Privacy and security issues in e-ticketing

Bart Jacobs

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

Joint work with Pim Vullers, Jaap-Henk Hoepman et al

FCS-Privmod 2010

Outline

Mifare problems: card vulnerability & privacy
- E-ticketing in NL & elsewhere
- Privacy in e-ticketing
- Mifare Classic
- Current situation

Privacy-friendly solutions
- Anonymous credentials
- Elliptic Curve Crypto with pairing
- Card-terminal protocols
- Implementation and Analysis

Conclusions

The Mifare Team

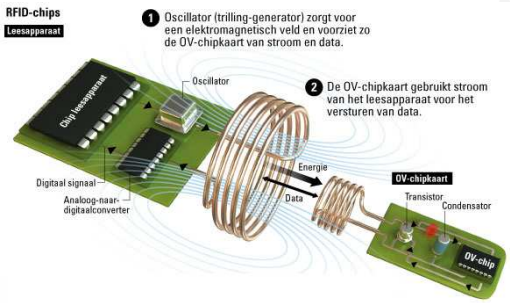
Flavio Garcia, Wouter Teepe, Peter v. Rossum, BJ, Vinesh Kali
Ruben Muijrers, Roel Verdult, Gerhard de Koning Gans, Ravindra Kali

Some publications & publicity

- F. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R. Wichers Schreur and B. Jacobs, *Dismantling Mifare Classic*. In: ESORICS 2008, Springer LNCS 5283, 2008.
- F. Garcia, P. van Rossum, R. Verdult and R. Wichers Schreur, *Wirelessly Pickpocketing a Mifare Classic Card*. In: Security and Privacy, 2009. Outstanding Paper Award
- B. Jacobs and R. Wichers Schreur, *Logical Formalisation and Analysis of the Mifare Classic Card in PVS*, Techn. Rep.
- *University Hackers Test the Right To Expose Security Concerns*, Science, 322(5906), nov. 2008.
- Item at BBC World's Click, Oct. 10, 2008.

Smart cards, with or without contacts

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



Timeline I

1. **'07** student projects start at RU, at first focusing on (free) parking (Roel Verdult & Gerhard de Koning Gans)
2. **Dec.'07** Karsten Nohl & Henryk Plötz present hardware attack on Mifare Classic, at Berlin Computer Chaos Club
   - Crypto1 stream cipher of Mifare reconstructed; not revealed
   - No (demonstrated) retrieval of secret keys
3. **Jan.'08** Roel Verdult demonstrates cloning of disposable OV-chipcard on national TV News
4. **March'08** RU breaks Mifare Classic and retrieves keys
   - Attacks demonstrated
   - National authorities & card producer NXP informed
   - Much national & international publicity
   - Intention to publish in half a year announced
5. **Mid April'08** Security vulnerability verified for London's Oyster card (on a quiet DLR station); top-up possible.

Timeline II

6. **July'08** NXP takes university to court in order to get a publication ban — but fails
7. **Oct.'08** Publication of Mifare Classic design & vulnerabilities at ESORICS conference
   - Algorithm appears on the web (not by Nijmegen)
   - Roll-out of OV-chip in NL continues
8. **Jan.'09** Rotterdam restricts metro ticketing to OV-chip
   - RU tops-up balance of journalists with 1 cent
   - Cards are not blocked; TLS claims they did detect
   - Much panic & (political) animosity
9. **May'09** Publication of card-only attacks at Security & Privacy, using more (embarassing) vulnerabilities
   - Card now completely broken
10. **Early'10** Number of manipulated cards appear in the wild.

Entrance gates with chipcard readers

E-ticketing 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

- Mifare Classic 4K smart card for travellers
- Complex nationwide infrastructure, with many parties and stakeholders
- Much secrecy about the whole set-up. Initially:
  - 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!
- Sector has learned tough lesson—and has changed (see eg. *open ticketing* initiative, see `openticketing.nl`)

OV-chip: three different cards

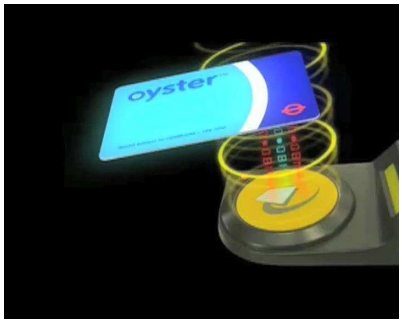
- **Disposable** non-reloadable card for incidental use, based on *Mifare Ultralight*
- **Personal**, (auto)reloadable card, with possible discounts, based on *Mifare Classic*
- **Anonymous**, reloadable, without discounts, also with *Mifare Classic*.

