FACULTY OF SCIENCE

Bart Jacobs
& the Mifare Team

Smart Cards in Public Transport: the Mifare Classic Case

Radboud University Nijmegen

Contents

Who is this guy?

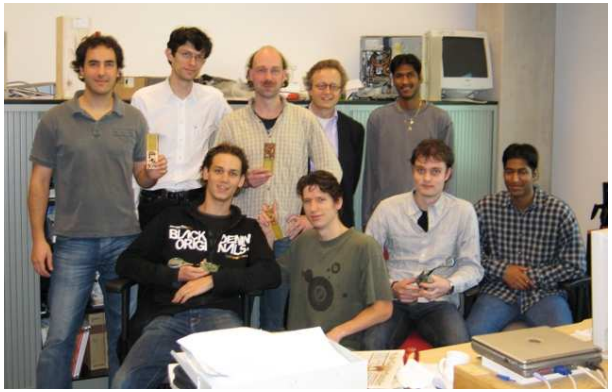
- Professor in computer security, at Nijmegen & Eindhoven (role in setting up EIPSI)
- Apart from academic abstract nonsense, involved in e-government / identity management, like biometric passports, voting, OV-chip
- Occasional role in media
- Author of online book *De Menselijke Maat in ICT*, see `www.cs.ru.nl/B.Jacobs/MM`

I. Background

Own involvement in OV-chip issues

- End-responsible for security research at Nijmegen
  - OV-chip & Mifare: at first only helicopter view
  - steering role when things got hot
  - no role in actual dismantling work
- Active in organisational/political/media issues (with Wouter Teepe)
- At a late stage: logical modeling & analysis of Mifare in theorem prover (PVS)
- Ongoing work on possible alternatives

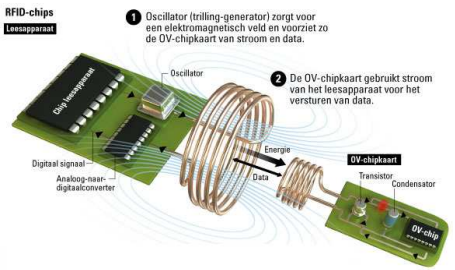
The Mifare Team



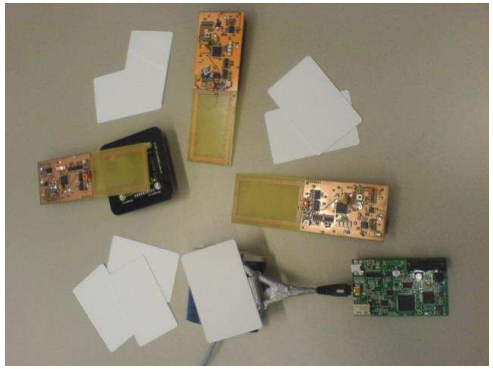
Flavio Garcia, Wouter Teepe, Peter v. Rossum, BJ, Vinesh Kali
Ruben Muijrers, Roel Verdult, Gerhard de Koning Gans, Ravindra Kali

Preceding steps

- Smart card (software) long term topic
- Eavesdropping contact-based cards is easy, with readily available, cheap devices
- Eavesdropping contact-less cards more difficult:



RFID tools used



Blank cards, Ghost, Proxmark, Open PCD

Eavesdropping & emulation devices

- ***Ghost*** (now largely obsolete)
  - Built at Nijmegen, with help from others
  - Firmware for ISO 14443-A by Roel Verdult
  - Can emulate card & eavesdrop card reader
- ***Proxmark*** (available since may 2007)
  - Hardware & some software (GPL) available
  - Can act as card, as reader & 2-way eavesdropper
  - Fully programmable, via FPGA
  - ISO 14443-A added by Gerhard de Koning Gans (& Mifare emulation!)

