

FACT SHEET FS-2008-03

Vulnerabilities of Mifare Classic chips in access passes

Since the beginning of 2008 a much debated topic in news and politics alike was the hacking of the OV-chip card (the RFID public transport card used throughout the Netherlands) and building access passes. This debate was caused by the electronic chip used in both: the Mifare Classic RFID chip. Scientists have discovered vulnerabilities in the chip that enable its security to be hacked. If this happens, data on the chip card can be retrieved and the cards themselves can be cloned. All the research details on this subject were released in October 2008 and in the meanwhile software has become freely available with which the chips can indeed be hacked.

This fact sheet contains further information about the vulnerabilities that have been discovered, and the consequences for access systems that use the chip. First we describe the operation of Mifare Classic chips. We then go into the vulnerabilities that have been discovered and how it is possible to crack the security on the chips. The consequences for the practical applications of the chips are described next. Finally, measures are suggested that could be taken to restrict the risks.

How the Mifare Classic RFID chip works

The RFID chip (Radio Frequency Identification) is an electronic chip that enables short distance contactless exchange of data between a chip and a reader. The use of this chip has increased enormously over the past fifteen years, which is partly due to it being so inexpensive. It is for example used in logistics and retail, but also in building access passes and transaction systems.¹

One of the most commonly used RFID chips is the Mifare Classic by NXP Semiconductors (formerly a division of Philips). According to the manufacturer, more than one billion of these chips have been sold over the years².

The Mifare Classic chip has security mechanisms that protect the stored data. Thus communication between a chip and a reader can be deciphered. The chip and the reader also verify each other's security at the beginning of a transaction (mutual authentication). The key method (the encryption algorithm) used by Mifare Classic in these mechanisms, is called Crypto-1. This algorithm is the intellectual property of NXP Semiconductors and, until recently, its operation was not public. This secrecy contributes to the security intended for the chip.

An overview of the most important facts:

- > Researchers have hacked the security encryption of the Mifare Classic RFID chip - a chip used in the *OV-chipkaart* and in access passes, amongst others.
- > The discovered techniques of attack only apply to the Mifare Classic 1K, 4K and Mini chip.
- > The discovery of the secret encryption method on which the chip's security is based allows the chip to be hacked.
- > The encryption method's implementation contains weaknesses, which makes it much easier for the security to be hacked.
- > Once the security has been breached, card data can be read and, subsequently, passes can be cloned.
- > The researchers published their research details on 6 October 2008. As a result it became publicly known how to hack the security of Mifare Classic chips.
- > On 23 October the first ready-made programme code became available with which one could hack chips. To be able to make use of the programme code in practice it is necessary to combine it with a special RFID reader.
- > Users of Mifare chips in access systems can take additional measures (both technical and organizational) in order to minimize the risks of abuse.
- > In time, migration to improved, more secure access passes (and often pass readers) is in many cases required to combat the risks in the longer term.

¹ See http://www.rfidnederland.nl/upload/bestanden/20070507_122444.pdf

² See <http://www.nxp.com/products/identification/mifare/classic/>

Security vulnerabilities of the Mifare Classic

At the end of 2007 German researchers announced that they had reconstructed the secret Crypto-1 encryption algorithm.³ Apart from the already well-known use of the short 48-bit keys, they identified several weaknesses in the algorithm and the way in which the authentication protocol is implemented in the chip.⁴

Following the German researchers, researchers from Radboud University in Nijmegen announced on 12th March 2008 that they were capable of actually hacking and cloning the Mifare Classic chip.⁵ Their method enables the chip to be hacked in seconds using a standard PC and RFID equipment. These research findings have been validated by the AIVD (Netherlands General Intelligence and Security Service). When this was announced the Dutch Cabinet informed the Lower House.⁶ The researchers then kept the details of their research secret for six months, to give suppliers and users time to take appropriate measures.

On 6 October 2008 the Radboud researchers published all the details of their research.⁷ No new vulnerabilities were publicized as a result, but the cryptographic details underlying the potential to hack the security of the chips (which was announced in March 2008), were made public. The details that were released offer third parties the chance to develop software and hardware to hack Mifare Classic chips. On 23 October 2008 the first application with which to hack chips in practice became available.⁸ To be able to use this software it is necessary to combine this with special RFID equipment (e.g. Proxmark or OpenPCD). It is expected that complete packages of hardware and software will quickly appear on the market.