Only *Mifare Classic* has cryptographic protection

E-ticketing with Mifare Classic, elsewhere

- Used in many other places: London (Oyster), Boston(Charlie), Moscow, Beijing, ... (apparently $\geq$ 100 cities, worldwide)
- All these systems are broken, and will have to be replaced, at some stage.
- E-go system in Luxemburg:
  - Seemingly low risk because of small distances & low amounts, but restoring multi-ride cards may be lucrative
  - Weak set-up, where all cards have the same keys
  - Once these keys become public, cards can be read/manipulated easily
  - Apparantly no back-office for monitoring/fraud detection

The Oyster case



What we did in the UK

- **(Mid April'08)** Live vulnerability test in London by MSc students:
  - Keys retrieved from several Oyster cards
  - Balance changed (upwards), enabling further travelling
  - One gate accidentily blocked
- **(End April'08)** Official notification to UK transport ministry which informed Transport for London (TFL).
  - gate-blocking vulnerability also reported
  - TFL never reacted.
- **(Summer 2009)** Bit of background advice in Imperial College student project
  - Algebraic attack of Courtois (UCL) re-implemented with simple card reader
  - reconstruction of card data layout, both for Oyster (diversified keys) and Imperial's access cards (all cards with same key)

Anecdote

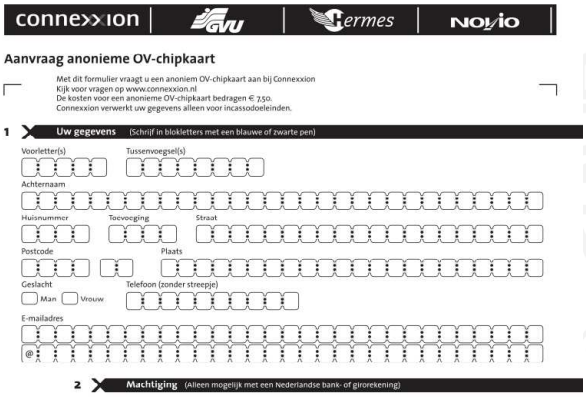
On their way out of London in April 2008, the Nijmegen MSc students saw these boxes . . .

. . . and were tempted to throw in an Oyster card with a balance of £100.000.

They had to catch a plane and had no time to do so. But it can still be tried!

We take your privacy very seriously!

Application form for anonymous OV-chip with lots of questions . . .



connexxion | GVU | Hermes | NOVIO

Aanvraag anonieme OV-chipkaart

Met dit formulier vraagt u een anoniem OV-chipkaart aan bij Connexxion
Kijk voor vragen op www.connexxion.nl
De kosten voor een anonieme OV-chipkaart bedragen € 7,50.
Connexxion verwerkt uw gegevens alleen voor incassodoeleinden.

1 **Uw gegevens** (Schrijf in blokletters met een blauwe of zwarte pen)

Voorletter(s) Tussenvoegsel(s)
Achternaam
Huisnummer Toevoeging Straat
Postcode Plaats
Geslacht Man Vrouw Telefoon (zonder streepje)
E-mailadres
@

2 **Machtiging** (Alleen mogelijk met een Nederlandse bank- of girorekening)

Privacy issues I

- Cards have fixed anti-collision identifier (UID) that shows up in electromagnetic field, making people universally recognisable
- Cards are broken, so your recent travel history (10 trips) can be read surreptiously (by someone sitting next to you in a bus)
- Back-office stores travel logs for seven years in NL (apparently enforced by tax office)
- Long fight in NL between transport companies and data protection office, yielding half-baked compromise:
  - opt-in for direct marketing
  - opt-out for "more aggregated" profiling for optimised travel advice, in order to stimulate the use of public transport

Privacy issues II

- Anonymous cards are a sad joke:
  - unattractive: no off-peak reduction
  - cards are traceable; travel history is recorded
  - privacy easily compromised, whenever cardholder is identified:
    - when you order your card via the web, see ealier form
    - when you charge with bank card, anonimity is compromised (charging with cash possible at only very few places)
    - whenever you want restitution after transaction failure
- For subscription/student cards check-in and check-out is compulsory (so that people are traced)
- Law enforcement authorities have discovered this data feast
  - "public transport tap" to be expected soon

