# Surveying the security of access systems in Uppsala, Sweden

Tomáš Přeučil, Martin Novotný
*Faculty of Information Technology*
*Czech Technical University in Prague*
Thákurova 9, 160 00 Praha, Czech Republic
{tomas.preucil | martin.novotny}@fit.cvut.cz

***Abstract*—Today, many people use several access systems on a daily basis without paying attention to the fact that many of the technologies in use are obsolete and insecure. For example, there are published attacks against all generations of MIFARE Classic cards and cloning a MIFARE Ultralight card is trivial. In this paper, we look into the security of several access systems in a student town Uppsala in Sweden.**

**We evaluate the security of the cards or tags used for access as well as some of the security of the systems themselves. We present a detailed report on the configurations, including any vulnerabilities, while also presenting attacks exploiting these vulnerabilities, as well as real-life examples of how these attacks can be dangerous to the end user.**

**We compare these systems to a well-designed system in the same city and suggest fixes for all vulnerabilities we found. When presenting the potential fixes, we pay attention to the ease and cost of the fixes.**

***Index Terms*—security, cryptanalysis, attacks, access systems, RFID, MIFARE Classic, MIFARE DESFire**

## I. Introduction

Access, loyalty and transit cards are so omnipresent that most people have several of them in their wallets without giving them much thought. Some of these systems can be very secure if appropriately configured—such as the Gallagher Access Control system running on MIFARE DESFire [1]. However, many of these systems use obsolete technologies, are improperly configured, or both.

If these systems are insecure, it can be problematic both for the user and for the operator of the system. For example, it can be very easy to clone a card that accesses a hotel room or a keyfob that serves as an access token for a building. In these cases, the tenant is going to suffer most of the damage. On the other hand, if one can clone or modify a card that holds transit passes or holds access data to a university campus, it is going to be the operator who suffers the damage.

In this paper, we look into the daily life of a student in the Swedish town of Uppsala. Such a person will use many of these access cards or fobs several times a day. We will focus on six of them and see which of those are secure and where the student could make their life easier by exploiting obsolete technology or improper configurations.

## II. Background

As discussed in section I, many systems that use RFID cards employ deprecated or downright insecure technologies. We aim to present some of the vulnerabilities and the attacks that can be mounted. After we introduce these (along with some basic terminology), we will present our analysis. From now on, we will use the terms card and tag interchangeably. The only difference between these two is their physical size.

Each card has a Unique Identifier (UID), a strictly read-only number that identifies a particular card from all others worldwide[1]. However, this is only true when we are talking about original cards. One can buy cards that can have their UID changed either by direct writing or using a particular command. These can be bought for most of today's card types and are commonly referred to as "magic" cards.

Even if we cannot buy a "magic" card, we can use an emulator such as Chameleon mini [2]. This device can emulate any 13.56 MHz card that its firmware supports. The device is entirely open-source, so support for any card can be added at any time. We can change the UID, card content, keys or anything else at will. We can also clone existing cards onto it.

Next, we will define a few terms concerning access systems. Each system must have a central unit. This can be a separate device or an of the shelf computer. One can use the central unit to manage the system and sometimes even issue the cards. This unit can either be standalone or connected to the company's computer network.

The central unit can communicate with the readers directly, either over the air or through a cable. In that case, all configuration edits are transmitted in real-time. The administrator can also see all the access logs immediately. We call a system like this *online*. The system is referred to as *offline* if the central unit does not directly communicate with the readers. Logs and configuration edits can be spread to the readers either through a specialized device that needs to be physically plugged into each one, or through the content of the cards (when a user presents a card to a reader, the reader writes some data on the card, and the next reader can read that data).

### A. RFID card technologies

RFID cards operate on two main frequencies. The first is 125 kHz or low frequency (LF). Those cards are the oldest and usually do not support any security and can be cloned easily. Therefore, they are a perfect example of an insecure card, and we will not focus on them.

[1]Today, some cards have an NUID—Non-Unique identifier as there are not enough bits to uniquely identify all existing cards.

