Wireless Devices and Cryptography: About Digital Pickpocketing, Open Sesame and Tracking Paranoia

Unsichtbare Funkchips: Von digitalem Taschendiebstahl, Sesam-Öffne-Dich und Verfolgungswahn

Timo Kasper*, Ruhr-Universität Bochum[1]

* Correspondence author: timo.kasper@rub.de

Summary Wireless embedded devices are employed for access control, identification, and payments. Cryptographic mechanisms serve as a protection against ill-intended usage or unauthorizedly accessing secured data. By security-analyzing commercial products, e. g., electronic passports, the remote keyless entry system KeeLoq, a Mifare Classic based contactless payment system, and Mifare DESfire cards, various security vulnerabilities are revealed. At hand of real-world attacks, the implications of a key extraction for the data protection and security of the respective contactless applications are illustrated.

►►► **Zusammenfassung** Funktechnologie kennzeichnet Produkte, dient zur Identifikation (z. B. elektronischer Reisepass), funktioniert als elektronische Geldbörse und öffnet Türen. Über die drahtlose Schnittstelle werden sensible Daten ausgetauscht, die per Lauschangriff ausgespäht oder unbemerkt aus der Entfernung modifiziert werden könnten. Verschlüsselungsverfahren sollen Manipulationen, Identitätsdiebstahl oder unbefugtes Eindringen verhindern. Der kryptografische Schutz vieler kommerzieller Produkte stellt sich jedoch häufig als unzureichend heraus und kann durch moderne Angriffsmethoden ausgehebelt werden – oft mit dramatischen Folgen für den Datenschutz und die Sicherheit des Gesamtsystems.

Keywords ACM CCS: Security and privacy; Real-world attacks; Keeloq; Mifare DESfire; Electronic passport; Contactless payments
►►► **Schlagwörter** Praktische Sicherheitsanalyse, Keeloq, Mifare DESfire, Elektronischer Reisepass, kontaktloses Bezahlen

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, for identifying animals, 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 trans-

[1] Dr.-Ing. Kasper earned his doctorate at the Faculty of Electrical Engineering and Information Technology of the University of Bochum. The examiners were Prof. Dr.-Ing. Christof Paar, University of Bochum, and Prof. Dr. Srđan Čapkun, ETH Zurich. The dissertation of Dr.-Ing. Kasper titled "Security Analysis of Pervasive Wireless Devices – Physical and Protocol Attacks in Practice" has been awarded with the CAST/GI Dissertation Award IT-Security 2012.

ponder 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 protection, 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 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 Analyzing Cryptographic Wireless Devices

The PhD thesis [1], as summarized in this article, focuses on portable devices with high security demands and limited computational power, i. e., 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).

To rate the feasibility and complexity of attacks and to determine the relevance of the respective security risks, a purely theoretical analysis is not sufficient. Thus, low-cost tools for practical security analyses have been developed, e. g., custom reader devices and emulators for contactless cards.

The performed practical analyses illustrate an evident lack of security in many commercial wireless systems, especially with respect to physical cryptanalysis. Pinpointing the flaws in the realization of several contactless applications shall help developers and designers to prevent similar wrong or naïve usage of cryptography and thereby improve future products. The often dramatic implications are illustrated, the privacy protection of individuals using modern contactless technology is highlighted, and other security-related aspects are discussed. Where applicable, best-practice countermeasures are proposed that can effectively hinder the attacks.

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: The cost-effective and freely programmable devices comprise a multi-function RFID reader and a card emulator for contactless smartcards. They disprove the common belief that highly sophisticated and expensive equipment is required to conduct physical attacks.

2.1 Customized RFID Reader

For the security analyses and practical attacks in the field a freely programmable RFID reader developed in [2] 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. 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 [3]. 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.

The device enables the creation of exact clones of such cards, including their Unique Identifier (UID). 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. Furthermore, the Chameleon can mimic contactless payment cards, 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 required to conduct so-called side-channel analysis (SCA): The side-channel information (e. g., electric current, voltage, EM emanation or timing information) of a cryptographic device is acquired during its normal operation. Analyzing the measurements, e. g., by means of Differential Power Analysis (DPA), enables to extract the secret cryptographic keys of any unprotected implementation of a cryptographic scheme.

A Picoscope 5204 dual-channel storage USB2.0-oscilloscope 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 measurement probes can be connected to the oscilloscope. Standard passive probes (as supplied with the Picoscope) 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[2] are utilized, e. g., an RF-U 5-2 probe suffices for an EM analysis of contactless smartcards, such as Mifare DESfire MF3ICD40 cards.

2.4 Parallel Computing for Cryptanalysis

A customized, reconfigurable hardware platform termed cost-efficient parallel code breaker and analyzer (COPACOBANA) has been developed at the Chair for Embedded Security (EMSEC). COPACOBANA is a reconfigurable parallel Field Programmable Gate Array (FPGA) machine optimized for code breaking tasks. A total of 120 low-cost Xilinx6 Spartan3-XC3S1000 devices are installed on the COPACOBANA cluster[3].

The hardware is optimized for computational problems which are parallelizable onto independent nodes with low communication and memory requirements, e. g., exhaustive key search. The next chapter employs COPACOBANA for extracting the secret keys used for the encryption of electronic passports.

3 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) complies with the ISO/IEC 14443 standard for contactless smartcards. 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. The passports provide sophisticated cryptographic mechanisms to protect the private (biometric) data stored on it, including both public-key and symmetric cryptography.

