Range Extension Attacks on Contactless Smart cards

Yossef Oren, Dvir Schirman, and Avishai Wool

Cryptography and Network Security Lab, School of Electrical Engineering
Tel-Aviv University, Ramat Aviv 69978, Israel
{ yos@eng | dvirschi@post}.tau.ac.il, yash@acm.org

Abstract. The security of many near-field RFID systems such as credit cards, access control, e-passports, and e-voting, relies on the assumption that the tag holder is in close proximity to the reader. This assumption should be reasonable due to the fact that the nominal operation range of the RFID tag is only few centimeters. In this work we demonstrate a range extension setup which breaks this proximity assumption. Our system allows full communications with a near-field RFID reader from a range of 115cm – two orders of magnitude greater than nominal range – and uses power that can be supplied by a car battery. The added flexibility offered to an attacker by this range extension significantly improves the effectiveness and practicality of relay attacks on real-world systems.

Keywords: RFID, Contactless smart card, ISO/IEC 14443, Relay attack

1 Introduction

1.1 Background

Over the last few years, radio frequency identification (RFID) and near field communication (NFC) technologies have become increasingly popular. They are used in applications which benefit from the ease of use, the increased data rate, and computational abilities offered by RFID technologies compared to traditional technologies like magnetic stripe or bar-code. There are in general two categories of passively-powered RFID tags: (a) **UHF tags** compliant with ISO/IEC 18000 which operate at a range of few meters and are mainly used for marking products or components, and (b) **HF tags** compliant with ISO/IEC 14443 which operate at a range of few centimeters and are used in a variety of security-sensitive applications such as payment cards, access control, e-passports, national ID-cards, and e-voting. In both categories tags are generally low cost devices which communicate with a more powerful **reader** over a wireless medium. This work focuses on physical layer security issues of ISO/IEC 14443 HF tags, which are also commonly referred to as **contactless smart cards**.

All of the applications mentioned above require security controls, whether to defend the user's privacy, to prevent unauthorized access, or to keep the user's

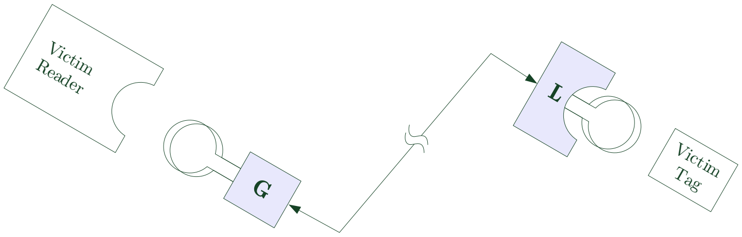

Fig. 1. An RFID channel under a relay attack. Device L is the leech, while device G is the ghost.

money safe. Most RFID applications deal with security issues through secure protocols and cryptography, but they also rely on the **assumption of proximity** between the tag and the reader as a security feature. In older technologies, like magnetic stripe credit cards or contact-based smart cards, the assumption of proximity was guaranteed due to the contact-based interface between the card and the reader. Near field RFID standards like ISO/IEC 14443 are also perceived to guarantee proximity since the nominal operation range for communication between a tag and a reader is only few centimeters. Therefore, most contactless smart card secure protocols inherently assume that the tag holder stands right in front of the reader.

1.2 Related Work

In [3] Desmedt et al. presented a generic way to defeat protocols with a assumption of proximity called the **mafia fraud attack**, or the **relay attack**. Previous works have already noted the relevance of relay attacks to the contactless smart card scenario [15] and have demonstrated that relays can be practically built and used to attack such systems [7,6,30,14,28]. As illustrated in Figure 1, a relay is established by placing two special communication devices (called the “ghost” and the “leech”) between the victim reader and the victim tag. The ghost and the leech communicate via a long-range channel such as a wireless connection. The leech transmits any packets sent by the victim reader to the victim tag, receives the victim tag’s responses, and sends them back to the ghost, which finally forwards them to the victim reader. Since the ghost and the leech are built and controlled by the attacker, they do not have to comply to any standard. This allows the communication ranges between leech and tag and between ghost and reader to be increased, beyond the nominal standards, improving the effectiveness of the relay attack. The work of [16] showed how to build a low-cost, extended-range RFID leech device. In [8] extended range eavesdropping and skimming attacks are described.

Despite the fact that relay attacks have been a known threat for several years, and that building a relay system is well within the budget of even a moderately-funded attacker, there is a surprising lack of reports on relay attacks occurring on real-world contactless smart card systems [2]. One possible explanation is the high risk incurred by the attacker: while the victim tag can be accessed with relatively low risk (for example, by following the victim and placing a skimmer near his back pocket), the victim reader is generally located in a high-security location such as a store counter or a border crossing, and is protected by additional security measures such as security cameras or guards.

1.3 Contributions

In this work we present a design for a modified ghost device which dramatically increases the range of the ghost-reader communication channel. The main novelty of our design is the use of two different antennas and RF front ends: One for the reader-to-ghost receive path, and one for the ghost-to-reader transmit path. Since our modifications are completely in the analog domain, they are not expected to increase the processing delay of the relay or otherwise interfere with the RFID protocol.

