Eavesdropping Attacks on High-Frequency RFID Tokens

G.P. Hancke

Smart Card Centre, Information Security Group
Royal Holloway, University of London
Egham TW20 0EX, UK
ghancke@ieee.org

Abstract. RFID systems often use near-field magnetic coupling to implement communication channels. The advertised operational range of these channels is less than 10 cm and therefore several implemented systems assume that the communication channel is location limited and therefore relatively secure. Nevertheless, there have been repeated questions raised about the vulnerability of these near-field systems against eavesdropping and skimming attacks. In this paper I revisit the topic of RFID eavesdropping attacks, surveying previous work and explaining why the feasibility of practical attacks is still a relevant and novel research topic. I present a brief overview of the radio characteristics for popular HF RFID standards and present some practical results for eavesdropping experiments against tokens adhering to the ISO 14443 and ISO 15693 standards. Finally, I discuss how an attacker could construct a low-cost eavesdropping device using easy to obtain parts and reference designs.

Keywords: Eavesdropping, RFID, contactless, near-field communication

1 Introduction

High-frequency RFID tokens, using near-field channels, are used to store valuable information in cashless payment systems and even travel documents. No physical contact needs to be made with the reader, which simplifies operation and increases overall transaction speeds. A growing security concern with RFID devices is the possible release of the user's personal information, or location, to unauthorized parties. For example, some consumer groups have rallied against the 'big brother' potential of RFID technology [31]. As RFID tokens are also used for transactions of increasing value, they could become the target of lone opportunistic attackers, who, if able to gain access to the information on the RFID token, might be able to engage in the act of 'digital pick-pocketing' while just standing next to the victim. The two main attacks usually considered are skimming and eavesdropping.

Eavesdropping attacks are a well known risk for RFID devices and there are several claims about the possibility of these attacks on RFID tokens, for example [32]. The distances at which these attacks are possible are often debated and used as an indication of RFID security, for example [27], so this is an important factor when considering the threat model for RFID devices. Despite this interest, few publications provide details about possible experimental setup or practical results. In this paper I discuss the implementation of eavesdropping attacks on HF RFID and present some practical results for eavesdropping on systems using the ISO 14443A/B and ISO 15693 standards. In each case I provide a detailed explanation of the experimental method and description of the setup. My main contribution is to provide

[1] Proceedings of the 4th Workshop on RFID Security (RFIDsec'08), pp 100–113, July 2008.

a reference experimental setup for RFID eavesdropping to provide a better understanding of the attack's physical constraints as opposed to theoretical simulation. This would hopefully allow system designers to comprehend the eavesdropping threat in order to select appropriate technologies and countermeasures. Finally, I also discuss how an attacker with limited resources could construct and eavesdropping receiver.

2 Eavesdropping scenarios

Eavesdropping normally occurs when the attacker intercepts communication between an RFID token and an authorized reader. The attacker does not need to power or communicate with the token, so he is able to execute the attack from a greater distance than is possible for skimming. He is, however, limited in terms of location and time window, since he has to be in the vicinity of an authorized reader when a transaction that he is interested in, is conducted. The attacker needs to capture the transmitted signals using suitable RF equipment before recovering and storing the data of interest. The degree of success that the attacker will achieve depends on the resources available to him. An attacker with expensive, specialized RF measurement equipment will almost certainly be able to eavesdrop from further away than an attacker with a cheap, home-made system. The attack is still a viable threat either way. An opportunistic attacker could possibly recover the travel card details of the person standing in front of him at an entrance gate if he had a small, portable system that could eavesdrop at 50 cm. Alternatively, if the attacker is able to successfully eavesdrop the communication from 10 m he could sit in a vehicle outside his local corner store and record the payment transactions conducted inside.

In the HF RFID standards the communication schemes used for reader-to-token (forward channel) and token-to-reader (backward channel) are different. As a result the distances at which an attacker can recover the data sent on the forward and backward channels differ. There are three distances to consider for this attack:

- The distance at which an attacker can detect a transaction, i.e. he can see the forward channel but cannot reliably recover the actual data.
- The distance at which an attacker can reliably recover the data sent on the forward channel.
- The distance at which an attacker can reliably recover the data sent on the backward channel.

Near-field communication generally uses different modulation schemes for the forward and the backward channel. In practice, this means that the eavesdropping ranges for each of these channels are different. I therefore define D_{EF} as the distance at which the forward channel can be observed and D_{EB} as the distance at which the backward channel can be observed. The data transmitted depends on the specific application, but the attacker is typically more interested in the backward channel because this contains data contained in the token, rather than generic instructions sent by the reader. The exceptions are when an attacker simply wishes to determine whether a transaction took place, in which case he only needs to recover the channel with the greatest eavesdropping distance, or when information on the weaker backward channel is echoed on the stronger forward channel. For the purpose of my work I assume an eavesdropping attack to be successful at a certain distance when both the forward and backward channels can be observed at this distance.