The second, and arguably most used today, frequency is 13.56 MHz. The security of the cards operating on this frequency can range from completely insecure to state-of-the-art AES encrypted. We will discuss these cards next.

*1) MIFARE Classic:* MIFARE Classic [3], manufactured by NXP, was the pioneer RFID card that works in the 13.56 MHz spectrum. The UID can be 4 or 7 bytes large, and the card offers up to 4 kb of data storage. The memory is organized in sectors of 64 B (if the cards' data storage is bigger than 1 kb, some of the sectors can be larger). Each sector has two access keys that can be used for read and write operations (each key can have different privileges). The card allows encrypted communication using the CRYPTO1 stream cipher designed by NXP [4].

The CRYPTO1 cipher is not secure. There are multiple attacks exploiting both the weaknesses in the ciper as well as bad implementations, for example, [5] or [6]. So-called nested attack [7] exploits the way the card authentification works as well as the weaknesses in random number generation on the card. This means that if we know at least one key to a single sector on the card, we can recover all the remaining keys of the entire card within seconds or, at worst, a few minutes (depending on the device we perform the attack on). If we do not know any keys, we can use the dark side attack [8] to recover one of the keys, which takes 30 seconds to an hour (again, depending on our reader).

Some of the aforementioned vulnerabilities were fixed in a new revision called MIFARE Classic EV1 [3]. Even though this made the dark side attack impossible, a different variant of the nested attack, referred to as hardnested [9], still works. Even though the attack process differs, the results are identical to the nested attack. However, the prerequisite of knowing one key is still valid. We can get this key either by collecting nonces from a reader or by sniffing the communication between the card and the reader [10]. NXP no longer recommends using MIFARE Classic in any application where security is needed and recommends upgrading to different technologies [3].

*2) MIFARE Ultralight:* MIFARE Ultralight [11] cards always have a 7-byte UID, are manufactured by NXP, and are intended for limited use. This means that they are suitable for tickets and other situations where it is expected that the data on the card will not be overwritten (the memory can be locked as read-only). The memory is structured in pages.

There are several types of Ultralight cards. The simplest one, Ultralight, does not support any encryption and can be freely read and written (unless the memory was set as read-only). Ultralight EV1 supports password protection, while Ultralight C allows 3DES authentication. In 2022, NXP also released Ultralight AES, which allows authentication with AES instead of 3DES [11].

It is very easy to clone a (pure) Ultralight card onto a magic card or a Chameleon. We only need to read the card once. We can clone an Ultralight EV1 by sniffing the traffic between the card and the reader. More research is needed for Ultralight C and Ultralight AES. Both cards seem to be secure.

*3) Other technologies:* The remaining cards in the MIFARE lineup are MIFARE DESFire [12] and MIFARE Plus [13]. Mifare Plus has a Mifare Classic compatibility mode which is insecure in the same way as MIFARE Classic EV1. There are no attacks known to the authors for the situation when the card is used in AES mode.

MIFARE DESFire is considered a state-of-the-art access card. It offers both 3DES and AES encrypted communication and stores data in the form of applications and files that can also have backups. As of 2023, the current generation of DESFire is EV3, and there are no attacks published against EV1 or newer cards. However, there is an attack against DESFire EV0 [14].

There are other manufacturers of RFID cards as well. These include Legic [15], Thales (formerly Gemplus) [16] and others. These cards are out of the scope of this paper as we did not encounter them in Uppsala at all.

### *B. Securing insecure cards on the application level*

One can attempt to secure insecure cards on the application level, for example by computing a checksum over the card content (including the UID), encrypting that checksum with a key that is not stored on the card, and writing this encrypted checksum into a sector/page. Something similar was implemented by Gallagher in the form of a MIFARE Enhanced Security block (MES block). This can protect the manipulation of the data but will not protect against full cloning with a magic card or the Chameleon mini [17].

## III. Method

In this paper, we analyze six card systems that the student in Uppsala can encounter:

- The access system to housing offered by the university
- The access system to storage and laundry in the same building
- The access system to the building of a student organization
- The access system of Uppsala university
- The public transportation system in Uppsala
- The access system to housing offered by some student organizations

We evaluate each system based on the type of access cards that it uses. We look into basic security, the type and generation of the access cards and whether they can be cloned. We try to use both the Chameleon mini and the magic cards.