We experimentally verify the effectiveness of our modified ghost device in a series of experiments. In our experiments we show an effective reader-to-ghost range of 140cm, an effective ghost-to-reader range of 115cm, and therefore, a full bi-directional range of 115cm. These ranges are two orders of magnitude greater than the nominal tag-to-reader range. Most significantly, our device can be built with a moderate-to-low budget and uses power that can be supplied by a car battery.

We also study the implications of the improved ghost device on the security of several contactless RFID scenarios. Specifically, the extended range can increase the severity of relay attacks by allowing the attacker to move away from the victim reader, possibly even to the next room or to a nearby car. Beyond posing a significant threat to the security of contactless smart card applications, we also show how the range extension setup can also be used for legitimate purposes – e.g., to allow handicapped persons to use their RFID tag from a distance.

Document Structure

This paper is organized as follows. The next section gives a brief background of contactless smart card standards and describes relay attacks. Section 3 presents the design of our range extension system. Section 4 presents the experimental results. Section 5 discusses possible attack scenarios and legitimate uses for our setup. Finally, section 5.3 summarizes the implications of our work.

2 The ISO/IEC 14443 standard

Most close range RFID applications are based on the ISO/IEC 14443 standard. This standard specifies the operation method and parameters for proximity-coupling smart cards. The nominal operation range for this standard is 5-10 cm. The standard calls the RFID reader a Proximity Coupling Device (PCD), so we will use the terms reader and PCD interchangeably. The tag is called a

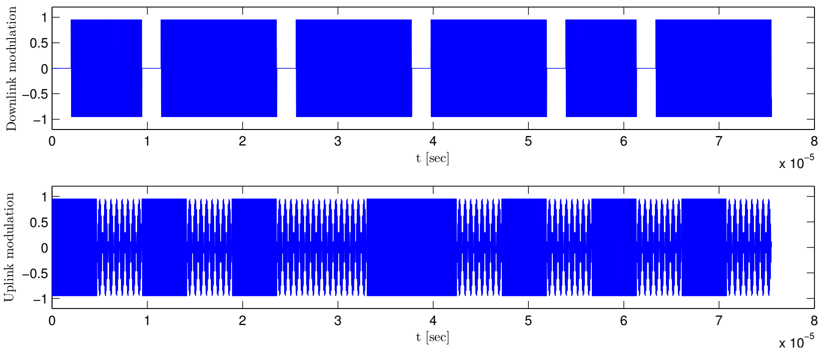

Fig. 2. Example communication signals for ISO/IEC14443-2 type A. Top: Downlink modulation, Bottom: Uplink modulation

Proximity Integrated Circuit Card (PICC), so we will use the terms tag and PICC interchangeably.

The standard consists of 4 parts: part 1 covers the physical characteristics of the PICC [10]; part 2 specifies the characteristics of the fields to be provided for power and bi-directional communication between the PCD and the PICC [12]; part 3 defines the routines for the initialization of the PICC as well as an anti-collision routine for multiple PICCs [13]; part 4 specifies a half-duplex block transmission protocol featuring the special needs of a contactless environment and defines the activation and deactivation sequence of the protocol [11]. Note that the higher parts of the standard are intended to be used in conjunction with the lower parts.

The standard defines two types of tags, type A and type B. The two types differ in modulation techniques, initialization protocols, and transmission protocols. Our work focuses on type A, hence the following sections will describe only type A properties.

The parts of the standard that are relevant to the design of our range extension setup, are parts 2,3, and 4, we highlight their relevant features here.

2.1 ISO/IEC 14443 Part 2: Radio frequency power and signal interface

This part defines the physical layer interface between the PCD and the PICC. the PICC (tag) is passive – it has no source of power, and draws all its energy from the reader's transmission signal. The communication is based on inductive coupling between an active reader and a passive tag. We will refer to the channel from the reader to the tag as the **downlink** channel, and the channel from the tag to the reader as the **uplink** channel.

According to the standard the carrier frequency of the reader is $f_c = 13.56\ MHz$. The operating magnetic field produced by the reader should lie within the range of 1.5 A/m rms to 7.5 A/m rms. And, the bit rate during initialization part is defined as $f_c/128 \approx 106\ kbits/S$.

Downlink modulation: The communication from the reader to the tag uses Amplitude Shift Keying (ASK) with modulation depth of 100%. The transmitted bits are coded with modified Miller coding as shown in Figure 2 (top). In order to guarantee a continuous power supply to the passive tag, the length of the blanking intervals is only 2-3 µs.

Uplink modulation: Since the tag has no independent power source, it transmits its signal by means of load modulation of a sub-carrier at $f_{sc} = f_c/16 \approx 847\ kHz$. This modulation is physically carried out by switching a load inside the PICC on and off.

The transmitted bits are Manchester coded and modulated by on/off keying of the sub-carrier (i.e., the sub-carrier is ASK 100% modulated by the Manchester coded bits) – see Figure 2 (bottom).

2.2 ISO/IEC 14443 Timing Parameters

The ISO/IEC 14443 standard defines two critical timing parameters called the Frame Delay Time (FDT), which defines the maximal time delay during the initialization protocol [13], and Frame waiting time (FWT) which defines the maximal time delay during the transmission protocol [11]. Both of these parameters define the time delay allowed from the end of a PCD's frame transmission to the start of the PICC's response reception. These parameters are set to about 90µs during initialization of the protocol (FDT), and to about 300µs-5s (FWT).