2.1 Related work

Eavesdropping attacks are not new and are mentioned regularly in the literature. Recent reports by the National Institute of Standards and Technology (NIST) [22], the Department of Homeland Security (DHS) [6] and the German Federal Office for Information Security (BSI) [3], along with academic surveys, e.g. [16], all mention scenarios for eavesdropping attacks in the RFID environment. These reports, however, do not show practical results or fail to clarify the experimental setup if they do.

Different scenarios exist for eavesdropping attacks and therefore the experimental setup should be known in order for published results to be useful. In earlier reports terms used to describe the attacks were also confusing. A report on 'Port of Entry' tests done in 2004 [7] states that signals from e-passport systems could be 'detected' at 20 m. The report does not explain whether this implies that the attacker could detect that a transaction occurred, or whether he could recover the actual data. The test also covered a number of different systems and no details were given about which system yielded the result. There were also press reports that NIST eavesdropped the RFIDs to be used in USA passports from as far away as 9 m [37]. Reports, however, often used the term 'read', which implied a skimming attack, while they were actually describing eavesdropping. There are also cases where reports do not state clearly which type of token they were referring to when describing attack distances. RFID is a collective term for several systems and in reality refers to devices adhering to a number of different standards. An HF token used for a contactless smart card is not the same as a UHF token used in logistics. Therefore, if somebody can read a razor's tag from 1 m it cannot be assumed that the same is true for an e-passport. It is therefore important to clearly state the type of RFID system when describing these attacks. Yet the American Civil Liberties Union (ACLU) demo, where a 'passport' was read from 1 m, used 'similar' RFID technology and not an ISO 14443 token as used in a real e-passport [27].

The first academic short paper discussing practical attacks on HF RFID devices was officially published in early 2006 [10]. Another work-in-progress report was released by researchers at the BSI, where they demonstrated eavesdropping at a distance of 2 m [8] on an ISO 14443A card. Riscure, a Dutch security company, later claimed that it was possible to eavesdrop the backward communication at a distance of 5 m, and the forward channel at a distance of 25 m [32]. They have, however, not actually implemented the attack. At the end of 2006 NIST published a report [9], which was reported in [22], to show that ISO 14443 tokens could be eavesdropped at 15 m. I have only recently obtained a copy of this document, the content of which is discussed together with my own results in Section 5. Other industrial studies are often referenced in literature, e.g. NXP white paper [36] cited in document by Eurosmart [30], but then unavailable as public documentation. My work tries to build on the early work-in-progress papers [8, 10] by formalising the experimental process and expanding the experimental results to include ISO 14443B and ISO 15693 tokens.

2.2 Significance

The recovery of useful data by eavesdropping can be prevented by encrypting the transmitted data with a suitable algorithm. Some HF RFID tokens are basically contactless smart cards, which can easily cope with implementing application layer security. So why are these attacks still important? In earlier systems near-field communication was seen as secure because the specified operational range was seen to be limited and as a result several weak security measures were implemented. This section briefly discusses some security sensitive RFID applications and their perceived weaknesses soon after deployment.

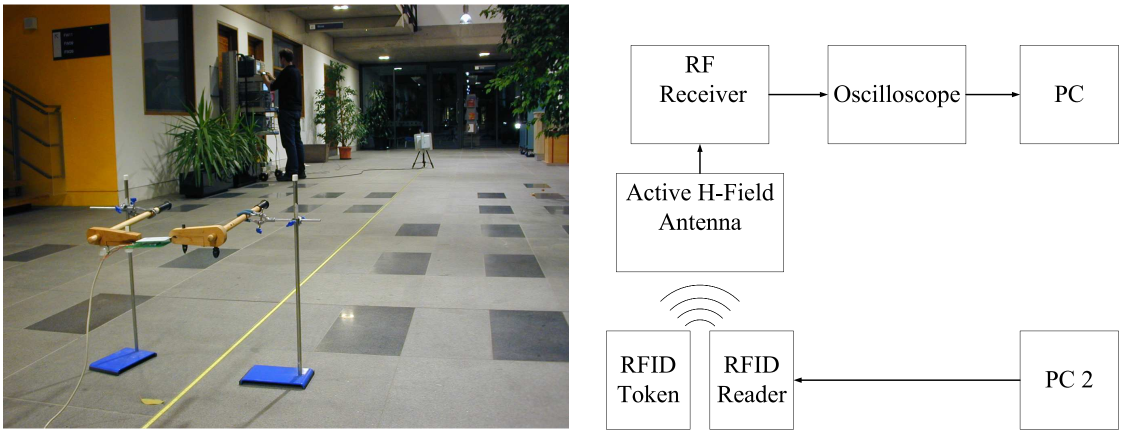
Credit cards: New contactless payment systems, of which the majority adhere to ISO 14443A, are in widespread use today. RFID credit cards have, however, been used in the USA since 2003, where these are also implemented using the ISO 14443B communication standard. Not enough information is currently available to comment on the new contactless payment systems, but a study has shown there to be a number of vulnerabilities in the first generation of USA credit cards [11]. User and banking information were often sent in plaintext between the reader and the RFID-enabled cards. An attacker could also retrieve the data by implementing a skimming attack and the information transmitted on the RF channel was allegedly sufficient to imitate a valid card.

