Security of Wireless Embedded Devices in the Real World

Timo Kasper · David Oswald · Christof Paar

Chair for Embedded Security
HGI, Ruhr-University Bochum
Universitaetsstrasse 150
44801 Bochum, Germany
{timo.kasper | david.oswald | christof.paar}@rub.de

Abstract

In the past years, wireless embedded devices have become omnipresent. Portable tokens communicating via an RF (Radio Frequency) interface are employed in contactless applications such as access control, identification, and payments. The survey presented in this paper focuses on those devices that employ cryptographic mechanisms as a protection against ill-intended usage or unauthorizedly accessing secured data. By analyzing different commercial products, i.e., electronic passports, the remote keyless entry system KeeLoq, a Mifare Classic based contactless payment system, and a public transport system relying on Mifare DESfire cards we demonstrate that it is feasible to recover the secret cryptographic keys from various cryptographic tokens. At hand of the real-world examples, the implications of a key extraction for the security of the respective contactless application are illustrated.

1 Introduction

Wireless tokens have become ubiquitous in our everyday life. RFID (Radio Frequency Identification) technology is used in the supply chain as a barcode replacement, in the medical sector (pace makers, patient wristbands), as a countermeasure against product piracy, or helps to prevent car theft in the form of car immobilizers. Contactless cards, representing the most powerful variant of RFIDs, enable amongst others comfortable ticketing, contactless payments and secure access control. Active, battery-powered remote controls possess their own transmitter enabling greater operating ranges. They are often used in Remote Keyless Entry (RKE) systems that have already replaced the conventional mechanical keys for accessing the majority of modern cars and buildings.

Wireless communication implies new, additional threats as compared to contact-based systems: a transponder residing in a pocket or wallet could be read out or modified without the owner taking note of it and the transmission of data via the RF field can be monitored or relayed from a distance. Hence, many wireless applications require protecting the over-the-air interface: a private phone call must not be monitored by a neighbour, a door must not be opened by an intruder, and it must be made impossible for a customer to charge his contactless payment card except at a dedicated charging terminal by paying money into the system. To realize security mechanisms that prevent from fraud and unauthorized access, or to establish confidentiality and data protec-

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 1-16

tion, cryptography in distinct flavours is widespread in today's wireless tokens. Encryption or authentication schemes incorporating secret cryptographic keys shall guarantee security, data integrity, and ensure the intended functionality of the wireless systems in general.

1.1 Pervasive Wireless Technology

The huge variety of wireless applications implies that the products differ amongst others in the dimensions, operating frequency, the maximum achievable range for a query, and their computational power [Fin03]. Some examples of wireless tokens are illustrated next.

1.1.1 Passive Wireless Devices (RFID)

Passive RFIDs as exemplified in the top of Figure 1 are generally restricted with respect to their energy consumption, i.e., the amount of switching transistors during their operation [LSR06], since their energy is supplied wirelessly by the RF field of a base station or reader. This limitation has a direct impact on the cryptographic capabilities of RFID devices — implementing state-of-the-art cryptography is sometimes infeasible [RCT06].

The cost-efficient transponders at the low end are used for applications in which no security is required, e.g., in the supply chain Electronic Product Code (EPC) Gen 2 tags [EPC10] enable the wireless identification of tagged objects from a distance and without a line-of-sight ("auto-ID"). Other applications of non-cryptographic RFID transponders include baggage handling at airports, automated toll collection (eToll), and the identification of animals, e.g., tracking cattle and tagging pets. Besides, RFIDs are used to tag humans: wristbands identify patients in hospitals to avoid mixing them up and (unsecured) RFID interfaces integrated in pace makers [HHBR+08] enable to (re)program their operating parameters through the human tissue.

More advanced RFID devices providing simple encryption schemes are integrated into car keys for anti-theft systems, i.e., immobilizers, and are used in medium-security applications for access control purposes. Cryptographic transponders can also help to prevent product forgery: RFID chips are integrated into spare parts, such as batteries of mobile phones, ink cartridges of printers, and (mechanical or electrical) components of cars. The protected devices operate only if genuine parts are identified by means of their transponders and otherwise report fraud or malfunction, e.g., a printer will not work if a forged ink cartridge is inserted.

Contactless smartcards as standardized in ISO/IEC 14443 [Int01] are basically smartcards or memory cards, augmented with a wireless interface. They are used worldwide in a wide range of security-sensitive applications, e.g., for identification, access control, and payment purposes. They (optionally) offer a wide range of security features, including cryptographic co-processors for encryption. Various multi-purpose applications have emerged that rely on contactless smartcards, e.g., the OpenCard in Prague (Czech Republic) combines micro-payments, ticketing for public transport, and services of the public library.

1.1.2 Active Wireless Devices

Battery-powered, active tokens illustrated in the bottom of Figure 1 enable operating ranges in the order of tens or hundreds of meters and can provide strong cryptography. They often serve as remote controls for RKE systems, e.g., for opening cars. Simple one-button key fobs operate unidirectionally without encryption or other security measures. More advanced devices possess

a bidirectional RF interface and implement protection schemes, e.g., authentication by challenge-response schemes before access to a secured area is granted.

Semi-active devices combine passive communication interfaces with battery-powered technology, e.g., sensors for monitoring and recording environmental conditions [Sav10]. The advanced transponders are mainly used in the supply chain for tagging containers with large assets, e.g., for the transportation of medical supplies, food and other goods.

1.1.1 Comparison of Wireless Devices

However, the computational power and the corresponding achievable level of security differ largely in each of the two groups: while read-only RFIDs and fixed-code tokens for the purpose of simple object identification and tracking provide no security, memory cards such as Mifare Classic and unidirectional (transmit-only) rolling-code devices such as KeeLoq remote controls employ some type of encryption mechanism. Contactless smartcards, e.g., Mifare DESFire, can execute modern, secure ciphers and hence enable secure challenge-response schemes, as also implemented in corresponding active, bidirectional keyfobs.

