HTW Berlin, IMI-B, WTAT1: Cryptography

Smartcard Cracking Research Paper

Felix Lausch & Jan Schelhaas

What are Smartcards?

Smartcards, also known as Integrated Circuit Cards (ICC), are credit card – sized paper or plastic cards with a chip that controls access to the card's data and often has cryptographic capabilities. Most modern smartcards use RFID for communication in the 13.56 MHz High Frequency Spectrum. They are powered by a card reader when in proximity (about 0 – 10 cm) and do not have any other power source. A lot of cards also feature a golden contact square, which allows for direct communication with a reader.

Examples for smartcards include Credit Cards with Chip, which are the only type credit cards issued in Europe, Cards for public transportation and the Mensa Card of the HTW. Smartcards have a microprocessor to ensure security. The limited instruction set of these processors allows for cryptographic operations and access control.[1] Like many other electronic products, smartcards can be hacked. In this paper we discuss how this can be possible and list examples of successful hacks of smartcards. Based on that information, we will evaluate the security of different smartcards.

We are going to focus on Mifare cards because the producer NXP Semiconductors is the global market leader for smart cards. Smart cards from other producers are not flawless either: You could for example: create a hotel master key from a single room key. But this hack goes way beyond just smart card cracking.

Mifare Classic

For a long time, the Mifare Classic was the most popular product for RFID cards. It is produced by NXP, which was formerly Philipps and introduced in 1994. It is basically just able to store data and give access to read / write operations. It is available with either 1024 or 4096 bytes of memory and uses the proprietary crypto-1 cipher.[2]

The card has a very simple layout and includes storage, a random number generator and a cryptographic processor, using Crypto1. (→Figure 1)

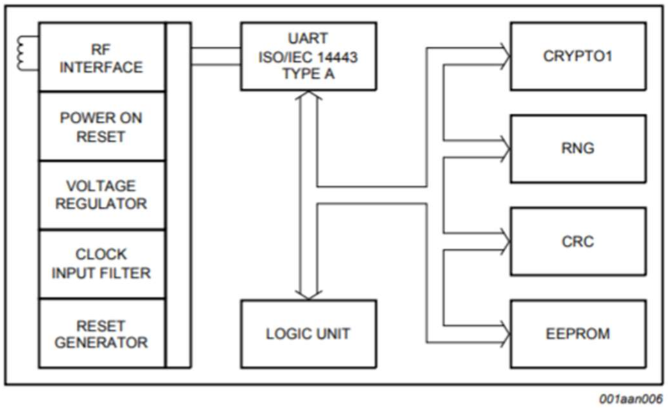


Figure 1: Mifare Classic Schematic, from https://www.nxp.com/docs/en/data-sheet/MF1S70YYX_V1.pdf [2/1/2020 5:06 PM]

[1] https://computer.howstuffworks.com/question332.htm [2/1/2020 4:57 PM]
[2] https://en.wikipedia.org/wiki/MIFARE#MIFARE_Classic_family [2/1/2020 4:41 PM]

OV Chipkaart & Oyster Card are broken

When the vulnerabilities of the Mifare Classic were first rumored, it was the most popular RFID chip around & was widely used for public transit networks, for example in London, Amsterdam, Oslo & Los Angeles. After the release of a paper by Dutch researchers, Bruce Schneier described the security of the cards as "terrible", calling it "kindergarten cryptography", in an essay published in The Guardian.[3] Researchers were able to read out all information on the cards. The paper published on this issue still considered the keys to be secret but said that they "are making good progress in developing a very efficient attack to recover arbitrary sector keys of a Mifare Classic Card"[4]. To no one's surprise people succeeded and were able to clone cards and ride for free on the Amsterdam Metro. The Manufacturer NXP tried to block the release of that paper, arguing that the release would jeopardize the security of their product. NXP's challenge was dismissed by a Dutch court[5], allowing for the release of the secret Crypto1 algorithm used by the Mifare Classic.

