Examining the Cyber Security of a Real World Access Control Implementation

Julian Jørgensen Teule
Department of Electronic Systems
Aalborg University
Aalborg, Denmark
jteule18@student.aau.dk

Marius Frilund Hensel
Department of Electronic Systems
Aalborg University
Aalborg, Denmark
mhense15@student.aau.dk

Victor Büttner
Department of Electronic Systems
Aalborg University
Aalborg, Denmark
vbattn18@student.aau.dk

Jonathan Velgaard Sørensen
Department of Electronic Systems
Aalborg University
Aalborg, Denmark
jvsa16@student.aau.dk

Magnus Melgaard
Department of Electronic Systems
Aalborg University
Aalborg, Denmark
mmelga16@student.aau.dk

Rasmus Løvenstein Olsen
Department of Electronic Systems
Aalborg University
Aalborg, Denmark
rlo@es.aau.dk

***Abstract*—As smart cards have become increasingly prevalent in electronic access control systems, this paper investigates an implementation at a national institution, which uses a smart card with publicly known weaknesses.**

The main outcome is a set of recommendations which can be used for securing electronic access control systems against the discovered flaws of this work: The implementation did not follow guidelines from the manufacturer of the cards, the content of the restricted sector was printed onto each card, and in-house services with inherent security flaws were built around the cards, but not maintained.

These flaws meant that the civil registration number of any employee at the institution could be revealed. Additionally, the flaws allowed for changing the PIN code of any card in the system.

***Index Terms*—MIFARE Classic 1K, Crypto1, Smart Cards, Electronic Access Control**

I. Introduction

Electronic access control in enterprises and institutions is widely used. In 2019, 49% of companies with more than 250 employees in Denmark used sensors for security and access control [1].

These systems often utilise the MIFARE Classic Smart Cards, which have had known weaknesses since 2008 [2]. This has been seen in the Dutch OV-chipkaart (Public Transport chipcard) used for public transport, where TNO (Netherlands Organisation for Applied Scientific Research) predicted that the weaknesses enable abuse and fraud [3].

More than 10 years later and MIFARE Classic is still being used, which prompted this work. This work will examine to what extent the smart card access control implementation at a national institution (from now on referred to as NI) can be exploited and the outcome will be a set of recommendations that secures the system against the shown attacks.

The implementation at NI was created in collaboration with a security company operating in Denmark and it allows for the use of smart cards and terminals to grant access to a building or room.

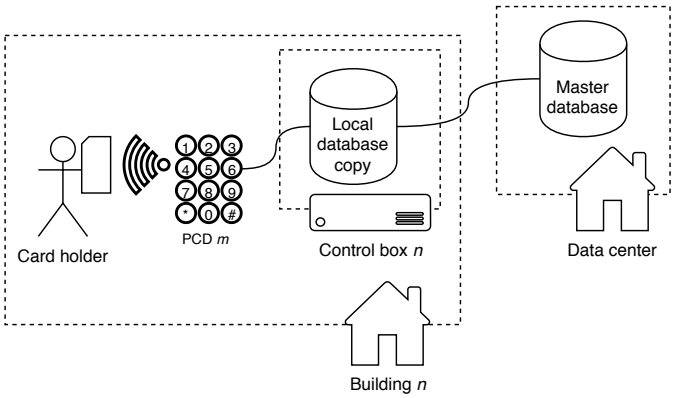

Fig. 1. Simplified representation of the smart card access control implementation at NI.

Section II will cover the known exploits in the MIFARE Classic smart cards, which allow reading and writing of the locked cards. In section III and IV the specific implementation at NI will be examined.

This practical insight will form the basis of the recommendations in section V.

II. Background

The model used at NI is Role-Based Access Control (RBAC) in order for the cards to have different permissions. The smart cards used are MIFARE Classic 1K which are manufactured by NXP and issued by the security company.

The MIFARE Classic 1K has 1 kB of storage which is split between 16 sectors (0 through 15), each containing four 16 byte blocks [4]. The last sector of each block, called the sector trailer, is dedicated to two 48 bit authentication keys, key A and key B, alongside permission bits for each block of that sector. These bits control the read and write permissions of the sector blocks, alongside which keys are needed to have these permissions.

In principle an adversary can not get access to the blocks that are restricted by the permission bits without a correct key [4].