Karsten Nohl & Henryk Plötz

- Known in NL as “the German hackers”
- Presented hardware attack on Mifare Classic (end of dec.’07, at Berlin Computer Chaos Club)
- Reconstructed secret Crypto1 stream cipher of Mifare Classic & revealed nonce generation weakness
- They did not reveal Crypto1
- No (demonstrated) retrieval of secret keys
- Privately disclosed 48-bit LFSR structure to Nijmegen

II. OV-chipcard

Entrance gates with chipcard readers

OV-chip background

- Introduced by *Trans Link Systems* (TLS),
  - consortium of public transport companies,
  - covering 80% of market
  - founded in 2002, to introduce OV-chip
- NL system modeled after Hong Kong's
- National government (deliberately) has limited role
- Experiments since 2007 in R'dam & A'dam
- Nationwide originally foreseen in 2008.

OV-chip goals

- Detailed insight in actual trips
  (for optimisation & division of revenues)
- Public safety through restricted access
- Fraud reduction
- Cost reduction (fewer ticket inspectors)
- Convenience, for travelers
- Individual travel data, for marketing.
- High tech image (?)

OV-chip realisation

- System copied from abroad (Hong-Kong)
- Mifare Classic 4K smart card for travellers
- Complex nationwide infrastructure, with many parties and stakeholders
- Much secrecy about the whole set-up
  - no independent evaluation
  - message: your data are in reliable hands, but everything is so secret & sensitive, . . .
  - we cannot tell how things work – just trust us!

OV-chip: three different cards

- ***Disposable*** non-reloadable card for incidental use, based on *Mifare Ultralight*
- ***Personal***, reloadable card, with possible discounts, based on *Mifare Classic*
- ***Anonymous***, reloadable, without discounts, also with *Mifare Classic*.

Only *Mifare Classic* has cryptographic protection

Privacy issues I

- Cards have fixed anti-collision identifier (UID), making people universally recognisable
- Complaints about back-office, eg. CBP (Data Protection Authority) calls the system ***illegal***:
  - too much personal data at enrollment
  - travel data kept too long, at individual level
  - data insufficently protected
    (soon: DVD with travel data of all of us left in train?)
  - insufficent clarity about what happens to data

Privacy issues II

- Anonymous cards are a *sad joke*:
  - unattractive: fewer options & more expensive
  - privacy easily compromised:
    - loading with cash only possible with coins
    - loading with bank card reveals identity

Privacy is add-on (at most), not in architecture

OV-chipcard problem history I

- Mid'07: UvA students discover software error wrt. disposable cards (fixed by TLS)
- Dec.'07: CCC presentation of Nohl & Plötz about hardware attack on Mifare Classic
  - Crypto1 cipher discovered, but not published
  - No immediate impact on OV-chipcard yet
  - Sparked off media attention
  - Led to TNO investigation & eventually RHUL counter-investigation

OV-chipcard problem history II

- Jan'08: RU students demonstrate that disposables can be cloned (no fix)
- Mar'08: RU team reveals Mifare Classic crack
  - Focus on Mifare Classic **access** cards
  - Crypto1 re-discovered via crypto-analytic means
  - Secret keys recovered & cloning demonstrated
  - No immediate impact on OV-chipcard yet
- Late Mar'08: RU team demonstrates breaking OV-chipcard
  (keys of all its 15 sectors recovered in seconds)

Reports from TNO & RHUL

- ***TNO*** (26/2/08)
  - No alarm: no criminal business case
  - Replace cards in 2 years
  - Advanced equipment needed for cracking
- ***RHUL*** (14/4/'08, evaluating TNO)
  - Fraud more likely, with nationwide system
  - Greater urgency: replace cards now
  - Open design & review needed
  - System must be modular, to allow easy updates

III. Mifare Classic

Mifare Classic essentials

- Developed by Philips, now NXP
- Technology from early/mid 90s: limited computing power on chip
- Memory card (1K & 4K) with proprietary "Crypto1" stream cipher protection (48-bit key)
- Mutual authentication required before reading/writing
- Unique fixed identifier (UID) per card
- Separate keys per memory sector (64/256B)

