Sweet Dreams and Nightmares: Security in the Internet of Things

Timo Kasper, David Oswald, and Christof Paar

Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany
{timo.kasper,david.oswald,christof.paar}@rub.de

Abstract. Wireless embedded devices are predominant in the Internet of Things: Objects tagged with Radio Frequency IDentification and Near Field Communication technology, smartphones, and other embedded tokens interact from device to device and thereby often process information that is security or privacy relevant for humans. For protecting sensitive data and preventing attacks, many embedded devices employ cryptographic algorithms and authentication schemes. In the past years, various vulnerabilities have been found in commercial products that enable to bypass the security mechanisms. Since a large number of the devices in the field are in the hands of potential adversaries, implementation attacks (such as side-channel analysis and reverse engineering) can play a critical role for the overall security of a system. At hand of several examples of assailable commercial products we demonstrate the potential impact of the found security weaknesses and illustrate "how to not do it".

1 Introduction

Today's embedded devices are equipped and interconnected with various (wireless) interfaces. They often possess sensors and audiovisual peripherals, store and process private data of users and their surroundings, and can exchange information with other (embedded) devices — usually imperceptible and without a user interaction. Medical instruments, IDs, payments cards, cars, door locks, and smartphones are just a few examples for these ubiquitous devices that can directly or indirectly access the Internet. Thus, in theory all data stored and processed by the embedded devices could be collected in big data bases and analyzed, which could be harmful for the data protection of the individual. Many of the devices control critical appliances of our everyday life that in case of malfunctioning could become a threat even for the safety of the user, e.g., automotive or medical devices.

To ensure reliable, secure operation of systems, prevent fraud, and protect the data of individuals, often cryptography is employed. However, many commercial devices are not conform to the state-of-the-art in research and implement other — often proprietary and low-cost — algorithms and schemes. They seem to provide some suitable protection at first glance, but after a more thorough investigation turn out to be vulnerable to "off-the-shelf" attacks, often with a

D. Naccache and D. Sauveron (Eds.): WISTP 2014, LNCS 8501, pp. 1–9, 2014.

dramatic impact. Researchers have in the past approx. 10 years started to analyze the security of cryptographic schemes implemented in commercial products, to identify and pinpoint their weaknesses, and repair them on the long term. The important process of publicly disclosing cryptographic primitives, cryptanalyzing them to separate secure from weak proposals, with the result of trusted and peer-reviewed ciphers being available for everyone today, is well known from the mathematical world. In the following, we emphasize the importance of security checks of implementations in the real world at hand of several practical examples of assailable systems in the Internet of Things (IoT).

2 Security-Analyzing NFC Applications

One widespread type of participant in the IoT are Radio Frequency IDentification (RFID) and Near Field Communication (NFC) tokens. Next, we describe cost-efficient hardware for security-analyzing them and illustrate practical attacks.

2.1 Contactless Smartcards and NFC

Many applications for ticketing, micro payments, access control, and identification rely on contactless cards that are compliant to the ISO 14443 standard [Int01], e.g., NXP's Mifare family of cards, electronic ID cards, and passports. NFC [Int04] is compatible to ISO 14443 and is widespread in embedded devices, such as smartphones, door locks, and other objects. An NFC-enabled object can function as an active reader in one moment and as a passive contactless card in the next moment.

2.2 Tools

Commercial NFC readers and cards usually contain chips that automatically execute manufacturer-specific schemes and thus provide restricted functionality. Many types of security analyses require freely programmable devices. The open-source hardware described next is handy for penetration tests, but can also serve as a flexible, low-cost alternative for realizing manufacturer-independent NFC applications.

NFC Reader. The freely programmable RFID reader presented in [KCP07] gives full control of the NFC communication and can support any contactless card or RFID tag operating at a frequency of 13.56 MHz. The customized device allows to manipulate the Radio Frequency (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.

Chameleon. The credit-card shaped Chameleon is a versatile tool for practical NFC security analyses in the field and compliance tests. On the other hand, it can also serve as a passive counterpart for an active NFC device, e.g., a smartphone in reader mode, and thus provide an energy-efficient interface for embedded systems like door locks.