However, these permission restrictions do not quite suffice in practice:

In 2007 Nohl et al. published weaknesses of Crypto1, the proprietary cryptographic algorithm used by the smart cards. These weaknesses were later used to fully reverse engineer the cryptographic algorithm [2].

The main weaknesses revolve around the insufficient size of the keys, the insufficient randomness provided by the 16 bit Linear Feedback Shift Register (LFSR) and the properties of the 48 bit LSFR [2]. Therefore, adversaries can extract the key used to encrypt secret data on a card.

III. Dissecting Smart Cards

NI utilises the content of sector 15 for authentication and sector 15 is the only sector restricted by a non-zero 48 bit key. Sector 15 will be referred to as the restricted sector.

A. Accessing the restricted sector

After investigating the known weaknesses, it became apparent that all of the tested smart cards from NI share the same key. This means if the key to a single smart card is cracked, the key to all the smart cards is cracked, and thus the contents of the restricted sector can be accessed.

B. Contents of the restricted Sector

Using a cracked key revealed that sector 15 is used to store some data. An example of this can be seen in fig. 2.

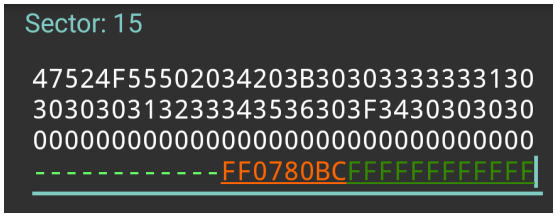

Fig. 2. A cropped screen shot of MIFARE Classic Tool [5] reading a smart card with card number 123456. This requires the sector key which has been removed from the screenshot.

The following pattern appeared when decoding the contents of 12 cards as American Standard Code for Information Interchange (ASCII).

```
GROUP 4 ;0033310
000XXXXXX0?Y0000
```

Where `XXXXXX` is the users' card number and `Y` seemed to vary between `0x30` and `0x3F`. In this pattern, it is speculated that this is a check digit determined by formula 1.

$$Y_{10} = 48 + \left(\left(\sum_{n=1}^{6} d_n - 1 \right) \mod 16 \right) \tag{1}$$

Where d_n is the n'th digit of the card number, 6 is the length of the card number, Y_{10} is the decimal representation of the ASCII character `Y` and 48 is the decimal representation of `0x30`.

C. Card numbers

Since the content of sector 15 depends solely on the card number, the security of the card is reduced to this number. This means that an adversary with access to the global key can duplicate cards using only a users card number.

The six digit card number might provide adequate security if it is kept secret. However several flaws in the implementation and usage of this number were found.

1) Card numbers are printed on the outside of cards, making scanning unnecessary to reveal the data on the locked sector.
2) Card numbers are used for identification, meaning they are not kept secret by employees. For instance, card numbers are written on pieces of paper when requesting permission to access a room.
3) Card numbers are sequential, meaning employees can guess other card numbers by counting up or down from their own.

Even though these flaws allow for remote duplication of cards, many rooms still require PIN code authentication which greatly limits the extent to which the mentioned flaws can be utilised. Section IV will cover these PIN codes and the services built around them.

IV. PIN Codes

PIN codes are implemented separately from the card itself, meaning compromising a smart card will not yield the PIN code. The PIN code is instead fetched from a central database every time one tries to enter. This PIN code is cached at each building, in the case the central database is offline (see fig. 1).

It was discovered that PIN codes are four digit numbers and must not start with a 0, which allows for 9000 different combinations.

NI provided a number of services that made use of- or manipulated PIN codes. As shown in the following sections, flaws in these services could enable an adversary to extract and/or change PIN codes. NI has addressed these flaws as a result of this work.

A. Library Login Page

The library at NI provided a login page where employees could login using their card number and PIN code. No rate limiting was employed meaning PIN codes could be brute-forced if the card number is known. Even though the server did not employ rate limiting, it was very slow. As such, all possible PIN code combinations could be tested in 7.5 hours at a rate of one password every 3 seconds.

B. Set PIN Code Page

NI provided a page where employees could set their PIN codes. To log in on this page, one had to provide a matching Danish Civil Registration Number (CPR number) and card number. The CPR number consists of one's birth date with a four digit number. The parity of the four digits represents sex.