e-Passports: By 26 October 2006 the USA required that 27 countries issue their citizens with e-passports in order to still qualify under the Visa Waiver Program. E-passports adhere to operational specifications as defined by the International Civil Aviation Organisation (ICAO) [12] and use the ISO 14443 standard. ICAO allows for optional security protocols, such as Basic Access Control (BAC), that provides both authentication and encryption services. BAC derives a key from the passport serial number, expiry date and the user's birthday, read off the OCR strip inside the passport. The idea is that anyone presented with the passport can read the OCR data, derive the key and retrieve the data off the RFID token inside. Security problems of this scheme have been pointed out [17], especially with the effective size of the key. Theoretically the data can be used to generate a key with an effective length of at least 50 bits [19]. Predictability in the data could however decrease the effective key length to 35 [32] or even 27 [17] bits, which makes a brute force key search attack feasible. This implies that an attacker could eavesdrop communication between a passport and reader and try to decrypt it at a later stage exploiting this weakness in the key. An overview of the latest issues regarding e-passports is presented in [2].

Travel and Access Control Tokens: HF RFID tokens are also used in a number of travel and access control systems. Recently, the proprietary Crypto1 cryptographic algorithm used in NXP's Mifare Classic product range was reverse engineered and published [25]. Further analysis of this cipher revealed cryptographic vulnerabilities that could be exploited to recover key material in a matter of minutes [5]. An attacker wishing to execute such attacks, however, might first need to reliably eavesdrop transactions between the card and the reader.

3 Experimental setup

I set up a simple eavesdropping attack as shown in Figure 1. The reader and the token were placed in clamps and the antenna positioned at the same height on a tripod so that all three loops were in the same horizontal plane. The antenna, which was connected to the RF receiver, was kept stationary while the reader and token were moved further away. Data signals from the receiver were captured using an oscilloscope and read into Matlab where further DSP functions were performed to recover the data. It should be noted that a number of factors, as discussed later in this section, affect the results of an eavesdropping attack. As a result this work is not about establishing a maximum eavesdropping distance but rather about



(a) Observing and capturing communication (b) Experimental setup

Fig. 1. Setup for the eavesdropping experiment

practically implementing a proof-of-concept attack using a documented method that can be re-created by other researchers to obtain comparable results for their specific environment.

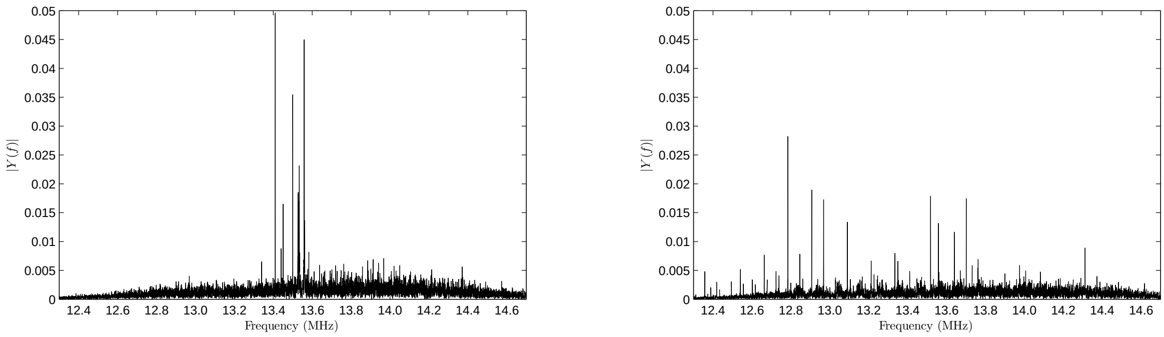
3.1 Equipment

There are commerical RF receivers available that can be used to demonstrate the eavesdropping attack. I used the R-1250 Wide Range Receiver and the R-1150-10A Portable Antenna Kit, both manufactured by Dynamic Sciences. The R-1250 is a superheterodyne receiver operating from 100 Hz to 1 GHz with 21 selectable bandwidths, increasing in steps of 1-2-5 from 50 Hz to 200 MHz, centered around 200 kHz or 30 MHz IF frequencies. The receiver allows the user to adjust the RF and pre-detection gain over 50 dB and 30 dB respectively. The user can then choose whether to use the AM, FM or IF output available. Detailed information about the R-1250 receiver, including calibration data for the specific receiver used in the attack, can be found in [20, pp 23–33]. The antenna kit includes a set of H-field ferrite core antennas for field-strength measurements in the 100 Hz to 30 MHz range. Looking at the H-field is of particular interest when taking into account the dominance of the H-field in the near-field of loop antennas.

Currently there are three popular standards for passive near-field devices operating at the frequency of 13.56 MHz: ISO 14443A, ISO 14443B [13] and ISO 15693 [14]. Since each standard has a different communication scheme it would not suffice to make claims about eavesdropping HF devices without investigating all the standards.

