Physical Authentication at The University of Michigan

David Adrian
University of Michigan
davadria@umich.edu

Matthew Diffenderfer
University of Michigan
mjdiffy@umich.edu

Mike Grzych
University of Michigan
migrzych@umich.edu

Abstract

The University of Michigan employs several card-based identification and authentication mechanisms to regulate physical access to campus properties. Magnetic stripes are used for the university's dormitory keys and Mcard student IDs, with the latter also employing contactless smart card technology for building access. Prior published works have shown these technologies to often be inadequate for security purposes, resulting in the university having to update their systems in recent years with the goal of bolstering campus security. We present a security analysis of the current iteration of the Ann Arbor campus systems for authentication via Mcards and dormitory key cards, and a survey of past and potential future attacks against these systems.

1 Introduction

The University of Michigan uses identification cards called Mcards [9]. Mcards have a magnetic stripe that can be used as an authentication mechanism for restricting access to rooms and buildings. Additionally, Mcards can be linked to a TCF Student Checking account, if the student so desires [6]. It was shown in 2005 that Mcards were vulnerable to forgery attacks, and an update was subsequently rolled out to the Mcard system [15]. More recently, the University rolled out smart Mcards that are read using near-field communication (NFC) when placed within a few centimeters of a card reader. After the initial vulnerabilites were disclosed, little work has been put into verifiying that the new systems are actually secure replacements for the vulnerable old systems.

For dormitories at the University, dorm room access is controlled using electronic key cards. These electronic key cards have a magstripe that is read when inserted into the lock, as well as a PIN that must be entered into the lock. If both a valid PIN and valid key is presented, the lock opens. No independent prior work investigating the security of dorm room doors has been performed at the University.

We aim to evaluate the security of the current physical authentication options at the University of Michigan. We present an overview of each type of authentication technology and its implementation, as well as describe the authentication protocols used by each technology. We also present a security analysis of all three types of card-based authentication - Mcard, smart Mcard, and dorm room keys, and describe possible attacks against those systems. We provide recommendations to improve security going forward.

The remainder of our paper is as follows. In Section 3 we define our threat model for the purposes of our security evaluations. In Sections 4 and 5 we explore the magnetic stripe and contactless authentication mechanisms on Mcards, and in Section 6 we explore the university's dormitory key card system; each of these sections are laid out to provide background regarding their respective mechanisms, how they are employed on the University of Michigan campus, and our security analysis for that mechanism and its implementation. Finally, we describe future work in Section 7.

2 Related Work

Jon Oberheide disclosed a vulnerability in the Mcard system in 2005 that required the University to update what data was stored on each card in order to prevent Mcard forgery [15]. Our analysis will center around the system that was built to prevent this attack.

Developments in recent years involving contactless authentication systems like MIFARE Classic and DESFire smart cards have sparked renewed interest in security concerns regarding the deployment of these technologies. Reverse engineering of relevant cryptography protocols and mechanisms has led to exploitation through projects like Chameleon [14], which can clone existing smart cards or load arbitrary information

while impersonating legitimate cards. Our work investigates how these developments apply to University smart Mcards.

Attacks against a similar system to the dorm locks used in hotels called the "Onity HT" lock system were disclosed in 2012 [10]. Onity has since rolled out updates to hotel chains [12] to improve security. However, no attacks have been published against the Onity Integra system used by University of Michigan dormitories.

3 Threat Model

For the purposes of our threat model, we have considered an adversary with limited resources with respect to time and money —the "opportunity attacker." We assume that such an adversary might be armed with simple tools that could easily be carried on one's person, such as a smart phone equipped with near field communication (NFC) capabilities or a magnetic stripe reader attachment, and access to a magnetic stripe writer. In short, our adversary seeks means to violate security by attacking the Mcards and dormitory keys themselves, rather than the infrastructure which relies on them.

To be explicit, the kinds of attacks which fall outside our threat model include attempts against the networks and infrastructure supporting security mechanisms, direct attacks on the card readers through reprogramming or affixing skimming devices, and any other attack which would require a nontrivial amount of time or money to execute. "High cost" attacks like these have the potential to be far more dangerous for reasons other than merely accessing doors, and at a certain point the expenditure of such resources would be better spent on simpler methods like bribery.

By reducing our threat model to our "opportunity attacker," we believe that our analysis presents a more realistic view regarding the kind of common adversary one should expect on the University of Michigan campus.