Table I summarizes the card systems a student in Uppsala can encounter, the types of cards used in these systems, attacks that are applicable to these systems, and the solutions to fix the problems. We bring a detailed analysis in the following text.

### *A. Housing offered by the university*

An international exchange student coming to Uppsala University is eligible for housing through the Uppsala University Housing office [18]. If the student decides to live in the city centre, they will live in a decommissioned hotel repurposed as student accommodation.

The student will be issued a card used for access to their room and the building itself. If the student loses their card, replacing it costs about 1050 SEK (around 95 EUR). The same fee incurs when the card is forgotten inside the room.

The type of the card is MIFARE Ultralight (pure Ultralight, not E1, C, or AES). Therefore, the content of the card can be

TABLE I
OVERVIEW OF CARD SYSTEMS IN UPPSALA, CARD TYPES USED, APPLICABLE ATTACKS, AND AVAILABLE FIXES.

| System | Card type | Attack(s) | Solution/fix |
|---|---|---|---|
| **Housing by UU** | MF Ultralight | Direct clone | Use MF Ultralight C/AES, or upgrade to MF DESFire |
| **Laundry** | MF Classic | UID clone | Use MF Plus or MF DESFire |
| **Student association** | MF Classic | Nested + UID clone | Upgrade the Salto system to use MF DESFire or use iLOQ |
| **University** | MF Classic EV1 | Hardnested + UID clone | Use MF Plus or MF DESFire |
| **Public transport** | MF Classic EV1 | Hardnested + UID clone | Use MF Plus or MF DESFire |
| **Housing by s. assoc.** | 125 kHz + iLOQ | 125 kHz clone | Not needed |

easily cloned. The locks use the VignCard LCU6333 reader and connect to the central unit over ZigBee—they are online. The locks run on several AA batteries that can only be changed from inside the room. The service of the system is provided by Avarn [19], which is a security group operating in the Nordics. The VignCard reader can be seen in Figure 1.

Besides the locks for the rooms, the keycard is also used for the elevators. Those use the same reader. Unfortunately, we were not able to confirm if this reader is also used for reading the cards at the entrances to the building.

We tried simulating the card's UID using a Chameleon Mini without copying the content of the card. We also tried cloning the content of the Ultralight card onto another Ultralight (that had a different UID). We were not able to access the building or the room in either of these configurations. However, as expected, when we emulated the entire card (UID and content) using the Chameleon Mini, we could access the building and the room. This allowed us to access the facility as if we were using the original card. The same situation happened when we used a "magic" card with a cloned UID of the original one.

Since all the locks are online, we expected that the data on the card might be updated on a regular or non-regular basis to fix the most critical vulnerability—cloning the card with a single touch of a reader. However, this was not the case. The content of the card stays the same for up to a year (shorter if the renting period is shorter). Therefore, one can easily make as many clones of their card as they want. This makes the entire system extremely insecure. We also learned that the cards need to be updated manually every time there is a change. Therefore, the tenant needs to go to the office.

The aforementioned vulnerabilities are severe but only allow cloning of the cards—one-time access to the card is needed. This is still a critical issue as many people leave their (clearly distinguishable) cards in places where others can read them inconspicuously. However, once we compared several cards, we could see how the data are structured in the card's memory. For example, it is easy to distinguish the page containing the lock/room identifier and so on. We will not publish the details, but we have reasons to believe that even the data structure on the card is not secure.

### B. Storage and laundry

In case the student living in the aforementioned accommodation wants to park their bike in the designated bike room, do laundry, or even throw away their trash, they need another access card. All indications are that this system is completely isolated from the one providing access to the building. It allows the users to enter the bike and garbage rooms, and one can


Fig. 1. Card reader in UUHO housing (left, VignCard, cover off) and in the student association (right, CU5000)

book a time slot for laundry using the same tag. The laundry system counts the number of bookings and will allow the user to book only five slots per month. We found out that the Uppsala University Housing Office cannot edit these values (extra laundry slots cannot be loaded onto the tag).