After the initialization protocol is completed, if a PICC requires a longer calculation time, it can ask for additional time through sending a WTX request [11], which can extend the FWT up to its maximal value of about 5 seconds. The WTX request can be sent multiple times in order to achieve longer calculation times.

One of the practical limitations that relay attacks face is the issue of timing. Without careful attention, the relay can introduce delays into the communication channel, which may break the protocols: As mentioned above, the initialization protocol has strict delay constraints, while during the transmission protocol longer delays can be established, but not without actively interfering in the activation protocol.

3 Ghost System Design

Our goal in this work is to demonstrate an extended-range ghost device – i.e., a device that can pretend to be a tag to a legitimate reader. Unlike a real tag our ghost device is an active device that has a power source.

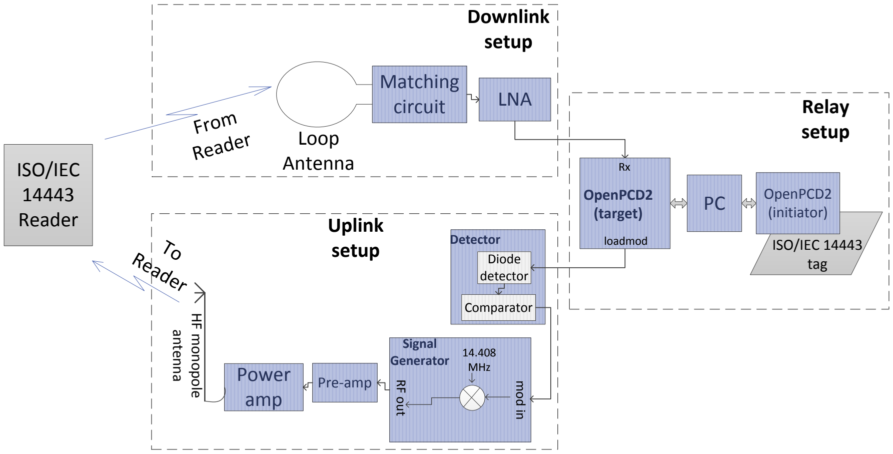

Fig. 3. Block diagram of full range extension system

We made the following design decisions when creating our ghost device: (1) We use two separate antennas, one for the downlink, and one for the uplink. The downlink reception antenna is a large loop antenna which allows greater sensitivity and therefore, can receive the signal from a greater range. For the uplink transmission we use the close range magnetic field emitted from an HF monopole antenna. (2) We use active load modulation for the uplink, to overcome the nominal range limitations of the magnetic coupling. (3) We perform a relay of protocol level 4, while implementing protocol level 3 independently in front of the reader and the tag, to overcome the strict timing requirements of the initialization protocol at level 3.

The system can be divided into three independent building blocks: downlink, uplink, and relay. In the following sections these three building blocks are described. The system is designed to be mounted on a car, and to get its power from a standard car battery. A block diagram of our design can be seen in Figure 3.

We tested our ghost using a relay infrastructure. We used standard unmodified hardware for the leech device, while making all the required changes for range extension only on the ghost device.

3.1 Downlink Channel Design

The relay setup is based on two OpenPCD2 [17] boards. OpenPCD2 is a RFID/NFC open source development board based on NXP's PN532 chip [22]. Thus, the control logic for the Ghost device is based on one of the openPCD2 devices (see figure fig:Diagram).

Our extended range downlink is based on connecting a large loop antenna to the antenna ports of the PN532 (on the OpenPCD2 board). We used a 39

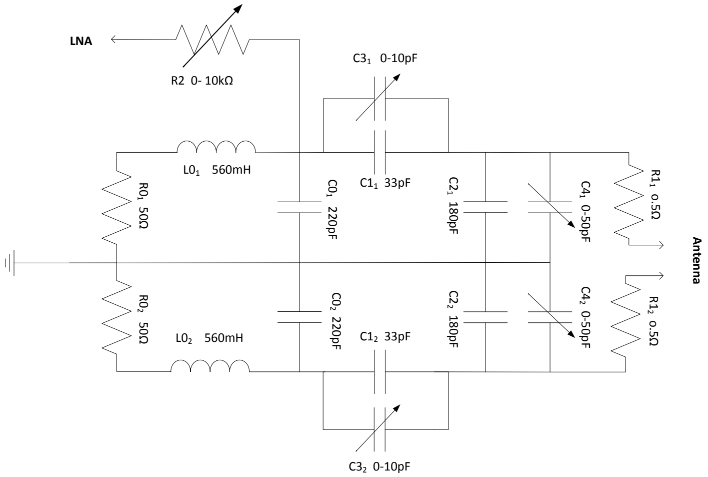

Fig. 4. Downlink antenna matching circuit. The fixed components values are roughly tuned for our antenna, the variable components are used for fine tuning.

cm copper tube loop antenna built for a previous leech project in our lab [16]. The antenna is connected via a matching circuit through a low noise amplifier (ZFL-500LN [18]) to the Rx port of the PN532.

Matching the antenna: In order to transfer maximum power from the antenna to the PN532's input an impedance matching circuit is needed. The circuit was designed according to NXP's application note [21]: First measuring the antenna impedance, then calculating appropriate values for the tuning capacitors and resistors. The Q resistor (R1) value was chosen to achieve a quality factor of 25 as recommended by NXP. Since we use the antenna only for reception, the Tx1 and Tx2 ports of the PN532 chip were not connected to the matching circuit, and instead 50Ω resistors ($R0_{1,2}$) were added. The matching circuit scheme can be seen in Figure 4.