The vulnerabilities that have been revealed only apply to the Mifare Classic 1K, 4K and Mini chips and the Mifare Classic element of cards which contain Mifare Classic emulation. At time of going to press the Mifare "Desfire" and "Desfire8" are not vulnerable to the developed techniques of attack. The Desfire8 chip uses a publicly known long key encryption algorithm (triple DES or AES). At the beginning of 2008 NXP Semi conductors announced the follow-up to the Mifare Classic: the Mifare Plus, which uses the AES encryption algorithm. No additional information about the security of this chip is available as yet.

The media also focused on the Mifare Ultralight chip, which is used in the daily pass version of the OV-*chipkaart*. The security level of this chip is minimal and the chip is easy to clone⁹. This makes this chip different from the Mifare Classic. Because of the lack of encryption this chip is not generally used to secure physical access to buildings.

Security breakthrough

The aim of hacking Mifare Classic chips in access systems is to gain unauthorized access to secure environments. This is easiest if the access security for an environment is solely based on the unique number of a Mifare Classic chip, the UID. This UID is in fact exchanged between a pass and a pass reader in clear-text. This means that it is possible to listen in on communication between a pass and a pass reader, so as to determine the UID and to consequently place this UID on a new pass. It is possible to gain access to the secure environment with this pass. Access provision on the basis of only a UID is generally used in low risk areas, such as car parks.

Different types of Mifare chips

Type	Vulnerable?
> Mifare Ultralight	🔒 Yes*
> Mifare Classic 1K/4K/Mini	🔒 Yes
> Mifare Desfire/Desfire8	🔒 No

* The Mifare Ultralight is less secure than the Mifare Classic and was therefore already easy to clone.

³ See: <http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html>

⁴ The weaknesses include the encryption being too linear and weaknesses in the random number generator.

⁵ See: <http://www.sos.cs.ru.nl/applications/rfid/persverklaring.pdf>

⁶ See: <http://www.minbzk.nl/contents/pages/91905/briefaantweedekameroverchiptechnologietoegangs-passen.pdf>

⁷ See: <http://www.sos.cs.ru.nl/applications/rfid/2008-esorics.pdf>

⁸ See: <http://code.google.com/p/crpto1/>

⁹ See: <https://ovchip.cs.ru.nl/images/1/15/Ru-report.pdf>

A safer form of access security with the Mifare Classic chip uses identification information that is stored on the chip in encrypted form. It is necessary to crack this encryption in order to read the pass and copy it. This is possible by eavesdropping on the communication between a pass and a pass reader. The cryptographic key can be retrieved by analyzing this communication and access can then be gained to the data stored in the card¹⁰. The data can then be read and stored in a new chip. If a chip reader has no additional security measures in place it will not be able to differentiate the cloned chip from the original chip.

In general there are two different attack scenarios as regards eavesdropping on and decrypting encrypted communication between a pass and a pass reader:

1. *Eavesdropping on communication between a real pass and a pass reader*

By listening to the communication between a real pass and a real pass reader (belonging to the same access system) just once and deciphering it with a cracking programme, the encryption can be broken.

2. *Eavesdropping on communication between a fake pass and a pass reader*

It is also possible to break the encryption code by listening to the communication between a fake pass and a real pass reader (not belonging to the same access system) twice and deciphering it. The advantage of this method for attackers is that they can themselves determine the moment of eavesdropping with a fake pass. It is also easier to decrypt the secret key using this method.

Given recent rapid developments, it is not inconceivable that attacks will be discovered where just a real pass is sufficient to read encrypted material and data from the pass. In this case the attacker does not need to eavesdrop on communication with a pass reader.

The consequences for its implementations

The most important applications of the Mifare Classic chip are in physical access systems and (micro) transaction systems. It is realistic to expect attacks on these applications as soon as resources for hacking the Mifare chip become available. If additional measures are not taken, unauthorized third parties will be able to use cloned passes to gain access to areas that are safeguarded by a Mifare Classic based access system.

However the security of access control systems that use Mifare technology usually depends on more factors than just the chip itself. The ultimate impact depends on the additional measures that have been taken for a particular application. Additional measures can encompass a range of matters, such as the use of security guards, additional access control mechanisms such as PIN codes or biometry, and procedures for the issuing, use and collection of passes.

Which measures can you take to minimize the risks?

Given the risk that access passes based on the Mifare Classic can be hacked, we strongly recommend you take action as soon as possible. The following steps offer a guideline:

- *Determine whether the Mifare classic chip is used within the organization.*
In order to evaluate potential risks and determine whether further action is needed you must first determine whether the Mifare Classic chip or a chip with Mifare Classic emulation is used.
- *Evaluate the existing security measures;*
Access systems often have additional security measures in addition to the Mifare Classic's standard security features. An inventory of these additional measures must therefore be drawn up for each application in order to evaluate the actual impact there may be on your own environment.