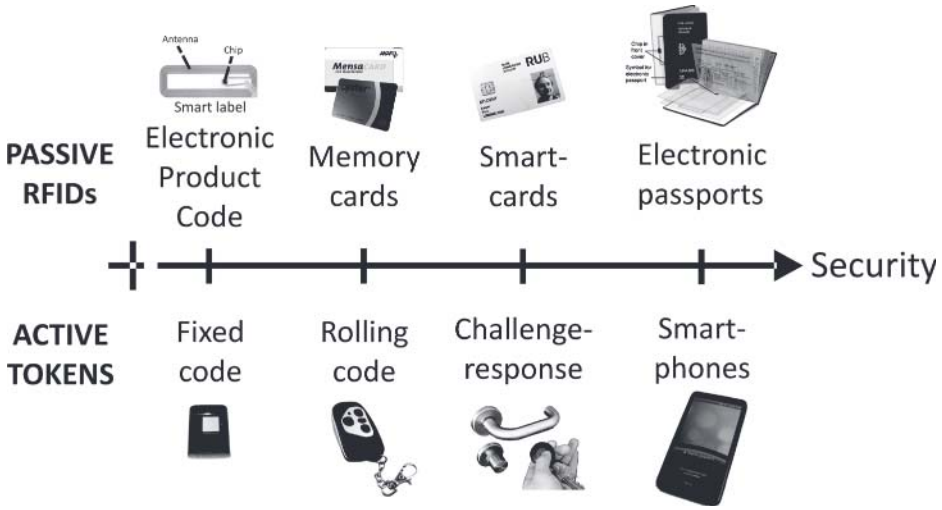

Fig. 1: Computational power and security level differ amongst active and passive tokens.

The most powerful passive device is probably the electronic passport [BSI]: it enables computationally demanding cryptographic schemes including public-key ciphers, and in addition features a protection against Man-In-The-Middle (MITM) attacks. Smartphones on the active side contain even more powerful microcontrollers. They can basically perform any desired type of cryptography and provide various communication channels, such as Wi-Fi, Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), and Bluetooth. Some phones possess a Near Field Communication (NFC) interface [ECM] that is compatible to contactless smartcards and hence constitutes a link between active tokens and passive RFID devices — smartphones equipped with NFC can connect passive devices to the cloud.

1.1.3 Security Considerations

Embedded systems are generally prone to security risks, since they are often in the possession of potential adversaries in large amounts. In the context of wireless technology some special threats evolve or are of particular importance. For example, copying a mechanical key premises physical access to the key or at least to the door lock. In contrast, circumventing a contactless system may be possible from a distance and without leaving any physical traces.

The limited energy supply of RFID tags and the cost sensitivity of high-volume applications often tempts manufacturers to minimize the production costs at the expense of the quality, e.g., by using outdated but "cheap" cryptographic components. As a consequence, cryptography and other security measures may be very lightweight or not employed at all, even when security or privacy issues are relevant.

1.2 Focus and Organization of the Paper

The scope of this paper is narrowed to certain wireless embedded devices that are analyzed by a low-skilled adversary, as detailed in the following. Next, an outline of the paper is given.

1.2.1 Analyzed Wireless Devices

Simple low-end devices, such as read-only RFID transponders and active fixed-code systems, provide no effective security measures — the corresponding threats are obvious and hence no in-depth analysis is required. Smartphones are also excluded from the investigations, since they can be regarded as portable computers and hence different attack vectors apply: for extracting secrets, in most cases computer-related threats such as trojan horses, root kits, and computer viruses play a more important role, compared to physical or cryptanalytical attacks. This survey instead focuses on the remaining portable devices with high security demands and limited computational power, i.e., the most widespread contactless smartcards and active keyfobs that employ cryptography. Applications relying on weak, proprietary cryptographic schemes (Mifare Classic cards and KeeLoq remote controls) are considered as well as those incorporating publicly known, highly secure ciphers (Mifare DESFire cards and electronic passports).

1.2.2 The Attacker

Ross Anderson and Markus Kuhn [AK98] and a paper by IBM [ADDS91] give a good classification of adversaries according to their funding and skills. The authors distinguish between three types of adversaries, i.e., clever outsiders, knowledgeable insiders, and funded organizations. This paper focuses on those attacks that are realistic for an adversary with a limited budget, i.e., attacks that can be performed by clever outsiders or knowledgeable insiders.

The cryptographic algorithm itself is assumed to be known to the attacker (no security only by obscurity!). Still, the specific implementation of the device to be attacked and other confidential information, e.g., the source code or an open sample device, is assumed to be not available to the attacker. The adversary has access to equipment such as oscilloscopes etc. that can be found in university labs. The auxiliary tools for physical and protocol attacks, as introduced in Section 5, are hence low-cost devices and often self-built from off-the-shelf components, with their design typically being publicly available.

1.2.3 Outline of the Paper

Tools for security analyses are introduced in Section 2. Next, the evolving real-world attacks are illustrated by analyzing commercial wireless products: as an example for a weak key derivation scheme enabling a recovery of the secret keys by means of brute-force, the approach of decrypting the communication of electronic passports is detailed in Section 3. The impacts of extracting the keys of a KeeLoq remote keyless entry system by means of power analysis are covered in Section 4. A flawed contactless payment system relying on Mifare Classic cards is attacked in Section 6 by exploiting a weak implementation on the card and mathematical vulnerabilities of the cipher. Finally, Section 7 illustrates that side-channel analysis can also be applied to contactless smartcards by recovering the keys of Mifare DESfire cards employing 3DES. Our attack is exemplified by decrypting the content of "Opencards" used in Prague for public transport and other purposes.