4 Mcard Swipe Access

4.1 Magnetic Stripe Cards

University of Michigan Mcards are magnetic stripe ("magstripe") cards. Magnetic stripe cards store data by altering the magnetism of the card [18]. Standard magnetic stripe cards can store data on three separate Tracks that vary in information density, following the ISO/IEC 7813 standard [2], which we explain below.

Track 1 of the magnetic stripe uses a DEC SIXBIT encoding with an odd parity bit, for a total of seven bits per character. This allows for $2^6 = 64$ possible values stored in the first six bits, and uses the final seventh bit for redundancy. DEC SIXBIT allows for alphanumeric text, along with several special characters [1].

Track 2 of the magnetic stripe uses a five bit scheme that contains four data bits and one parity bit, for a total of $2^4 = 16$ possible values. These values correspond to the ASCII characters in range 0x30 - 0x3f, which contain the numbers `0-9` as well as the special characters `:;.<=>?`.

Track 3 does not have a standard encoding scheme. It is encoded with a bit density of 210 bits-per-inch, which allows for 535 bits on a normal magstripe card [18]. Some applications will use a five-bit character size; others will treat the entire strip as a raw byte array.

There are two types of magnetic stripe cards - *high coercivity* and *low coercivity*. High coercivity cards ("HiCo") have a magnetic field strength of 4000 Oe, whereas low coercivity cards ("LoCo") have a magnetic field strength of 300 Oe [3]. Due to the stronger magnetic field, HiCo cards are require more energy to erase than LoCo cards, and are therefore more resistant to damage from common magnets and magnetic fields such as those generated by cell phones. HiCo cards are more commonly used for longer-life applications, such as credit and identification cards, whereas LoCo cards are more commonly used for shorter-lived applications, such as hotel room keys.

4.2 Mcard Magnetic Stripes

Mcards have a high coercivity magnetic stripe, in which only the first two Tracks have data written to them, and only a subset of the data on Track 2 is read by the scanners attached to door locks. The data on Track 1 is encoded using variant 'B' of a standard format prescribed for financial data cards [2], which is decribed below.

- **Start Sentinel and Format Code**: A single character (`%`) that indicates the start of the data, followed by a character for the format code (`B`).
- **Account Number**: An up-to 19 character identifier that usually matches the number written on the front of a card, such as a credit card number or identification number. The account number used for an Mcard matches the card number printed on the front of the card (see Figure 1). A former study by Jon Oberheide showed that an Mcard number takes the form `600847` $\|$ `UMID` $\|$ r $\|$ L_n where `600847` is a constant prefix, `UMID` is the student's University of Michigan Identification Number, which is also printed on the front of the card, r is a single-digit revision number for the card (usually 0 or 1), and L_n is the Luhn checksum of the preceding digits [15].
- **Name**: Up to 26 characters representing the name of the issuee. An Mcard stores the last name and

Figure 1: The standard example Mcard used by the University. The card number is listed on the left, under the logo and UMID.

first initial of the issuee as text in the form `LAST/F`, e.g. `ADRIAN/D`.

- **Expiration Date**: Year and month the card expires, in `YYMM` format, e.g. `1608` for an expiration date in August 2016.
- **Service Code**: A 3-digit number, where the first digit indicates if the card can be used internationally, the second digit indicates any restrictions on types of goods that could be purchased by the card, and the third digit indicates if the card requires a PIN to use. Mcards all have a service code of `120`, which indicates that the card can be used internationally, for the purchase of any good, and requires a PIN. This is only relevant to users who link their Mcards to their TCF checking account for use as a debit card [6].

The data on Track 2 is similar and duplicates some of the information on Track 1. Track 2 consists of the account number, expiration date, service code, and an extra *discretionary data* field. This field contains a nine-digit random ID that appears to have no relation to any other identification number, and is assigned at the time an Mcard is printed.

Track 1 uses `%` as a start sentinel and `^` as a field separator. Track 2 uses `;` as a start sentinel and `=` as a field seperator. Both Tracks use `?` as an end sentinel.

Combining all the fields in order, we can see an Mcard for David Adrian, UMID 02793408, that expires in August 2016 would be encoded as[1]:

```
1=%B6008470279340818^ADRIAN/D^1608120?
2=;6008470279340818=1608120=123456789?
3=None
```

[1]We altered the 9-digit ID on Track 2 for privacy reasons.