For the eavesdropping experiment I used the ACG Multi-ISO RFID Reader (Antenna dimension: 9 cm $\times$ 6 cm). I then used the following tokens: NXP Mifare Classic [24] for ISO 14443A, contactless payment card for ISO 14443B and NXP I-Code [23] for ISO 15693. I would like to point out that I used these products because they were good examples of different HF systems implemented today using the three main HF RFID standards. I do not wish to imply that any of these products are more at risk of eavesdropping than another comparable product.

3.2 Environment



(a) Main entrance hall

(b) Hardware lab corridor

Fig. 2. Comparative frequency-domain representations of background noise in two locations (RF Receiver: f_c=13.56 MHz, BW = 2 MHz)

It is expected that the magnitude of the H-field will decrease rapidly in the near-field, d$\leq \lambda_{f_c} \cdot \frac{1}{2\pi} \approx 3.5$ m, proportionally to $\frac{1}{d^3}$. At larger distances the decrease in the H-field will be proportional to $\frac{1}{d^2}$. The eavesdropper requires a favourable signal-to-noise ratio (SNR) to recover the data. The nature of the background noise will therefore affect the eavesdropping distance. This experiment was not performed in an empty, shielded chamber but in a laboratory that houses equipment that might emit RF signals, or contain metal, which could interfere with the magnetic field originating from the reader. My experiment was conducted in the University of Cambridge's Computer Laboratory. Figure 2 shows the frequency characteristics of the background noise for two possible eavesdropping locations: The main entrance hallway Laboratory and the corridor outside the security group's hardware laboratory. The average power of the input signal to the receiver in both cases is approximately -86.5 dBm.

Apart from the background noise there are several other practical factors influencing the eavesdropping environment. The antenna size and transmitted power depend on the specific reader used in a system. At the same time the coupling between the token and reader also influences the eavesdropping distance as it affects the carrier amplitude and the modulation index of the backward channel. These variations are not easy to quantify since any loop antenna or oscilloscope probe used to measure these values will also influence the system. Similarly, the orientation and the proximity of the card to the reader can also effect the eavesdropping range [9].

4 Method

The main goal of my experiment was to show that eavesdropping on HF RFID devices are possible at non-trivial distances. As mentioned already there are multiple environmental variables to consider. Since it was not feasible to try all possible variations I limited my experiment to a single reader and three tokens adhering to different operating standards. Secondary goals were to determine to what extent the different modulation schemes influenced the eavesdropping range and to investigate whether data could be reliably recovered from a recording with a low SNR. The experiment was repeated in two different locations as discussed in the previous section.

4.1 Reference data

The first step of the eavesdropping experiment was to generate a set of reference data for later comparison to the recovered data, and to identify the frequency bands containing the data I wanted to eavesdrop. To generate reference data I required a transaction where the data transmitted on the forward and backward channel was repeatable. The standards in question all have a command instructing the token to return a unique identifier, which was ideal as the data always stayed the same. I recorded the signal at the antenna of the reader and demodulated it to obtain the reference data. I then computed the frequency spectrum for the forward and backward channels using the Fast Fourier Transform (FFT) to confirm my theoretical estimation of the frequency bands that are of interest.

ISO 14443A: The reader transmits 106 kbit/s Modified Miller encoded data using 3 µs pulses. The forward channel data should therefore be in the first 330 kHz of the spectrum. The token transmits 106 kbit/s Manchester encoded data, which is ASK modulated onto a 847 kHz subcarrier. The backward channel should be in a 424 kHz band centered around 847 kHz. The forward channel is amplitude modulated onto the 13.56 MHz carrier with a modulation index of 100%, while the backward channel has a modulation index of 8–12%.

ISO 14443B: The reader transmits 106 kbit/s NRZ encoded data. The forward channel data should therefore be in the first 106 kHz of the spectrum. The token transmits 106 kbit/s NRZ encoded data, which is BPSK modulated onto a 847 kHz subcarrier. The backward channel should be in a 212 kHz band centered around 847 kHz. The forward channel is amplitude modulated onto the 13.56 MHz carrier with a modulation index of 10%, while the backward channel has a modulation index of 8–12%.

ISO 15693: The reader uses a ‘1 of 4’ PPM code with a 9.44 µs pulse to transmit 26.48 kbit/s data. The forward channel data should therefore be in the first 106 kHz of the spectrum. The token transmits 26.48 kbit/s NRZ encoded data, which is ASK modulated onto a 423 kHz subcarrier. The backward channel should be in the 53 kHz band centered around 423 kHz. The forward channel is amplitude modulated onto the 13.56 MHz carrier with a modulation index of 10%, while the backward channel has a modulation index of 8–12%.