2 Tools for Security Analysis

In order to conduct physical attacks, (customized) hardware for performing the security analyses, the communication with the different targets, and assisting the data acquisition need to be developed. In [KOP10] a unified framework for advanced implementation attacks is introduced that allows for conducting automated side-channel analysis, fault injection, and other physical attacks. It enables analyzing all kinds of (wireless) embedded cryptographic devices including RFIDs. The developed cost-effective and freely programmable devices comprise a multi-function RFID reader and a card emulator for contactless smartcards. The low-cost framework disproves the common belief that highly sophisticated and expensive equipment is required to conduct physical attacks. All further details about the realization of the customized RFID hardware are described in [Kas06, KCP, KOPvM11].

2.1 Customized RFID Reader

For the security analyses and practical attacks in the field the freely programmable RFID reader developed in [KCP] is used. In contrast to commercially available products, the customized device enables to fully control the communication and inject faults by manipulating the RF field with a high timing accuracy of approximately 75 ns, which is a key advantage in the context of key-recovery from Mifare Classic cards (see Section 8). The multi-purpose reader device is equipped with an Atmel ATmega32 microcontroller; an RF interface for 13.56 MHz, as required for implementing the ISO 14443 protocol for smartcards; and some components for signal processing. All relevant protocols for communicating with electronic passports, Mifare Classic, Mifare DESfire, and many other contactless cards are implemented.

2.2 Chameleon

A custom-built hardware for emulating contactless smartcards compliant to ISO 14443, that can cooperate with the customized reader, has been developed in [KOPvM11]. The device, termed Chameleon, is based on an Atmel XMega microcontroller and can support basically all relevant (cryptographic) protocols used by contactless smartcards today, e.g., those based on AES or Triple-DES (3DES). The versatile device, which is open-source and can be built for less than 20 €, can technically appear as any modern contactless smartcard.

As a proof of concept, a full emulation of Mifare Classic cards on the basis of a highly optimized implementation of the stream cipher Crypto1 has been implemented. The device enables the creation of exact clones of such cards, including their Unique Identifier (UID). Further implementations realize the first emulation of DESfire and DESfire EV1 cards in the literature. The capabilities of the emulator are practically demonstrated by spoofing several real-world systems, e.g., doors secured by a widespread access control system based on identifying the UID of Mifare Classic cards are unauthorizedly opened. In Section 8, the Chameleon emulates a contactless payment card, which allows an attacker to set the stored credit balance as desired and hence make an infinite amount of payments.

2.3 Data Acquisition

- A controlling PC and a USB oscilloscope form the basis of the data acquisition system, as used for the side-channel attacks in this article. The acquired data can be side-channel information (e.g., current, voltage, EM emanation or timing information), or communication data such as bitstreams in any format which then later can be evaluated by a PC.
- The Picoscope 5204 dual-channel storage USB2.0-oscilloscope [Pic08] is used for digitizing physical observables during the attacks, e.g., information leakage in the context of a side-channel analysis (SCA). It costs approximately 2000 € and features a maximum sample rate of 1 GHz, an 8-bit Analog to Digital Converter (ADC) with a huge 128 MSamples waveform memory. The input bandwidth is 250 MHz, with a minimum input range of ±100 mV.
- Various types of probes for acquiring side-channel leakage and other information can be connected to the oscilloscope. The MI 145 passive high impedance probes that are supplied with the Picoscope have a bandwidth of B = 250 MHz at a 1:10 attenuation ratio (corresponding to B = 10 MHz for a 1 : 1 ratio). They are typically sufficient for measuring the power consumption of a device via the voltage drop at a resistor inserted into the supply path of the targeted device. For measurements of electromagnetic (EM) emanations, near-field probes manufactured by Langer EMV[1] are utilized, e.g., an RF-U 5-2 probe is used for the EM analysis of Mifare DESfire cards in Section 9. The captured signal is preamplified with the PA-303 amplifier [Lan] to meet the dynamic range of the oscilloscope.

2.4 COPACOBANA

This paragraph briefly introduces a customized, reconfigurable hardware platform termed cost-efficient parallel code breaker and analyzer (COPACOBANA). The architecture of the high-performance, low-cost cluster that can be realized for less than US$ 10,000 has been publicized in 2006 [KPP+06]. COPACOBANA appears to be the only reconfigurable parallel Field Programmable Gate Array (FPGA) machine optimized for code breaking tasks reported in the open literature. Depending on the actual algorithm, the parallel hardware architecture can outperform conventional computers by several orders of magnitude [GKN+08].

Since cryptanalytical applications demand for plenty of computing power, a total of 120 low-cost Xilinx6 Spartan3-XC3S1000 devices are installed on the COPACOBANA cluster[2]. The top level entity of COPACOBANA is a host-PC which is used to initialize and control the FPGAs, as well

1 www.langer-emv.de
2 see http://www.copacobana.org for all details

as for the accumulation of results. Data transfer between the FPGAs and the host-PC is accomplished by a dedicated control interface that connects COPACOBANA to a computer either via USB or Ethernet.

The hardware is optimized for computational problems which are parallelizable onto independent nodes with low communication and memory requirements, e.g., exhaustive key search. Note, that more than one COPACOBANA device can be attached to a single host-PC in order to further increase the performance. The next chapter employs COPACOBANA for extracting the secret keys used for the encryption of electronic passports.