We determined by experimenting with different cards and the Bob and Betty Beyster Building door and elevator readers that only Track 2 is read by the card reader. Data on Track 1 is not read and may be left blank. From Track 2, the reader sends the card number and random ID over the network for authentication. It does not read the expiration date or service code, and accepts zeroed-out versions of those values. Therefore, the following card would be sufficient to allow card access as David Adrian:

```
1=None
2=;6008470279340818=0000000=123456789?
3=None
```

We also note that Mcards do not contain any revealing personal identification that is not otherwise available on the cards, such as a social security number or bank account number.

4.3 Security Analysis

The main attacks against swipe cards are duplication and forgery. We define forgery as the creation of a duplicate Mcard by a third-party that impersonates the first-party card, without the third-party ever reading the data on the original MCard. We define duplication as forgery where the third-party first obtains access to a legitimate Mcard and reads the data stored on the magnetic stripe in order to create a duplicate card. Forgery of an Mcard capable of swiping into restricted areas requires access to a HiCo card writer, which can be purchased for less than $200 on Amazon, and knowledge of two numbers - the card number and the random ID.

An Mcard number consists of public and non-secret information. UMIDs are not meant to be kept secret and are exposed in a variety of systems including those that process student grades. The revision number is usually 1 or 0, and only has 10 possible values. Since the `600847` prefix is fixed, and the Luhn checksum is a deterministic function of the rest of the number, a motivated attacker should have little difficulty deriving the Mcard number to within 10 possible values where the revision number is the only unknown.

However, since the Track 2 data includes an random ID, an attacker attempting to forge an Mcard will need to resort to guessing that 9-digit value. With 10 possibilites per digit and assuming it takes one minute to write an ID to a card and test if it is correct, this would take an average of $10^9/2$ minutes, or roughly 950 years to correctly guess. Therefore, we believe that Mcards are resistant to forgery.

In terms of duplication, Mcards are no less secure than any other magnetic stripe card against a malicious attacker. In order to prevent a malicious attacker from du-

plicating an Mcard, card holders should pay close attention to their Mcards to prevent unauthorized access.

Mcards do present a unique situation where the card holders could collude against the University and perform a group priviledge escalation attack if the group contains at least one member with pre-elevated priviledges. The University charges $25 to replace a lost Mcard [9]. During this process, the old Mcard is marked as inactive and can no longer be used for card access. A new random ID is assigned to the new card.

If a card holder purchases a new card for $25 without losing their original card, he then has the ability to write arbitrary identities to the original card that do not agree with the face, name, and number printed on the front of the card. Therefore, a group of malicious users can easily create a set of Mcards that physically look legitimate, but in fact share the same identity of one of the users in the group. This group of users could then use the rewritten Mcards to masquerade as a colluding higher-priviledged card holder, and have group access to restricted areas without needing the presence of the high-priviledge card holder. We take advantage of this to describe the "free food" attack.

The free food attack is slightly different from a high-priviledge card holder allowing a low-priviledge user to copy his Mcard to any blank magstripe card. Since the duplicated card in the free food attack is written to an actual Mcard of one of the attackers, it still passes the physical test where the photo and name on the Mcard are checked to match the person presenting the card for authentication. We assume a system where the card reader does not display the name of the card holder but instead just indicates if the card holder represented by the data on Track 2 has access. Verification of card holder to card is performed using physical verification by a human who compares the photo to the card holder. In this system, the free food attack could be used to falsely bypass authentication by masquerading as another card holder.

While such a system may initially seem ridiculous, this is in fact exactly how meals in the dorms at the University are managed. Students who choose to eat in the dorms sign up for meal plans with a varying number of total meals for the semester ranging from 50 to unlimited, with the larger meal plans available at higher cost to students. In order to gain access to the dining hall, students must swipe their Mcard into a machine that then displays the number of meals remaining. If the number of remaining meals is non-zero, the student is then let into the dining hall and the meal count is decremented (or left at unlimited, if the card is linked to an unlimited meal plan). Therefore, a group of students could purchase a single unlimited or high-value meal plan for a single student accout, and apply the free food attack to all use the same meal plan. For $25 per person, the colluding students can all eat at the reduced rate of p/n per semester, where p is the original price of an unlimited meal plan for one semester, and n is the number of students colluding under the same meal plan.

5 Mcard Contactless Access

5.1 Background

The contactless smart card technology used in University of Michigan Mcards is from the MIFARE series of chips, manufactured by NXP Semiconductors. The cards are compliant to the ISO/IEC 14443-A contactless smart card standard, and operate using near field communication (NFC) technology. The intended use of the cards is to be engaged by card readers positioned outside most main building entrances on the Ann Arbor campus, which authenticate cardholders and grant door access.