Our originally published card emulator [KvMOP11] has been completely redesigned in the meantime: The new ChameleonMini can now be manufactured at a cost of less than 10 $ and is continuously maintained as an open-source project. The hardware supports Amplitude-Shift Keying (ASK) modulation (10% and 100%), can generate ASK or Binary Phase-Shift Keying (BPSK) load modulation with a subcarrier, and thus can emulate any ISO 14443, NFC, and ISO 15693 card and other types of transponders operating at 13.56 MHz. The ATXmega processor is connected to an external non-volatile memory that can store up to eight virtualized contactless cards (e.g., Mifare DESfire, Mifare Classic, Mifare Ultralight, and many others), while the processing of the relevant cryptographic schemes (e.g., Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), or Crypto1) and the answering time is usually even faster than the original cards.

The modular firmware is programmed mostly in C, can be uploaded via a Universal Serial Bus (USB) bootloader, and is easily expandable to new cards and standards. The ChameleonMini can be controlled and configured from the USB interface with its own dedicated command set, e.g., to obtain status information, upload new card content or set a different Unique Identifier (UID). A logmode can be used to monitor and record NFC communication and a user-programmable button enables, for example, to cycle through the different virtualized cards stored inside the ChameleonMini.

We intend to make the device available at a low cost for educational purposes and aim at developing teaching material with practical know-how about both the physical layer of NFC and the higher protocol levels, including efficient implementations of cryptography for RFID. The ChameleonMini can be employed to virtualize several personal cards in one device, e.g., to open NFC-enabled door locks, operate NFC-barriers of parking lots, rent bicycles, or execute contacless payments in the system described in the next section.

2.3 Contactless Payments

The security vulnerabilities we found in the analysis of a widespread contactless payment system, as publicized in [KSP10], are overwhelming: NXP's Mifare Classic cards serve as a digital wallet, with all cards of one instantiation of the system containing an identical set of cryptographic keys. Taking into account the known weaknesses of the Crypto1 stream cipher and the flawed Random Number Generator (RNG) on these cards, this had been an extremely bad design choice: A random nonce generated by the card depends only on the time elapsed between the power-up of the card and the issuing of the authentication command by the NFC reader. Hence, the same random numbers can be reproduced in subsequent

protocol runs. This and other weaknesses enable a key extraction from any Mifare Classic card with the above described customized reader, in seconds.

After extracting the secret keys of several payment cards, we examined their content and the functioning of the system with a series of practical tests. The credit balance turned out to be stored without any additional cryptographic protection — modifying it was very simple and not detected after weeks. In addition, neither the UID nor the card number stored on the card by the vendor was checked in the back-end. Note, that the content of the payment cards of other customers can be manipulated from a distance of 25 cm in milliseconds, enabling devastating attacks. After informing the system operator about the found vulnerabilities, the security of the payment system had allegedly been improved.

In March 2014, approximately five years after the initial analysis and subsequent improvement of the system, we performed a post-analysis to verify what has been changed exactly: Newly issued cards are now the much more secure (and more expensive) DESfire EV1 cards. Likewise, all NFC readers in the system were updated at a high cost, to support the new cards. However, to our surprise the system still accepts the old Mifare Classic cards, for downward compatibility reasons — with the identical key set and configuration as described above. The back-end still has no automated means to detect fraud and blacklist cards. We successfully verified that payments can still be carried out with the above described ChameleonMini in Mifare Classic emulation mode. For the tests, the user button has been programmed to increase the credit amount by 10 € on each button press, which worked very well. Upon our request, the system operator reported that some customers are known to fraudulently recharge their payment cards and use services for free, bu these crimes are tolerated as rare events.

2.4 Side-Channel Analysis of Mifare DESfire

In contrast to Mifare Classic, Mifare DESfire (MF3ICD40) cards employ a mathematically secure cipher, i.e., 3DES. They often serve for identification purposes in companies and can be found in large payment and public transport systems around the world, e.g., the Clippercard employed in San Francisco or the Opencard deployed in Prague.

