A Not So Smart Card -
but no card can be smarter than its issuer

Bernd Fix <Bernd.Fix@aspector.com>, Zürich / Switzerland

The story I am going to tell you in this lecture is quite long - it actually spans a 23 year period – but I think it is an interesting lesson about computer security in "real life": we as hackers tend to over-estimate the technological aspects of security problems and solutions, therefore its always interesting to shed some light on other forces that govern the process...

What we are talking about...

The Postcard is a debit card issued by the Swiss PostFinance since 1991. It can be used to withdraw money from so-called "Postomaten" (PostFinance-owned ATM, introduced in 1978) as well as from "Bancomaten" (ATM owned by another bank, "EC-Automaten", introduced in 1968) in Switzerland and abroad. It also allows on- and offline payments at many EFT/POS -Terminals (discounters, gas stations, ticket machines, telephones,...) and is used by around 2.4 million people in Switzerland, generating a yearly revenue of over eight billion Swiss Francs with 700 million transactions. Cards are valid for a four year period.

What happened?

It all started in Zürich four years ago, when a student, who had owned a Postcard for some years, got unexpected mail from the PostFinance. The letter informed him that his Postcard "is full" and he was advised to use the new accompanying Postcard from now on and to discard the old one.

This may happen many times a year in Switzerland, but this case was special: the student was bright enough to ask one simple question: "Full of what?" and to ask the PostFinance for an explanation. In a reply they stated that all transactions are logged on the card itself. So if someone used the Postcard "over standard", the transaction log on the card runs out of space rendering the card itself unusable for further transactions.

But the student was not only bright but also a civil rights activist involved with the BigBrother Awards in Switzerland. He didn't took the answer for granted – he wanted some independ research on this. So he sent his old card and all letters to a Chaos-related smartcard expert in Germany.

First of all you will look at the chip itself. Some manufactures have their name on the chip; sometimes you can identify the chip by using reference books. Knowing the manufacturer certainly helps in further investigations. The chip on the Postcard was identified as a Bull CP8 – a chip with a long history; it was first introduced in 1979. Since its newer versions are ISO 7816 compliant, the next step was to find the class codes supported by the card. No surprise that "BC" is supported – it is kind of "standard" for bank-issued cards. You can now check some ISO 7816 instructions (like "B0" to read data from the card) to see what happens.

Maybe you find some interesting data – maybe you don't. If you don't have access to an actual terminal so you can log the communication between the card and the device (directly or with the help of a logger card), you are normally stuck at this point. Only a lucky punch can now help you to untangle the card secrets...

Such a lucky punch happened in this case – and it was Google hitting the problem really hard:

```
Bull CP8 "BC B0"
```

On the very first result page you find a French website http://www.parodie.com/monetique that may be overseen on first sight; indeed we are doing serious work and are certainly not interested in funny jokes about money. But believe it or not: this side holds all the information we have been looking for – and much more.

L'affaire des cartes bancaires

The website describes the case of Serge Humpich, an electronic engineer from France, who was able to reverse engineer the french banking card "carte bleue" (blue card) based on a Bull CP8 after four years of work. In mid-1998 he was able to successfully draw a ticket from a ticket machine with a cloned card. Although this was a demonstration for journalists to proof the insecurity of the system, he was consequently charged for computer crime and got a two year probation. France had always its unique way to deal with computer security problems as the CCC knows from own experience.

France had been an early adoptor of smartcards in the banking industry. The specification for the card in question dates back to 1983; deployment of actual chipcards started around 1988 and was complete in 1992 – all banking cards had the chip on them to allow electronic payments. Banking cards issued after around 2001 have an enhanced security, but it is still possible to clone existing cards.

Insecurity Reloaded

It doesn't take much to try out the procedure described for the French banking card on the Swiss Postcard – we have nothing to loose...

Can you imagine the surprise to find out that the Postcard is identical to the old French banking card? Acutally you can follow the tutorial on the French website step by step – and it all works for the Swiss Postcard just as described.

