OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Contacless payments insecurity

Renaud Lifchitz – renaud.lifchitz@oppida.fr
8.8 Computer Security Conference
October 24-25, 2013 – Santiago, Chile

8.8

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Speaker's bio

- French computer security engineer working at Oppida, France
- Main activities:
  - Penetration testing & security audits
  - Security research
  - Security trainings
- Main interests:
  - Security of protocols (authentication, cryptography, information leakage, zero-knowledge proofs...)
  - Number theory (integer factorization, primality testing, elliptic curves...)

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

What is contactless payment?

- Everyday payment with no need for card insertion nor card PIN code
- Main systems:
  VISA payWave & MasterCard PayPass
- Small payments (a few times $5-$100 in a row)
- >> 15 millions NFC-enabled credit cards in the U.S.

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

How to recognize an NFC-enabled credit card?

Small wave logo printed on the card:

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Contactless payment goals

- Achieve faster & easier payments
- Make people buy more (MasterCard Canada has seen “about 25 percent” higher spending by its PayPass users)
- Interoperable systems

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

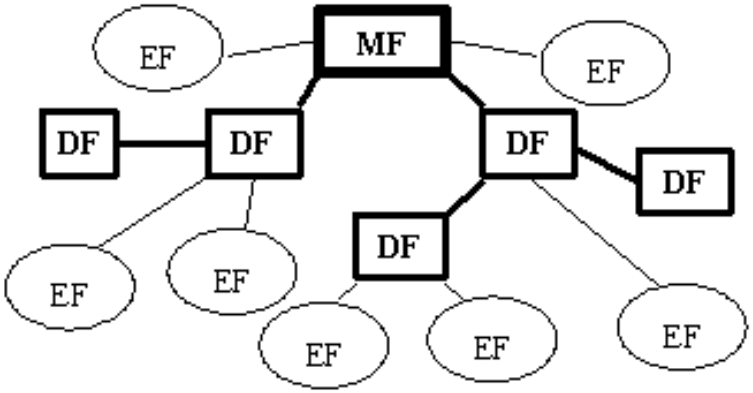
Credit card standards

- Data storage and security:
  EMV standards
  (Europay MasterCard and VISA)
- Protocol commands and cards storage layout:
  ISO 7816 standards

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

EMV

- Card memory:
  a real filesystem with a root directory (MF), folders (DF) and files (EF) identified by 2 bytes, according to ISO 7816-4



- Data encoding: BER TLV (very near from ASN.1)
  → online decoder: http://www.emvlab.org/tlvutils/

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

ISO 7816-4

- Requests - simplified command sets:
  - Class (1 byte)
  - Instruction (1 byte)
  - Parameter 1 & 2 (1 byte each)
  - Length of data (1 byte)
  - Data field
  - Length of expected response (1 byte)

Header				Body		
CLA	INS	P1	P2	Lc	Data Field	Le

- Answers:
  - Data field
  - SW1 & SW2 error codes (1 byte each)

Body	Status Word	
Data Field	SW 1	SW 2

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

The idea

- French Navigo contactless transportation cards also use ISO 7816 encapsulation over RFID but:
  - No personal data on card (card ID ≠ cardholder ID)
  - Use good encryption
  - Use good authentication
  - Use digital signature
- RFID passports:
  - Use encryption
  - Use a combined reading to avoid rogue access (optical+RFID)

→ RFID credit cards (= money) should be as secure as those two, shouldn't them?

NO, BECAUSE THERE IS SIMPLY NO AUTHENTICATION NOR ENCRYPTION!!!

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

NFC

- Different names for nearly the same thing: RFID/NFC/Cityzi
- HF (13,56 Mhz) & LF (125-134 kHz) usages
- Most common HF protocol: ISO 14443 (ISO 14443-1 to ISO 14443-4)
- Can be used for tunneling/encapsulation

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

NFC readers

- USB readers:
  - SCM SCL3711 (40€ dongle)
  - ACS ACR120U/ACR122U (flat)

- Phones:
  - Samsung Nexus S, Samsung Galaxy S3
  - BlackBerry Bold 9900/9930, BlackBerry Curve 9350/9360/9370
  - Nokia N9/C7/603