In [OP11] we verify, whether an implementation attack, i.e., side-channel analysis, enables a key extraction. Side Channel Analysis (SCA) exploits information leakage in the power consumption (or timing behaviour) of a cryptographic device in order to extract its secrets. The powerful SCA attacks are especially convenient for extracting keys of implementations employing mathematically unbreakable ciphers.

In the first non-invasive Electro-Magnetic (EM) analysis of commercial cryptographic RFIDs in the literature [KOP09], the customized reader (see Sect. 2.2) again serves for the communication with the cards. Due to lack of contacts to measure the power consumption directly, the EM emanation of the RFID card is captured with near field probes and then digitized with a Picoscope 5204 1 GHz oscilloscope. The acquired measurements (and communication data) are

pre-processed and then evaluated on a Personal Computer (PC). Despite the secure 3DES cipher and "RFID obstacles", we are able to extract all 112-bit keys (max. 250k measurements , i.e., approx. 7 hours, per key) and hence can gain full access to any Mifare DESfire MF3ICD40 card.

We had informed the manufacturer, NXP Semiconductors, about the described attacks several years before naming the product in a publication [OP11]. In the meantime, the MF3ICD40 DESfire cards had been discontinued and replaced by a follow-up product (DESfire EV1) incorporating side-channel resistance. Meanwhile, many NFC systems have been upgraded to the new product, e.g., newly issued Opencards in Prague are now DESfire EV1.

3 Electronic Access Control

For electronic locks and access control in buildings and cars, instead of NFC devices often active remote controls are used. The security analysis of two widespread systems is summarized in the following.

3.1 KeeLoq

The KeeLoq block cipher uses a 64-bit secret key and is widely used for Remote Keyless Entry (RKE) to cars and garages and for operating alarm systems. After the algorithm became public in 2006, various mathematical weaknesses of the cipher were found [ABDM+10]. However, mathematical attacks cannot break the most widespread "Rolling-Code" KeeLoq systems in practice: 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 means of a (cryptographic) function involving a manufacturer key. Knowing the latter hence implies knowledge of all device keys in a KeeLoq system.

The extraction of a device key from a remote control with SCA requires at least 10 power measurements of a remote control [EKM+08]. The practical impact of this attack is tolerable, since it is comparable to duplicating a mechanical key, given physical access. The recovery of the manufacturer key (contained in all receivers of one manufacturer) is feasible with only one power measurement, without knowing neither plaintext nor ciphertext [KKMP09].

Knowing the manufacturer key, even a low-skilled intruder can spoof a KeeLoq receiver via the wireless link with technical equipment for less than 40 € and take over control of an RKE system, or deactivate an alarm system, without leaving physical traces. The case of KeeLoq illustrates that 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 also in electronic keys and similar wireless consumer products. The manufacturer of KeeLoq products, Microchip, agreed with the publication of our cited papers.

3.2 Simons Voss

The Simons Voss digital locking system 3060 G2 caught our attention, because it is installed in banks, universities, prisons, airports, factory sites and other locations with high demands for security and flexibility. Electronic cylinders replace their standard mechanical counterparts in the doors, while a remote control is used instead of a mechanical key. The door locks can be accessed and programmed remotely from a central PC via a wireless 868 MHz link.

After circumventing the read-out protection of the microcontrollers and reverse-engineering the contained data and program code, it became clear that in addition to a modified DES cipher a proprietary obscurity function is used as a cryptographic primitive. The first key-recovery attacks by means of SCA, or based on reading out the content of the microcontroller, evolved [OSS+14]. Since physical access to a door lock or a remote control is required, the attacks again resemble duplicating mechanical keys and may be tolerable in certain applications.

A short time after the internal functioning of the system components became clear, a devastating mathematical attack was found [SDK+13], that is clearly not tolerable: An adversary can open a door solely using the wireless link between door lock and remote control. The attack exploits (besides the bad cryptographic properties of the obscurity function) that an internal value processed by the algorithm is used as a "random number" (and thus leaked to the adversary) in the next run of the challenge-response protocol.

