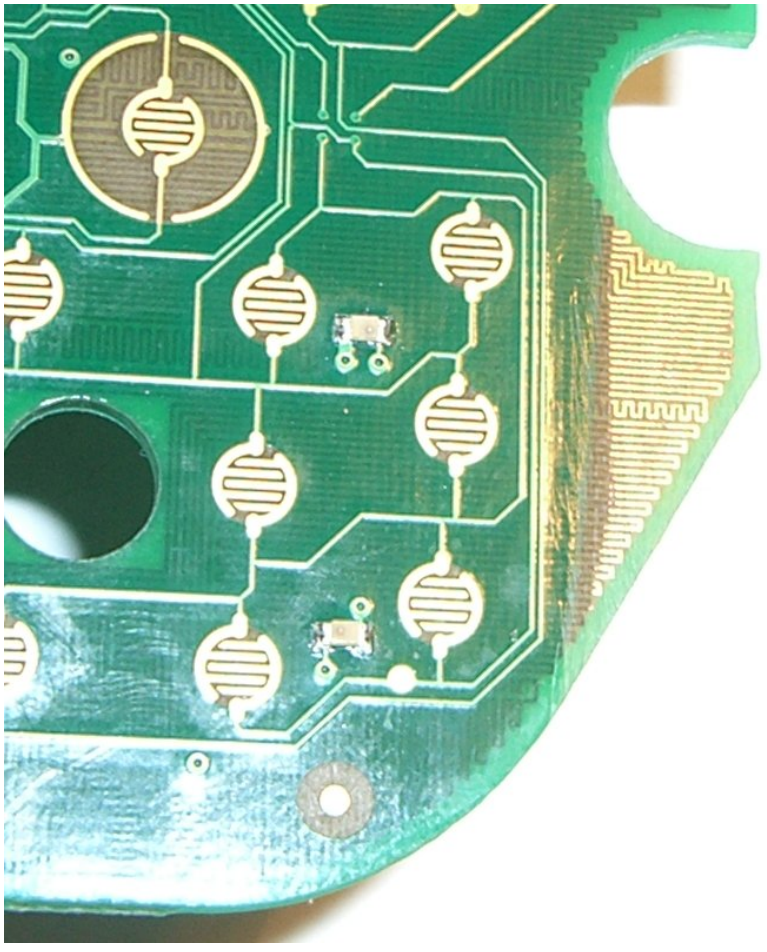




Ingenico i3300

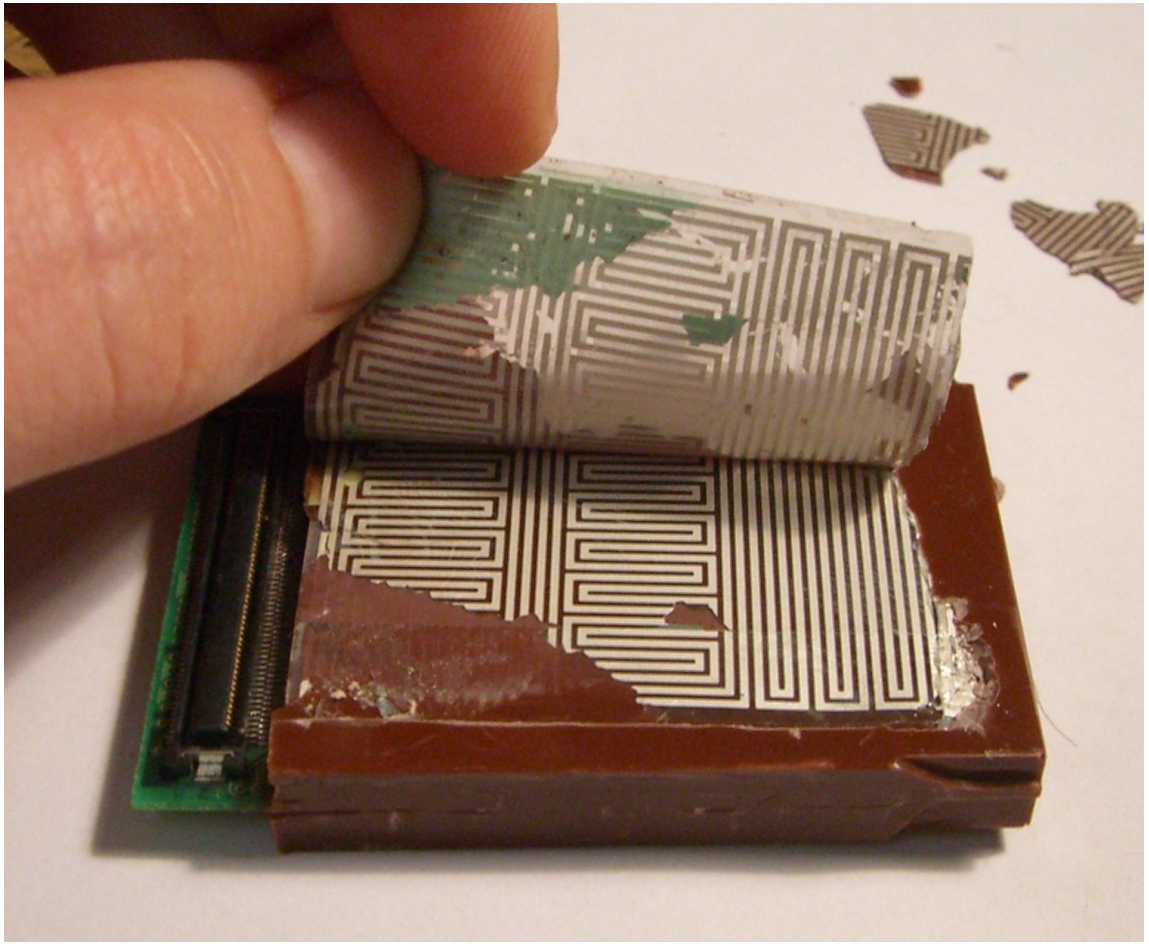
Protection measures: tamper meshes





Ingenico i3300

Protection measures: tamper meshes



Ingenico i3300

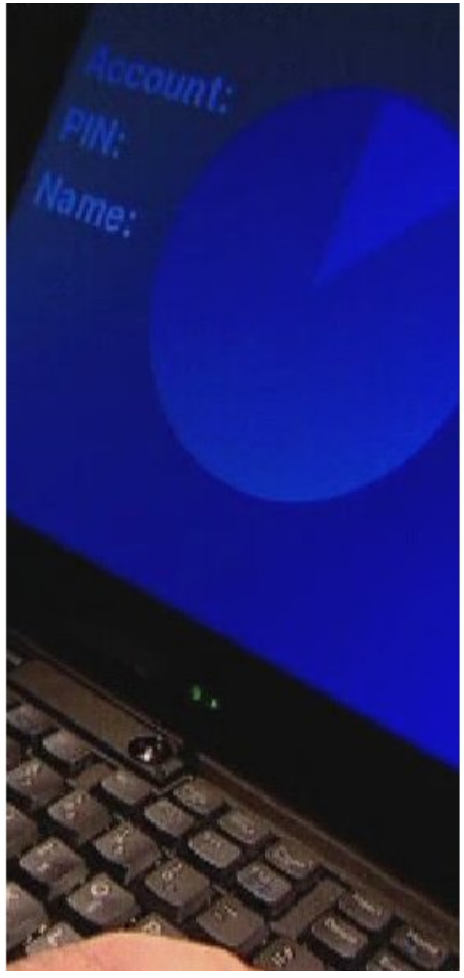
Protection measures: potting

Dione Xtreme

Tamper resistance protects the banks' keys, not the customer's PIN

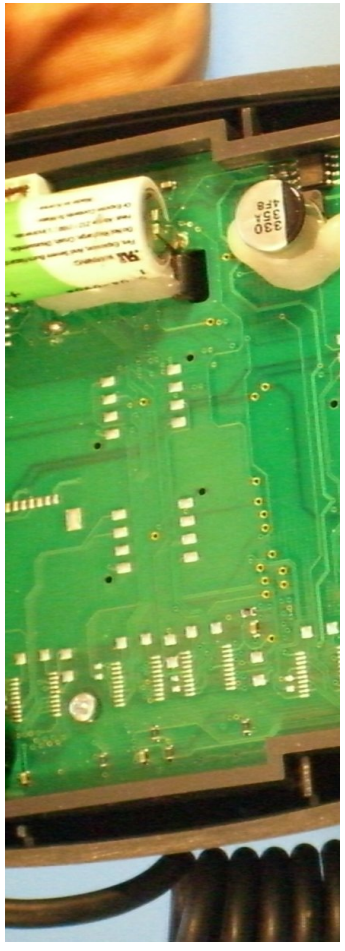
- Recall (*) that a copy of the magnetic strip details, and PIN, are sent unencrypted between card and PED
- If a fraudster can capture this information a fake card can be made, and used in some UK ATMs and many abroad
- We found that deployed tamper proofing measures failed to protect communications between card and PED
- To demonstrate the weakness, we tried our attacks on a real Ingenico PED