The matching circuit was first tuned by transmitting a 13.56 MHz carrier wave signal from a signal generator through another loop antenna, and measuring the amplitude at the Rx output with a scope, while the circuit is connected to the OpenPCD2 board. The variable capacitors were tuned for the maximum amplitude value. Finally, the matching was verified using a network analyzer by measuring the S_{11} value of the matching circuit and the antenna (i.e., the input return loss of the antenna).

3.2 Uplink Channel Design

A key idea behind the uplink is to replace the load modulation technique with an **active** modulation technique and transmit the signal through a power amplifier and a mobile monopole HF antenna.

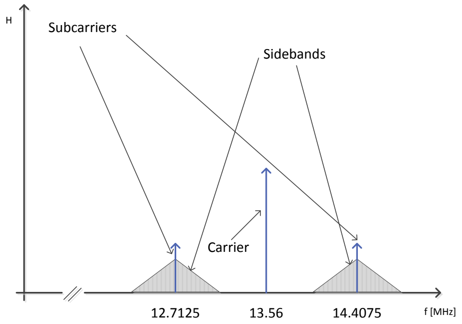

Fig. 5. Spectral image of ISO/IEC 14443 communication

Active load modulation is a technique introduced by Finkenzeller et al. in [4,5]. This technique uses active circuitry which produces the same spectral image as ISO/IEC 14443 type A load modulation, causing the reader to observe the transmitted signal as if it was a standard load modulated signal. Active load modulation operates in the following way:

As described in Section 2.1 the uplink transmission channel of ISO/IEC 14443-2 is based on an ASK modulation of a sub-carrier. When looking at the spectral image of this modulation the result is two sidebands centered at $f_{1,2} = f_c \pm f_{sc}$, and each band functions as carrier for the Manchester coded bits (see Figure 5). According to [5] a typical ISO/IEC 14443 compliant reader evaluates only the upper side band, hence the relevant part of the spectral image is the upper sideband centered at $f_{USB} = f_c + f_{sc} = 13.56 + \frac{13.56}{16} = 14.4075\ MHz$. Therefore, In order to emulate the load modulation signal we can directly modulate the Manchester coded bit stream using an ASK 100% modulation of a 14.4075 MHz carrier signal.

Doing so, with an active powered transmitter, allows us to bypass the need for near-field magnetic coupling, and achieve transmission ranges that are 2 orders of magnitude greater than the nominal range.

The transmitting antenna: Nominal RFID communication is based on magnetic coupling between two loop antennas. As explained in [5] an effort to increase the range of an active transmitting signal requires either to dramatically increase the current injected to the antenna, or to increase the area of the loop (which also introduces more noise). An alternative approach is to use the field generated by an HF monopole antenna. Monopole antennas are designed for electric field (plane wave) transmission rather than magnetic coupling. However, the antenna still produces a magnetic field in the near field region. Moreover, there may be a coupling between the electric field produced by the monopole antenna to the reader's circuit, which also contributes to the range extension.

There are several advantages of using a monopole antenna for this setup. First, since it usually looks like a simple pole it is easier to hide, which helps in disguising an attack setup. Second, there is a variety of commercial antennas in the ham radio market which are designed for the desired frequency range. And third, we hypothesize that the uplink range will be longer, and the power consumption will be reduced in comparison to our 39cm loop antenna.

In order to choose the appropriate antenna we conducted a preliminary jamming experiment (see section 4.2). We got the best jamming range with a military broadband helically wound antenna, NVIS-HF1-BC. The considerations for choosing the uplink antenna are further described in [23].

Implementation: In order to produce an active load modulation signal from the PN532 chip we made use of a little-used output pin named LOAD_MOD. This pin is meant to be connected to an external load, and therefore carries the modulated sub-carrier signal. The OpenPCD2 board does not make use of the LOAD_MOD pin, and the regular libnfc code does not instruct the PN532 to activate the pin. Thus, we needed to solder a connector directly into the pin and modify the libnfc code to activate it.

For our setup we needed to work with the digital Manchester coded bit stream rather than the modulated sub-carrier signal. Therefore, we built a simple detector circuit consisting of a diode detector and a comparator which extracts the bit stream from the modulated sub-carrier signal. We used the extracted bit stream to modulate a 14.4075 MHz carrier. Note that for our experiments we produced the modulated signal by entering the bit stream into a signal generator (Agilent N9310A). The signal generator can be easily replaced by a simple circuit containing an oscillator and a mixer.

Since our signal generator's output power reaches only up to 15 dBm, we needed to amplify the signal. We used a Mini-Circuits ZHL-32A [19] amplifier which serves as a pre-amplifier, and a RM-Italy KL400 [26] (a ham radio amplifier) which serves as a power amplifier. The amplifier output is connected to our uplink antenna described above.

The KL400 amplifier is a mobile amplifier intended to be used in a car mounted setup. It requires a $12V_{DC}$ power supply, and when working at full power it uses up to 24A, which can be supplied from a standard car battery.

3.3 Relay setup

Since our focus was the construction of the ghost system and not the relay itself, we implemented the relay part of the attack inside a single PC. For the leech device we used an unmodified OpenPCD2 board. The ghost antennas are connected to a second OpenPCD2 board. The OpenPCD2 boards run a libnfc compatible firmware and are both connected to a PC running Linux Fedora 17 with libnfc [1].