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

Mifare Classic essentials

- Developed in Austria, bought 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)

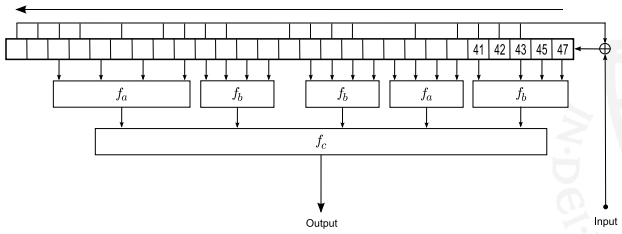
Mifare protocol

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

Essential (card) ingredients: "Crypto1"

- **Random number generator**
  - Only 16-bit LFSR, revealed at CCC; predictable
- **Stream cipher LFSR**
  - 48-bit, apparently first discovered by Nohl & Plötz (but published at ESORICS'08)
  - Fully reversible
- **Filter function**
  - produces stream bits from LFSR; essential secret
  - Also reversible, through weakness

LFSR Schematics, now public



Main design weaknesses

- In the LFSR:
  - regularity of feedback connections, at odd positions
  - first bit included in feedback; hence LFSR can be rolled back.
  - Complexity reduced from $2^{48} = 281.474.976.710.656$ to merely $2^{21} = 2.097.152$ bits.
- In the communication:
  - 'one-time' key stream re-used for parity bits, leaking one bit of information per byte
  - In successive sector authentication the nonce is predictable and encrypted with (new) sector key, leaking 32 bits key info
- Failed authentication gives encrypted (known) error code!

Esorics oct'08 publication

- Mathematical details appeared in okt'08; manuscript sent to NXP before summer (and to "Dutch NSA/GCHQ")
- Mid july'08: NXP tries to stop "irresponsible" publication, via court injunction.
- We argue: providing legal protection to companies with crappy products is not a long-term societal interest
- Judge refuses to forbid publication, basically on freedom of expression. Judge also stated:
  - University acted with due care, warning stakeholders early on
  - Damage not result of publication, but of apparent deficiencies in cards (!!)
- NXP did not appeal

What are open source developers doing?

- First open implementation of cypto1 appeared in okt'08, under the name crapto1
  (hosted on code.google.com/p/crapto1)
- Open hard/soft ware available:
  - Proxmark generic device, see proxmark.org
  - NFC library eg. for cheap Tikitag reader, see libnfc.org
- All software is now openly available for reading/manipulating Mifare Clasic cards, but not yet for script-kiddies.
- A few manipulated OV-chip cards have shown up in the system (not by Nijmegen); one person got arrested.

What are Mifare Classic operators doing?

- Different reactions in access control:
  - At first mostly denial by integrators
    ("our systems are secure, are not affected")
  - Ministries in NL have accelerated move to new card
  - Military in NL continued Mifare Card project
    ("we already payed for these #! ∗ %!∗ cards")
- Transport sector in NL (TLS):
  - Migration plan developed
  - NXP's advanced SmartMX (Java) card chosen
  - Migration will start when fraud levels become too high
  - First card-to-card migration in the world
  - Separate open foundation handles standards, see openticketing.nl, and funds two PhDs

What are academics doing?

- Mifare Classic is dead, (also) as research topic.
- Much attention for anonymous credentials on smart cards: part II of the talk.

Context

Currently

- Smart cards are "Big Brother's little helper" (Stefan Brands)
- With OV-chipcard / Oyster / Charlie / . . . , you tell who you are when you get on a bus, metro, train, . . .
- As we have seen: serious privacy concerns!

Possible solution

- Attribute-based autorisation
- Anonymous credentials: card only says "I'm a first class year pass valid in 2010"
- *Subtle point*: attribute may be non-identifying, but signature may be used for tracing cards/individuals

Credentials

Why anonymous credentials?

- Identity-based solutions violate their users' privacy (and increase identity-fraud risk)
- Anonymous credentials can provide same level of security
- Such attributes are sufficient for functionality

Why yet another approach?