BBC Newsnight filmed our demonstration for national TV



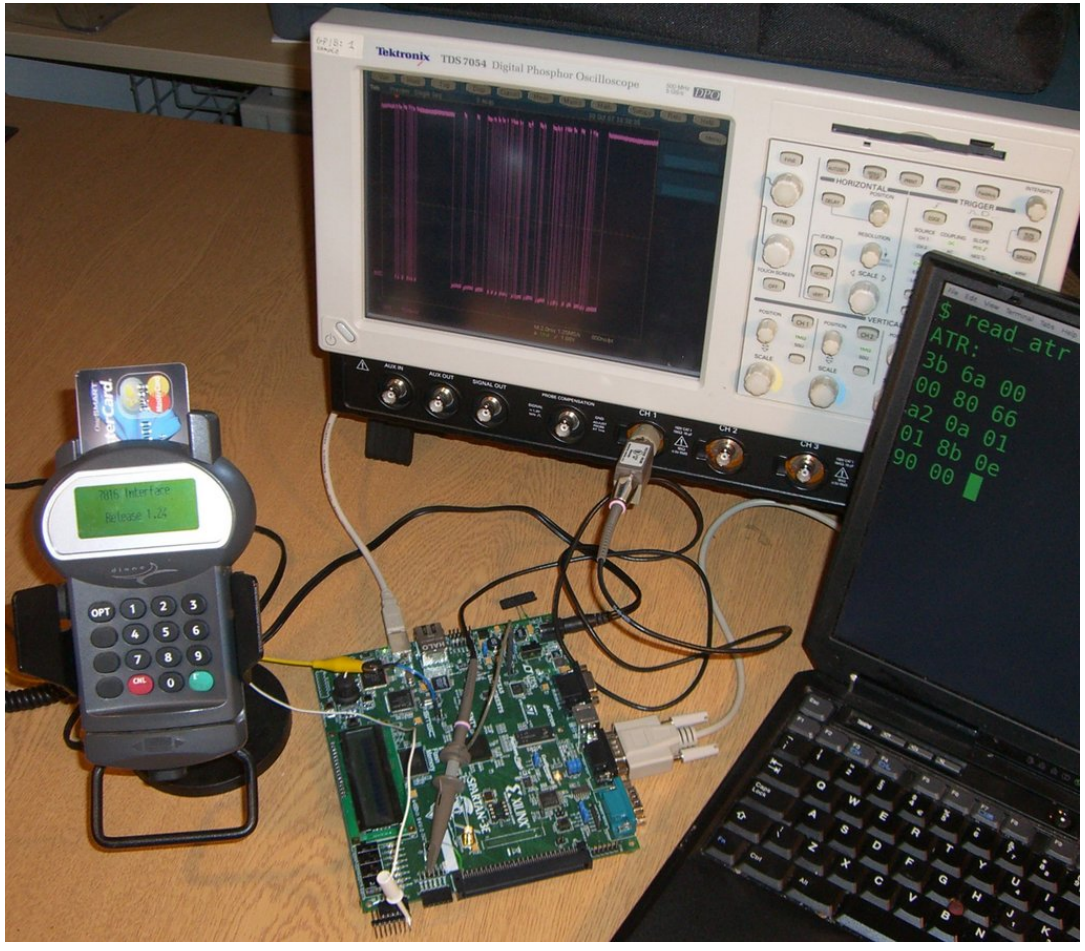
BBC Newsnight, BBC2, 26 February 2008

Holes in the tamper mesh allow the communication line to be tapped



An easily accessible compartment can hide a recording device

The Dione PED also routes card details outside the tamper resistant boundary



We constructed an FPGA design for capturing data

While the proximate failure is clear, the root causes are complex

The PEDs we examined failed to adequately protect the smartcard communication line. Because the UK system doesn't encrypt PINs, they are vulnerable. Why did this situation occur?

Engineering challenges: There are 3 662 pages in the public Visa Chip & PIN specification. Due to the complex inter-module security dependencies it is unreasonable to expect every engineer to have a full understanding

Economic incentives: Banks set the standards for PED security – their keys appear to be reasonably well protected. Customers have little say – their PINs are left vulnerable

Failure of certification: Both of these devices passed their necessary certification requirements, despite the flaws we found

Chip & PIN security needs both technical and economic improvements

PED design: PED design can be improved, but the smartcard communication line is inherently difficult to protect

Card configuration: Therefore, the encrypted PIN verification should be mandatory. Also a copy of the magnetic strip should never be stored on the chip

The voluntary UK banking code of practice states that banks must refund disputed transactions unless they can show that customers have been negligent or complicit in the fraud

However, the position taken by banks is that they have shown negligence if the fraudulent transaction was authorised by PIN

Banks can improve security but are not responsible for fraud. Putting liability on banks corrects the incentives

Why did the certification process not detect these vulnerabilities?

The Ingenico i3300 PED was evaluated under the Common Criteria (APACS PED Protection Profile)

CESG, the UK body responsible for management of the Common Criteria, stated that the Ingenico PED was merely “evaluated”, not “certified”. Hence its evaluation report was not public

APACS, the banking trade body for the UK, stated that the device was evaluated by a organisation accredited to perform Common Criteria certifications, but refused to say which