4.2 Capturing and calibration

The second step was to capture the signals with the RF receiver and record them on the oscilloscope. In the experiments described in [10] the oscilloscope was triggered on the serial communication between the host PC and the reader. I decided to change this method as it was not an accurate reflection of an attacker’s actions. There was also a possibility that the additional cables connected to the reader could aid signals of interest to radiate, thereby providing an inaccurate result. Instead I captured the 30 MHz IF output of the RF receiver for a duration of 320 ms at a sampling frequency of 100 MS/s, while the reader was continuously querying the token's identifier. For each eavesdropping scenario I made two captures, the first with the receiver's center frequency and bandwidth set to 13.56 MHz and 2 MHz respectively and the second with the center frequency set to the applicable sideband, 14.4 MHz and 13.98 MHz, with bandwidths of 500 kHz and 200 kHz respectively.

The RF gain of the receiver is adjusted by turning a knob, which does not provide an accurate indication of the actual gain introduced. The relative gain of the receiver was therefore measured before each sequence capture. This was done by providing a reference signal, a center-frequency sine wave, as input to the receiver. Its power in dBm was then adjusted until the receiver's output corresponded to a chosen value on the oscilloscope: 224 mV root-mean-square for the 30 MHz IF output signal, which is approximately 0 dBm. This gain value can then be used to determine the power of the corresponding input from the antenna to the receiver.

4.3 Data recovery

The final step is to recover the data from the recorded signal. The SNR of the data decreases with distance and eventually the data can no longer be verified visually, or recovered with a simple threshold function such as a comparator with hysteresis. This does not mean that the data is lost, but that recovery requires further processing to limit the effect of the noise. A common way to reduce the effect of noise is to average several recordings of the same signal. I do not consider this option, because the attacker does not have multiple recordings as the transaction is run only once. A number of receivers optimized to recover signals corrupted by Additive White Gaussian Noise (AWGN) have been proposed, such as the correlation receiver [29, pp 233–244]. The correlation receiver uses N correlators, which projects the received signal $r(t)$ onto N base functions $f_k(t)$.

$$y_k = \int_0^T r(t) f_k(t) d_t, \ k = 1, 2, \ldots, N$$

It should be noted that if the base function is rectangular the correlator becomes an integrator.

$$y_k = \frac{1}{\sqrt{T}} \int_0^T r(t) d_t,$$

I used additional pre-filtering and a correlation receiver to recover data from the stored noisy signal. For each of the standards' forward and backward channels $N = 1$ and the base function is rectangular. The only important parameter is T, which was assigned the following values:

- ISO 14443A: Forward channel $T = 3$ µs, backward channel $T = \frac{1}{212 \text{ kHz}} = 4.72$ µs.
- ISO 14443B: Forward channel $T = \frac{1}{106 \text{ kHz}} = 9.44$ µs, backward channel $T = \frac{1}{106 \text{ kHz}} =$ 9.44 µs.
- ISO 15693: Forward channel $T = 9.44$ µs, backward channel $T = \frac{1}{52.96 \text{ kHz}} = 18.88$ µs.

An example for recovering the data on the backward channel for ISO 14443A is shown in Figure 3. The process is as follows: (a) is the noisy signal, (b) is the data after it has

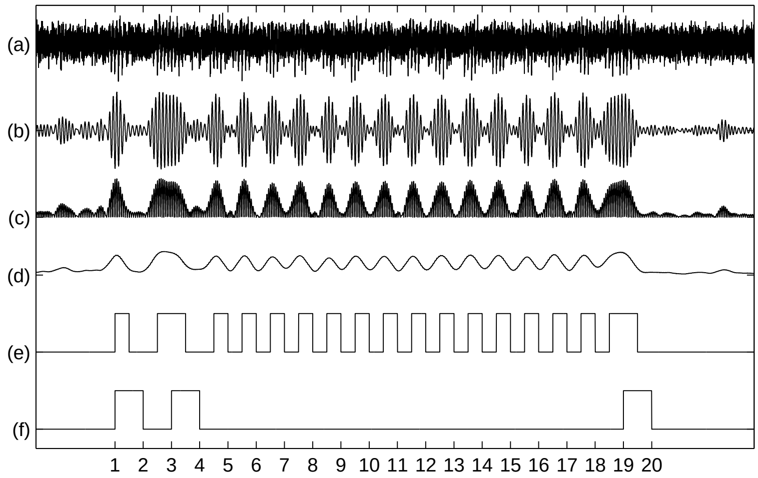


Fig. 3. Recovering the data from a noisy signal

been filtered using Finite Impulse Response (FIR) filters. The next step is to demodulate the sub-carrier. For ASK I rectified the signal shown in (c) before correlating it with the base function. (d) is the correlator output, which is then sampled to obtain the Manchester encoded data (e). The Manchester data is decoded to NRZ and compared to the reference data. The ISO standards define a strict bit-period grid, relative to the last bit sent by the reader, in which the token's response must be sent. The sampling times can therefore be derived from the forward channel data. Alternatively, a clock recovery scheme as described in [20, pp 125] can be implemented. The attacker can use known data, e.g. ISO 14443A *ATQA* and *SAK* responses, to optimize his sampling thresholds, etc.