- We think we can do better/faster
- New approach based on Elliptic Curve Cryptography (ECC)
- Blinded signatures via bilinear pairings

Related Work on Smart Cards

- Bichsel et al. (IBM Research, 2009), ± 7.5 sec
  Camenisch & Lysyanskaya anonymous credential system
- Tews & Jacobs (RU Nijmegen, 2009), ± 5 sec
  Selective disclosure of Brands; now in Microsoft's U-prove
- Sterckx et al. (KU Leuven, 2009), ± 3 sec
  Direct anonymous attestation

Our results

- Batina et al. (RU Nijmegen, Cardis 2010), ± 1.5 sec
  Self-blindable certificates of Verheul
- Current (optimised) running time: < 0.8 sec

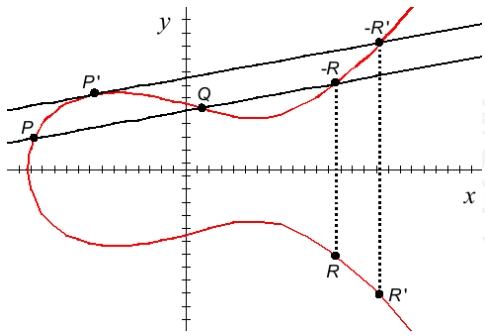
Transport sector requires less than 0.3 sec transaction time!

Elliptic Curve Cryptography

- Koblitz and Miller proposed the use of elliptic curves for cryptography in the mid 1980's
- Nowadays this technology is widely accepted
- Provides the functionality of RSA and more
  - Smaller keys
  - Pairings
- Standard public key cryptography for embedded platforms

The Operations

- Point addition: $P + Q = R$
- Point doubling: $2P' = R'$



Elliptic Curve Cryptosystem

- Point multiplication (repeated addition): $k \cdot P = Q$
- *Easy* to compute (double and add)
- EC discrete log problem: Given P and Q, determine k
- This problem is believed to be *hard*

- Point multiplication is a one way function which can be used to build public key cryptosystems
- The public key is Q; and the private key is k
- Allows for key agreement (Diffie-Hellman), signatures (DSA), encryption (ElGamal), and more ...

Pairings

- A bilinear pairing is a map $e : G_1 \times G_2 \to G_T$ which is bilinear, that is, linear in both components:

$$\begin{array}{rcl} e(P + P',\ Q) & = & e(P,\ Q) \cdot e(P',\ Q) \\ & \text{and} & \\ e(P,\ Q + Q') & = & e(P,\ Q) \cdot e(P,\ Q') \end{array}$$

- As a result, $e(n \cdot P,\ m \cdot Q) = e(P,\ Q)^{n\,m}$

Self-blindable signatures

Pairing-based Signatures

- Signature $S = s \cdot P$ over a point P is multiplication by a private key s
- Check $e(P, s \cdot Q) \stackrel{?}{=} e(S, Q)$ to verify a signature S over P: both sides are equal to $e(P, Q)^s$.

Self-blinding

- card generates random blinding number b
- forms new pair

$$\begin{array}{rcl} P_b & = & b \cdot P \qquad \text{with signature} \\ S_b & = & b \cdot S = b \cdot s \cdot P = s \cdot b \cdot P = s \cdot P_b \end{array}$$

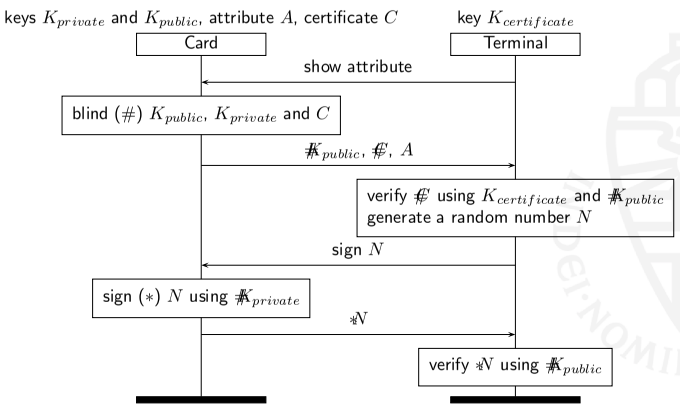
- Verification of blinded P and S: $e(b \cdot P, s \cdot Q) = e(b \cdot S, Q)$