After realizing (and verifying) the implications of this discovery - "Does the Postcard also have the same weakness?" any hacker will be in a very different mental state for some days. An ethnologist who wrote a thesis about computer hackers a few years ago, said hackers live in two different modes: "Teaching mode" and "Learning mode" - she simply missed the "God mode".

Let's dive into the technical details and see what this means: When the system was designed in 1983, it was targeted a large user base (millions of people) utilizing many EFT/POS terminals. Back then having all terminals online with the bank computer system for authentication was simply wishful

thinking. So the card had to be able to authenticate itself during an offline transaction.

The design uses a simplyfied form of digital signatures to provide that offline authentication. The card issuer holds a RSA key pair; the public key is hard-coded into all card terminals and the private key is used to “sign” cards. For that purpose the write protected memory of the chip contains two data areas:

- The first block contains information like cardnumber, valid from/to, cardholder name and some other bank internal data in **plain** text (binary/ASCII)
- The second data block contains information from the plain text encrypted (signed) with the private key of the card issuer (**cipher** text).

During an offline transaction the terminal reads both data blocks from the card and uses the built-in public key of the card issuer to decrypt the cipher block. It then checks if that decrypted information is identical to the plain text data; if it is, the card is authenticated.

You may now ask: “What about the PIN you have to enter?” - To put it plain: a PIN is not really needed. This step is all about proving the authenticity of the card, not of the cardholder! Actually I have heard about gas stations in Switzerland, where you can “pay” for gasoline on a terminal without entering a PIN...

But the PIN for the Postcard is not a complete fake: The PIN authorizes access to the writable memory of the chipcard, and as you might guess: That's the transaction log we heard of in the beginning. The terminal tries to log the transaction on the card and therefore needs the PIN for authorization. If it can't write that log entry, the transaction is aborted (that's why “full” cards are unusable).

Cloning an (exisiting) card

By now we know how to clone an existing card: Read plain and cipher data from an existing card (you don't need the PIN to do that!) and put them into a cloned card (PIC) that behaves like a real Postcard. Of course you design a new command handler that accepts any PIN value for authorization. On the French website such cards are called “YesCard”, because the say “Yes, correct PIN entered” regardless of what you type.

Fine, we now can clone existing cards, but we still need to have physical access to them to retrieve the data. But what about creating new “authentic” cards?

To issue new cards yourself you only need one thing: the private key of the legitimate card issuer – and that is something built into the production hardware; quite well protected I guess. So the only way to get the private key is to factorize the RSA modulus of the key pair.

This is normally just another “no go” situation: Factorizing large numbers can be really, really hard – the largest (publically) factorized modulus at the time of this writing is around 768 bits (a little bit smaller indeed) and was factorized with some 5'000 computers in a few weeks. Therefore an expected length of 1024 bits for the modulus would put an end to our investigations.

Our first job is to retreive the modulus. This is normally not a problem because the modulus is a “public”

information and is contained in the certificate for the public key of a signer. But in this case the design is simplified; there is no CA, a certificate or anything like that – just a key pair. The public key is built into the terminals, but it is not publically available.

Assuming you have no access to a terminal to rip the public key out of it, you need plain and cipher texts from two Postcards to compute the modulus yourself; all that is explained quite well on the french website. Once you have computed the modulus you start to understand where the **real** problem is: the length of the modulus is just 320 bits.

Anyone up-to-date in cryptography knows we are currently discussing the security of RSA-1024 and beyond; so talking about the security of RSA-320 is a waste of time – there simply is none. Back in 2002 it took me about 24 hours to factorize this modulus on a standard PC using an optimized mpqs4linux.

Once the modulus is factorized you can compute the private key of the card issuer and start producing new “authentic” cards. These cards are accepted by all terminals; they cannot tell the fake.

Of course you need to take care of the magnetic stripe on the card as well; I will not elaborate on this in this talk – but it's interesting matter for sure.

Chaotic procedure

There is a kind of standard Chaos approach in cases like this that worked well in many cases over many years: First of all it demands to have the first talk with the company involved, not the press. Getting in contact with PostFinance was a bit harder – all three of us were aliens. Not just to the company culture (that's the normal case), but also in terms of nationality. But in the end we had a meeting with high-ranking officials and board members of PostFinance in Bern.

