Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems

Ziv Kfir and Avishai Wool
School of Electrical Engineering,
Tel Aviv University, Ramat Aviv 69978, ISRAEL.
kfirziv@post.tau.ac.il, yash@acm.org .

***Abstract*— A contactless smartcard is a smartcard that can communicate with other devices without any physical connection, using Radio-Frequency Identifier (RFID) technology. Contactless smartcards are becoming increasingly popular, with applications like credit-cards, national-ID, passports, physical access. The security of such applications is clearly critical. A key feature of RFID-based systems is their very short range: typical systems are designed to operate at a range of $\approx$ 10cm. In this study we show that contactless smartcard technology is vulnerable to relay attacks: An attacker can trick the reader into communicating with a victim smartcard that is very far away. A "low-tech" attacker can build a pick-pocket system that can remotely use a victim contactless smartcard, without the victim's knowledge. The attack system consists of two devices, which we call the "ghost" and the "leech". We discuss basic designs for the attacker's equipment, and explore their possible operating ranges. We show that the ghost can be up to 50m away from the card reader—3 orders of magnitude higher than the nominal range. We also show that the leech can be up to 50cm away from the the victim card. The main characteristics of the attack are: orthogonality to any security protocol, unlimited distance between the attacker and the victim, and low cost of the attack system.**

Keywords: RFID, Contactless Smartcard, Payment Systems, Security.

I. Introduction

A. RFID systems

Radio frequency identification (RFID) systems are being widely used in various applications such as physical security, tracking, payment systems and many more (cf. [Fin03], [GSA04], [Eco02] and [Yos05]). The usage of RFID systems has grown quickly over the last decade and is rapidly becoming a common part of everyday life. The aim of contactless smartcard technology is to provide low cost "no-touch" communication, which can create an authenticated, and optionally, encrypted channel of communication between the card reader and the nearest smartcard.

A key feature of contactless smartcard technology is that the smartcard is passive: it does not have an independent power source (e.g., it does not contain a battery). Using RFID, the card derives all of its power from the energy emitted though the card reader's transmission.

Because of this feature, contactless smartcard systems are usually designed for very short ranges: e.g., systems based on the ISO-14443 standard are designed to operate over a distance of 10cm. This proximity is inherently viewed as a security feature: In a regular, contact, smartcard system, the assumption is that the card that is physically present in the slot (a) is the card that is communicating with the reader, and (b) was presented by the person in front of the reader. Contactless smartcard systems make the same inherent assumptions, even though the communication is wireless. The assumption is that (c) since the card is only 10cm from the reader, assumptions (a) and (b) are valid.

Unfortunately, we shall demonstrate that assumption (c) does not hold, causing a collapse of the first assumptions, and exposing such systems to attacks.

A typical application we have in mind is a point-

of-sale system. In such an application, the reader is connected to the merchant's cash register. When a customer wishes to pay, rather than swiping her card in the reader, she "waves" her card near the reader, and the transaction is complete. During this "wave", the reader powers up the card, executes an authentication protocol, and upon successful authentication, the customer's electronic wallet (on the card) is charged by the purchase cost (or, alternatively, her credit card is charged). This is not the only application of contactless smartcards, but it suffices demonstrate our attack. If an attacker can build a device that will charge someone else's card for his purchase—he will have defeated the system.

RFID-related risks, mostly regarding privacy issues, have appeared in the trade and popular press over the last year. However, many of these reports are inaccurate and easy to misunderstand. E.g., it was recently reported that, according to a NIST experiment, "the electronic passport can be read from as far as 30 feet away" [All05]. In fact, the snooping device was 30 feet away from the *card reader* and could pick up *its* signal. The RFID-equipped passport itself was 10cm away from the reader, and its transmission could not be snooped. These distances agree with what we report here. However, our goal is more ambitious than passive, half-duplex, snooping: we propose a simple and cheap system that can receive *and transmit* to *both* the contactless smartcard and the reader.

Organization: Section II provides an overview of contactless smartcards. Section III explains the basic relay attack. In Section IV we show how to extend the Reader-to-Ghost range, and Section V illustrates how to extend the Leech-to-Card distance. Section VI discusses some countermeasures. Section VII discusses related work and we conclude with Section VIII. Additional details can be found in an appendix.