3 Extracting Keys of Electronic Passports

This section tackles the security of the probably most secure wireless system based on passive RFID technology: the e-Pass (electronic passport), as specified by the International Civil Aviation Organization (ICAO) is deployed in many countries all over the world. To ensure interoperability between different countries, all e-Passports comply with the ISO/IEC 14443 standard. Technical specifications published by the European Commission [Eur06] are binding for the Schengen agreement countries. All e-Passports issued in the EU contain an embedded contactless chip that holds at least the same information that is printed on the identity information page of the passport, e.g., the name of the holder, date of birth, and a facial image. Optionally, an e-Passport can contain biometric identifiers, e.g., a fingerprint or an iris scan of the holder of the passport. The passports provide sophisticated cryptographic mechanisms to protect the private (biometric) data stored on it, including both public-key and symmetric cryptography [FOfIS]. The correctness of the private data is proven by a certificate of the issuing country and the digital photograph stored in the passport is optimized for automatic face recognition [JMV07].

The security of the first generation of passports is questionable, as detailed in this section. The key-search attacks presented in [LKLRP07] tackle the implementation of a security mechanism in the electronic passport as issued in Germany since November 2005 and are applicable to electronic passports of various other countries. After publicizing our findings as summarized in this section, a new version of the German electronic passport (additionally containing two fingerprints of the passport holder) was released in November 2007 with an improved variant of the here attacked key derivation scheme.

3.1 Related Work on Electronic Passports

The security and privacy threats have been widely discussed, e.g., in [JMW05, KK05, HHJ+06, JMV07, CLRPS], and have provoked public debates. In 2010, an attack for tracking the movements of a particular passport without having to break the passport's cryptographic key has been proposed in [CS10]. The authors show that the duration of computing a MAC during the authentification is key-dependent and hence enables identifying individual passports without decrypting the communication. While this attack requires actively interrogating the passport from a maximal range of some centimetres, the findings presented in this section allow tracking of individuals from a distance of several meters by means of eavesdropping.

3.2 Basic Access Control

The Basic Access Control (BAC) provides a means of mutual authentication and encrypting the data exchanged between the e-Passport and an RFID reader. Current realizations of the BAC, that shall prevent unauthorized access to the data stored on electronic passports, deploy symmetric cryptography based on SHA-1 and Triple-DES. The secret keys for the BAC are derived from the Machine Readable Zone (MRZ) printed on the document which contains data such as the passport number, date of birth and expiration date. The mechanism also serves as a protection against relay attacks.

Deriving the encryption and authentication keys for the BAC from the MRZ data is the cause for a security flaw: as we have shown in [LKLRP07], low entropy of the derived BAC keys enables straightforward attacks with a relatively small complexity compared to an exhaustive key search attack on Triple-DES. Instead of filling the digits of the MRZ with random alphanumerical values (which would result in sufficient entropy to prevent from a key recovery) the keys are generated from predictable personal information and other data with low entropy (such as dates).

3.3 Recovering the Secret Keys

Using the code-breaker COPACOBANA introduced in Section 3, in realistic scenarios the key for the BAC can be recovered almost in real-time, i.e., the time needed for a person to pass an inspection system at the border control: the achieved throughput of the implemented brute-force attack is 240 million, i.e., approx 2^{28} BAC keys per second. Testing 2^{35} key candidates, corresponding to a realistic scenario in which some personal data of the victim is known to the attacker, requires 2 minutes and 23 seconds on one COPACOBANA.

This enables to extract the keys from eavesdropped communication with an electronic passport and decrypt the intercepted private data. Two approaches for the key recovery are presented: one requires monitoring both directions of the communication, while for the second attack eavesdropping on the far-ranging requests of the reader is sufficient. Despite the secure cryptographic primitives being employed, the private data interchanged during the BAC is hence at risk of getting into the hands of unauthorized persons or organizations.

Such information is exploitable by criminals. Ari Juels et al. [JMW05] point out problems that are imposed on e-passport holders such as identity theft, tracking, and hotlisting. In the worst case scenario, an attacker may devise an RFID enabled bomb that is keyed to explode when reading a particular individual's RF identifier [JMW05]. The main cause for the found security vulnerabilities is the flawed key derivation from the MRZ.

4 A Remote Keyless Entry System: KeeLoq

Compared to passive RFID devices, active, battery-powered systems possess much more resources and are capable of performing basically any type of cryptographic operation. "Do real-world wireless systems relying on actively powered components accordingly provide a higher level of security?" To answer the question, the potency of power analysis when applied to active wireless tokens and the corresponding receivers is demonstrated at hand of the security analysis of KeeLoq Rolling Code systems in [vTJ11, KKMP09, EKM+08, MK09, NK09], as summarized next.

4.1 The KeeLoq Cipher and Rolling Code Scheme

The KeeLoq block cipher is widely used for security relevant applications, e.g., RKE and alarm systems for securing the access to a car or a building, as well as passive RFID transponders for car immobilizers [Mic]. The cipher was developed in the 1980s in South Africa and licensed by Microchip Technology Inc. in the 1990s. Since then, it has been integrated in many products incorporating their secure authentication product family. The cipher had been kept confidential for about two decades.

KeeLoq did not receive much attention until 2006, when the algorithm got known to the public and moved into the focus of the international cryptographic research community. Shortly after the first cryptanalysis of the cipher [Bog07], more analytical attacks were proposed [CBW08, IKD+08], revealing mathematical weaknesses of the cipher. Despite the impressive contribution to the cryptanalysis of the cipher, the real-world impacts of the existing attacks are limited, as described in more detail in [EKM+08].

In the most widespread "rolling-code" mode of KeeLoq, the unidirectional remote controls generate dynamic codes based on encrypting a counter with the device key of the remote control. The individual device keys are derived from the (known) serial number of the remote control by a (cryptographic) function involving a manufacturer key. Knowing the latter hence implies knowledge of all device keys in a KeeLoq system.