5 Results

Before presenting my results I first discuss the details of the eavesdropping test described in [9]. This test uses a NXP Pegoda ISO 14443A reader and seven different ISO 14443A tokens from 4 manufacturers. The authors use a matched loop antenna and a 'receiver system' (unspecified whether commercial equipment or custom build) in addition to an oscilloscope and a protocol analyser to capture a token's ID. A high level functional diagram of the receiver is provided but no details are given about the filters, amplifiers and IF sections shown. An eavesdropping attempt is considered successful when the receiver's output has a SNR greater than 6 dB, which is the level needed by the protocol analyser to obtain the correct ID. The experiment is performed with two different antenna setups: All three loops centered around the same horizontal axis, which resulted in an eavesdropping distances of 5–6.5 m, and all three loops in the same horizontal plane, the same as my setup, which resulted in eavesdropping distances of 8–15 m. The fact that seven tokens, adhering to the same standard and communicating with the same reader, yield different results is a good example of how eavesdropping distances vary depending on the specific system components.

My results are shown in Table 1. Even with additional signal processing I did not manage to achieve the distances in [9], although my results for ISO 14443 A tokens are similar to those presented in [8]. There are, however, some interesting conclusions. The forward channel of the ISO 14443 A and ISO 15693 communication can be eavesdropped at a much greater distance than the backward channel, but for ISO 14443 B D_{EB} is greater than D_{EF}. In addition, it is once again shown that results can vary for different locations since the ISO 14443B forward channel and ISO 14443 A backward channel could be recovered in one location, but not the other. In my environment I only achieved a SNA of 6 dB at a distance of approximately 1 m.

	ISO 14443A	ISO 14443B	ISO 15693
Entrance hall			
1 m	FB	FB	FB
3 m	Fx	xB	Fx
5 m	Fx	xx	Fx
10 m[1]	Fx	xx	Fx
Lab corridor			
3 m	FB	FB	Fx
4 m	Fx	xB	Fx

Table 1. Eavesdropping results: F – Forward channel recovered, B – Backward channel recovered.

6 Eavesdropping attacks in the real world

An attacker can execute an eavesdropping attack if he acquired a suitable antenna, an RF receiver and a method to sample and record the data. Even though I illustrated the eavesdropping attack using commercial RF equipment I also want to point out that these attacks can work outside 'laboratory conditions' with cheap and portable hardware.

6.1 Receiver

The RF receiver converts the modulated HF carrier to a chosen IF after which the signal is filtered to isolate the frequency components that are of interest. The use of RF mixers is well documented, e.g. [28], and detailed reference designs for receivers are publicly available, e.g. [26]. As a result, it is feasible to design and construct an RF receiver that could be used to observe both the forward and backward communication of an ISO 14443 HF RFID system for less than £50. The receiver mixes the 14.40 MHz upper sideband down to an IF of 10.7 MHz before using a 500 kHz band-pass filter to recover the sideband data and attenuate the strong carrier. The filter also passes some higher harmonics of the forward channel data. The forward channel pulse shapes are distorted although they are still in the correct position, which is enough information to recover the data in this case. My self-constructed receiver did not achieve the same results as the commercial RF receiver but I managed to observe communication at a range of 60 cm, with no additional amplifier between the antenna and mixer and a antenna of 10 cm radius. However, it shows that even a cash-strapped attacker can construct a suitable receiver that could be used in a real attack. In reality one should

[1] Alternative antenna setup with all three loops on the same horizontal axis.

assume that an attacker may have more resources available, in other words he might be in the position to purchase commercial RF equipment.

Antennas: A number of sources describe how to build HF antennas for receiving RF signals, e.g. [4, 18]. Unfortunately these concentrate mainly on E-field antennas for radio applications, although some practical construction and tuning tips still prove useful. The simplest option for building a magnetic antenna is to implement one of the reference designs from TI's Antenna Cookbook [34], since most of the matching components and construction material are already specified. Alternatively, any form of loop antenna can be implemented and then matched using the guidelines in [35]. It should be noted that these guidelines specify components with a higher power rating, since the antennas are also intended for transmitting. When the antennas are only used to receive signals, components with less stringent power requirements can be used. Enameled copper wire and adhesive copper tape can easily be used to construct HF loop antennas of different sizes and number of loops. The resonant antenna also acts as a crude bandpass filter around the chosen center frequency. The width of the passband can be adjusted by changing the Q-factor.

Mixer: An optional amplifier stage can be added between the antenna and the mixer. The amplifier's gain depends on the intended range of the receiver, i.e. short range protocol analyzer or longer range eavesdropping, although it should be kept in mind that most commercial mixer ICs expect an input signal with smaller amplitude and some ICs also have integrated amplifiers. The mixer's function is to move a spectral band of interest to a chosen intermediate frequency (IF) through direct downconversion. Normally, the advantage of IF systems is that any input signal can be moved to a single IF frequency by using an adjustable mixing frequency, which simplifies the design of the filter bank. In my case the local oscillator's frequency can be fixed, but using an IF still simplifies the filter implementation since this allows the use of off-the-shelf filters designed for other applications. It is also possible to implement zero-IF receivers that mixes the input down to the baseband (0 Hz). A lowpass filter can then be used to remove the unwanted high frequency components.

