Wireless Security Threats: Eavesdropping and Detecting of Active RFIDs and Remote Controls in the Wild

Timo Kasper, David Oswald, Christof Paar
Chair for Embedded Security
Horst Görtz Institute for IT Security
Ruhr-University Bochum, Germany
{Timo.Kasper,David.Oswald,Christof.Paar}@rub.de

Abstract

This paper deals with security threats concerning RFID and other wireless devices. We focus on eavesdropping and introduce a portable setup for monitoring the communication of active RFIDs in practice. We then investigate an active RFID tag operating at 433 MHz in order to determine how much its specified coverage can be extended in the context of attacks. Assuming an adversary with limited know-how and funds, we conduct all analyses solely with commercially available low-cost and easy-to-use equipment. By performing practical experiments we demonstrate that the ranges can be increased up to a factor of eight and thereby prove that this type of RFID is vulnerable to certain attacks from a distance. Our results can be applied to other wireless devices, e.g, remote controls for remote keyless entry systems.

1. Introduction

Passive Radio Frequency Identification (RFID) devices are commonly employed for access control, ticketing and identification purposes, e.g., in the form of contactless smartcards operating at a frequency of 13.56 MHz or car immobilizers operating at 125 kHz. The devices possess no own energy supply, e.g., a battery, and are solely powered by the electromagnetic (EM) field of an interrogating reader device, which implies amongst others a limited operating range — maximally in the order of some meters.

In the contrary, *active* RFIDs are usually battery-powered and achieve operating ranges in the order of tens or hundreds of meters. They often communicate at Industrial, Scientific and Medical (ISM) frequencies in the Ultra-High Frequency (UHF) range, i.e., in Europe very often at a frequency around 433 MHz, and serve for instance as remote controls for Remote Keyless Entry (RKE) systems, e.g., for opening cars (often combined with a passive transponder in the car key). Actively powered solutions are required in all situations where a high reading range or a short interrogation period is required and hence passive tags are no option, e.g., license plates of vehicles that are queried while driving past at a high speed. Furthermore, the active RFIDs are often equipped with sensors for monitoring and recording various environmental conditions, such as temperature or humidity, and provide security features, such as the capability to trigger a real-time alarm upon the detection of an intrusion by means of light or shock sensors. These 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, in order to track their route while assuring that certain environmental conditions are met.

In this contribution as our *Device Under Test (DUT)* we investigate a transponder of the lastly mentioned active type which is widely used, e.g., for tracking of goods in the supply chain and tagging vehicles, and is employed worldwide both in the commercial and military sectors. Our DUT complies to the ISO 18000-7 standard for active RFID [1], provides more than 128 kB of rewritable memory and communicates employing Frequency Shift Keying (FSK) at a frequency of 433 MHz and a bitrate of 27.8 kBit/s at a specified range of 400 ft (122 m). The energy supply is provided by a 3.6 V lithium battery that according to the data sheet lasts for 5 years when issuing two queries per day.

For estimating the real-world threat of our findings, we assume an *attacker* with limited skills and funds, e.g., an electronic hobbyist or a terrorist with some electrical engineering background. Accordingly, for all practical analyses presented in this paper we employed no special equipment or know-how but consistently opted for low-cost and easy-to-use solutions based on equipment that is commercially available to everyman. Consequently, we suppose that our results for the eavesdropping and detection ranges, as presented in Sect. 5, can be further improved by a well-funded and highly skilled adversary (or organization).

1.1. Related Work

The topic of ranges for eavesdropping on RFID communication has been widely discussed in the literature for the case of *passive* RFIDs. For example, it is well-known that the channels for the forward communication from reader to tag and the backward direction from tag to reader have an asymmetric characteristic, i.e., often the backward channel is more difficult to detect. Especially in the case of identification documents based on contactless smartcards, such as the electronic passport (ePass), eavesdropping poses a severe threat for the privacy of individuals [2] and has been thoroughly analyzed:

their active operating range (specified with 8 . . . 15 cm) can be increased up to approximately 30 cm [3], [4], while passively monitoring the communication in both directions is practically feasible from a distance of several meters [5], [6]. Recording only the forward channel is possible from a distance up to about 25 meters [7], while simulations by NXP confirm the possibility of eavesdropping from a maximum of 50 m [8].