We make use of one of the programs in libnfc, called nfc-relay-picc, which is a relay application built for boards using the PN532 chip. nfc-relay-picc was designed to overcome the timing issues discussed in Section 2.2, which limit the effectiveness of relay attacks. The program operates in the following way:

- One device is selected as initiator (a leech in our terminology), and the other device is selected as target (a ghost in our terminology).
- The leech is placed in front of a victim tag, emulating a reader. It performs the initialization and activation protocols defined in the standard, towards the tag (further description of these protocols can be found in [13,11]).
- The tag credentials are acquired by the leech and relayed to the ghost device.
- The ghost emulates a tag with the data acquired from the original tag and waits for a reader to activate it.
- When the ghost is activated by the victim reader, it performs the initialization and activation protocols directly with the reader, using the victim tag's credentials acquired earlier, thus overcoming the very strict delay constraints of the anticollision level 3 protocol.
- While a transmission protocol is established between the ghost and the reader, a parallel transmission is established between the leech and the tag.
- After both transmission protocols are established, each APDU (level 4) frame from the reader is relayed through the ghost→PC→leech relay to the tag, and vice versa.
- In order to overcome timing issues during the transmission itself, the ghost sends WTX requests each time the FWT period is about to expire.

Note that in itself the nfc-relay-picc program and the OpenPCD2 boards are designed to operate within the nominal range of 5-10cm.

To use this program with our uplink setup we had to slightly change the libnfc source, in order to enable an output of the modulated sub-carrier signal out of the LOAD_MOD pin of the PN532 chip.

4 Experiments and Results

In this section we describe the experiments done to test our setup, including preliminary experiments to validate our assumptions, and measurements of the final setup. All of the experiments described below were done with a TI MF S4100 Reader [9] acting as the victim reader, and a ISO/IEC 14443 type A sample tag which was provided inside the OpenPCD2 package as the victim tag. The MF reader was selected since it generates read requests at a high rate (more than 10 times per second). In addition, the TI reader's controller software emits a loud beep when it receives an answer from the tag.

4.1 Reader-to-ghost (downlink) range estimation

Our first experiment was to measure the reception range of our downlink copper tube loop antenna in isolation. For this purpose we connected the antenna and the matching circuit to a simple detector circuit consisting of a diode detector and a comparator, connected the detector's output of a scope, and measured the received pulses. In order to estimate the reception performance we used the following metric:

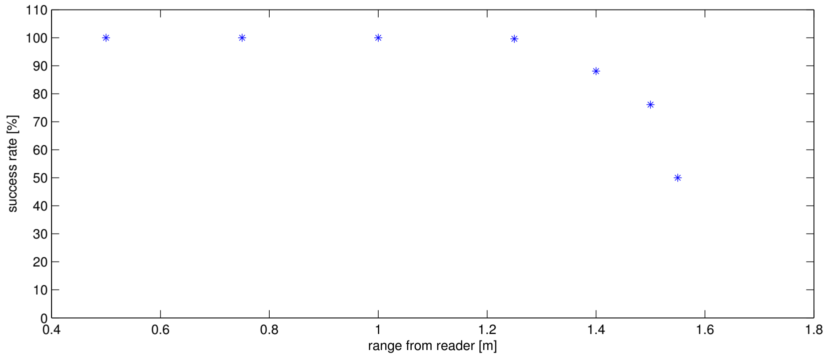

Fig. 6. Downlink performance as a function of the distance from the reader

- A reference measurement was taken at a close range, measuring the reception of few repeated REQA frames.
- For each measurement the number of positive pulses was counted.
- For each measurement, we define an error rate metric as the normalized difference between the number of pulses in this measurement and in the reference measurement.

Figure 6 present the results of the experiment. We observed good downlink reception up to a range of 140cm, followed by a dramatic drop in quality within less than 20 cm. A similar experiment was done using a spectrum analyzer with an analog output as the detector, and we observed a reception range of about 350cm. However, we believe that our detector's 140cm range predicts the expected results more accurately, since the ghost's PN532 chip needs to receive the messages error-free in order to decode them.

Based on [25] we believe that a greater downlink range may well be possible. However, we must note that the ghost range is bounded by both the uplink and the downlink ranges.

4.2 Ghost-to-reader (uplink) range estimation

An isolated estimation of the uplink performance was a more challenging task, since transmission from the tag to the reader occurs only after a successful reception of a reader's frame by the tag (i.e., a working downlink channel is required). Hence, in order to test the performance of the RF part of the uplink channel (signal generator, amplifier, and antenna) we conducted a jamming experiment. The basic principle of the jamming setup is to use the same setup as the uplink channel, only without modulation, in order to transmit a continuous wave signal at the upper side band frequency (14.4075 MHz, recall Figure 5). By transmitting a powerful signal towards the reader at the same frequency as the tag's transmission, we block the tag's response and jam the communication between the reader and the tag.

Antenna	Full jamming range [cm]	Partial jamming range [cm]
39 cm loop	95	125
Hustler	110	165
Helically wound	200	230

Table 1. Jamming experiment results

We assume that since in the jamming case the signal should only interfere with a legitimate signal, and not transmit any information, jamming should be an easier task than uplink transmission. Therefore, by measuring the jamming range we obtain an upper bound on the achievable uplink range.