Filter bank: Filtering helps to isolate the data of interest and remove unwanted frequency components. The filter bank implementation depends on the IF chosen. Choosing an IF that is often used in radio systems, like 10.7 MHz, simplifies the implementation since suitable filters can be purchased. If the system needs to work at another IF it will require the design of custom filters. Information on filter design and relevant tools can be found from most of the large semiconductor manufacturers, e.g. [1, 21, 33]. It should be noted that both passive and active high-frequency filters are sensitive to stray capacitance, or inductance, introduced by the circuit layout. The operational amplifiers selected for use in the active filters must also have adequate slew rate and gain bandwidth to function at the chosen IF.

6.2 Signal capture and demodulation:

The attacker needs to capture and demodulate the signal from his receiver. The sampling rate used by the attacker is dependent on the output of his receiver, since the rate needs to be at least twice the highest frequency component of the output to prevent aliasing effects. For example, if he used a zero IF receiver with a 1 MHz low pass filter he would need to sample at 2 MHz. An attacker can choose to make a recording and perform data recovery later or implement a real-time demodulator/decoder using a fast enough FPGA or DSP device. If the attacker chose to store a recording the amount of memory needed will depend on the sampling rate chosen. For example, an attacker taking 8-bit samples at a rate of 2 MHz for 10 s would need 20 MB of memory to store each recording. This would be higher if he uses oversampling or if he needs to sample a higher IF output. These requirements are not unrealistic taken into account that an attacker can acquire suitable hardware for a few £100, since most Field Programmable Gate Arrays (FPGA) or Digital Signal Processing (DSP) development kits come with the necessary Random Access Memory (RAM) and Analog-to-Digital Converters (ADC).

7 Conclusion

HF RFID devices using near-field communication are used in a number of secure application such as e-passports and credit cards. The RF communication interface of these devices are vulnerable to eavesdropping attacks. This attack is a well known risk for RFID devices, yet few publications give details about possible experimental setup or practical results.

In this paper I present results from practical proof-of-concept eavesdropping attacks implemented against HF RFID devices. I successfully performed eavesdropping attacks against devices implementing the three most popular HF standards: ISO 14443A/B and ISO 15693. In each case I describe the equipment needed and document the attack setup and execution. I also describe the implementation of an RFID receiver kit that could be constructed for less than £50, which can be used to observe RFID communication. Even though the self-build RF receiver did not achieve the same results as commercial equipment it does illustrate that eavesdropping is not beyond the means of the average attacker.

Eavesdropping attacks are dependent on a variety of factors so someone else with different RF equipment and environmental conditions might achieve a different result. In the attacker's perfect world, or with 'advanced monitoring equipment and ideal environmental conditions, including optical line of sight transmission, low humidity, and no radio interference', to quote [22], eavesdropping could be possible at much greater distances as is indeed shown to be the case in [9]. My main contribution was therefore not so much the actual attack distances, but rather the experimental setup that provides other researchers with a reference attack, which they can study and improve upon. That said, my results do confirm that near-field devices are not rigidly location limited and that an attacker can definitely recover data beyond the advertised operating range. It also provides a practical result to debate, which is important for RFID technology where attack distances are so often seen as a measure of security. By demonstrating practical eavesdropping techniques I hope to promote a better understanding of these attacks. In turn I hope that my work will to assist system designers to better comprehend the eavesdropping threat in order to select appropriate technologies and countermeasures.

There is still scope for further work on RFID eavesdropping, such as testing different readers and developing better data recovery methods. I started doing some preliminary work on testing how the tuning of the reader and the token affects the eavesdropping range. For example, I placed the antenna 1 m away from the reader and displayed the AM demodulated output of the RF receiver on the oscilloscope. By changing the parallel tuning capacitor value on the reader the amplitude of the backward channel data recovered by the receiver could be largely reduced. This also decreases the operational distance, although this might be an acceptable sacrifice to limit the risk of eavesdropping. I have also not yet looked at using E-field antennas to eavesdrop on the communication between the reader and the token.

Finally, it is interesting to note that the ISO 18092 "Near-Field Communication (NFC)" standard [15], prescribes the same modulation scheme as ISO 14443A. Devices can operate in *passive* mode, where one device acts as a reader and the other as a token, as well as in *active* mode, where both devices act like a reader. In *active* mode the devices take turns to transmit data using 100% ASK modulation of their respective carriers, effectively creating a 'forward' channel in both directions. Such a system could possibly be more vulnerable to eavesdropping, since the eavesdropping distance would be equal to D_{EF}.

I wish to thank Markus Kuhn for his advice and assistance during my experiment and all the anonymous reviewers for valuable comments.