4.2 Power Analysis of KeeLoq

The developed highly efficient SCA attacks based on Simple Power Analysis (SPA) and Correlation Power Analysis (CPA) techniques enable to break the wireless access control system with minimal efforts. The attacks efficiently reveal both the secret key of a hardware implementation in the remote control and the manufacturer key stored in a software implementation in the receiver. As a result, a practical key recovery of a remote control, e.g., in order to clone it, is feasible in few minutes from only ten power traces. For a full key-recovery of the 64 bit manufacturer key of commercial products by SPA, one single measurement of a fraction of a KeeLoq decryption is sufficient, without the prior knowledge of neither a plaintext nor a ciphertext.

4.3 Cloning Remote Controls by Eavesdropping

After the one-time extraction of the manufacturer key as a prerequisite, recovering the secret key of a remote control and replicating it from a distance, just by eavesdropping on at most two transmitted messages, is demonstrated. This cloning approach without physical access to the remote control has serious real-world security implications, as the eavesdropping attack can be conducted by an unskilled adversary, while the technically challenging part (i.e., the SCA attack) can be outsourced to specialists. Furthermore, a denial-of-service attack can be mounted. An instantiation of an exhaustive key-search on COPACOBANA, to evaluate the security of other (seed-based) key-derivation schemes for KeeLoq, is detailed in [NK09]. All the described attacks have been verified on several commercial KeeLoq products.

The single point-of-failure in the key distribution in the system, i.e., deriving the keys of the remote controls from their serial number via a manufacturer key, enables dramatic attacks once the

manufacturer key has been recovered. Even a low-skilled intruder can spoof a KeeLoq receiver with technical equipment for less than 40 € and take over control of an RKE system, or deactivate an alarm system, leaving no physical traces.

The case of KeeLoq illustrates how widespread commercial applications, claiming to be highly secure, can be practically broken with modest cost and efforts using SCA. Thus, physical attacks must not be considered to be only relevant to the smartcard industry or to be a mere academic exercise. Rather, effective countermeasures need to be implemented not only in high-value systems such as smartcards, but also in wireless security applications.

5 Pitfalls of a Mifare Classic-based Payment System

Mifare Classic cards [NXP08b, NXP08a] have made their way into many public transportation systems such as the Octopus card in Hong Kong [Oct97], the Oyster card in London [Tra03], the OV-Chipkaart in the Netherlands [OV-05] and the CharlieCard in Boston [Mas06]. The cards are widely used for access control and are also employed for payment applications, e.g., in the contactless payment system analyzed in [KSP], as summarized next.

5.1 Mifare Classic

Mifare Classic cards comply with ISO/IEC 14443 and are basically memory cards, i.e., information can be stored in the internal EEPROM with an integrated digital control unit to handle the communication with a reader. Authentication and encryption with the integrated proprietary Crypto1 stream cipher shall prevent replay attacks, cloning and eavesdropping.

Soon after the reverse-engineering of the Crypto1 cipher and the Random Number Generator (RNG) on the Mifare Classic cards [NESP08], security vulnerabilities were found: a random nonce generated by the card is only dependent on the time elapsed between the power-up of the card and the issuing of the authentication command by the reader. Hence, by controlling the timing, the same nonce can be reproduced with a certain probability. This weakness has been first exploited by a key-stream recovery attack requiring to eavesdrop on genuine authentications [dKGHG08]. A secret key can then be derived from two eavesdropped authentications between a card and a genuine reader [GdKGM+08]. Later, the first card-only attacks emerged [GvRVS09, Cou09] that enable a key extraction from any Mifare Classic card utilizing a customized RFID reader.

5.2 Analyzing a Contactless Payment System

We have combined the existing card-only attacks and implemented the most efficient key-recovery attack to date on the low-cost RFID reader introduced in Section 3.1. The developed reader enables precise control of the communication and the RF field such that the RNG is completely bypassed and, exploiting properties of the weak Crypto1 cipher, an efficient key-recovery becomes possible. Using this implementation to extract the secret keys from payment cards and employing the Chameleon introduced in Section 3.2 we investigated a large commercial contactless payment application based on Mifare Classic cards [KSP].

During the analysis it turned out that the commercial payment cards store the credit balance (up to 150 €) autonomously and no effective countermeasures against fraud are implemented in the back end. With our hardware set-up it takes less than 2 minutes to recover the relevant secret keys from the used payment card (less than 30 seconds per sector key). Once the keys of one card are compromised, the security of the whole system collapses instantaneously, as all contactless payment cards turn out to have *identical secret keys* and no additional cryptographic mechanisms or obvious other checks are implemented on the system level.

An adversary can, in 40 ms and imperceptibly for the victim, read out a card or write to it, increase or decrease its credit balance, clone his card and impersonate the victim. Furthermore, a criminal can sell counterfeit cards or program the Chameleon to emulate a new random card, and hence permit an unlimited amount of payments. Another fatal flaw on the organizational level enables converting fraudulently increased virtual money to real cash. Most attacks, including the key recovery, can be carried out by an unskilled adversary using an RFID reader and open-source software for extracting the keys and modifying the cards.

The key-recovery is feasible due to a weak RNG and the usage of an outdated cipher in Mifare Classic cards. The analyzed system amplifies the evolving risks by the lack of a key distribution. While basic measures improving the security of such a flawed system, such as individual keys for each card and consistency checks in the back end are commonly known, they have been fully ignored by the system integrator, enabling straightforward fraud. The obvious idea of solving the security problems of the analyzed contactless payment system just by upgrading to a more sophisticated class of cryptographic contactless cards, e.g., Mifare DESfire, is not promising, as illustrated in the next section.

6 EM Side-Channel Attacks on Mifare DESfire

Mifare DESfire (MF3ICD40) cards [NXP04a] are employed in several large payment and public transport systems around the world, e.g., the Clippercard employed in San Francisco or the OpenCard deployed in Prague. The contactless smartcards employ a mathematically secure cipher, i.e., 3DES. Hence, mathematical cryptanalysis and attacks on the protocol level are not promising and another class of implementation attacks, i.e., side-channel analysis, is required for a key extraction. Again, the customized reader introduced in Section 3.1 serves as the basis for performing the first non-invasive side-channel attacks on commercial cryptographic RFIDs in the literature [KOP09], that rely on extracting and processing the information leakage contained in the EM emanations.