Visa (who certified the Dione PED) did not respond to our questions

Customers are being asked to rely on a secret report by an undisclosed evaluation laboratory

Who can revoke certification of devices or evaluation laboratories?

CESG stated that APACS were responsible:

> *In the case of the devices that you discuss in your paper these devices have not been certified, and so the UK CB [certification body] has no knowledge of the devices concerned. You will therefore need to* ***discuss these directly with APACS*** *and/or the manufacturers.*

APACS said that it was CESG who should investigate:

> *The only body that can revoke an evaluation laboratories evaluation accreditation is the evaluation scheme management body. In the case of the Common Criteria* ***that is CESG for UK labs****, the National Technical Authority for Information security.*

Sunlight is the best disinfectant

Common Criteria certification requires that evaluation reports are made publicly available, but this approach is resisted by APACS:

> *we are not aware of any widely recognised and credible evaluation methodology process, in security or otherwise, which makes evaluation reports publicly available.*

APACS also resist the application of Kerckhoffs' principle:

> *The evaluation reports contain detailed information as to* ***how the security features of a terminal work****. Releasing the document into the public* ***would reduce the effectiveness of these controls****, and therefore defeat the object of performing the security evaluation...*

Hostile evaluation of devices, rather than being done by a manufacturer appointed laboratory, will correct incentives

In summary, Chip & PIN, is a useful case study of failures in design, certification, regulation and incentives

- Due to protocol designers making unrealistic assumptions of tamper resistance, bank customers are at risk of fraud
- Finding a way to manage the evolution of a system, while maintaining security, is an important part of the solution
- Incentive design, both in the financial industry and certification processes, is needed to prevent flaws of the types we found
- The lessons from banking will apply to other fields (e.g. voting machines): complex systems, conflicting incentives, obstructive authorities and sham evaluations

More information (video, letters from vendors, extended paper):

`http://www.cl.cam.ac.uk/research/security/banking/ped/`