It is worth noting that the use of MIFARE chips inside Mcards is not the university's first experience with contactless access, and that prior use of such technology included the use of HID Corporation's Prox system in the early 2000s. Originally targeted for use within the University of Michigan Health System (UMHS), the deployed Prox RFID tags had unique identification numbers and were used to determine access privileges on the medical campus. Prox was a basic mechanism that could easily be cloned or relayed [16], prompting the decision to use MIFARE for wide scale deployment to students in 2011.

NXP's offerings for the MIFARE line are many, the longest-running being the MIFARE Classic. Available since 1994, MIFARE Classic is an ASIC-based device that is still widely used for electronic wallets and balance, access control, enterprise ID, and transport ticketing. MIFARE Classic is notable for its use of NXP's proprietary Crypto-1 security protocol [7], which was reverse engineered in 2008 [17] and has since been opened up to more comprehensive exploitation. One of the most notable projects to stem from this has been Chameleon [14], a small device capable of being loaded with arbitrary data while being recognized by readers as an legitimate MIFARE Classic tag.

MIFARE DESFire was released in 2002, and used Triple-DES encryption instead of Crypto-1. In addition, the DESFire chip shipped flashed with 4kB of storage and the proprietary mask-ROM MIFARE DESFire operating system, which provided basic directory and file constructs. DESFire-compatible readers can access directories and files on the smart cards using native DESFire commands over the ISO/IEC 14443-A compliant RF interface or through APDU commands from the ISO/IEC 7816-4 standard [5].

DESFire was considered secure until 2011, when it

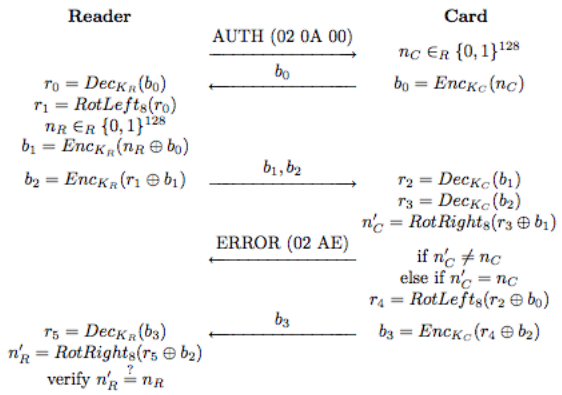

Figure 2: The basic authentication protocol for DESFire EV1. CBC is modified so all en- and decryptions are chained despite being on different datagrams, and the Initialization Vector (IV) is dependent on the previous en- or decryption operation.

was shown by Kasper, Oswald, and Paar [13] that DESFire tags were susceptible to side-channel analysis and could leak their secret keys. NXP already had plans to discontinue DESFire at the end of 2011, leaving customers seeking DESFire functionality to migrate to NXP's DESFire EV1 tags. DESFire EV1 brings all of the same functionality as its predecessor, and makes several improvements over the original DESFire offerings including support for 128-bit AES, improved ISO/IEC 7816 compatibility, up to 8kB of data storage, random IDs for transactions, and mutual authentication [5]. At the time of writing, DESFire EV1 is the technology used for smart Mcards at the University of Michigan.

5.2 Smart Cards on Campus

The University of Michigan began integrating smart card technology with the Mcard system in 2011, and employs the use of smart Mcards across its Ann Arbor campus for the purposes of authenticating entry to buildings and certain rooms within them. Students and faculty interact with small readers positioned near building entrances by holding their Mcard against the face of the reader, causing the Mcard and reader to perform the requisite steps of the DESFire EV1 authentication protocol.

The authentication protocol used by DESFire EV1 is outlined in 2; this protocol uses encryption and decryption in the common sense, being that sent data is encrypted and received data is then decrypted, and is a departure from the original DESFire protocol which transmits decrypted data for one of its steps [14]. Further, the smart card hardware and operating system are Common Criteria certified at the EAL 4+ level [4], which validates that the card's security features are correctly implemented and highly resistant to attack, including side channel analysis like that performed against the original DESFire protocol [13]. To further mitigate against attackers, the DESFire EV1 chips used in Mcards are configured to generate a different random 7-byte UID after each authentication attempt, which ideally protects the owner of the tag from replay and relay attacks.