Eavesdropping a few (4–5) subsequent door opening attempts (and their corresponding "random numbers") allows an attacker to compute the cryptographic key of a remote control and clone it in a few seconds. For executing the attack, a valid ID of a remote control needs to be known or guessed by the adversary. In several real-world systems analyzed by us, we were able to guess a valid ID that even functions as a master key for the installation, i.e., it can open all doors of that installation. The manufacturer had been informed about the security flaws and our planned publications beforehand and meanwhile offers a firmware update, for download via the Internet, that is providing a fix for the described mathematical attack.

4 FPGAs and Bitstream Encryption

Xilinx(45–50%) and Altera(40–45%) together make up for approximiately 90% of the Field Programmable Gate Array (FPGA) market. Their products are widely used in consumer products, network routers, cars and military equipment. To protect the configuration ("bitstream") of the FPGAs that has to be loaded from an external non-volatile memory on every start-up, the market leaders offer a feature termed bitstream encryption: A designer can generate an encrypted bitstream with a secret key that is also stored in the target FPGA. A dedicated hardware on the silicon die of the FPGA then decrypts the bitstream during each start-up or reconfiguration of the FPGA. The feature enables, amongst others, to securely distribute firmware updates via insecure channels (the Internet).

After the initial successful power-analysis attacks on the 3DES implementation protecting the bitstreams of the Xilinx Virtex-2 family of FPGAs [MBKP11], similar attacks targeting the AES-256 implementation of their successors Virtex 4, Virtex 5, and the Spartan 6 evolved [MKP12]. Next, the product lines Stratix II (AES-128) Stratix III (AES-256) produced by Altera were found to have the same security vulnerabilities [MOPS13]. As in our previous publications, the manufacturers were informed about the found attacks a long time before their publication.

As a result, the vast majority of products on the market that are secured with the bitstream encryption feature can be duplicated by competitors, or secrets and IP contained in the unencrypted bitstream can be reverse-engineered. Further, scenarios like Hardware Trojans that are placed, for example, in network routers, and leak information through some covert channel, are conceivable.

5 One-Time Password Tokens

Yubikey 2 USB tokens are widely used to generate one-time passwords, e.g., for two-factor authentication instead of traditional username-password credentials. The passwords are generated by means of an AES cipher with a 128-bit secret key.

We demonstrate in [ORP13] that SCA attacks are a relevant threat for the tokens: A non-invasive side-channel analysis exploiting the EM emanations of the AES implementation requires approximately 500 EM measurements to recover the full key. Given approximately one hour of access to a Yubikey 2, an adversary can impersonate the legitimate owner and generate valid one-time passwords, even after the token has been returned. The attack leaves no physical traces on the device and can be performed using low-cost equipment.

Before publication, we notified the vendor Yubico about the found vulnerability towards SCA. Yubico acknowledged our results and has taken measures to mitigate the security issues: Tokens with an updated firmware (version 2.4) are resistant to the attacks and hence provide a significantly increased security level.

6 Conclusion

In the IoT, it is mandatory to protect privacy and security relevant information by means of cryptography. The implementation platform, i.e., the actual microcontroller, FPGA, or a similar device that stores secrets and provides the cryptographic functions, has become increasingly important for developing secure embedded systems. At the same time, the choice has become more complicated, since a large number of devices with different security features are available on the market. Besides the cryptographic strength of the employed algorithms and protocols, developers have to consider the existence and potential impact of physical attacks. The on-going research about security analyses of real-world devices provides essential know-how to the designers, e.g., for choosing respective system ingredients and parameters, as well as countermeasures. Likewise,

the manufacturers obtain feedback about necessary improvements to establish the desired security strength in the next product generations.

Acknowledgement. This work was supported in part by the German Federal Ministry of Economics and Technology (Grant 01ME12025 SecMobil).