In contrast, to our knowledge the true ranges for eavesdropping on *active* RFIDs have never been practically evaluated in the literature, despite the fact that a common interest in the topic is evident: in a Crypto 2008 paper [9], an attack on the widespread RKE system KEELOQ is presented that allows to extract the secret keys of remote controls (and consequently produce duplicates, open doors, etc.) from eavesdropping one single (encrypted) transmission. The results of practical eavesdropping on active RFIDs are comparable to KEELOQ remote controls that are operating at the same frequency range, and hence allow to assess the real security risk evolving for these and other active wireless devices. In general, evaluating the vulnerability of active RFIDs is of great importance, since the devices are employed in various security-, privacy-, and safety relevant applications, in which the system integrators are often not aware about the threats discussed in the following.

1.2. Contribution of this Paper

This paper briefly introduces security threats and attacks on wireless devices in Sect. 2. We pinpoint the relevance of eavesdropping and then evaluate the susceptibility of active RFIDs with respect to this threat. For this purpose, we introduce fundamentals about active RFIDs technology in Sect. 3. We detail on a low-cost setup for eavesdropping in Sect. 4 that is tailored to passively monitor the communication of wireless devices at a frequency of 433 MHz and can further actively query our DUT by emulating a compliant reader. Finally, in Sect. 5 we conduct practical experiments with respect to eavesdropping that result in determining a lower bound of the range for this threat.

2. Security Threats for Wireless Devices

The over-the-air communication channels used by wireless embedded devices, such as RFIDs, can be exploited by an adversary in an unwanted manner. Well-known security risks include *skimming*, i.e., the adversary unauthorizedly activates an RFID tag and communicates with it, and *eavesdropping*, i.e., she passively monitors the communication initiated by an authorized reader. Knowing the interchanged data may enable a *replay attack*, in which the previously recorded communication data is reproduced in order to pretend the presence of a genuine tag or reader. Replay attacks can be prevented by implementing cryptographic schemes, e.g., a challenge-response protocol to establish mutual authentification.

Man-In-The-Middle (MITM) attacks operate on the bit level and hence enable to circumvent most systems employing cryptographically secure authentication and strong encryption. MITM attacks on Radio Frequency (RF) devices, as described in [10] and practically realized in the context of contactless smartcards in [11] and [12], have recently also been conducted on keyless entry and start systems in modern cars [13]. In practice two adversaries, that are interconnected with a wireless link, combine their efforts: one remains in the vicinity of the victim to wirelessly access his keyfob or contactless card while the other one steals the car or carries out a payment on behalf of the victim. A countermeasure impeding MITM, called distance-bounding, has been introduced already more than a decade ago in [14] and has been proven to be practically feasible [15].

Denial-of-Service (DoS) attacks aim at rendering a wireless system out-of-service. *Jamming*, i.e., sending a disturbing signal at the frequency of the targeted system, can locally hinder the communication between legitimate devices. *Blocker tags* pretend the presence of a large amount of RFID transponders, such that the requesting device cannot handle all requests [16], [17]. Some RFID tags can be permanently disabled by means of a "kill"-password which can be obtained by an adversary [18]. *Malware* as known from Personal Computers (PCs), i.e., worms, trojan horses and computer viruses, constitutes a real-world threat also for RFIDs [19]. For example, it has been shown that a virus can be programmed that spreads via RFID tags [20]. *Sleep deprivation* aims at exhausting the energy source of an active tag by repeatedly sending requests at the maximum repetition rate.

Detecting and tracking of objects or individuals by an unauthorized party can pose a severe privacy risk [2]. A further extremely dangerous risk related to the detection of an RFID tag is triggering explosives when a wireless device is sensed: Juels et al. publicized the notion of an RFID bomb already in 2005 [21].