The type of tag is MIFARE Classic, and there is no content loaded onto it. The system only checks the UID and compares it to its whitelist. In the case of the laundry booking system, it also checks the UID against its database of bookings. Emulation using the Chameleon Mini and cloning the tag using a "magic" card are both trivial.

As in the case of the cards used for access to the rooms (subsection III-A), only cloning is possible. Randomly generating a UID that would have access to the system is unlikely. However, the key tags have a very distinguishable shape and labels, which makes it easy to spot them when someone leaves them by their booked laundry machine.

### C. Student organizations

There are 13 student nations in Uppsala. A nation means a student institution that is not part of the university (therefore, it is not a union) but is still affiliated with it. We chose one mid-sized nation for our analysis.

The building of the nation uses an access system from Salto [20]. They have a central unit (type CU50ENSVN, called high security by the manufacturer), three online locks powered from the mains (of the CU5000 type) and many offline locks (XS4 and XS4 mini) powered by AAA batteries. The front end (the part to which the user presents their keytag) of the mains-powered readers can be seen in Figure 1.

Each employee or volunteer is issued a tag that is supposed to grant them a particular level of access (as with any access system). For example, only people associated with the restaurant are supposed to have access to alcohol storage and, critically, no one other than the full-time employees should have access to the server room.

The tags that people receive are Salto branded and MIFARE Classic. This should have already been a red flag for an

institution that stores very expensive things behind these locks. However, things get even worse. Some of the keys are left at default, so a simple nested attack (see subsubsection II-A1) is sufficient to recover all the keys. We also found out that all the tags use the same keys. No key diversification is applied. Therefore, any volunteer can crack the keys at home and clone their boss's tag easily, gaining access to all the secured spaces.

After disclosing the abovementioned facts to the institution, we were asked to analyze the system more and to suggest fixes. First, we discovered some additional functionality that was supposed to enhance security. This included periodic updates of the data on the keytags and collecting logs. If the data on a particular keytag were not updated for a fixed period of time, the keytag would not allow access into some spaces. This functionality (for both logging and updating) relied on Salto's control software which had to be running for this functionality to be available.

We discovered that this software was severely outdated and was running on an office PC with MS Windows, and it would not start automatically after the PC was turned on. Therefore, if the PC was shut down or automatically rebooted due to a Windows update, all of this functionality would be unavailable and, after a certain time, would prevent access to a part of the building. Also, access logs would not be collected, rendering the building even more insecure.

We spun up a Windows VM on a server in the institutions server closet to prevent the rebooting problem. We installed an updated server version of the control application on it. We obtained the updated version of the control application directly from Salto.

When communicating with Salto, we also mentioned the cloning problem described above. They initially responded that they "heard of the issue but never actually saw anyone clone their cards". We sent them a video and proceeded to secure the building using the method described in subsection IV-B.

### D. University access

Uppsala University is the oldest university in Sweden. The whole institution uses MIFARE Classic EV1 cards with no default keys for access. This makes them more secure than the cards described in subsection III-C but still vulnerable. We can either get the nonces from a reader or sniff one authentication as discussed in subsubsection II-A1. Then we can calculate all the keys. We did not pursue these attacks because we ended our stay in the city.

### E. Public transport

The public transit system in Uppsala uses the same type of cards as the university. This means the cards are MIFARE Classic EV1 (in the 4kb variant). They have no default keys. Therefore, there are the exact same problems as in subsection III-D. We aim to look into this system further as there seems to be severe security through obscurity issues.

### F. Housing through student organizations

The student nations described in subsection III-C also provide housing. There are several large areas where this housing is situated. We chose one of these sites as a good example

Fig. 2. Three iLOQ keys

of an appropriately secured site that still keeps most of the convenience for the users.

This system must work for thousands of students living in thousands of apartments while allowing access to communal areas and supporting the booking of laundry rooms and saunas. Therefore, the housing association adopted two systems that are not connected in any way for these tasks.