Another objective of the jamming experiment was to determine which antenna is the best for the uplink channel.We tested the following three antennas:

a. 39cm copper tube loop antenna (the one used for the downlink setup)

b. New-Tronics Hustler: MO-4 (mast) + RM-20-S (resonator), which is designed for the 14–14.35MHz ham radio band [20] (See [29, §6-29])

c. Broadband vertical helically wound antenna: NVIS-HF1-BC (See [29, §6-37])

Note that in the jamming experiment the KL400 power amplifier was not used, and the signal was amplified only with the Mini-Circuits pre-amplifier. Furthermore, since no information was transmitted, we did not need to worry about distortion, and the amplifier was operated with 15dBm input power, above its 1dB compression point. The results of the jamming experiments are summarized in Table 1. Jamming was identified using an ISO14443A compliant tag placed next to the reader. Using TI's demo software the computer beeps every time a tag is recognized. We distinguish between two jamming types: full jamming is defined when no beep is heard from the reader for more than 10 seconds, while partial jamming is defined when 1-2 beeps per second are heard, but still significantly fewer beeps than with no jamming signal at all (5-10 beeps per second).

We notice that the helically wound antenna gives the best jamming range, and therefore, it was chosen for use in the uplink channel. The jamming experiment is described in further details in [23].

4.3 Full range extension experiment

After estimating the achievable ranges of the different building blocks in isolation, we constructed a full range extension device (ghost). All the range extension experiments were done with the helically wound antenna chosen during the jamming experiments as the uplink antenna, and the 39cm copper tube loop antenna as the downlink antenna.

A successful downlink can be observed by watching the PN532 response to a reader's frame, which is manifested in a signal on the LOAD_MOD pin. As a diagnostic tool, a scope was used to monitor the LOAD_MOD output, in order to identify a successful downlink. The measured downlink range is **120cm** – two orders of magnitude greater than the nominal range, and enough in many cases for an attacker to move far enough from the victim reader to avoid capture.

On the other hand, uplink measurements were more complex, since the uplink channel was found to be very sensitive to the surrounding environment and cable orientation. A successful uplink was identified by hearing the TI reader's demo software beep for a successful read of a tag. So, a successful uplink also meant a successful range extended relay. Our first attempts with measuring uplink ranges produced suspiciously high ranges. We discovered that the high range was due to an unwanted coupling effect as noticed by [30]. In our initial setup a coaxial cable was passing between the uplink setup and the reader (not connected to any of them), serving as a waveguide for the uplink signal.

We then decided to move our setup outside of the building in order to work in a clear and robust environment. The first measurements were held with only the Mini-Circuit's 25dB pre-amplifier which has an output-1dB-compression-point of 29dBm (~800mW). In practice, we noticed that at output levels of above 25dBm (~300 mW) the performance of the uplink channel was severely degraded. We believe that this is the result of noise created by operating the amplifier close to its compression point. Therefore, all the measurements were done using a 0dBm power at the output of the signal generator.

At first, the experiment was held with the monopole antenna alone, and we achieved only a 35cm uplink range. We believe that this is due to the fact that monopole antennas need to be placed over a proper ground plane for optimal performance. Since the wave length of our uplink signal is ~20m a true ground plane is impractical. Instead, we assumed a car mounted setup, in which the car itself can serve as a ground plane. To emulate a private car's dimensions we used a $1m^2$ tin plate as a ground plane. With the antenna bolted onto the tin plate and using only the pre-amplifier we managed to get an uplink range of 85cm. We noticed that this setup is very sensitive to the orientation of the antenna cable regarding the tin plate – with different cable orientations the maximal uplink range varied between 45cm to 85cm. We further noticed that the best uplink ranges were achieved when the antenna was facing the side of the victim reader and not its front. A possible explanation is that when the uplink antenna was placed in front of the reader, it was jamming the downlink antenna from receiving the reader's signal, and therefore preventing a full relay.

At last, after establishing a good setup for the uplink antenna, we added the power amplifier into the transmission chain. Since our pre-amplifier can only produce up to 300mW without distorting the signal, yet the RM-Italy KL400 amplifier's input power must be at least 1W, we had to bypass an internal relay inside the amplifier's circuit in order to let the amplifier open for transmission with lower input power. During our experiments we set the KL400 only up to its 2^{nd} power level (out of 6 possible levels) due to radiation hazard concerns (both for the equipment, and for our safety). Later we measured the output power of the modified KL400 amplifier set to its 2^{nd} level and found out the output power of our system was about 7W.

Antenna setup	Amplifier	Full bidirectional range [cm]
no ground plane	pre-amplifier ($P_{out} = 300mW$)	35
$1m^2$ground plane	pre-amplifier ($P_{out} = 300mW$)	85
$1m^2$ground plane	pre-amplifier + power amplifier ($P_{out} = 7W$)	115

Table 2. Range extension results

After all modifications, the measured uplink range including the power amplifier was **115cm**, which is almost the same as our measured downlink range, and again enough for an adversary to mount his attack from the next room. The results of the different uplink setups are summarized in Table 2. The final setup including the tin plate and the power amplifier can be seen in Figure 7.