If a person's birth date is known, that person's CPR number has 540 different remaining combinations and half that if the

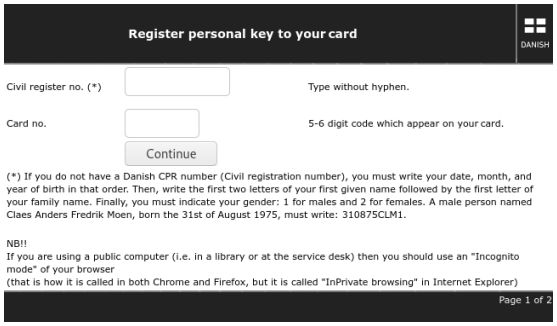

Fig. 3. Page enabling employees to set their PIN codes by specifying CPR number and card number. A flaw enabled changing of PIN codes without specifying correct CPR number.

sex is also known [6]. This enables brute-forcing the login if the card number is known, which also reveals that person's personal CPR number.

It was discovered that this page had two visible endpoints `login` and `pin`. `Login` redirects the user to `pin` if the CPR number and card number are correct, while `pin` enables the user to change the pin for the specified card number.

Unfortunately `pin` did not check if user is authenticated in `login`, meaning PIN codes can be changed without knowing the correct CPR number.

Because of the seemingly sequential card numbers an adversary can generate valid card numbers by counting up or down from an observed card number. This enabled changing PIN codes and/or extracting CPR numbers from card numbers.

V. Recommendations

NXP, the manufacturer of MIFARE Classic 1K, are aware of some vulnerabilities hereof, and as such, has given recommendations with regards to the implementation of the card. Following these recommendations, and keeping up to date with them, will mitigate some of the flaws. The manufacturer recommendations are as follows:

- *Avoid using MIFARE Classic* – MIFARE CLASSIC 1K cards should not be used, as it does not provide adequate cryptographic security.
- *Use unique keys* – Keys should not be reused and should be unique to each card.

Additionally, as a result of this work:

- *Limit the number of PIN attempts* – When verifying with PIN, the number of allowed attempts should be rate limited to counteract brute-force attacks.
- *Do not print contents of the restricted sector, on the card* – The data on the restricted sector should preferably be randomly generated, and not used for any other purpose.
- *Do not let services remain unmaintained* – Keep services up to date with best practices and beware that these services can compromise an access control implementation.
- *Generate card numbers randomly* – If card numbers are to be used for logging in, they should be random and more than six digits.

VI. Conclusion

Having examined the implementation at NI it is concluded that several flaws exist, aside from the ones covered in section II. They are rooted in implementation flaws of the smart cards, and the addition of several in-house services by NI.

Collectively, these flaws allow remote duplication of smart cards, thus granting access to locked rooms on behalf of employees. This requires a valid card number of an employee with access to the locked room. However, card numbers can be guessed by counting up or down from a known card number. Alongside remote duplication, these flaws also allow revealing the civil registration number of any employee at the institution.

Due to these flaws several recommendations, in addition to the manufacturer's recommendations, were determined.

Acknowledgment

Jens Myrup Pedersen for his invaluable feedback and inspiration.

Johan Hempel Bengtson for sharing his experience with the MIFARE Classic 1K and partially inspiring this work.

NI for assistance during this work and for addressing these flaws.

Aalborg University for providing the opportunity to work on this as a semester project.

Nicholas Bernth Strømgaard Hansen for his contributions to this work as a semester project.

References

[1] Statistics Denmark. (2019) Virksomhedernes brug af avancerede teknologier (10+ ansatte) efter emner, virksomhedsstørrelse og tid. [Online]. Available: https://www.statistikbanken.dk/ITAV7

[2] F. Garcia, G. Gans, R. Muijrers, P. van Rossum, R. Verdult, R. Schreur, and B. Jacobs, "Dismantling mifare classic," *Lect. Note. Comput. Sci.*, vol. 5283, pp. 97–114, 10 2008.

[3] TNO. (2008, Feb). [Online]. Available: https://files.gendo.ch/TNO_ICT_-_Security_Analysis_OV-Chipkaart_-_public_report.pdf

[4] (2018) Mifare classic ev1 1k - mainstream contactless smart card ic for fast and easy solution development. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf

[5] G. Klostermeier. Mifareclassictool. [Online]. Available: https://github.com/ikarus23/MifareClassicTool

[6] Personnummeret i cpr-systemet. [Online]. Available: https://cpr.dk/media/17534/personnummeret-i-cpr.pdf