II. Overview of Contactless Smartcard Technology

A. Terminology

An RFID-based contactless smartcard system consists of a reader, an RF-antenna and a tag.

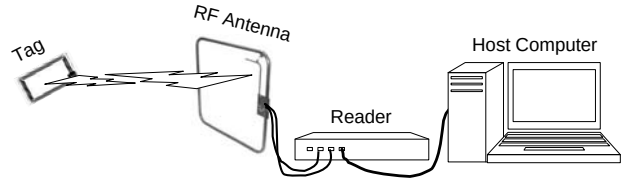

Fig. 1. Contactless Smartcards use RFID technology.

We use the terms "Tag" and "Smartcard" interchangeably. Figure 1 shows a typical contactless smartcard system.

The reader is an active (powered) device that communicates with the smartcard (tag) on one hand and with a security system (based on computerized database) on the other hand.

The antenna is an important part of any RFID system. The antenna converts the electric signal from the reader into the magnetic signal transmitted over the air. Typical reader antenna sizes vary from 5x10 cm^2 up to 50×100 cm^2. In some systems antennas are built inside a reader device, while in others antennas are external. Many technical guides for building RFID antennas can be found on the Internet (cf. [TI03a], [TI04] and [TI03b]).

The tag in a contactless smartcard systems is the smartcard: it is embedded in a plastic credit card, including its antenna. Thus, the contactless smartcard's antenna dimensions are 5×8 cm^2 since it is embedded in a credit card plastic.

B. Standards and Deployment

Most contactless smartcard applications are based on the ISO/IEC 14443 standard [ISO00a]. This standard specifies the RF signal interface, initialization, anti-collision and protocols for wireless interconnection of closely coupled devices. It operates at 13.56MHz, with a bit-rate of 106Kbps, and is designed for a range of 10cm. Such systems are currently being deployed by credit-card companies (see [All04a] and [All04b]) in Point-of-Sale payment systems.

Another relevant RFID standard is ISO/IEC 15693 [ISO00b] - which operates at a range of 1 m but does not provide enough energy to activate an

IC, therefore typical applications are simple fixed-logic devices.

Contactless smartcard systems use the ISO/IEC 7816.4 [ISO95] standard for their transport layer. This is, in fact, part of the main standard that governs contact (regular) smartcard systems. The ISO/IEC 7816.4 standard defines interindustry commands for interchange and secure messaging on the structures of APDU messages.

A parallel RFID standard is NFCIP-1/ECMA340 (also called ISO/IEC 18092). This standard is designed for larger devices like cell phones, PDAs, and laptops. Recently Nokia has announced the availability of an NFC-equipped phone (cf. [Com04] and [Gua04]). The NFCIP standard is being adopted by many companies, see ECMA TC32-TG19 member companies [ECM04].

The NFCIP-2 standard defines a gateway mechanism between any ISO/IEC 14443, ISO/IEC 15693 and ISO/IEC 18092 interface standards. What makes the NFCIP standard interesting is that (1) An NFCIP device can act both as a reader and as a tag; (2) A typical NFCIP device has additional communication channels it can use, such as Wireless-LAN or GPRS; (3) NFCIP devices typically have convenient and powerful programming interfaces; (4) The NFCIP standard and the ISO 14443 standards are compatible below the transport layers. Therefore, since NFCIP are much easier to program—they offer the potential of becoming a convenient platform from which to attack contactless smartcard systems. Figure 2 compares the NFCIP standards to contactless smartcard standards.

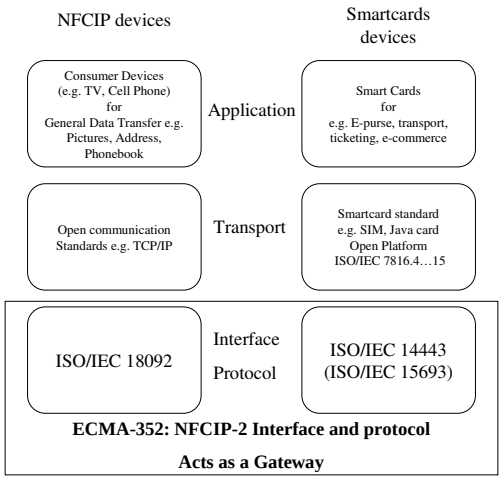

Fig. 2. NFCIP devices vs. Smartcards devices.