Mifare protocol

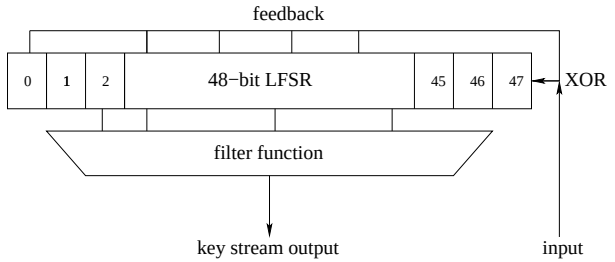
- **Anti-collision**: several cards for 1 reader
- Mutual **authentication**, via card & reader nonces (leads to key stream, for XOR-encryption)
- **Read/write** commands, per sector
- **Halt**

Essential (card) ingredients

- **Random number generator**
  - Only 16-bit LFSR, revealed at CCC; predictable
- **Stream cipher LFSR**
  - 48-bit, feedback privately revealed (Nohl & Plötz)
  - Reversible, see later
- **Filter function**
  - produces stream bits from LFSR; essential secret
  - Also reversible, through weakness

Feedback & Filter remain secret, for now

LFSR Schematics



LFSR logically, in PVS (own hobby)

- LFSR state is 48-bit bitvector:

```
lfsr :  TYPE = bvec[48]
```

- One step operation:

```
shift1in :  [lfsr, bit -> lfsr] =
  LAMBDA(r:lfsr, b:bit) :
    LAMBDA(i:below(48)) :
      IF i < 47
      THEN r(i+1)
      ELSE b XOR feedback(r)
      ENDIF
```


LFSR, elementary properties in PVS

- Feedback function also allows “shift-out”
- Multiple times, each others inverses:

```
shiftNin :[lfsr, bvec[N] -> lfsr]
shiftNout :[lfsr, bvec[N] -> lfsr]
```

- For stream cipher: shift-in zero’s yields action

```
advance :[lfsr, int -> lfsr]
```

$$\texttt{advance}(r, 0) = r$$

$$\texttt{advance}(r, i+j) = \texttt{advance}(\texttt{advance}(r, i), j)$$

LFSR can be moved forwards and backwards

Consequences: attack

- Elementary protocol steps can be rolled back:
  - shifting in of card nonce
  - updating state with reader nonce
  - applications of filter function

Roll-backs yield secret key from keystream fragment

- Attack in 0.1 second, given 1 trace
- (Post-hoc justification in PVS of properties of LFSR exploited by attack code in C)

Esorics'08 publication

- Mathematical details appear in okt'08
- Mid july: NXP tries to stop "irresponsible" publication, via injunction *(kort geding)*
- Judge refuses to prohibit, basically on freedom of expression. Also:
  - University acted with due care, warning stakeholders early on
  - Damage not result of publication, but of apparent deficiencies in cards (*sic!*)
- NXP did not appeal

Attack demo's I

- ***Access card*** cloned early March
  - university access card; UID ignored by reader
  - on YouTube (look for "Mifare Hack")
  - warning by Interior Minister on March 12
- ***OV-chipcard*** read out end of March
  - all 15 sectors read
  - cumulative encryption of card nonces
  - shown privately to HEC/RHUL & TLS
  - basis of big blow to card

Attack demo II

- April'08: vulnerabilities also demonstrated in London's Oyster card
- *Hit-and-run* Tube visit:
  - Prepaid card bought, with initial value £5.80
  - Upon entrance, communication eavesdropped & cryptographic keys retrieved from trace
  - After trip remaining value £1.80
  - Restored to £5.80 & used for another trip
- Transport for London: "no reason for concern".

