Security & Computer Forensics
Where is the Field Heading?
What Are the Research Challenges Ahead?

David Naccache
Goal of This Presentation

- Illustrate to what length white collar criminals can go to hack embedded electronic devices.
- Illustrate the kind of challenges that forensic scientists face today.

Goal: raise awareness to the level of threats that forensic experts will have to face in the coming years.
The Five Major Forensic Research Challenges

• The emergence of anti-forensic countermeasures
• The problem of live system forensics
  • How to audit a system in evolution?
• Time patine generation
• Analyzing unknown, protected or black-box systems
• Keeping up with an extremely high pace of novelty emergence
The Five Major Forensic Research Challenges

• The emergence of anti-forensic countermeasures
• The problem of live system forensics
  • How to audit a system in evolution?
• Time patine generation
• Analyzing unknown, protected or black-box systems
• Keeping up with an extremely high pace of novelty emergence

We selected a concrete example in which the above 3 aspects are present
A forensic assignment.
Context

In May 2011: The French’s bankers Economic Interest Group (GIE Cartes Bancaires) noted that a dozen EMV cards, stolen in France a few months before, were being used in Belgium.

The net loss caused by this fraud is estimated to stand below 600,000€, stolen over 7,000 transactions using 40 modified cards.

A forensic investigation was hence ordered by Justice
The Judicial Seizure
The Judicial Seizure

- What appears as an ISO/IEC 7816 smart card.
- The plastic body indicates that this is a VISA card issued by Caisse d’Épargne (a French bank).
- Embossed details are:
  - PAN= 4978**********89;
  - expiry date in 2013;
  - and a cardholder name, hereafter abridged as P.S.
  - The forgery’s backside shows a normally looking CVV.
- PAN corresponds to a Caisse d’Épargne VISA card.

PAN=Permanent Account Number (partially anonymized here).
CVV=Card Verification Value.
The backside is deformed around the chip area.

Such a deformation is typically caused by heating. Heating (around 80°C) allows melting the potting glue to detach the card module.
Visual Inspection

The module looks unusual in two ways:
1) it is engraved with the inscription “FUN”;
2) glue traces (in red) clearly show that a foreign module was implanted to replace the **89 card’s original chip
Yellow Smart Card

The Smart Card YELLOW, also known as a Funcard 4, is a field programmable, ISO-7816-1 pin-out compatible multi-chip Smart Card featuring the ATMEL ATmega8515 + 24C64 die.

Product Details
FUNCARD’s Inner Schematics
Side-views show that forgery is somewhat thicker than a standard card (0.83mm).
Extra thickness varies from 0.4 to 0.7mm suggesting the existence of more components under the card module, besides the FUNcard.
FUNCard Under X-Ray

1. External memory (AT24C64)
2. μ-controller (AT90S85515A)
3. Connection wires
4. Connection grid
FunCard vs. Forgery under X-Ray
Forgery vs. FunCard

⑤ Stolen card module
⑥ Connection wires added by fraudster
⑦ Welding points added by the fraudster
Pseudo-Color Analysis

**Definition:** Materials may have the same color in the visible region of the EM spectrum and thus be indistinguishable to the Human eye. However, these materials may have different *properties* in other EM spectrum parts. The reflectance or transmittance spectra of these materials may be similar in the visible region, but *differ in other regions.*

Pseudo-coloring uses information included in the near-infrared region (NIR) i.e. 800-1000nm to discriminate materials beyond the visible region.
Pseudo-Color Analysis
Pseudo-Color Analysis

Stolen chip
Forgery Structure Suggested so Far
Forgery Structure Suggested so Far

Stolen card speaks to reader but instead of the reader the communication is intercepted by the fun card
Forgery Structure Suggested so Far

What the stolen card says goes into the FUNcard
Forgery Structure Suggested so Far

FUNCARD talks to the reader
Electronic Analysis Attempt

It is possible to read-back FunCard code if the card is not locked.

Attempted read-back failed. Device locked.
Anti-forensic protection by fraudster.
Magnetic Stripe Analysis

The magnetic stripe was read and decoded. ISO1 and ISO2 tracks perfectly agree with embossed data. ISO3 is empty, as is usual for European cards.
Electronic Information Query

Data exchanges between the forgery and the PoS were monitored.