6.1 Related Work

Oren and Shamir [OS07] presented a successful side-channel attack against Class 1 EPC tags operating in the UHF frequency range which can be disabled remotely by sending a secret “kill password”. Small fluctuations in the reader field during the communication with the tag allow to consecutively deduce to the correct password bits. However, the very limited type of RFID tag does not offer any cryptography.

At the CHES 2007, Hutter et al. [HMF07] performed an EM attack on their own AES implementations on a standard 8-Bit microcontroller and an AES co-processor in an RFID-like setting. The

antenna and analogue frontend are separated from the digital circuitry, while on a real RFID tag these components are intrinsically tied together. In contrast to their work, we face the real-world situation, i.e., we have no knowledge about the implementation details of the unmodified contactless smartcard to be attacked. We analyze a black-box device with all RFID and cryptographic circuitry closely packed on one silicon die and get no help like artificial triggering for the alignment.

6.2 Key Extraction via the EM Side Channel

For the side-channel analysis, an EM probe (see Section 3.3) is placed close to the antenna of the contactless card. Then, known plaintexts are sent to the device. Its energy consumption during the encryption with 3DES is digitized and then processed with a PC. By correlating the measured information leakage with the modelled power consumption, details about the data processed by the card can be deduced. In [KOP09], we illustrate new techniques for facilitating a key recovery by means of Correlation Power Analysis (CPA) in the presence of the field of an RFID reader. We develop special analogue circuitry and evaluations methods, tailored to the analysis of contactless smartcards, that aim at isolating the information leakage contained in the EM emanations and that are generally applicable for analyzing all kinds of cryptographic RFIDs.

The effectiveness of the developed methods is practically verified by analyzing the security of Mifare DESfire cards. We investigate the leakage model applicable for the data bus, locate the time window of the encryption, and describe a CPA on the 3DES hardware implementation running on the contactless smartcard. The analysis pinpoints weaknesses in the protocol, reveals a vulnerability towards side-channel attacks (despite of integrated countermeasures), and results in the first successful key-recovery of the secret 112-bit keys of the cryptographic smartcard [KOP10]. The extraction of one 3DES key requires approximately 250,000 traces, which can be recorded in 7 hours with our current measurement setup. After that, all necessary evaluation steps can be carried out offline, without further physical access to the card, in approximately 12 hours using a standard PC.

6.3 Extracting the Secret Keys of Opencards

A Mifare DESFire MF3ICD40 offers 4 kByte of storage that can be assigned to up to 28 separate applications. 14 possible keys per application plus one master key amount to a maximum of 393 secret keys that can be used for protecting the card. For extracting each key, a separate side-channel attack is required. In practice, however, usually only a few keys are actively used, so most attacks can be carried out within a reasonable timespan. To verify the efforts required for extracting all keys of a commercial system, we analyzed the Opencard system deployed in Prague. In the multi-purpose Opencard application, Mifare DESfire cards enable amongst others ticketing in the public transport, usage of the public library, and payments for parking in the city centre.

The access to the application list of an Opencard is not restricted (it could also be secured by a key), i.e., this information can be read without any authentication. We found three applications: from our experiments we deduce that very likely one is dedicated to public transport, another one to payments, and the last application contains general information such as the expiry date of the card. With our attack we extracted the secret keys of all applications as used by the Opencard system and read out the (decrypted) content of several Opencards. We found that the master key

for altering various security parameters of the cards seems to be identical for all cards. Likewise, the key for the application storing general information on the cards, containing three files, is the same for all analyzed cards. The application for public transport containing one large file (480 bytes) and the application for payments containing three files are both secured with diversified keys that seem to be individually derived for each card. We were able to reveal personal data such as the date of birth from personalized cards, and intend to continue the analysis of the system.

6.4 Consequences of the Key-Recovery Attack

This section demonstrates that the mathematical security of a cipher is not sufficient to guarantee the desired protection in a real-world product: implementation attacks such as side-channel analysis pose a real threat and allow for extracting secret keys even from implementations of secure ciphers, if physical access to the device is given. Appropriate countermeasures against power-analysis attacks are also required for RFIDs: the strong noise induced by the EM field of the reader does not hinder extracting cryptographic keys, as demonstrated at the example of Mifare DESfire MF3ICD40 cards[3] used for the commercial Opencard system. Knowing all keys, an attacker can arbitrarily access the content and functionality of a Mifare DESfire card. The non-invasive key-recovery attack requires no modification of the card and leaves no physical traces.

7 Conclusion

A cost-effective toolset that is optimized for physical and protocol attacks on the security of wireless devices was presented, which can be extended to analyze virtually any type of cryptographic device. By analyzing real-world wireless systems with this toolset, various significant security vulnerabilities were pinpointed that can be exploited by a malicious opponent.

A brute-force attack implemented on the code-breaker COPACOBANA targets the basic access control scheme securing electronic passports: in practical scenarios the cryptographic keys protecting the private data are revealed in seconds. Further, the most efficient practical key-recovery attack on Mifare Classic cards known to date has been implemented. It enables to extract one sector key of a payment card in approximately 30 seconds. Since identical keys are used in all payment cards of the system, the key-recovery enables straightforward fraud.

Powerful side-channel attacks on commercial products were demonstrated in practice: the cryptographic keys of KeeLoq remote controls and the corresponding receivers of the remote keyless entry system can be extracted from approximately 10 power measurements and one single power measurement, respectively. Side-channel analysis of the electromagnetic field emanated by Mifare DESfire cards reveals the 112-bit secret keys used by their 3DES engine, however, with comparatively large efforts.