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Tools

- ISO 7816 (contact) prototyping: `scriptor`
- NFC (contactless) prototyping: `libnfc pn53x-tamashell`
- Final coding: `libnfc`
  (EOF, SOF and CRC are automagically handled)

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Remotely available data

- Everything from EMV standards like with a contact interface?
- Confirmed:
  - Cardholder: gender, first name and last name
  - PAN (Primary Account Number)
  - Expiry date
  - Magnetic stripe data
  - Transaction history
- Probably: general card information (issuer, public keys, …)
- But no CVV! (just a one-time-CVV functionality)

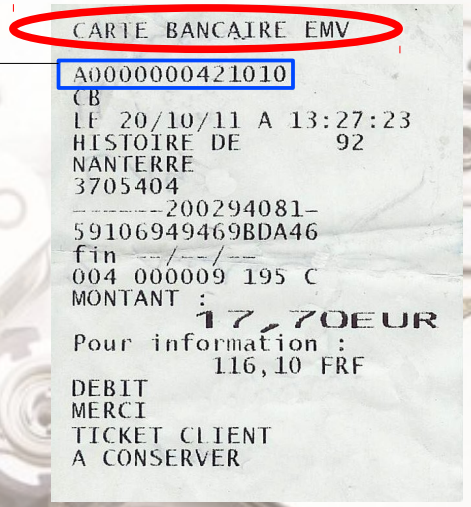
OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Possible attacks

- Read victim's card data and use it on e-commerce websites: CVV is not always mandatory and CVV can be bruteforced
  (only 1000 possibilities...)
- Remote card DoS?
  (send 3 times a bad PIN code)
- Create a magnetic stripe dump remotely
  (card clone will be useful where chip card/PIN is not mandatory: most EU countries, USA, …)
- User identification and tracking (terrorism...)

Typical minimal libnfc attack sequence

- 1) Initiator List Passive Targets (wake up card!):
  - 4A 01 00
- 2) Select banking application (AID):
  - 40 01 00 A4 04 00 07 A0 00 00 00 42 10 10 00
- 3) Read specific EMV record:
  - 40 01 00 B2 02 0C 00 00



libnfc prefix/suffix opcode
ISO-7816 command
EMV specific

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

AID selection

- Some well known AIDs:
  - Visa debit/credit: A0 00 00 00 03 10 10
  - MasterCard credit: A0 00 00 00 04 10 10
  - American Express: A0 00 00 00 25 00 00
  - CB: A0 00 00 00 42 10 10
- Be careful: EF ids can vary accordingly!
- A better way if to use the PSE (Payment System Environment) to find the correct AID & EF ids

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Proof of Concept

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Proof of Concept desktop computer

```
$ ./readnfccc
Cardholder name: LIFCHITZ/RENAUD.MR
PAN: 4970 [redacted] 2586
Expiration date: 12/2013

07/04/2012 Payment      24,50€
06/04/2012 Payment      73,00€
05/04/2012 Withdrawal   60,00€
05/04/2012 Payment      7,85€
02/04/2012 Payment      6,95€
30/03/2012 Payment      30,00€
30/03/2012 Withdrawal   60,00€
30/03/2012 Payment      59,90€
26/03/2012 Payment      70,00€
24/03/2012 Payment      40,88€
23/03/2012 Payment      108,07€
21/03/2012 Payment      47,00€
20/03/2012 Payment      9,40€
14/03/2012 Payment      48,00€
14/03/2012 Payment      18,35€
14/03/2012 Payment      35,50€
11/03/2012 Payment      21,00€
11/03/2012 Payment      24,50€
11/03/2012 Withdrawal   90,00€
11/03/2012 Payment      45,00€
-------------------------
```

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Proof of Concept
Android smartphone

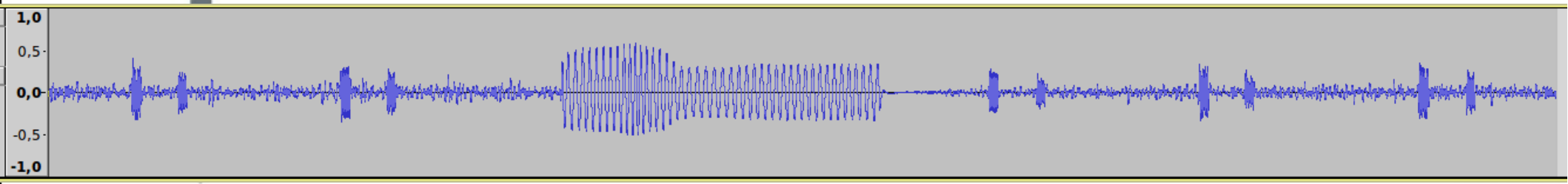
OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Attack limitations