Crypto1

The German researcher Karsten Nohl published the Algorithm in 2008 as a Doctoral Candidate at the University of Virginia. He first announced that the Crypto-1 Cipher was broken at 24C3 Conference in 2007. They cracked the Algorithm by scraping of tiny layers from the chip and observing the logic gates under a microscope.[6] When he published the algorithm, the Dutch government still thought that cracking the card would be impractical for a few more years and cost a lot of money. He was able to perform an attack within minutes using commodity hardware. The algorithm was flawed, as it presented a statistical weakness in a filter function, which together with a linear feedback shift register (LFSR), formed the Crypto1 algorithm. The use of a deterministic random number generator on the reader helped facilitate the attack.[7] The main issue of the Crypto1 algorithm was its secrecy. Good cryptographic algorithms never rely on secrecy. The proprietary Crypto1 algorithm was only secure while no one knew about it.

Consequences

Immediately after the findings have been made public TfL, which manages the Oyster Card system, promised to disable cloned cards. In 2009, TfL decided to retire Mifare Classic cards and moved to the more secure Mifare DESFire EV1, which uses the AES-128 standard.[8] New Oyster Cards are therefore no longer susceptible to cloning attacks. The Dutch OV-Kaart still used the Mifare Classic in 2012, when the operator decided to switch to chips from the German company Infineon, called the SLE 77, which allowed a step-by-step migration to newer cards, as it was able to emulate the older ones. This allowed for the charging process to use the new Infineon mode, while for checking in and out, the card would emulate a Mifare Classic until the readers at the stations get replaced.[9] The Mifare Plus is a direct replacement for the Mifare classic and was announced shortly after NXP lost the court

[3] https://www.theguardian.com/technology/2008/aug/07/hacking.security [2/1/2020 2:57 PM]

[4] http://www.cs.ru.nl/~flaviog/publications/Attack.MIFARE.pdf, Chapter 8: Conclusions & Recommendations (Page 14) [2/1/2020 3:15 PM]

[5] https://uitspraken.rechtspraak.nl/#zoekverfijn/ljn=BD7578&so=Relevance [2/1/2020 3:26 PM]

[6] https://www.computerworld.com/article/2537817/how-they-hacked-it--the-mifare-rfid-crack-explained.html [2/1/2020 3:36 PM]

[7] http://www.cs.virginia.edu/~kn5f/Mifare.Cryptanalysis.htm [2/1/2020 3:47 PM]

[8] https://www.alphr.com/technology/1002164/how-does-an-oyster-card-work [2/1/2020 4:04 PM]

[9] https://webwereld.nl/nieuws/security/trans-link-veiliger-ov-chip-niet-meer-van-nxp-3759249/ [2/1/2020 4:16 PM]

battle over publishing the Crypto-1 algorithm, in March 2008.[10] Mifare Plus is used in all contactless credit cards we tested.

The scale of such a vulnerability is huge, as Mifare cards are used all over the world, according to Mifare by over 1.2 billion people in over 750 cities.[11] Every new issue with security in those cards has a significant impact on people and infrastructure all around the world.

Mifare Classic is still in use

Although being broken for over 10 years already, the Mifare Classic is still widely used today. Examples include many hotels, the Danish Public Transit Card, Rejsekort, and the keycards used in gyms by RSG Group (McFit, John Reed & High5) across Europe.

When looking at the member card for McFit, it is very simple. There is just your membership number printed on – and nothing more. The storage of the Mifare Classic 1K, which is 1KB, is completely unused, at all times. The only information on the card is a UUID, which the manufacture of the card, NXP, formerly Philipps, puts on each Mifare Classic they produce. This is comparable to a MAC Address on networking equipment or an IMEI on modern phones. RSG Group uses that UUID to identify you. The studio's computer system will look up that UUID and check if your membership is valid. In their systems, there is also a photo of you, which the studio personnel can look at to verify that the person entering through the gate is also the person that has the membership. This, of course, only happens when there is someone sitting at the front desk to look at the computer.