IV. Perspectives

Messenger perspective I

- Assume university research reveals that popular medicine has bad side-effect
  - Keeping information secret is immoral
  - Releasing it will not make producer happy
- Naively, everyone wants to invent effective, new medicines, but finding negative consequences also contributes to progress
- Finding flaws is essential part of security research

Messenger perspective II

- What to do when software bugs are found?
- Confidentially informing the producer usually has little effect
- Publishing vulnerabilities (with attack code) leads to quick fixes
- Grown practice: ***responsible disclosure***
  - inform producer, and
  - publish after, say, a month

Messenger perspective III

- In Mifare Classic case:
  - 7 months delay (march – oct. 2008)
  - unusually long in CS-community . . .
  - . . . but not enough to replace installed base
- Time to take additional security measures
  - redo risk analysis
  - strengthen other security layers
  - human guards at main gates, checking photo-id
  - increase backoffice checks (transport)
  - replace cards (and readers) at some stage

Producer perspective

- NXP has several more advanced cards
  - DESfire, SmartMX, Mifare Plus (announced)
  - but more expensive . . .
- Should NXP have decided itself to stop producing & selling Mifare Classics?
- Reputation damaged, but opportunity to sell new cards

Customer (TLS) perspective

- “Customer makes wrong choice”
  (Paul de Bot, NXP vice-president, De Gelderlander, 14/3/08)
- Within OV-chip project:
  - political pressure to keep costs low for traveller
  - system simply copied from elsewhere
  - no critical attitude wrt. security (and privacy!)
    “It works elsewhere!”
  - Completely surprised by these card vulnerabilities

“Security by obscurity” issue

- Derided in academic community
- But subtle issue: also for hardware?
  - HW reverse engineering more common (Nohl)
- Rewards, for producers, in general:
  - more points in Common Criteria evaluation
  - keeps off competition / cheap clones
  - mechanism to enforce quality standards for licence holders
- **Not reasonable** for crypto algorithms & protocols

IV. *Quid nunc?*

What next? NL Options I

I. Proceed roll-out as planned
- "we can handle" approach, used until Apr.'08
- No longer an option, also politically

II. Roll-out old cards and upgrade asap
- Introduces legacy problem from the start
- Fragile: handle both old (broken) & new cards
- Current strategy

III. Postpone roll-out to new cards
- Simpler but longer delay

What next? NL Options II

IV. Major upgrade: also renew backoffice
- with privacy-friendly, open architecture
- should have been chosen in the beginning

V. Stop the current OV-chip project altogether
- Complete loss of investement & prestige
  (not unique: has happened with Sydney's Tcard)
- Wait for payments via mobile phones (NFC)
  - standard not foreseen before 2012
  - will it be any better?

Ongoing own research: OV-chip 2.0

- Build data/privacy protection deep into the architecture (no Stasi-style database of all trips)
- attribute-based, not identity-based, access
  - Possession of valid monthcard enough to make trip
- Crypto protocols already exist
  - based on zero-knowledge proofs (Brands/Idemix)
  - computationally heavy
  - challenge to get them on smart cards
- Next big step in idenitity management
  (supported by NLnet)

V. Conclusions

Conclusions I

- Mifare Classic is broken
- *Security by obscurity*: does not work
- *Secrecy of convenience*: invoke secrecy argument to hide own failures (?)
- As a society we still need to learn how to properly employ ICT. Basic issues:
  - central vs. decentral architecture
  - open vs. closed design & evaluation
  - in times of identity fraud & datamining, personal identities & data need better protection

Conclusions II

- Transport Ministery could have played stronger role
  - define requirements & architecture, for market ("architecture is politics")
  - requires own (not outsourced) expertise & vision
  - useful lessons for *Road Use Charging*.
- NL has strong computer security community
  - nuisance or opportunity (if you can make it there. . .)
  - NL now also exports eco-technology (after environmental disasters, at first)

Conclusions III

- Common defence: everything can be broken
  - Sometimes also: "by such smart guys"
  - But properly designed system is practically unbreakable
- Design modularly; plan for critical HW/SW/Crypto updates; review regularly
- Culture of NDAs (non-disclosure agreements) hampers critical feedback
- Logical formalisation irrelevant for Mifare attack, but possibly useful in certification

Finally. . .

Thanks for your attention!