The developed tools and techniques set new lower bounds for the cost and efforts required for extracting keys with power analysis and other practical attacks. We demonstrate that many real-world systems are fully assailable and should be secured with modern cryptographic measures.

3 NXPs follow-up product Mifare DESFire EV1 [NXP08c] promises a higher security level, including a protection against side-channel analysis, and is not (yet) broken.

References

[CBW08] Nicolas T. Courtois, Gregory V. Bard, and David Wagner. Algebraic and Slide Attacks on KeeLoq. In FSE 2008, volume 5086 of Lecture Notes in ComputerScience, pages 97–115. Springer, 2008.

[CLRPS] Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, and Ahmad-Reza Sadeghi. E-Passport: The Global Traceability or How to Feel Like an UPS Package. InWorkshop on Information Security Applications (WISA 2006), volume 4298 of Lecture Notes in Computer Science, pages 391–404. Springer.

[Cou09] Nicolas Courtois. The Dark Side of Security by Obscurity - and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime. In SECRYPT, pages 331–338. INSTICC, 2009.

[CS10] Tom Chothia and Vitaliy Smirnov. A traceability attack against e-passports. In Financial Cryptography and Data Security, volume 6052 of Lecture Notes in Computer Science, pages 20–34. Springer, 2010.

[dKGHG08] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A Practical Attack on the MIFARE Classic. In CARDIS, volume 5189 of Lecture Notes in Computer Science, pages 267–282. Springer, 2008.

[ECM] Standards ECMA-340 and ECMA-352 for the Near Field Communication Interface and Protocol. http://www.ecma-international.org.

[EKM+08] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In CRYPTO 2008, volume 5157 of Lecture Notes in Computer Science, pages 203–220. Springer, 2008.

[EPC10] EPCGlobal GS1. EPC Tag Data Standard 1.5, August 2010. http://www.gs1. org/gsmp/kc/epcglobal/tds.

[Eur06] European Commission. EU - Passport Specification. http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_ 909_en.pdf , June 2006.

[Fin03] Klaus Finkenzeller. RFID Handbook: Fundamentals and Applications in Con- tactless Smart Cards and Identification. John Wiley and Sons, 2nd edition, 2003.

[FOfIS] Germany Federal Office for Information Security. Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control. http://www.bsi.de/fachthem/epass/EACTR03110_v110.pdf .

[GdKGM+08] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling MIFARE Classic. In ESORICS, volume 5283 of Lecture Notes in Computer Science, pages 97–114. Springer, 2008.

[GKN+08] Tim Güneysu, Timo Kasper, Martin Novotný, Christof Paar, and Andy Rupp. Cryptanalysis with COPACOBANA. IEEE Transactions on Computers, 57(11): 1498–1513, 2008.

[GvRVS09] Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly Pickpocketing a Mifare Classic Card. In IEEE Symposium on Security and Privacy, pages 3–15. IEEE, 2009.

[HHBR+08] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In Proceedings of the 2008 IEEE Symposium on Security and Privacy, pages 129–142. IEEE Computer Society, 2008.

[HHJ+06] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In Hiroshi Yoshiura, Kouichi Sakurai, Kai Rannenberg, Yuko Murayama, and Shin ichi Kawamura, editors,

First International Workshop in Security (IWSEC 2006), volume 4266 of Lecture Notes in Computer Science, pages 152–167. Springer, 2006.

[HMF07] Michael Hutter, Stefan Mangard, and Martin Feldhofer. Power and EM Attacks on Passive 13.56 MHz RFID Devices. In Pascal Paillier and Ingrid Verbauwhede, editors, Cryptographic Hardware and Embedded Systems - CHES 2007, LNCS 4727, pages 320 – 330. Springer, 2007.

[IKD+08] Sebastiaan Indesteege, Nathan Keller, Orr Dunkelman, Eli Biham, and Bart Preneel. A Practical Attack on KeeLoq. In EUROCRYPT 2008, volume 4965 of Lecture Notes in Computer Science, pages 1–18. Springer, 2008.

[Int01] International Organization for Standardization (ISO). ISO/IEC 14443: Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards, Part 1-4, 2001. www.iso.ch.

[JMV07] S. Vaudenay J. Monnerat and M. Vuagnoux. About Machine-Readable TravelDocuments. In Workshop on RFID Security (RFIDSec'07), pages 15–28, 2007.

[JMW05] Ari Juels, David Molnar, and David Wagner. Security and privacy issues in e-passports. In Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005., pages 74–88. IEEE, September 2005.

[Kas06] Timo Kasper. Embedded Security Analysis of RFID Devices. Master's thesis, Ruhr Universität Bochum, July 2006. http://www.emsec.rub.de/media/crypto/attachments/files/2010/04/timo_kasper___embedded_security_analysis_of_rfid_devices.pdf .

[KCP] Timo Kasper, Dario Carluccio, and Christof Paar. An Embedded System for Practical Security Analysis of Contactless Smartcards. In Workshop in Informa- tion Security Theory and Practice, WISTP 2007, volume 4462 of Lecture Notes in Computer Science, pages 150–160. Springer.

[KK05] G.S. Kc and P.A. Karger. Security and Privacy Issues in Machine ReadableTravel Documents (MRTDs). RC 23575, IBM T. J. Watson Research Labs, April 2005.

[KKMP09] Markus Kasper, Timo Kasper, Amir Moradi, and Christof Paar. Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed. In Progress in Cryptology - AFRICACRYPT 2009, volume 5580 of Lecture Notes in Computer Science, pages 403–420. Springer, 2009.

[KOP09] Timo Kasper, David Oswald, and Christof Paar. EM Side-Channel Attacks on Commercial Contactless Smartcards using Low-Cost Equipment. In WISA 2009, volume 5932 of Lecture Notes in Computer Science, pages 79–93. Springer, 2009.