First, there is a system that allows access to the buildings themselves, the communal areas and the aforementioned bookings. It is essential that access to the building is hassle-free. Therefore, they use 125 kHz EM4100 tags with the appropriate readers. Even though these can be cloned very easily, it does not matter much in this case since a few hundred people have access to each building, and it is not possible to go any further than the communal areas. The only potential damage a hacker could make is stealing someone else's laundry time (or the actual laundry) or a few tables. This could be fixed by upgrading the system to MIFARE DESFire with a single application that communicates in an encrypted way. However, in this case, the cost would be too high for the potential payoff.

The second system is a lot more secure. It serves only for entrance to individual rooms or apartments. This system is provided by iLOQ [21] and requires a conventional key (see Figure 2) with an embedded and correctly programmed microchip that works similarly as, e.g., a car immobilizer. If the authentication succeeds, the lock unblocks itself and lets the user open the door. For authentication, the microchip uses either AES-256 or a 64-bit challenge and SHA-1 computed 160-bit MAC pair. If a (conventional) key is lost, it can be removed from the system as an NFC card would. The insertion of the key into the lock induces electricity, which powers the lock. The lock then creates an electromagnetic field which powers the microchip in the (conventional) key. This can be problematic sometimes, and users may need to insert the (conventional) key into the lock several times. However, since this system only secures the valuable part of the property (the rented rooms or apartments), and the tenant is already sheltered from the weather, it does not matter much. We believe that combining these two systems leads to a highly secure building with minimal inconvenience for the tenants.

## IV. Suggested fixes

In this section, we suggest fixes for all the systems. The summary of the vulnerabilities and the possible fixes can be seen in Table I.

### A. Housing offered by the university and laundry

We start with the housing and laundry (subsection III-A and subsection III-B). We present two options. The institution could either keep the systems separate (and use two different cards) or merge the data onto one card.

In the first case (keeping both systems completely separate), the institution could leave most of the building's access system (access to the building and the rented rooms) in place as all the VignCard readers already support MIFARE Ultralight C. We would suggest exchanging all cards for this type. The only modification needed is the authentication process, after which the reader can read the cards as usual. This would prevent the cards from being cloned and drastically increase the system's security. It would render all hypotheses about the security and encoding of the data on the card irrelevant. The laundry tags would be replaced for MIFARE Plus in AES mode, replacing the UID-based authentication. We did not investigate if the readers would need to be changed in this case.

The second option would be to upgrade to MIFARE DESFire cards. In this case, there would be two applications on one card. One would be used to enter the building (which might require changing the readers), and the other would serve the laundry booking system (again, with a possible change of the readers). This would secure the access and laundry systems from cloning attacks and be a practical and cost-effective solution. The locks would read one encrypted application, and the laundry system would read the other one. At the same time, the only use of the UID would be key diversification, securing both systems further.

### B. Student organizations

In the case of the student association (subsection III-C), we suggested an upgrade to MIFARE DESFire as the Salto system supports this type of card out of the box. The whole upgrade would only mean changing the tags and upgrading the firmware of the readers. As there was no company able to support this system in the region anymore, we were asked for a suggestion for a replacement system. We recommended iLoq for the (mainly security-related) reasons described in subsection III-F, and the new system was installed in December 2022.

### C. University access and public transport

Even though the public transport (subsection III-E) and university access (subsection III-D) cards were the most secure systems of those still relying on MIFARE Classic (EV1) cards, we would still suggest changing them to MIFARE Plus or MIFARE DESFire for the reasons described in the respective subsubsections. However, we do recognize that this may not be worth the expense, especially in the case of the university.

## V. Summary

We evaluated the security of several access systems in Uppsala (Sweden). We presented the systems used day to day by many students while looking into all the necessary details for our evaluation. During our research, we found many vulnerabilities, most of which are present due to the lack of maintenance on the systems. The most notable vulnerabilities are tied to the use of deprecated cards, namely MIFARE Classic (in all variants). These cards use obsolete encryption and can be modified and cloned without major effort. On the other hand, secure systems do exist. One of them (an access system for housing provided by student organizations) was presented. This system uses a combination of modern and secure access control for areas such as apartments and convenient and quick access control for hallways, so the user is not left outside for too long.