For practically conducting the above sketched attacks in the real world, the achievable ranges for actively communicating with the RFID transponders and passively eavesdropping on their information exchange play a highly important role. The bigger the distance from which the attack can be carried out, the more severe is the evolving threat, for example RFID tags in a warehouse can be considered secure if their maximal operating range is in the order of meters, but they become subject to possible attacks if they are feasible from several hundreds of meters, i.e., from outside the warehouse.

3. Active RFID Fundamentals

The UHF interface of the analyzed RFID system is implemented according to ISO 18000-7 [1] and hence uses a binary FSK, i.e., the frequency is increased or decreased by 50 kHz to transmit a 0 or 1, respectively, at a carrier frequency of $f_c = 433.92$ MHz. In its default state, a tag is usually in a sleep state to save power. In order to activate a tag, a reader has to send a "wake-up" signal by transmitting a constant-frequency signal at 433.92 MHz + 30 kHz for a duration of 2.5. . .2.7 ms. On receiving this signal, a tag responds with its Unique Identifier (UID) as the starting point for the further bi-directional data exchange.

The transmitted information is encoded using a Manchester code [22], i.e., the bits are encoded in the transitions of the signal, not in its level. The nominal data rate is 27.8 kBit/s,

employing a packet-oriented transmission protocol. Each such packet (sent by the reader or the tag) starts with a synchronization preamble of 1.2 ms, followed by a start bit that also encodes whether the transmission originates from a reader or from a tag. For error detection and synchronization purposes, each data byte ends with an additional stop bit, and besides, a 16-bit Cyclic Redundancy Check (CRC) is appended to each packet to ensure data integrity.

Theoretical Background of Eavesdropping. The Friis transmission equation [23] describes the relationship (in the far-field region) between the transmitted and received power, depending on the distance between two antennae and is denoted in its most basic form as:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2, \quad (1)$$

where P_r denotes the received power, P_t the transmitted power, G_t the gain of the transmitting antenna, G_r the gain of the receiving antenna, λ the wavelength and d the distance between transmitter and receiver.

4. Mobile Measurement Setup

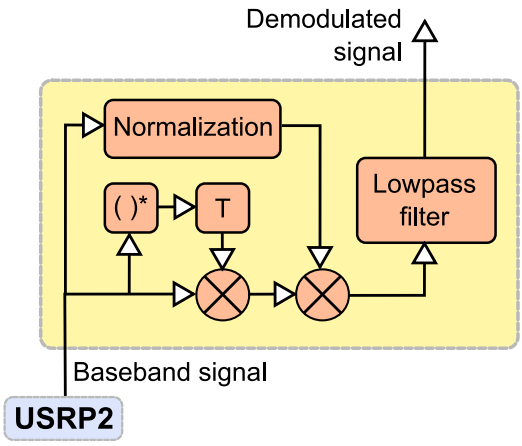
For practically evaluating the ranges for eavesdropping in a real-world scenario all required tools, readers and transponders need to be portable, in order to be transported and autonomously actuated at their destination in the wild, or to be operated from our measurement vehicle. The latter is equipped with the mandatory armamentarium, i.e., a ladder and mechanical tools to fix transponders at objects, several lead-acid batteries serving as independent energy supplies, and a 300 W DC-to-AC power converter to provide a 220 V mains supply from the 12 V DC provided by the batteries, as depicted on the right top of Fig. 1. For convenience,

Figure 1. Mobile eavesdropping equipment. Left: Yagi-Uda antenna, connected to the data acquisition unit consisting of laptop and USRP in the measurement vehicle (right bottom) ; right top: voltage converter and car battery for the power supply in the wild.