The security of the first generation of passports is questionable, as detailed in this section. The key-search attacks presented in [1] 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 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 (Man-In-The-Middle) attacks.

Deriving the encryption and authentication keys for the BAC from the MRZ data is the cause for a security flaw: as shown in [1], 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).

3.2 Recovering BAC Keys

Using the code-breaker COPACOBANA, 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.

[2] http://www.langer-emv.de

[3] see http://www.copacobana.org for all details

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, e. g., for 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. The main cause for the found security vulnerabilities is the flawed key derivation from the MRZ.

4 A Remote Keyless Entry System: KeeLoq

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. The cipher had been kept confidential for about two decades.

In 2006 the algorithm got known to the public and various mathematical weaknesses of the cipher were found. Despite the impressive contribution to the cryptanalysis of the cipher, the mathematical attacks do not allow to break the most widespread "rolling-code" mode of KeeLoq: In this mode of operation, 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.

4.1 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.

4.2 Cloning 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: Open Sesame! 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 [1]. 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

NXP's Mifare Classic cards are widely used, e. g., for ticketing, access control and are also employed for payment applications, e. g., in the contactless payment system treated 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, 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 and other weaknesses enable an efficient key extraction from any Mifare Classic card.

5.2 Analyzing a Payment System

By combining the existing card-only attacks, the most efficient key-recovery attack to date has been implemented in [1] on the low-cost RFID reader [2]. Using this implementation to extract the secret keys from payment cards and employing the Chameleon [3] a large commercial contactless payment application based on Mifare Classic cards is investigated.

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. Recovering the relevant secret keys from the used payment card takes less than 2 minutes (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 Analysis of Mifare DESfire

Mifare DESfire (MF3ICD40) cards 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. Instead, an implementation attack, i. e., side-channel analysis, enables a key extraction. Again, the customized reader [2] serves as the basis for performing the first non-invasive side-channel attacks on commercial cryptographic RFIDs in the literature, that rely on extracting and processing the information leakage contained in the EM emanations. No knowledge about the implementation details of the contactless smartcard is known in advance: The "black-box analysis" of an RFID device with all analogue and cryptographic circuitry closely packed on one silicon die is described in detail in [1].

6.1 Key Extraction via the EM Side Channel

For the side-channel analysis, an EM probe 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. New techniques for facilitating a key recovery by means of Correlation Power Analysis (CPA) in the presence of the field of an RFID reader are introduced in [1]. Special analogue circuitry and evaluations methods, aiming at isolating the information leakage contained in the EM emanations, are developed and can be applied to analyze various other kinds of cryptographic RFIDs.

The effectiveness of the developed methods is practically verified by analyzing the security of Mifare DESfire cards. After identifying a leakage model applicable for the data bus and locating the time window of the encryption, a CPA on the 3DES hardware implementation running on the contactless smartcard is described. 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. Today, with improved attack methods, 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.

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, thus full access to a Mifare DESfire card, as used in a typical application, is given in a reasonable timespan.

6.2 Implementation Attacks: A Real Threat

This section demonstrated 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[4]. 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 developed, which can be extended to support virtually any type of embedded 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.

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

References

[1] Timo Kasper. Security Analysis of Pervasive Wireless Devices – Physical and Protocol Attacks in Practice. PhD thesis. 2011. Web: https://wiki.crypto.rub.de/Counter/get.php?id=1.

[2] Timo Kasper, Dario Carluccio, and Christof Paar. An Embedded System for Practical Security Analysis of Contactless Smartcards. In Workshop in Information Security Theory and Practice, WISTP 2007, volume 4462 of Lecture Notes in Computer Science, pages 150–160. Springer. Open-Source Project: http://sourceforge.net/projects/reader14443/.

[3] Timo Kasper, Ingo von Maurich, David Oswald, and Christof Paar. Chameleon: A Versatile Emulator for Contactless Smartcards. In ICISC 2010, Seoul, Korea, Lecture Notes in Computer Science. Springer, 2011. http://sourceforge.net/projects/chameleon14443.

[4] David Oswald, Christof Paar. Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. Workshop on Cryptographic Hardware and Embedded Systems. Lecture Notes in Computer Science Springer.2011.

Received: February 27, 2013

Dr.-Ing. Timo Kasper is a researcher at the Horst Görtz Institute for IT Security (HGI) in the field of security of embedded cryptographic systems. His Diploma thesis (2006) and PhD thesis (2011) were supervised by Prof. Dr.-Ing. Christof Paar and were both decorated with the first place award for IT security (CAST, Darmstadt). Timo is co-founder of the security engineering company Kasper & Oswald GmbH.

Address: Chair for Embedded Security (EMSEC), Ruhr-University Bochum, ID 2/605, Universitaetsstrasse 150, 44780 Bochum,
e-mail: timo.kasper@rub.de

Preview on issue 4/2013

The topic of our next issue will be "Internet Challenges" (Editors: A. Feldmann) and it will contain the following articles:

- *H. Paulheim:* Ontology-based Application Integration on the User Interface Level
- *St. Uhlig and F. C. Latasha:* Recent Changes in the Internet Landscape
- *P. Trangia:* Crowdsourcing and its Impact on Future Internet Usage
- *D. Perouli et al.:* An Experimental Framework for BGP Security Evaluation