• The forgery responded with the following information:
  • PAN = 4561**********79;
  • expiry date in 2011;
  • cardholder name henceforth referred to as H.D.

All this information is in blatant contradiction with data embossed on the card.

The forgery is hence a combination of two genuine cards
Chip and PIN is Broken

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond

University of Cambridge
Computer Laboratory
Cambridge, UK
http://www.cl.cam.ac.uk/users/{sjm217,sd410,rja14,mkb23}

Abstract—EMV is the dominant protocol used for smart card payments worldwide, with over 730 million cards in circulation. Known to bank customers as “Chip and PIN”, it is used in Europe; it is being introduced in Canada; and there is pressure from banks to introduce it in the USA too. EMV secures credit and debit card transactions by authenticating both the card and the customer presenting it through a combination of cryptographic authentication codes, digital signatures, and the entry of a PIN. In this paper we describe and demonstrate a protocol flaw which allows criminals to use a genuine card to make a payment without knowing the card’s PIN, and to remain undetected even when the merchant has an online connection to the banking network. The fraudster performs a man-in-the-middle attack to trick the terminal into believing the PIN verified correctly, while telling the card that no PIN was entered at all. The paper considers how the flaws arose, why they remained unknown despite EMV’s wide deployment for the best part of a decade, and how they might be fixed. Because we have found and validated a practical attack against the core functionality of EMV, we conclude that the protocol is vulnerable and that alternative solutions are required.

Figure 1. Fraud statistics on UK-issued cards [6]
Flashback 2010
The problem is here!
Flashback 2010
Flashback 2010
Flashback 2010

Figure 5. Carrying out the attack. Although we entered the wrong PIN, the receipt indicates that the transaction was “Verified by PIN.”
Modus Operandi Hypothesis

PoS terminal

FUNcard

Stolen card

External I/O Communication

Internal I/O Communication

00 A4 04 00 07

A4

A0 00 00 00 03 10 10

61 30

00 A4 04 00 07

A4

A0 00 00 00 03 10 10

61 30
Problem with Hypothesis!

no visible signal activity here!
Back to X-Ray: Solution to Riddle!

no visible signal activity here!
Anti-Forensic Protection by Fraudster
Using Power Consumption Analysis

Select command
7 data bytes sent by the PoS

I/O Activity

Power consumption

Procedure byte 0xA4 sent by the stolen card

Procedure byte 0xA4 sent by the FUNcard

7 patterns = 7 bytes

FUNcard repeats the 7 bytes to the stolen card

7 patterns = 7 bytes
PoS sends the ISO command 00 A4 04 00 07
Command echoed to the stolen card by the FunCard
Stolen card sends the procedure byte A4 to the FunCard
FunCard retransmits the procedure byte to the PoS
PoS sends data to FunCard
FunCard echoes data to stolen card
Stolen card sends SW to FunCard
FunCard transmits SW to PoS
Power Consumption During GetData

Confirms the modus operandi
VerifyPIN Power Trace Analysis

Power trace of the forgery during VerifyPIN command.

Note the absence of retransmission on the power trace before the sending of the SW
Having Finished All Experiments

We can ask the judge’s authorization to perform invasive analysis.

Authorization granted.
Invasive Analysis

① Connection grid
② Stolen card module (outlined in blue)
③ Stolen card’s chip
④ FunCard module
⑤ Welding of connection wires
Invasive Analysis

① FunCard module
② Genuine stolen card
③ Welded wire
Original EMV Chip Clipped by Fraudster

Cut-out pattern overlaid
Wiring Diagram of the Forgery
The Five Major Forensic Research Challenges

• The emergence of anti-forensic
• The problem of live system forensics
  • How to audit a system in evolution?
• Time patine generation
• Analyzing unknown or black-box systems
• Keeping up with an extremely high pace of novelty emergence

And 7 key technical areas
In Conclusion

Attackers of modern embedded IoT devices
• Use advanced tools
• Are very skilled engineers
• Are well aware of academic publications
• Use s/w and h/w anti-forensic countermeasures

If you do not design your IoT device with that in mind and if stakes are high enough, the device will be broken.