References

ABDM+10. Aerts, W., Biham, E., De Moitié, D., De Mulder, E., Dunkelman, O., Indesteege, S., Keller, N., Preneel, B., Vandenbosch, G., Verbauwhede, I.: A Practical Attack on KeeLoq. Journal of Cryptology, 1–22 (2010), doi: 10.1007/s00145-010-9091-9

EKM+08. Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M.T.M.: On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 203–220. Springer, Heidelberg (2008)

Int01. International Organization for Standardization (ISO). ISO/IEC 14443 Parts 1–4 (2001), `http://www.iso.ch`

Int04. International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 18092 (Near Field Communication (NFCIP-1)) (2004)

KCP07. Kasper, T., Carluccio, D., Paar, C.: An Embedded System for Practical Security Analysis of Contactless Smartcards. In: Sauveron, D., Markantonakis, K., Bilas, A., Quisquater, J.-J. (eds.) WISTP 2007. LNCS, vol. 4462, pp. 150–160. Springer, Heidelberg (2007)

KKMP09. Kasper, M., Kasper, T., Moradi, A., Paar, C.: Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 403–420. Springer, Heidelberg (2009)

KOP09. Kasper, T., Oswald, D., Paar, C.: EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment. In: Youm, H.Y., Yung, M. (eds.) WISA 2009. LNCS, vol. 5932, pp. 79–93. Springer, Heidelberg (2009)

KSP10. Kasper, T., Silbermann, M., Paar, C.: All You Can Eat or Breaking a Real-World Contactless Payment System. In: Sion, R. (ed.) FC 2010. LNCS, vol. 6052, pp. 343–350. Springer, Heidelberg (2010)

KvMOP11. Kasper, T., von Maurich, I., Oswald, D., Paar, C.: Chameleon: A Versatile Emulator for Contactless Smartcards. In: Rhee, K.-H., Nyang, D. (eds.) ICISC 2010. LNCS, vol. 6829, pp. 189–206. Springer, Heidelberg (2011), `https://github.com/emsec/ChameleonMini`

MBKP11. Moradi, A., Barenghi, A., Kasper, T., Paar, C.: On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks: Extracting Keys from Xilinx Virtex-II FPGAs. In: Chen, Y., Danezis, G., Shmatikov, V. (eds.) ACM Conference on Computer and Communications Security, CCS 2011, pp. 111–124. ACM (2011)

MKP12. Moradi, A., Kasper, M., Paar, C.: Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures – An Analysis of the Xilinx Virtex-4 and Virtex-5 Bitstream Encryption Mechanism. In: Dunkelman, O. (ed.) CT-RSA 2012. LNCS, vol. 7178, pp. 1–18. Springer, Heidelberg (2012)

MOPS13. Moradi, A., Oswald, D., Paar, C., Swierczynski, P.: Side-Channel Attacks on the Bitstream Encryption Mechanism of Altera Stratix II – Facilitating Black-Box Analysis using Software Reverse-Engineering. In: ACM/SIGDA International Symposium on Field-Programmable Gate Arrays – FPGA 2013, pp. 91–100. ACM (2013)

OP11. Oswald, D., Paar, C.: Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 207–222. Springer, Heidelberg (2011)

ORP13. Oswald, D., Richter, B., Paar, C.: Side-Channel Attacks on the Yubikey 2 One-Time Password Generator. In: Stolfo, S.J., Stavrou, A., Wright, C.V. (eds.) RAID 2013. LNCS, vol. 8145, pp. 204–222. Springer, Heidelberg (2013)

OSS+14. Oswald, D., Strobel, D., Schellenberg, F., Kasper, T., Paar, C.: When Reverse-Engineering Meets Side-Channel Analysis – Digital Lockpicking in Practice. In: Lange, T., Lauter, K., Lisonek, P. (eds.) Selected Areas in Cryptography – SAC 2013. LNCS, vol. 8282, Springer, Heidelberg (2014)

SDK+13. Strobel, D., Driessen, B., Kasper, T., Leander, G., Oswald, D., Schellenberg, F., Paar, C.: Fuming Acid and Cryptanalysis: Handy Tools for Overcoming a Digital Locking and Access Control System. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 147–164. Springer, Heidelberg (2013)