On first glance, it seems to be pretty secure as all validation is happening on the server-side, the card does nothing on its own. But since Mifare Classic Cards and the crypto1 algorithm have been broken, it is not only possible to read out cards, but also to clone them. While an original Mifare Classic does not allow write access to Section 0, Block 0, which contains the UUID, there are plenty of cards easily obtainable online, that are not original Mifare Classic's and do allow writing to the UUID block. It is therefore possible, when being in proximity of a card, to clone any member card. This is significant, as people tend to not have an eye on those cards all the time, e.g. when taking a shower or just having a chat with someone else. You can use a cloned member card to unlock someone else's locker or identify as that person to a vending machine and use the funds stored on their account to buy snacks and equipment.

All of this is only possible because the Mifare Classic is broken and RSG Group uses the default keys, which speeds up the process of reading the cards even more.

Cloning a member card does not give you access to a studio on another person's membership as studio staff can look at the photo when you enter the studio. But it would allow a person with criminal intent to easily unlock someone's locker or use the funds associated with that card. You should therefore treat your member card like a credit card & use RFID-blocking material around it and never hand it over to persons you do not trust.

We intended to, with studio personnel approval, clone our own member card and try it out but did not obtain the needed cards, which would be Chinese clones of Mifare Classic cards, required to pull this off.

[10] https://en.wikipedia.org/wiki/MIFARE#MIFARE_Plus_family [2/1/2020 4:38 PM]

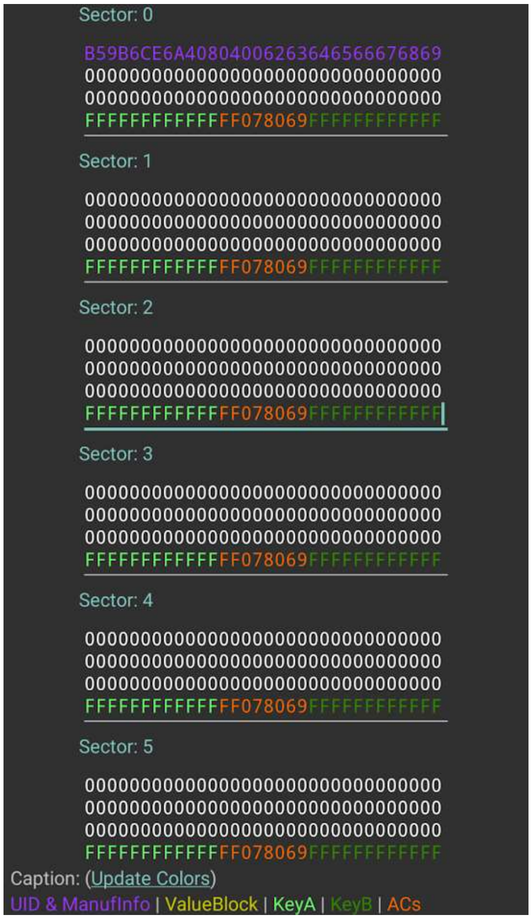
[11] https://www.mifare.net/celebrating-innovation-25-years-of-mifare-and-the-new-normal/ [2/1/2020 5:35 PM]

Clone a Mifare Classic

The Mifare Classic Tool[12] allows anyone with an Android Smartphone to read and write Mifare Classic Cards. It is also able to break the encryption by using a list of default and known keys. The app is able to create a key map on reading a tag and can write data in hexadecimal format. It allows you to edit all sectors of a card and on special, Chinese, Mifare Classic cards, it even allows you to write to the block that stores the UUID. Using the app, you can read a card, store the dump, eventually modify it and write that dump to another card. If you have a card that supports writing the UUID, you can create an exact copy of any Mifare Classic. In →Figure 2, you can see how the dump would look like for an expired McFit Member card.