Set up for attribute proving

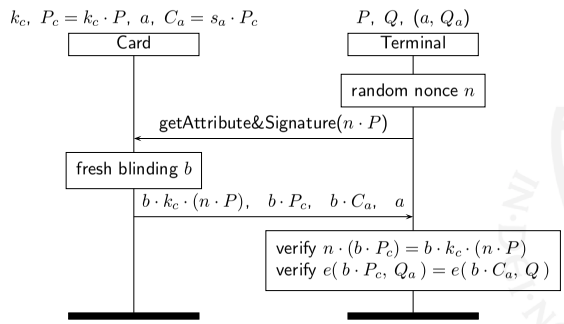
- Public fixed point Q and a finite set of attributes
- A secret key s_a and public key $Q_a = s_a \cdot Q$ for each attribute a
- The associated pairs $(a,\ Q_a)$ are publicly know, and stored in all terminals together with the fixed point Q

- Card c generates a key pair $k_c, P_c = k_c \cdot P$
- Private key k_c is stored in a protected manner, in the card
- Card c receives an attribute together with a certificate $C_a = s_a \cdot P_c$ linking its public key P_c to the attribute a

Sketch of the Protocol



Optimised protocol for Attribute-proving



Java Card Applet

The platform

- Java Card: Java language with specialised (limited) API
- Support for ECC by the cryptographic coprocessor: primitives for EC Diffie-Hellman (DH), EC DSA and key generation

Implementation details

- *Abuse* EC key generator to generate blinding factor
- *Abuse* EC DH primitive for point multiplications

Terminal Application

Components

- Bouncy Castle Library with an extension for Pairings
- `javax.smartcardio` Smart Card IO Library

Implementation details

- Needs to cope with the shortcomings of the Java Card applet
- Point reconstruction: derive y using $y^2 = x^3 + ax + b$
- Signature verification: just guess the sign
- Certificate verification: exploit bilinearity property: either $e(b \cdot P_c, Q_a) = e(b \cdot C_a, Q)$ or $e(b \cdot P_c, Q_a)e(b \cdot C_a, Q) = 1$

Test Results

key length (bits)	attribute & signature (ms)	verification (ms)	protocol total (ms)	communication (bytes)
192	787	116	904	155
160	645	102	747	135
128	535	82	617	115

key length (bits)	key generation (ms)	key agreement (ms)	processing overhead (ms)
192	379	98	114
160	307	78	104
128	242	62	107

Analysis

Achievements

- On-card time of below one second is possible
- Cryptographic coprocessor is used for all calculations
- Amount of communication is far less than RSA approaches: only 155, 135 and 115 bytes for key lengths of 192, 160 and 128 bits, fitting in one adpu

Issues

- Key generation on the card is time consuming
- The card only returns the x-coordinate of the blinded values point reconstruction (involving guessing) is required
- Not fast enough for actual use (recall: 300 msec requirement)
- ECC support on the smart card is rather limited, sofar

Challenges

Privacy The attribute may be used for tracing
- Use a small set of fairly general attributes

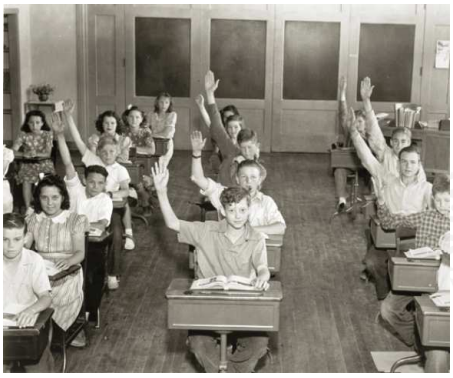
Efficiency This protocol proves only a single attribute
- Combine multiple attributes into a single point

Revocation Not supported by the current protocol

Ongoing work: attributes for Identity Management

- Integration of attributes in national identity cards with PKI functionality
- After PKI-based authentication, attributes ('over 18', 'over 65', 'citizen of Nijmegen' etc) can be obtained from government portal
- Blinded attributes can then be used online, e.g. at webshop
  - Note: card/user can keep track of which blinding is used for which shop, so re-use of attributes can be traced
  - Challenge: shops must not be able to re-blind
  - timing is less critical in such applications.

Main points

- Mifare Classic lessons:
  - Security by obscurity does not work; may even work as cover-up of failures.
  - Wake-up call for both producers and operators: independent investigators and individuals use systems in various ways
  - security and privacy issues can make or break large ICT-projects
- Privacy of travellers seriously compromised by current approach in e-ticketing
- Good news:
  - Anonymous credentials on smart cards are becoming possible
  - Major bottleneck is the limited access to the cryptographic coprocessor of the smart card
  - Will the sector want to use anonymous credentials? Who pushes/forces them?

Thanks for your attention! Any questions/remarks?