Upon authentication, the reader verifies the user's credentials against a connected database on the university's internal network and - if permitted - electronically disengages the locks on the reader's associated door. While it may be possible for an attacker on the university's network to circumvent this security measure, we have already discussed above that such an attacker is not part of our threat model for this analysis.

5.3 Analysis

Our investigation of contactless smart Mcard security on the University of Michigan's Ann Arbor campus did not yield any particularly exciting results. The university's plan to use DESFire EV1 proved worth the expense when weaknesses in the original DESFire chip were found and shown in 2011 through side-channel analysis, while there is no published literature indicating the newer DESFire EV1 chips possess that vulnerability. We would like to note, however, that even if such analysis is possible, we assume the time and monetary resources necessary to carry it out will fall under the category of "high cost" attacks, which we defined in Section 3 as outside of our chosen threat model.

Also mentioned above is a potential weak link in security in the form of the network connection from the smart card readers —a vulnerability found at such a point in the process would allow an adversary to bypass the locks wholesale, thereby rendering the smart card components of Mcards to be functionally useless. Again, this kind of attack exists outside our threat model, as we assume that an adversary with such capability can also do much more than disengage locks.

6 Dorm Room Access

6.1 Dorm Room Keys

Access to residence halls is restricted through the use of an Mcard magstripe reader to prevent students who do not live in the dorms from entering a residence hall. Once inside the building, access to individual dorm rooms is maintained using a different electronic key locking system. Door rooms have a lock that can be opened by swiping a valid room magstripe card key, and entering in a four-digit PIN that corresponds to the key. Dorm room access is a rough form of two-factor authentication with

the PIN acting as "something you know", and the key as "something you have". The electronic system used is the Onity Integra 3. Onity is an electronic lock manufacturer for "hotels to the healthcare industry" [8].

All of the data on the key card is stored on Track 3. We analyzed all possible character sizes and determined that no parity bits are utilized and that the data is stored as a bytestring of length 21. Data on Track 3 is encrypted with what Onity calls the *sitekey*, which is unique to each deployment of the Integra platform. As such there is a single sitekey that encrypts all of the dorm keys used at the University. The contents of the plaintext are not fully known, but the similarity between the Onity Integra system and Onity HT system implies that the plaintext should be similar to the reverse-engineered and broken protocol for the Onity HT lock system used in hotels [10] [8].

6.2 Dorm Room Locks

The sitecode used to decrypt the room keys is stored in the lock on each door. The sitecode can be uploaded into the lock using an X Portable Programmer (XPP). According to the Housing Information Technolgoy Office (HITO), the XPP can also be used to power open a door. This further implies the Integra system uses a similar protocol to the HT system [10].

We built the lock-opening Arduino-based device for Onity HT locks described in [10], and attempted to unlock the Onity Integra locks on the dorm room doors, but found the device did not work as-is. According to the head of HITO, Onity has stated that the "Integra system is different and not vulnerable in the way the HT system is." We find this statment to be very carefully worded, and at this time believe the Integra system is vulnerable to a very similar attack as the HT system, as the Integra system was deployed in 2003 [11]. The simplest explanation for why the attack failed is that the Onity Integra locks store the sitecode at a different memory address than the HT locks. We have not successfully executed an attack against the Integra locks, and unless we obtain express permission from HITO as well as a test lock to experiment against, we do not intend to continue adapting the HT attacks to Integra. However, we would not be surprised if a similar attack is demonstrated against the Integra system in the near future.

6.3 Security Analysis

Contrary to our expectations, at this time it appears that due to the combination of encryption and required PIN, dorm room keys are less vulnerable to duplication and forgery than Mcards. However, the ecosystem surrounding Mcards and MIFARE smart cards is much more open than the ecosystem surrounding Onity locks. The cryptography used in Onity cards is not a publically documented protocol built on top of standard cryptographic primitives akin to the cryptography used in Mcards [10] [14]. If the similar cryptography is used in the Integra system as the HT system, then the cards are also vulnerable to chosen plaintext attacks and brute force attacks [10]. On an average desktop computer, it takes around nine days to brute-force all possible decryptions of the algorithm used on HT locks, since the sitekey for HT locks is 32-bits. We have been unable to determine if the same algorithm is used on the Integra locks. We would like to see Onity publish their protocol so that it can be publically audited for cryptographic vulnerabilities.

7 Future Work

We believe there is still much to be investigated regarding physical access mechanisms on the University of Michigan campus in Ann Arbor. While our first analysis focuses on a low-resource "opportunity attacker," future analysis should be done to explore the capabilities of an adversary with more resources than our current threat model allows. We offer two starting points for such future study, regarding the contactless entry systems and dormitory locks respectively.