How to minimize risks:

- > Draw up an inventory of the applications of Mifare Classic chips in your organization.
- > Determine which security measures are already in place in addition to the chip's own security.
- > Estimate what the level of risk would be once the chip's security has failed and evaluate whether this is acceptable.
- > If necessary, take further measures.
- > Find out whether it would be feasible to switch to a more secure chip in the long term.
- > Check for potential weaknesses in other access systems that are not based on Mifare Classic chips.

¹⁰See <http://www.ru.nl/ds/research/rfid/>

- **Evaluate the risk and if necessary take additional measures.**
Determine whether the existing measures are adequate, taking into account the sensitivity of the protected environments (which can vary within a location). The main question is: do the existing measures offer an adequate level of security, after taking into account the potential damage which unauthorized access to an area may have? If the measures are inadequate it is advisable to take additional measures in order to minimize the risks. See the box below for examples of measures.
- **Consider replacing the Mifare Classic chip with an improved version.**
Depending on the effect and costs of additional measures you may need to consider replacing the Mifare Classic chip with an improved version. Check whether the current pass readers - albeit after a software update - would be compatible with more complex chips. If this is the case, only the physical passes would need to be replaced, which would entail lower costs. Note: as chip replacement is often a lengthy process, taking additional measures will be inevitable.

Final words

It is important to realize that access systems that do not use the Mifare Classic chip may be even weaker than the systems that have now been hacked. This applies in particular to older systems which for example still use magnetic strips or do not use encryption in their communication. Although the level of attention that the media is currently giving the Mifare Classic chip may have a big impact, other physical access control systems must not be neglected.

Potential additional security measures

Here are some examples of the measures you can take to minimize the risks of the vulnerable Mifare chip. The actual measures which need to be taken depend on your particular application. If internal know-how in this area is limited you are advised to contact your supplier or an external expert.

Organizational measures:

- > Install visual controls on passes used for access systems (e.g. the entrance to a building), to monitor unauthorized attempts at access. Attention should be paid to details such as the appearance of the pass, passport photos (if present) and any other visual characteristics.
- > Make the wearing of access passes mandatory. Especially in larger organizations or in locations that have a high number of external staff - or visitors, the wearing of access passes helps identify unwanted visitors.
- > Increase levels of security awareness amongst staff, by communicating the risks and taken measures. In order to identify risks in the first place, the potential risks need to be made known.
- > Introduce procedures for the allocation and collection of passes in order to prevent passes going missing or ending up in the hands of attackers. Point out which action should be taken if passes are lost or stolen (such as blocking passes).
- > Aim to fine tune access entitlement of passes, in order to minimize the consequences of cloned passes. Pay particular attention to crucial spaces.
- > Ensure that procedures for handling and alerting to unauthorized access are in place.
- > Ensure that there are strict procedures for receiving and accompanying visitors. Ensure that the collection of visitor's passes is a general requirement.
- > Monitor and clear out access passes that have been distributed. Block passes belonging to staff members who have left.
- > Be fully alert to suspicious persons hanging around pass readers, in order to obstruct their attempts at eavesdropping communication.

Technical measures:

- > Preferably avoid access controls based solely on the UID of a chip.
- > Do not secure all passes on the basis of the same key, but use key diversification.
- > If possible ensure that the access system rejects passes based on the UID following several failed authentication attempts.
- > Install transaction counters, both in the access system and in passes, so that only sequential attempts are accepted. This is useful in preventing use of copied passes, because in that case the sequential numbering of transactions no longer tallies.
- > Aim to provide physical entry systems with an 'anti-passback' function. This means that a pass will be rejected if entry is attempted on two separate occasions without leaving the premises in between each attempt.
- > Aim to provide a function which enables unauthorized actions to be identified. For example if a pass is presented twice within a short period of time in two separate locations which are far away from each other.
- > Aim to introduce two-factor authentication for the most crucial spaces. Two-factor authentication not only monitors whether one is in possession of a pass, but also checks whether someone knows their pin code, or has a biometrical quality such as a finger print.
- > Supply protective pass holders that prevent the penetration of rays. Keeping passes in a holder means that they cannot be read whilst not in use. However, this does not prevent communication being tapped whilst passes are actually being used.
- > If necessary, deactivate card readers and switch to other forms of access monitoring (such as central door servicing or physical door checks).