- Main limitation is the distance
- ISO 14443 standards state:
  - Active read up to 3 to 5cm in practice
- But tweaking the devices:
  - Active read up to 1.5m (50x better!) using a dedicated amplifier (2000€) and antenna (1000€).
    Everything fits into a backpack...
  - Passive sniffing up to 15m (500x better!) using a radio receiver (e.g. USRP) with a standard telescopic antenna
- Remember: in August 2004, hackers succeeded in extending a Bluetooth dongle range from 10m to 1,7km!
  (http://trifinite.org/trifinite_stuff_lds.html)

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Passive sniffing

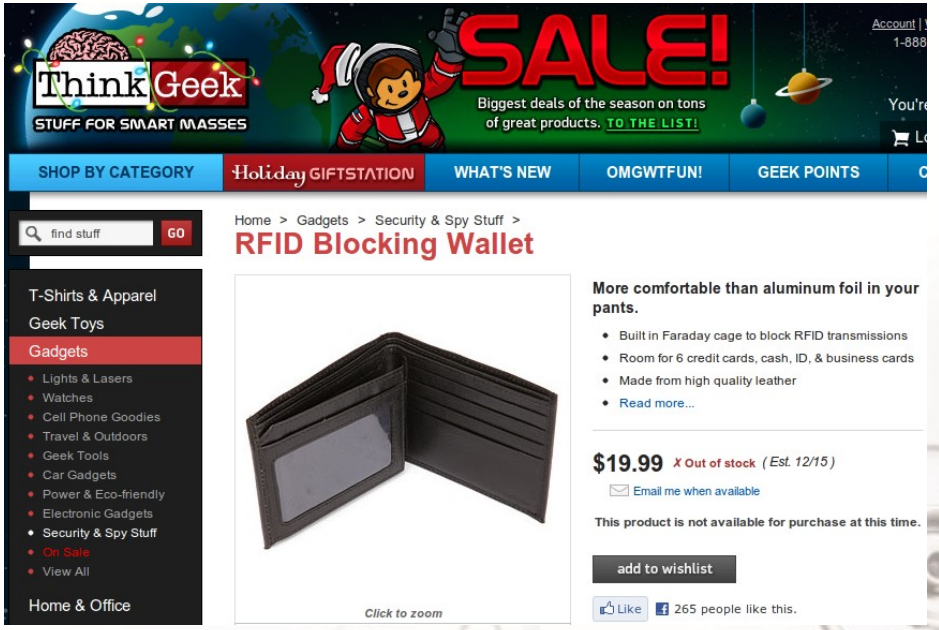


Reader probes, communication with the credit card, and then probes again

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

How to protect?

OR



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

How should security be?

- Contactless accesses should be authenticated
  to avoid rogue readers
- Contactless protocol should be encrypted
  to avoid eavesdropping
- Session integrity should be ensured (e.g. HMAC or signature)
  to avoid injection

This already exists!!!
(for example French Navigo transportation card)

Conclusion: EMV is poorly designed for NFC and needs a complete rewrite!...

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Regulatory compliance

- 2 major regulatory issues due to this lack of security:
  - PCI DSS compliance
  - Personal data protection

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

PCI DSS compliance (1/3)

- Intended for **organizations that handle cardholder information** (merchants, financial institutions, software & hardware developers, industry professionals...)
- "PCI Data Security Standard" *is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.* (https://www.pcisecuritystandards.org)
- PCI DSS is sponsored by the same who have designed and distributed NFC credit cards (Visa, MasterCard, ...) in order to avoid fraud

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

PCI DSS compliance (2/3)