First, thorough investigation should be made to determine how accessible the campus's card readers are over the local computer network. If the card reading devices or their subnets can be easily accessed, then proper investigation should determine how much of their traffic can be sniffed or intercepted, as well as how much of the nature or content of that traffic.

Second, new efforts should be made to find weaknesses in the Onity Integra 3 locks used in campus dormitories. Research along this path should either be carefully done with aid of HITO in the forms of express permission to carry out the research and a supplied test lock. Failing that, general study of Integra 3 locks might still be fruitful if a working lock is acquired first. The results of the study could then be applied in the context of the University dormitories.

8 Conclusion

We investigated physical authentication at The University of Michigan, centering around Mcard magnetic stripe access, Mcard contactless access, and dorm room key cards. We found opportunities for malicious Mcard holders to collude against the University when using swipe authentication, whereas we found the Mcard contactless authentication using NFC technology to be se-

cure. Therefore, we recommend the University move away from swipe authentication and use entirely contactless smart card authentication. We especially recommend against using swipe authentication to limit access to server rooms.

Dorm room keys and locks are part of the Onity Integra 3 product line. We found Integra 3 to be using secure principles, but we are not totally satisifed that the system is totally secure. We believe it may be possible to extract the sitekey used to encrypt all dorm room keys from a dorm room lock, however we have been unable to implement this attack ourselves. We have yet to hear a satisfactory response from Onity for the University that explains why this attack would not be feasible for a clever hardware hacker to perform. We present a call-to-arms to white-hat hardware hackers to attack the Onity Integra system, and responsibly disclose any vulnerabilites found.

9 Acknowledgments

The authors would foremost like to thank Ariana Mirian for her amenable attitude towards testing her door room door. We also thank Elson Liu, Ryan Landay, Kyle Schiller, Noah Cohen, and Sarah Paris for allowing us to read their Mcards. We especially thank Jeffrey Wright of the University of Michigan Housing Information Technology Office for answering questions about University Housing lock policy.

References

[1] Ecma standard for a six bit input/output code. Tech. rep., ECMA, 1963.

[2] 7813 – information technology – identification cards – financial transaction cards. Tech. rep., ISO, 2006.

[3] *MSR606 Magnetic Stripe Card Reader/Writer (High and Low Coercivity) Programmer's Manual*, June 2009.

[4] Nxp's mifare desfire ev1 technology receives trusted security stamp of approval, June 2009.

[5] *DESFIRE EV1 Data Sheet*, Dec. 2010.

[6] *Campus Banking - University of Michigan*, Apr. 2014.

[7] *DESFIRE Classic Datasheet*, Mar. 2014.

[8] Onity home page, 2014.

[9] *Treasurer's Office - Mcard*, Apr. 2014.

[10] BROCIOUS, C. My arduino can beat up your hotel room lock. In *Proceedings of BlackHat Conference 2012: Las Vegas* (Aug. 2012).

[11] GAZELLA, K. Locks, cameras help to reduce crime in residence halls. *University Record* (Jun 2003).

[12] GREENBERG, A. Lock firm onity starts to shell out for security fixes to hotels' hackable locks.

[13] KASPER, T., OSWALD, D., AND PAAR, C. Side-channel analysis of cryptographic rfids with analog demodulation. In *Proceedings of the 7th International Conference on RFID Security and Privacy* (Berlin, Heidelberg, 2012), RFIDSec'11, Springer-Verlag, pp. 61–77.

[14] KASPER, T., VON MAURICH, I., OSWALD, D., AND PAAR, C. Chameleon: A versatile emulator for contactless smartcards. In *Proceedings of the 13th International Conference on Information Security and Cryptology* (Berlin, Heidelberg, 2011), ICISC'10, Springer-Verlag, pp. 189–206.

[15] OBERHEIDE, J. Mcard vulnerability, Apr. 2005.

[16] OBERHEIDE, J. Rfid on campus, Jan. 2007.

[17] SCHREUR, R. W., ROSSUM, P. V., GARCIA, F., TEEPE, W., JACOBS, B., GANS, G. D. K., VERDULT, R., MUIJRERS, R., KALI, R., AND KALI, V. Security flaw in mifare classic, 2008.

[18] SVIGALS, J. The long life and imminent death of the mag-stripe card. *IEEE Spectrum* (May 2012).