We successfully attacked some of the insecure systems using known techniques such as nested and hardnested attacks or nonce sniffing, allowing us to present such attacks' dangers. The mentioned attacks allowed us to clone existing cards and access said areas/systems. We proposed fixes and countermeasures for all the vulnerable systems while paying attention to the cost and ease of the upgrade, for example, by proposing two alternatives while maintaining security. All systems we observed can be secured.

## Acknowledgements

This work was supported by the Czech Technical University (CTU) grant No. SGS23/208/OHK3/3T/18.

## References

[1] T. Preucil and D. Oswald, *Attacking the Gallagher access control system on MIFARE DESFire*, CARDIS, University of Birmingham, student poster, 2022.
[2] Kasper & Oswald, "Chameleon mini," https://github.com/emsec/ChameleonMini, 2014-2023.
[3] *MIFARE Classic Family*, NXP, [cit. 2023-01-28]. [Online]. Available: https://www.mifare.net/en/products/chip-card-ics/mifare-classic/
[4] *MF1ICS50 Functional specification*, NXP.
[5] N. T. Courtois, K. Nohl, and S. O'Neil, "Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards," Cryptology ePrint Archive, Paper 2008/166, 2008, https://eprint.iacr.org/2008/166. [Online]. Available: https://eprint.iacr.org/2008/166
[6] G. Gans, J.-H. Hoepman, and F. Garcia, "A practical attack on the mifare classic," vol. 5189, 04 2008.
[7] F. Garcia, P. van Rossum, R. Verdult, and R. Schreur, "Wirelessly pickpocketing a mifare classic card," 05 2009, pp. 3–15.
[8] N. Courtois, "The dark side of security by obscurity - and cloning mifare classic rail and building passes, anywhere, anytime." 01 2009, pp. 331–338.
[9] C. Meijer and R. Verdult, "Ciphertext-only cryptanalysis on hardened mifare classic cards," 10 2015, pp. 18–30.
[10] C. Herrmann, P. Teuwen, O. Moiseenko, M. Walker *et al.*, "Proxmark3 – Iceman repo," https://github.com/RfidResearchGroup/proxmark3.
[11] *MIFARE Ultralight Family*, NXP, [cit. 2023-01-28]. [Online]. Available: https://www.mifare.net/en/products/chip-card-ics/mifare-ultralight/
[12] *MIFARE DESFire Family*, NXP, [cit. 2023-01-28]. [Online]. Available: https://www.mifare.net/en/products/chip-card-ics/mifare-desfire/
[13] *MIFARE Plus Family*, NXP, [cit. 2023-01-28]. [Online]. Available: https://www.mifare.net/en/products/chip-card-ics/mifare-plus/
[14] D. Oswald and C. Paar, "Breaking Mifare DESFire MF3ICD40: Power analysis and templates in the real world," in *Cryptographic Hardware and Embedded Systems–CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13*. Springer, 2011, pp. 207–222.
[15] *Multi-purpose RFID ICs*, LEGIC Identsystems Ltd, [cit. 2022-12-27]. [Online]. Available: https://www.legic.com/products/smartcards/legic-smartcard-icss
[16] *Digital Identity and Security*, Thales, [cit. 2023-03-07]. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security
[17] M. Daley, "Gallagher research," https://github.com/megabug/gallagher-research, 2020.
[18] Uppsala University Housing Office, [cit. 2023-01-27]. [Online]. Available: https://housingoffice.se/
[19] Avarn Security, [cit. 2023-01-27]. [Online]. Available: https://www.avarnsecurity.com/
[20] *Salto inspired access*, SALTO Systems, [cit. 2022-12-27]. [Online]. Available: https://saltosystems.com/en/
[21] *iLOQ, Life made limitless*, iLoq Ltd., [cit. 2022-03-08]. [Online]. Available: https://www.iloq.com/en/