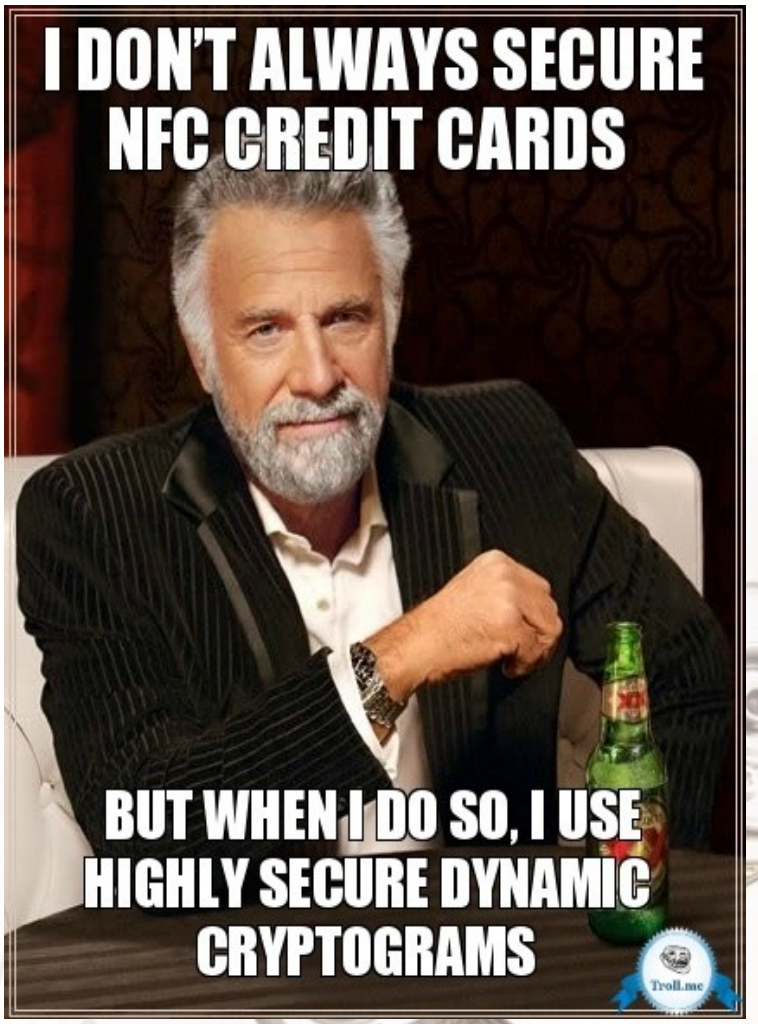
- Requirement 4 of PCI DSS - "Encrypt transmission of cardholder data across open, public networks":
  - Scope: all wireless technologies
  - Testing Procedure 4.1.a: “Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.”
- Unsolicited accesses and most solicited accesses to the credit cards are CLEARTEXT AND INCLUDE CARDHOLDER DATA

This is a MAJOR FAIL!
NFC payments are not compliant with PCI DSS and organizations may become non-compliant by accepting them...

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

PCI DSS compliance (3/3)

- However, one of the 2 biggest credit card supplier had stated in its public FAQ that "technically, the contactless functionality (...) protects cardholder information using **very secured dynamic cryptograms**"
- Indeed, it's cleartext!!!



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Personal data protection

- In France, it is a criminal offense not to protect personal data when you handle them
- You also have to comply with EU regulatory constraints on personal data protection

That's why credit card suppliers probably don't comply with several countries law too!...

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Recent security improvements

- In France since the end of 2013, cardholder name and transaction history shouldn't be readable from the contactless interface

- Other measures are being investigated:
  - A specific virtual PAN for the contactless interface
  - Encrypted communications
  - Button to press to enable communications

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Other additional security measures

- Use of RFID blocking wallet
  (blocks active reading but not passive sniffing)
- Software “kill-switch”
- Antenna cutting
  (can be illegal if the card belongs to the bank)

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Legal context

- This is NOT reverse engineering:
  EMV standard is available to everybody for a long time. The proof of concept is just a small EMV implementation
- This is NOT made for counterfeits:
  We have just extracted personal information that already belongs to us, and this is neither not necessary nor sufficient for counterfeits
- We HAVEN'T BROKEN any security or tried to, because there is none!

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

¡ Gracias por su atención !

Any questions?

Proof Of Concept:
http://code.google.com/p/readnfccc/