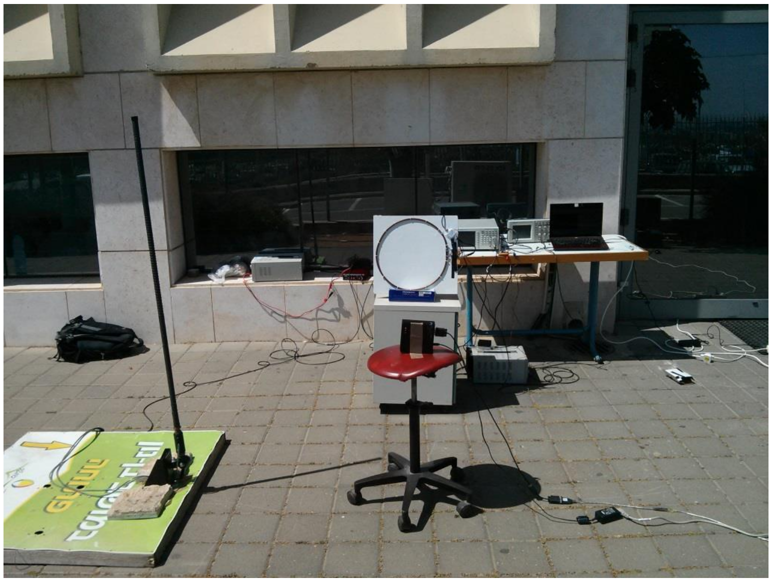

Fig. 7. The full range extension setup outside our building. The victim reader is located on the lab stool in the middle of the picture. The uplink antenna on its ground plane is on the left. The downlink loop antenna is behind the reader. The victim tag is on the table in the back, next to the laptop running the relay software.

5 Discussion and Conclusions

The range extension setup described in this work has significant implications on the security of close range RFID systems. The same setup can also be used for legitimate purposes, in order to enhance RFID capabilities. In this section we briefly introduce two attack scenarios and some legitimate use examples for this setup.

5.1 Attack Scenarios

E-voting The work of [24] presents a set of physical attacks on Israel's proposed e-voting system which uses ISO/IEC 14443 tags as voting ballots. Using a relay setup an attacker can mount a **ballot sniffing attack** (which allows him to learn at any time which votes were already cast into the ballot box), a **single dissident attack** (which can undetectably suppress the votes for any amount of voters), and finally a **ballot stuffing attack** (which gives the adversary complete control over previously cast votes).

Using a nominal-range relay the attacks mentioned in [24] are limited since the adversary must be in a range of 5-10 cm from the target ballots, which places him inside the ballot station's room, and in front of the election committee members. However, if the relay setup is enhanced with a range extension setup the attacks can be mounted from a distance, possibly even from outside the room, which allows the attacker to mount the attack without being detected.

Access control One of the most common application of close range RFID is for access control into restricted areas. Using personal RFID tags only authorized personnel can enter a restricted area.

Using a relay setup an adversary can use a victim worker's identity while he is away from the restricted door, and the tag lies in his pocket, to open the door. However, using a nominal relay setup, this attack scenario is limited, since when the attacker approaches the door holding his ghost device instead of a regular tag he can be easily spotted by the other workers who walk by. Alternatively, if the attacker mounts a range extension setup in a distance from the door (possibly even behind a wall), he can cause the door to open while an accomplice walks towards the door and waves a decoy blank tag in front of the reader. Since the accomplice does not carry any special hardware other than a decoy tag, the risk incurred by the attacker is drastically lowered.

An interesting twist on this attack would be combination of an RFID zapper [27] and an extended-range ghost. An RFID zapper is a low-cost device which can completely disable a victim tag by applying a high-energy electromagnetic pulse to its RF input. If an attacker first zaps a victim's tag, then applies an extended-range ghost attack to the reader just as the victim attempts to use his (now disabled) tag, it will give any human observers the impression that one tag is used, while effectively activating a different tag. This forces an innocent user to be an accomplice to the relay attack described above.

5.2 Legitimate uses for range extension

Besides breaking the close range assumption, and violating the system's security, the range extension setup can be used for legitimate purposes.

For example, a handicapped person sitting in a wheel chair might find it hard to use RFID tags, since most of the readers are placed out of his reach. By mounting a range extension setup onto the wheel chair, the user will now find it possible to enter through doors with RFID access control, or pay for public transportation without asking for help.

As another example, nowadays many parking lots have RFID tags for subscribers. Many drivers find it hard to reach the RFID reader through the car's window. By mounting a range extension setup onto his car, the driver can enter into the parking lot without the effort of reaching the reader at the entrance of the parking lot.

5.3 Conclusions

In this work we presented a range extension setup for contactless smart cards. The setup can be mounted on any car, and powered by a regular car battery. The entire setup costs about $2,000. The uplink antenna constitutes most of the sum, and can be replaced by a cheaper model for cost reduction.

Using this setup the close range assumption of ISO/IEC 14443 applications is broken, since the tag does not have to be placed 5-10cm from the reader, but can be at a distance of over 1m. Moreover, the more severe implication of this attack is in combination with the known relay attack. While one of the drawbacks of a regular relay attack is that the attacker can be seen operating a device right next to the reader or the tag, using our range extended ghost together with a range extended leech presented at [16] the attacker can conceal his devices, and in the case of the range extended ghost might even place his device in the next room.