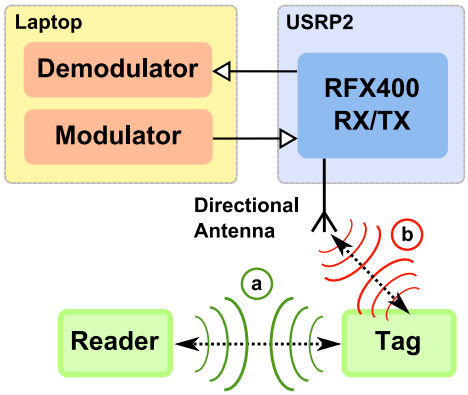
the measurement vehicle provides an adjustable antenna pole that can be manually steered from the inside to cover an eavesdropping angle of 360° at a tunable antenna elevation of 3.1 to 5 meters. The devices for the practical experiments comprise a genuine reader and genuine tags to be placed at appropriate locations in the wild, as well as a mobile data acquisition unit consisting of a directional antenna connected to a Universal Software Radio Peripheral (USRP) transceiver, which is controlled by a standard notebook, as depicted in Fig. 1. An iPhone is employed to accurately record the Global Positioning System (GPS) coordinates of the DUT and each eavesdropping location.

Directional Antenna. The employed Yagi-Uda antenna, as depicted on the left of Fig. 1, is a standard directional antenna (cost approx. 50 EUR) with a length of one meter, that is suitable for a frequency range of 430–440 MHz. It consists of an array of a dipole driven by the transceiver, a reflector and six closely coupled director elements that provide a directional gain of $G = 11$ dBi, while covering a horizontal angle of 44°.

Mobile Eavesdropping Unit. A battery-powered USRP2[1] transceiver combined with an RFX400 daughterboard serves for receiving and transmitting arbitrary UHF signals. Its integrated preamplifier is set to a gain of 30 dB throughout our experiments, corresponding to a transmission power of 200 mW.



(a) Demodulating UHF signals



(b) Measurement principle

Figure 2. Signal flow graph for demodulating received UHF signals and principle of passive eavesdropping ⓐ and active communication ⓑ.

1. www.ettus.com

The USRP is controlled from a GNURadio[2] software running on the notebook, that is programmed to enable communication according to Sect. 3. Our developed software comprises a receiver for the passive detection and eavesdropping of the communication, and can further emulate a genuine reader. Figure 2a shows the structure of the employed quadrature amplitude demodulation, where $()^*$ denotes complex conjugation, ⓧ a multiplier and $\mathtt{T}$ a delay unit. For actively sniffing transponders, a mode repeatedly transmitting a wake-up command and reading the response has been implemented. Figure 2b outlines our measurement setup, that is capable to both passively monitor the communication of the DUT with a genuine reader (ⓐ) and to actively initiate the communication in order to detect and interrogate a tag when no genuine reader is present (ⓑ).

5. Practical Experiments

Using the equipment and techniques described in Sect. 4, this section details on two extensive measurement campaigns carried out at a suitable location in Bonn, Germany, nearby the river Rhine. One campaign aims at determining the practical range in the context of a passive attacker, e.g., relevant for eavesdropping, detection and tracking of tags, while the second campaign targets the range for active communication, as required for active sniffing in order to detect a tag, perform a DoS attack or inject malware into an active RFID system. For MITM attacks, the ranges of both approaches have to be taken into account.

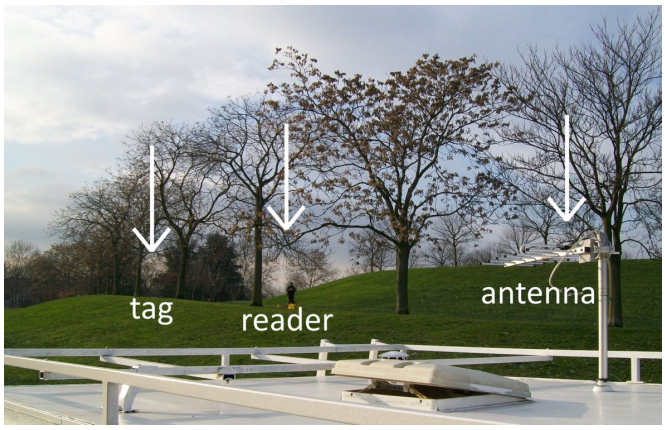
5.1. Passive Attacker

For analyzing the eavesdropping range we attached the DUT to the branch of a nearby tree and placed a genuine reader approx. 15 meters apart from it, as illustrated in Fig. 3a. The latter is programmed to repeatedly interrogate the DUT during our absence. We then moved away from the DUT in the measurement vehicle and recorded the requests of the reader and the answers of the tag, while increasing the distance in several steps. The exact locations of the measurement positions and their corresponding distances are depicted in Fig. 3b at hand of a satellite map by Google Earth. Reaching the end of the areal at a distance of 964 meters from the DUT we were still able to detect the communication with our mobile measurement setup. An exemplary response of the active tag, as acquired during our experiments, is illustrated in Fig. 4.

