Thinking inside the box

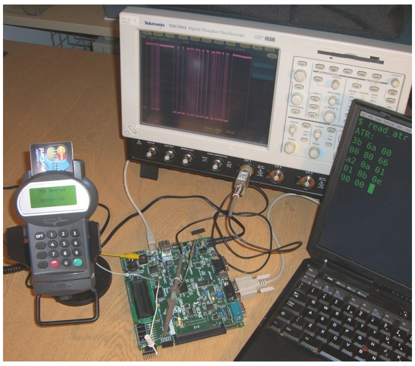
System-level failures of tamper proofing

Saar Drimer, Steven J. Murdoch, Ross Anderson

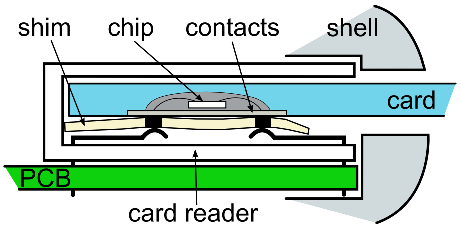
UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

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. We show that the tamper proofing of PEDs is unsatisfactory, as is the certification process.

Tapping and shim attacks



We have implemented practical low-cost attacks on two 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. This is done by attaching a wire to the communication line between the card and the processor inside of the PED. Since this communication is not normally encrypted at present, a small FPGA board can record the card details and PINs needed for card cloning and cash withdrawal at ATMs. The tap can be hidden so that cardholders cannot detect that the PED has been compromised.



We also discuss the possibility of a 'shim-in-the-middle' attack where a thin, flexible circuit board is inserted into the card slot, so that it lodges between the reader and the card's contacts. The shim is able to transmit the tap data to a nearby receiver that records transactions until it is later retrieved by the fraudster, or the data can be sent to him through SMS or Bluetooth. This attack completely bypasses all tamper protections and does not even require the collusion of any staff.

Possible defences

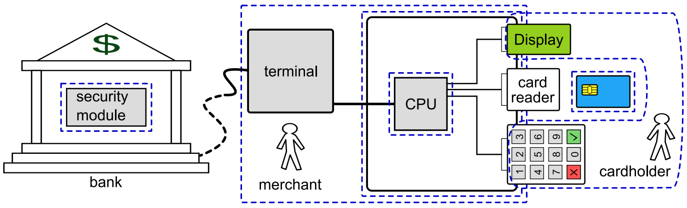
EMV allows for PIN encryption, though UK banks opted to deploy cheaper smartcards without this option. However, in some of the cards we examined, the card's indication that it is capable of PIN encryption is not signed, allowing the fraudster to modify it as the data is transmitted. Another way to prevent card cloning is by not storing an exact copy of the magnetic strip on the chip, so counterfeit cards cannot be created from this data. UK banks started issuing cards with this feature in 2008, even though it was suggested by MasterCard in 2002.

Ingenico i3300

Dione Xtreme

Analysis: security boundaries

The root cause of the protection failure is not the inadequate design of any one feature, but a poor design and evaluation process. It is impossible to validate that each module enforces the security guarantees that the other parts of the system require of it, as these guarantees are not made explicit. The EMV spec is thousands of pages long, which is a major impediment to a secure implementation of the system as a whole. We propose examining the system using 'security boundaries' in order to arrive at a concise 'architecture document' that specifies the security requirements of each component. This way, each sub-system engineer is aware of the security properties that must be maintained so that the failures we have identified are not repeated.



Certification issues and response

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. We found that even though the UK banking trade body APACS is using the Common Criteria name, the PEDs are not actually CC Certified, and GCHQ, the British CC certification body, does not prevent the abuse of its brand. APACS also claimed when we published our findings that the vulnerabilities were too technical and were uneconomical to exploit. Yet within a few months there were news reports of people being arrested for possessing tampered PEDs.

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

2008-09-18