References

1. Analog Devices. *FilterPro – MFB and Sallen-Key Low-Pass Filter Design Program.* http://focus.ti.com/lit/an/sbfa001a/sbfa001a.pdf
2. G. Avoine, K. Kalach and Jean-Jacques Quisquater. *ePassport: Securing International Contacts with Contactless Chips*. Financial Cryptography and Data Security, January 2008.
3. Bundesamt für Sicherheit in der Informationstechnik. *Security Aspects and Prospective Applications of RFID Systems*. October 2004.
4. J.J. Carr. *Practical Antenna Handbook*. McGraw-Hill, 2001.
5. N.T. Courtois, K. Nohl and S. O'Neil. *Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards*. Cryptology ePrint Archive, Report 2008/166, April 2008.
6. DHS Emerging Applications and Technology Subcommittee. *The Use of RFID for Human Identification*. May 2006.
7. E-Passport Mock Port of Entry Test. January 2005. http://www.epic.org/privacy/us-visit/foia/mockpoe_res.pdf
8. T. Finke and H. Kelter. *Radio frequency identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*. Bundesamt für Sicherheit in der Informationstechnik, September 2005. http://www.bsi.de/fachthem/rfid/whitepaper.htm
9. J. Guerrieri and D. Novotny. *HF RFID Eavesdropping and Jamming Tests*. Electromagnetics Division, Electronics and Electrical Engineering Laboratory, National Institute of Standards and Technology, Report No. 818-7-71, 2006.
10. G.P. Hancke. *Practical attacks on proximity identification systems (short paper)*. Proceedings of IEEE Symposium on Security and Privacy, pp 328-333, May 2006.
11. T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels and T. O'Hare. *Vulnerabilities in first-generation RFID-enabled credit cards*. Proceedings of Financial Cryptography and Data Security, February 2007.
12. International Civil Aviation Organization (ICAO). *Document 9303 Machine Readable Travel Documents (MRTD). Part I: Machine Readable Passports.* 2005.
13. ISO/IEC 14443. *Identification cards – Contactless integrated circuit cards – Proximity cards.*
14. ISO/IEC 15693. *Identification cards – Contactless integrated circuit cards – Vicinity cards.*
15. ISO/IEC 18092. *Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1).*
16. A. Juels. *RFID Security and Privacy: A Research Survey*. IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, pp 381–394, February 2006.
17. A. Juels, D. Molnar and D. Wagner. *Security and Privacy Issues in E-passports*, Proceedings of IEEE/CreateNet SecureComm, pp 74–88, 2005.
18. J.D. Kraus and R.J. Marhefka. *Antennas: For All Applications*. 3rd Edition, McGraw-Hill, 2001.
19. D. Kügler. *Security Mechanisms of the Biometrically Enhanced (EU) Passport*. Presented at the 2nd International Conference on Security in Pervasive Computing, April 2005.
20. M.G. Kuhn. *Compromising emanations: Eavesdropping risks of computer displays*. University of Cambridge, Technical Report UCAM-CL-TR-577, December 2003.

21. National Semiconductors. *A Basic Introduction to Filters – Active, Passive, and Switched-Capacitor*. Application Note 779, April 1991.
22. NIST: Special Publication 800-98. *Guidance for Securing Radio Frequency Identification (RFID) Systems*. April 2007.
23. NXP Semiconductors. *ICODE smart label solutions - contactless smart card ICs*. `http://www.nxp.com/products/identification/icode/index.html`
24. NXP Semiconductors. *MIFARE – Contactless and Dual Interface Smart Card*. `http://www.nxp.com/products/identification/mifare/index.html`
25. K. Nohl, D. Evans, Starbug and H. Plötz. *Reverse-Engineering a Cryptographic RFID Tag*. USENIX Security Symposium, July 2008.
26. *OpenPCD* Project. `http://www.openpcd.org`
27. PC World *ACLU's Barry Steinhardt RFID demonstration*. April 2005. `http://blogs.pcworld.com/staffblog/archives/000609.html`
28. Philips Semiconductors *Demodulating at 10.7 MHz IF with the SA605/625*. Application Note 1996, October 1997.
29. J.G. Proakis. *Digital Communications*. 3rd Edition, McGraw-Hill, 1995.
30. *RFID technology security concerns: Understanding Secure Contactless device versus RFID tag*. Eurosmart White Paper, October 2007.
31. M. Roberti, *Fear of Big Brother*, RFID Journal. `http://www.rfidjournal.com/article/view/276`
32. H. Robroch. *ePassport Privacy Attack*. Riscure presentation at Cards Asia Singapore, April 2006. `http://www.riscure.com/2_news/passport.html`
33. Texas Instruments. *FilterPro v2*. `http://focus.ti.com/docs/toolsw/folders/print/filterpro.html`
34. Texas Instruments. *HF Antenna Cookbook*. `http://www.ti.com/rfid/docs/manuals/appNotes/HFAntennaCookbook.pdf`
35. Texas Instruments. *HF Antenna Design Notes, Technical Application Report*. `http://www.ti.com/rfid/docs/manuals/appNotes/HFAntennaDesignNotes.pdf`
36. W. Tobergte and R. Bienert. *Eavesdropping and activation distance for ISO/IEC 14443 devices*. NXP White Paper, 2007.
37. J. Yoshida. *Tests reveal e-passport security flaw*. August 2004. `http://www.eetimes.com/showArticle.jhtml?articleID=\\45400010`