The second important point is not only to talk about the technical problem, but also about its implications. And these implications actually supercede the technical problem.

If you are a customer of PostFinance and request a Postcard, you sign a contract that lists your obligations (“Terms of Use”) - keeping the PIN secret and separat, not giving the card to anyone and things like that. In case of card misuse (somebody else draws money from your account) you are in a bad legal position: You have to proove that you fully obliged to the “Terms of Use” - and that's simply impossible. One the other hand PostFinance can claim a “secure system”, so that misuse is only possible if you have written down your PIN (possibly on the card) or gave the card and PIN to someone else intentionally. So generally the best you can get is a 40-60% refund (depending on your liabilty / attorney), but you have to sign another contract that you will not take any further legal steps.

This argument is of course no longer valid – if the system is **not** secure, fraud can happen to a customer that did nothing wrong. A misuse of a card is possible without physical access; all you need to know is the card number and validity period (that's the signed information).

While the PostFinance officials were pleased we showed them something they should have known for

years, they were quite talkative. But out of a sudden they quitted the meeting; just at the moment when we started to talk about the breakdown of their legal argument and the requirement for a new refunding policy in case of card misuse.

Our next step would have been to inform the EBK (“Eidgenössische Bankenkommission”), the controlling authority for swiss banks (and banks operating in Switzerland) – but the PostFinance is not a licenced bank, just a company that is allowed to “deal with money”. They are still controlled by the government (not only in terms of shares but also in terms of responsibility), and belong in a sense to the UVEK (“Umwelt,Verkehr,Energie und Kommunikation”) department headed by Moritz Leuenberger. This person also happens to be the active president of Switzerland – nonetheless he got a letter where he was informed about the problem, its implications and our feeling that the PostFinance is not willing to draw consequences in any direction. In his reply he ensured us, that the problem was well received and that of course adequate measures are on the way to provide further security.

Four years after

There are many reasons why we stopped working on this, especially why this was not published in 2002. Most of these reasons have nothing to do with the case itself; in the end the Postcard simply drifted out of focus.

A few month ago I remembered it again while working on some smartcard applications. So just for the fun of it I asked some friends of mine with Postcards for a donation: card data. I wanted to know what was changed in the last four years. Did they design a new (possibly) EMV-based solution? Did they change the key length (that's what the French did)? Did they at least change the compromissed issuer key?

I was prepared to refactor another modulus – but that was unneccessary. The very first analysis showed that nothing had been changed – not even the compromised issuer key had been replaced. My first thought was: We were quite right with our feeling that the problem was not well received by PostFinance.

Lessons learned

The second thought of course is: “Money rules the world”. Although the phrase is a bit simplifying, it is still true in its consequences. And I remembered the PostFinance officials when they talked guarantees the gave EFT/POS clients for investment protection – so it makes sense to try to understand the behaviour based on costs, ROI and so on.

I will not explain the details our our cost estimates for the different options possible – that's a lecture in its own rights. To put it short: Money is not likely to be the reason. Costs for a technical solution would range between 0.1% and 0.3% of the yearly card revenue (depending on the scenario and solution); something you can certainly spend to solve a serious problem and still make a huge profit that year.

If you do nothing, your reputation is at risk. It will cost you some spin doctors to keep it intact or to

rebuild it if necessary. But you probably can't have that for less than 0.1% of the card revenue – and it's still risky. If the strategy fails, your loss caused by client behaviour will supercede any possible cost for a technical solution – that's what we all think.

I start to believe that we also overestimate the “reputation” factor – at least in Switzerland: Its enconomy is much more oriented towards an American capitalism (which for some unknown reasons is called “liberal”) and “consumer protection” is simply underdeveloped.

What will happen, if we proove the insecurity of the Postcard by using cloned cards and publish the results? Sure, there will be press coverage – at least for some days. But will Postcard users understand the implications? When you read about “phishing” and things like that nearly every day and computer insecurity seems to be “normal”, a single case is forgotten quite soon. And PostFinance officials certainly know that...