5.2. Active Attacker

Similarly, we tested the range for active communication by sending wake-up commands and recording the received answers of the tag. This time, as illustrated in Fig. 5a, the measurement vehicle remains at a fixed location, while the tag, being carried by a research assistant, moves away. The GPS coordinates and distances between tag and antenna are shown in Fig. 5b.

2. www.gnuradio.org



(a) Side View

(b) Top View

Figure 3. Setup and GPS coordinates for passive eavesdropping and detection

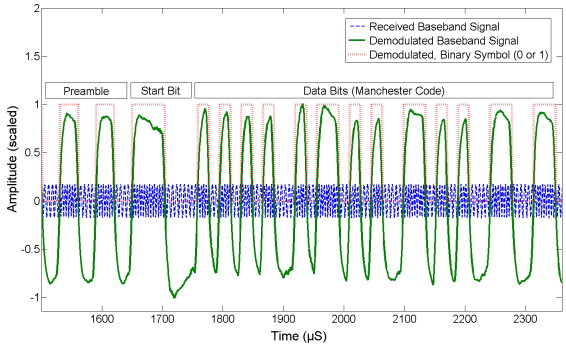
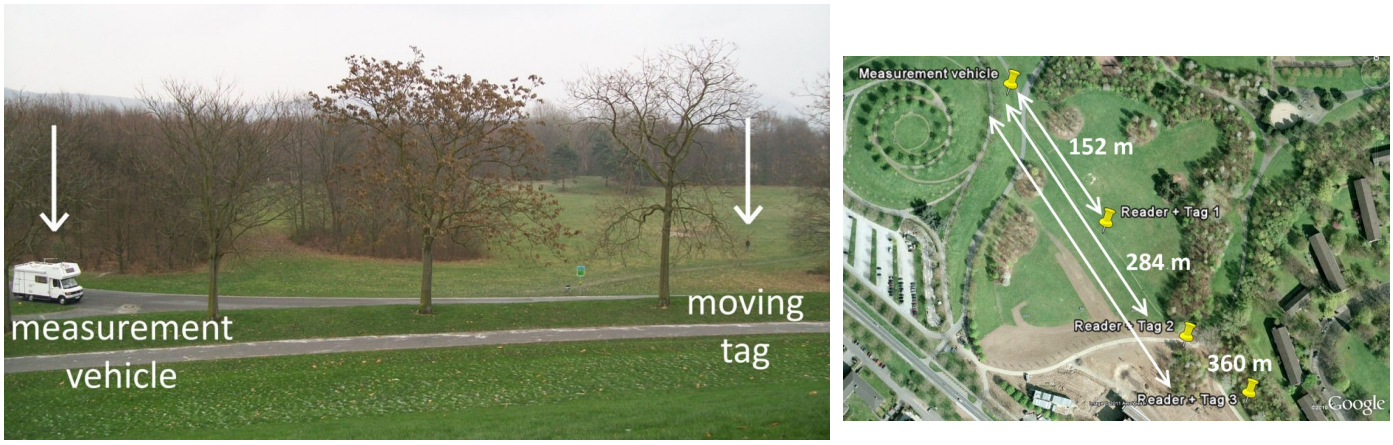


Figure 4. Received UHF signal: baseband (blue, dashed), demodulated (green, solid), converted to binary symbols (red, horizontally dashed)