Mifare DESFire

The Mifare DESFire, which was released in 2002, features a general-purpose Operating System on a chip that is based on the Intel MCS-51 from the 1980s.[13] The card uses the publicly known AES-128 algorithm for cryptographic functions which has not yet been cracked. Given the 128bit key length a brute force is not currently feasible. The first version of the DESFire Card has been cracked in 2011 by the same team that also hacked the Mifare Classic. This time however, cracking the card required expensive equipment and around 7 hours of access to the card.[14] Newer versions of the cards are not vulnerable to that attack.



```
Sector: 0

B59B6CE6A40804006263646566676869
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF

Sector: 1

00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF

Sector: 2

00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF

Sector: 3

00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF

Sector: 4

00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF

Sector: 5

00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Caption: (Update Colors)
UID & ManufInfo | ValueBlock | KeyA | KeyB | ACs
```

Figure 2: Dump of a Mifare Classic

The MensaCard of the HTW uses a Mifare DESFire EV1 chip, which makes it a secure card. It should not be possible to write to the card without knowledge of the proprietary protocols and keys the machines for loading money onto the cards use. Hacking the MensaCard would require reverse engineering one of those machines, but it is highly unlikely that someone could remove one and get away with it.

As with most modern cards, the security is determined by the system in which the card is used. For example, using the same key for each MensaCard would be a vulnerability, as it would mean that only one card needs to be cracked to be able to crack all the others. Using a different key for each card is more complex to implement but ensures that an attacker has little gain from cracking a single card.

Conclusion – How safe are smartcards?

At first glance it seems shocking to see how poor the security on some of the commonly used smart cards is. Most organizations where the Classic card is still in use have applied band-aid solutions that make them safe enough

[12] https://play.google.com/store/apps/details?id=de.syss.MifareClassicTool&hl=en [2/1/2020 4:44 PM]
[13] https://www.alphr.com/technology/1002164/how-does-an-oyster-card-work [2/1/2020 5:13 PM]
[14] https://www.theregister.co.uk/2011/10/10/mifare_DESFire_smartcard_broken/ [2/1/2020 5:30 PM]

for the moment but do not fix the real problem. Applying a quick fix is obviously a lot cheaper than replacing every card and card reader in use.

The RSG group example mentioned earlier is very unsecure. But they do not claim that their lockers are secure and explicitly tell you to not keep valuables in those safes. Copying another person's card just for free gym entry does not seem worth it and the member photo appearing on their display upon entering would probably get you caught sooner or later. The Danish Rejsekort is a similar story. Reading out or copying the information saved on those cards is simple enough. But the information is encrypted before being stored on the card, which makes reading them out rather useless. Students at DIKU however pointed at the aging encryption standard used for this, so this barrier might be breakable.[15] The information is also verified by a backend server when read out by an official card reader, which makes copying them useless in most cases.

Officially NXP states that Mifare Classic cards should not be used in security relevant applications anymore and recommends their Mifare DESFire or Mifare Plus cards instead.[16] Those cards implement known and trusted cryptographic algorithms such as TripleDes or AES and there are no known attacks for their other components at the moment.

Additionally, the last ten years have also shown a big shift in smart card applications. Nowadays most of them are verified by a server, not only does this add another step in the verification process, but it can also offer more convenience for the end user. Lost cards can easily be locked & replaced, and information regarding the card can be changed through the internet as well as the card directly. The only downside of this is that the card readers require a constant internet connection.

We think that modern smart cards like Mifare DESFire or Mifare Plus have reached a point where the security and encryption provided by these cards is so strong, it is unlikely that they are the weakest link in the entire application they are being used in. For security in general, the correct implementation of the technologies being used is more important than the technologies being used. Using the modern cards does not automatically make any application more secure but if done properly, they are a huge upgrade.

[15] https://www.version2.dk/artikel/diku-studerende-saa-let-er-rejsekortet-hacke-13683 [2/1/2020 4:28 PM]
[16] https://www.mifare.net/en/products/chip-card-ics/mifare-classic/security-statement-on-crypto1-implementations/ [2/1/2020 4:12 PM]