The attacks mentioned above operate at the physical layer of the standard, and therefore, are difficult to defend against by a protocol based solution. Designers of close range RFID applications like: credit cards, e-passports, access control, and e-voting should take into consideration the threats introduced by extending the nominal operation range of ISO/IEC 14443 tags.

References

1. libnfc website. Online, 2013. `http://nfc-tools.org/index.php?title=Main_Page`.
2. APACS. APACS response to BBC watchdog and chip and PIN. Press realese, February 2007. `http://http://www.chipandpin.co.uk/media/documents/APACSresponsetoWatchdogandchipandPIN-06.02.07.pdf`.
3. Yvo Desmedt, Claude Goutier, and Samy Bengio. Special uses and abuses of the Fiat-Shamir passport protocol. In *CRYPTO*, pages 21–39, 1987.
4. Klaus Finkenzeller. Battery powered tags for ISO / IEC 14443 , actively emulating load modulation. In *7th European Workshop on Smart Objects: Systems, Technologies and Applications (RFID SysTech)*, May 2011.
5. Klaus Finkenzeller, Florian Pfeiffer, and Erwin Biebl. Range Extension of an ISO / IEC 14443 type A RFID System with Actively Emulating Load Modulation. In

7th European Workshop on Smart Objects: Systems, Technologies and Applications (RFID SysTech), May 2011.

6. Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. *Radio Frequency Identification: Security and Privacy Issues*, pages 35–49, 2010.
7. Gerhard P. Hancke. Practical attacks on proximity identification systems (short paper). In *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pages 328–333, Oakland, CA, 2006. IEEE Computer Society.
8. Gerhard P Hancke. Practical eavesdropping and skimming attacks on high-frequency RFID tokens. *Journal of Computer Security*, 19(2):259–288, 2011.
9. Texas Instruments. Multi function reader series 4000. Online, March 2005. `http://www.ti.com/rfid/docs/manuals/pdfSpecs/RF-MFR-RNLK-00.pdf`.
10. International Organization for Standardization, Geneva. *ISO/IEC 14443-1 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics*, 2008.
11. International Organization for Standardization, Geneva. *ISO/IEC 14443-4 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol*, 2008.
12. International Organization for Standardization, Geneva. *ISO/IEC 14443-2 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface*, 2010.
13. International Organization for Standardization, Geneva. *ISO/IEC 14443-3 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision*, 2011.
14. Wolfgang Issovits and Michael Hutter. Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks. In *RFID-Technologies and Applications (RFID-TA), 2011 IEEE International Conference on*, pages 335–342. IEEE, 2011.
15. Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcards. In *International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 47–58, Los Alamitos, CA, USA, 2005. IEEE Computer Society.
16. Ilan Kirschenbaum and Avishai Wool. How to build a low-cost, extended-range RFID skimmer. In *Proceedings of the 15th USENIX Security Symposium*, Vancouver, B.C., Canada, 2006. USENIX Association.
17. Bit Manufaktur. OpenPCD2. Online, 2012. `http://www.openpcd.org/OpenPCD_2_RFID_Reader_for_13.56MHz`.
18. Mini-Circuits. ZFL-500LN low noise amplifier. Online. `http://www.minicircuits.com/pdfs/ZFL-500LN.pdf`.
19. Mini-Circuits. ZHL-32A coaxial amplifier. Online, August 2009. `http://www.minicircuits.com/pdfs/ZHL-32A.pdf`.
20. New-Tronics. mobile HF hustler antenna. Online, October 2008. `http://www.new-tronics.com/main/html/mobile__hf.html`.
21. NXP. AN1425 - RF Amplifier for NXP Contactless NFC Reader ICs. Online, August 2011. `http://www.nxp.com/download/grouping/10529/application_note`.
22. NXP. PN532 - Near Field Communication (NFC) controller. Online, September 2012. `http://www.nxp.com/documents/short_data_sheet/PN532_C1_SDS.pdf`.
23. Yossef Oren, Dvir Schirman, and Avishai Wool. RFID jamming and attacks on Israeli e-voting. *ITG-Fachbericht-Smart SysTech 2012*, 2012.
24. Yossef Oren and Avishai Wool. RFID-Based electronic voting: What could possibly go wrong? In *International IEEE Conference on RFID*, pages 118–125, Orlando, USA, 2010.

25. Florian Pfeiffer, Klaus Finkenzeller, and Erwin Biebl. Theoretical limits of ISO/IEC 14443 type A RFID eavesdropping attacks. *ITG-Fachbericht-Smart SysTech 2012*, 2012.
26. RM-Italy. KL400 Linear Amplifier. Online, 2005. `http://www.rmitaly.com/scheda.asp?IDGr=1&cat=0&tipo=96`.
27. Tilman Runge. Schriftliche arbeit jugend forscht: Der RFID-Zapper (in German). Online, February 2007. `http://rfidzapper.dyndns.org/RFID-ZAPPER.pdf`.
28. Luigi Sportiello and Andrea Ciardulli. Long distance relay attack. *RFIDSec*, July 2013.
29. R.D. Straw. *The ARRL antenna book: The Ultimate Reference for Amateur Radio Antennas*. Amer Radio Relay League, 2003.
30. Pierre-Henri Thevenon, Olivier Savry, Smail Tedjini, and Ricardo Malherbi-Martins. Attacks on the HF physical layer of contactless and RFID systems. *Current Trends and Challenges in RFID*, 2011.