(a) Side View

(b) Top View

Figure 5. Setup and GPS coordinates for actively sniffing and detection

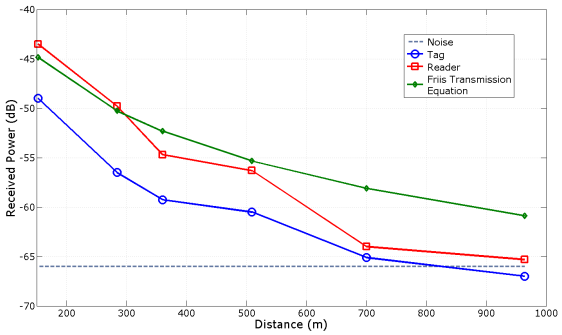
5.3. Resulting Ranges

The results for the feasible reading ranges for the case of a passive attacker and an active attacker are illustrated in Fig. 6a and Fig.6b, respectively. Concerning the passive approach, the ranges achieved for intercepting the communication from reader to tag and vice versa are similar, while the reader's signal is slightly easier to detect. For reference, Fig. 6a includes the theoretical results obtained when evaluating the Friis Equation (Eq. 1, Sect. 3) for the antennae used in our experiments.

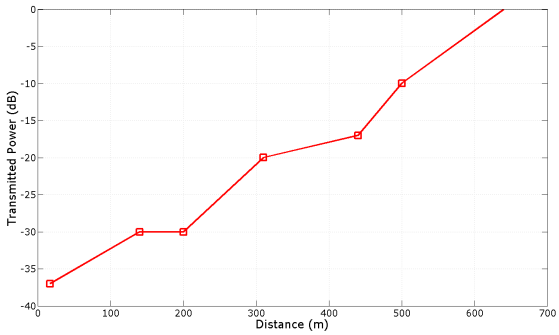
Eavesdropping on the communication in both directions is possible from up to 500 meters, where the eavesdropping is assessed to be successful in case that each received data packet is correctly decoded (evaluated at hand of the correct checksum). Detecting the communication was successful from a distance of approx. 1000 meters. The measured range for the active approach, transmitting with a power of 200 mW, is also in the order of 500 meters. Note that according to our experiments the range for emulating an active tag or a remote control at 433 MHz — which is straightforward with our low-cost setup — corresponds to the same range as for the active approach.

6. Conclusion

We sketched the relevant security threats in the context of RFID and other wireless devices to pinpoint that the practically achievable ranges for the wireless interface strongly influence many relevant attacks, to name sniffing, cloning, MITM attacks, DoS, RFID malware, as well as tracking and detection of the devices. We introduced our simple low-cost setup for transmitting and receiving information in the UHF band, assuming an unskilled adversary, and illustrated the practical attack methods. We then conducted the first real-world analysis of the ranges that can be achieved for an active RFID tag by actively interrogating it and by passively monitoring genuine communication. According to our experimental results, the feasible ranges for eavesdropping (or actively



(a) Received power



(b) Active Communication

Figure 6. Received power for eavesdropping on $T \rightarrow R$ (blue, circle) and $R \rightarrow T$ (red, square) and minimum required transmission power to activate and communicate with a tag, as a function of the distance.

sniffing) a successful communication and passive detection are increased by a factor of 4 or 8, respectively, compared to the specified operating range (122 m) of the tested active transponder. Note that the methods and equipment employed correspond to an unskilled attacker and the ranges hence have to be regarded as a lower boundary which can be extended

by a professional, well-funded adversary.

Implications. Our findings imply that the attacks related to the mentioned security risks are feasible in a practical scenario and pose a significant threat for wireless devices actively operating at 433 MHz. The devices can be easily cloned and malware could be injected from a distance of 500 meters, MITM attacks are feasible from afar, and the detection of the technology, e.g., to trigger an alarm, is feasible from up to one kilometer. The possible scenarios are manifold, e.g., performing an unauthorized inventory of the warehouse of a competitor, or reprogramming tags attached to containers to change their intended destination, falsify the information recorded by the sensors of the tag and many others.

Regarding sleep deprivation attacks, for a conservative estimation we assume 500 bits to be sent for one interrogation (compare with the 128-bit length of the UID) at a bitrate of 20,000 bit/s (compare with the specified bitrate of 27.8 kBit/s), corresponding to a speed of 40 interrogations per second. Taking a short recovery time into account, and being extremely conservative, let's assume one interrogation per second in practice. With respect to the specified lifetime of the tag's battery, i.e., 5 years at two queries per day, the resulting $5 \times 2 \times 365 = 3560$ queries take about 3560 seconds — an adversary may hence succeed to empty the battery with a sleep deprivation attack in less than one hour, from a distance of 500 meters.