[KOP10] Timo Kasper, David Oswald, and Christof Paar. A Versatile Framework for Implementation Attacks on Cryptographic RFIDs and Embedded Devices. Volume 10 of Lecture Notes in Computer Science, pages 100–130. Springer, 2010.

[KOPvM11] Timo Kasper, David Oswald, Christof Paar, and Ingo von Maurich. Chameleon: A versatile emulator for contactless smartcards. In ICISC 2010, Seoul, Korea, Lecture Notes in Computer Science. Springer, 2011.

[KPP+06] Sandeep Kumar, Christof Paar, Jan Pelzl, Gerd Pfeiffer, and Manfred Schimmler. Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker. In Louis Goubin and Mitsuru Matsui, editors, Cryptographic Hardware and Embedded Systems (CHES 2006), volume 4249 of Lecture Notes in Computer Science, pages 101–118. Springer, 2006.

[KSP] Timo Kasper, Michael Silbermann, and Christof Paar. All You Can Eat or Breaking a Real-World Contactless Payment System. In Financial Cryptography 2010, volume 6052 of Lecture Notes in Computer Science, pages 343–350. Springer.

[Lan] Langer EMV-Technik. Details of Near Field Probe Set RF 2. www.langer-emv.de

[LKLRP07] Y. Liu, T. Kasper, K. Lemke-Rust, and C. Paar. E-Passport: Cracking Basic Access Control Keys. In Proceedings of OTM'07, Part II, volume 4804 of Lecture Notes in Computer Science, pages 1531–1547. Springer, 2007.

[LSR06] Tobias Lohmann, Matthias Schneider, and Christoph Ruland. Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags. In Josep Domingo-Ferrer, Joachim Posegga,

and Daniel Schreckling, editors, Smart Card Research and Advanced Applications, volume 3928 of Lecture Notes in Computer Science, pages 278–288. Springer, 2006.

[Mas06] Massachusetts Bay Transportation Authorit. The Charlie Card Reusable Ticket System. http://www.mbta.com/fares_and_passes/charlie, 2006.

[Mic] Microchip. HCS410/WM, KeeLoq Crypto Read/Write Transponder Module. http://ww1.microchip.com/downloads/en/DeviceDoc/41116b.pdf.

[MK09] Amir Moradi and Timo Kasper. A New Remote Keyless Entry System Resistant to Power Analysis Attacks. In 7th International Conference on Information, Communications and Signal Processing (ICICS), pages 1062–1067. IEEE Press, 2009.

[NESP08] Karsten Nohl, David Evans, Starbug, and Henryk Plötz. Reverse-Engineering a Cryptographic RFID Tag. In Paul C. van Oorschot, editor, USENIX Security Symposium, pages 185–194, 2008.

[NK09] Martin Novotný and Timo Kasper. Cryptanalysis of KeeLoq with COPACOBANA. In Workshop on Special Purpose Hardware for Attacking Cryptographic Systems (SHARCS'09), 2009.

[NXP95] NXP. Mifare Classic. http://www.nxp.com, 1995.

[NXP04a] NXP. Mifare DESFire Short Form Specification MF3 IC D40, 2004. http://www.nxp.com/acrobat_download/other/identification/SFS075530.pdf .

[NXP08a] NXP. Mifare Classic 1K MF1 IC S50 Functional Specification. http://www.nxp.com/acrobat_download/other/identification/M001053_MF1ICS50_rev5_3.pdf , 2008.

[NXP08b] NXP. Mifare Classic 4K MF1 IC S70 Functional Specification. NXP, 2008. http://www.nxp.com/acrobat/other/identification/M043541_MF1ICS70_ Fspec_rev4_1.pdf .

[NXP08c] NXP. Short Data Sheet Mifare DESFire EV1 MF3 IC D41. http://www.nxp.com/acrobat_download/datasheets/MF3ICD21_41_81_SDS_2.pdf , 2008.

[Oct97] Octopus. Octopus Card in Hong Kong. http://www.octopuscards.com/ consumer/products/en/index.jsp, 1997.

[OS] Yossi Oren and Adi Shamir. Power Analysis of RFID Tags. http://www.wisdom. weizmann.ac.il/~yossio/rfid/.

[OS07] Yossef Oren and Adi Shamir. Remote Password Extraction from RFID Tags. Volume 56, pages 1292–1296, Washington, DC, USA, 2007. IEEE Computer Society. http://iss.oy.ne.ro/RemotePowerAnalysisOfRFIDTags .

[OV-05] OV-chipkaart. All about the OV-chipcard. http://www.ov-chipkaart.nl/ allesoverdeov-chipkaart, 2005.

[Pic08] Pico Technology. PicoScope 5200 USB PC Oscilloscopes, 2008.

[RCT06] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. The Evolution of RFID Security. volume 5, pages 62–69, Jan-Mar 2006.

[Rob] Harko Robroch. ePassport Privacy Attack, Presentation at Cards Asia Singapore, April 26,2006. http://www.riscure.com.

[Sav10] Savi Technology, Inc. Data Sheets of Savi ST-6XX Active RFID Tags, 2010. http://www.savi.com .

[Tex] Texas Intruments. Texas Instruments to deliver RFID solution for Master- Card PayPass. http://www.ti.com/rfid/docs/news/news_releases/2005/rel01-17-05a.shtml .

[Tra03] Transport for London. What is Oyster? http://www.tfl.gov.uk/tickets/ oysteronline/2732.aspx, 2003.

[Ver] R. Verdult. Proof of Concept, Cloning the OV-Chip Card. http://www.sos.cs.ru.nl/applications/rfid/2008-concept.pdf .

[vTJ11] Henk C. A. van Tilborg and Sushil Jajodia, editors. Encyclopedia of Cryptography and Security 2. Springer, September 2011. to appear.