The observed ranges also put other eavesdropping attacks, such as cloning KEELOQ remote controls, into a new light. Active devices operating at different frequencies are very likely as vulnerable as the DUT in this paper. Accordingly, the active technology should be used with extra care and in the case of security or safety critical environments other protection measures have to be established, e.g., fences at an appropriate distance and guarded transports of goods.

References

[1] ISO/IEC 18000-7, "Radio frequency identification for item management – Part 7: Parameters for active air interface communications at 433 MHz."

[2] Y. Liu, T. Kasper, K. Lemke-Rust, and C. Paar, "E-Passport: Cracking Basic Access Control Keys," in *Proc. of OTM'07, Part II*, ser. LNCS, vol. 4804. Springer, 2007, pp. 1531–1547.

[3] T. Finke and H. Kelter, "Radio Frequency Identification - Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems."

[4] I. Kirschenbaum and A. Wool, "How to Build a Low-Cost, Extended-Range RFID Skimmer," in *USENIX Security Symposium*. USENIX Association, 2006.

[5] G. Hancke, "Eavesdropping Attacks on High-Frequency RFID Tokens," in *Workshop on RFID Security*, 2008.

[6] G. P. Hancke, "Practical Attacks on Proximity Identification Systems (Short Paper)," in *Proc. of SP'06*. IEEE Computer Society, 2006, pp. 328–333.

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

[8] NXP, "AN200701: ISO/IEC 14443 Eavesdropping and Activation Distance," Tech. Rep., 2007.

[9] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani, "On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme." in *CRYPTO 2008*, ser. LNCS, vol. 5157. Springer, 2008, pp. 203–220.

[10] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard systems," Cryptology ePrint Archive, Report 2005/052, 2005, http://eprint.iacr.org.

[11] G. Hancke, "A practical relay attack on ISO 14443 proximity cards," http://www.cl.cam.ac.uk/~gh275/relay.pdf, 2005.

[12] T. Kasper, D. Carluccio, and C. Paar, "An Embedded System for Practical Security Analysis of Contactless Smartcards," in *WISTP*, ser. LNCS, vol. 4462. Springer, 2007, pp. 150–160.

[13] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," Cryptology ePrint Archive, Report 2010/332, 2010, http://eprint.iacr.org/.

[14] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," in *Proceedings of IEEE/Create-Net SecureComm 2005*. IEEE Computer Society Press, 2005, pp. 67–73.

[15] K. B. Rasmussen and S. Capkun, "Realization of RF Distance Bounding," in *19th USENIX Security Symposium*. USENIX Association, 2010, pp. 389–402, http://www.usenix.org/events/sec10/tech/full_papers/Rasmussen.pdf.

[16] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, 2003, pp. 103–111.

[17] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management," in *Information Security and Privacy, 10th Australasian Conference (ACISP)*, ser. Lecture Notes in Computer Science, vol. 3574, 2005, pp. 184–194.

[18] Y. Oren and A. Shamir, "Remote Password Extraction from RFID Tags," *IEEE Transactions on Computers*, vol. 56, no. 9, pp. 1292–1296, 2007, http://iss.oy.ne.ro/RemotePowerAnalysisOfRFIDTags.

[19] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "RFID Malware: Truth vs. Myth," *IEEE Security and Privacy*, vol. 4, pp. 70–72, 2006.

[20] ——, "Is Your Cat Infected with a Computer Virus?" in *Conference on Pervasive Computing and Communications (PerCom)*. IEEE Computer Society, 2006, pp. 169–179.

[21] A. Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-Passports," in *Proc. of SecureComm'05*. IEEE Computer Society, September 2005, pp. 74–88.

[22] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. John Wiley and Sons, 2003.

[23] T. H. Friis, "A Note on a Simple Transmission Formula," in *Proceedings of the IRE*, no. 34, 1946.