III. The Basic Relay Attack

A. System overview

The basic relay attack system is built using two devices, which we call the *ghost* and the *leech*, as described in Figure 3. The ghost is a device which fakes a card to the reader, and the leech is a device which fakes a reader to the card.

The main idea of the ghost and the leech is to create a bidirectional communication channel between the genuine reader and the victim card. The channel passes through the leech and the ghost and provides transparent communication between the reader and the card—at a range that is much greater than the nominal system range.

The typical communication scenario starts with a message that the reader sends to the ghost, which acts as a regular card. The ghost receives the message, sends the message to the leech using a fast digital communication channel and minimum delay, without any data manipulation. The leech receives the message, fakes the real reader and transmits the message to the real card. In the opposite direction (tag to reader) the communication scenario is reversed.

Using this technique gives the ability to create a relay, or repeater between a reader and a card. The relay is orthogonal to any higher level security protocols such as those defined in the ISO 7816.4 standard [ISO95]. Furthermore, using the two devices (the ghost and the leech) allows the distance between the reader and the real card to be practically unlimited.

B. The Threats

The attack described in Section III-A breaks the assumption that the reader is communicating with a card that is physically close. Using the relay attack, the attacker causes the reader to (unknow-

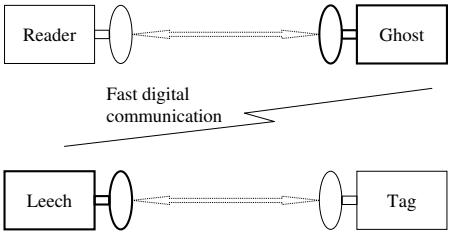

Fig. 3. Basic attack system overview.

ingly) communicate with a genuine card—which is far away. This opens several possible threats. A typical attack is to charge someone else's credit card or electronic wallet for a purchase. To mount such an attack, one could place a leech device close to the victim smartcard (e.g., slip the leech into the victim's handbag), and then present the ghost to the reader at payment time. One could also to open a secure door using someone else's key. Another possibility is hacking into victim's NFCIP device (like a PDA or mobile phone), and programming the device to act as a leech (works only if the NFCIP device is near the contactless smartcard).

Note that the relay attack is possible even if the card and the reader use strong authentication and encryption algorithms. However, in case the system uses weak privacy or security mechanisms then simpler variants can be used by attackers. For example, many governments plan to require a contactless smartcard IC to be integrated on their passports (e.g., see the USA plans [EEt04]). Using a relay attack a terrorist with an expired passport can cross a border using someone else passport ID. If the passport tag does not authenticate the reader, then the attacker can run the attack using a single device (a combined leech/ghost) by interrogating the victim passport in advance, and then replaying the data to the reader at passport control.

C. Limitations

The basic relay attack has some significant limitations, which could be the difference between theoretical attack and a realistic one. Specifically, using standard equipment, the leech-to-card distance needs to be around 10cm, and similarly, the ghost-to-reader distance needs to be 10cm. Being this close to the victim systems makes the attacker vulnerable to exposure. In the remainder of this work we shall show how these limitations can be overcome.

Note that timing limitations are not a real problem for the attacker. In the anti-collision specification of ISO/IEC 14443 ([ISO00a] part 3) the time-out is 5 msec. The data transfer time-out can be set to be up to 5 sec ([ISO00a] part 4). These are very long delays, that almost any modern digital communication channel (between the ghost and the leech) can meet.

IV. Increasing the Reader-to-Ghost Distance

A. From the Reader to the Ghost

As described in Section II, contactless smartcard systems are built from an active reader and a passive card. However, an attacker can build an *active* ghost to increase the distance from which the ghost can receive the reader's signal. In this way the ghost does not need to be within "activation range" since it is no longer powered by the transmitted energy.

In order to calculate the range from which a powered ghost can operate, we used the NEDAP [Foc00] model. This is a commonly used model of the physical (layer-1) communication characteristics of inductive RFID systems. The model uses the parameters of the tag, reader, and antenna, combines them with the effects of external noise and interference sources, and is able to simulate the various reading ranges. The NEDAP model is available as a C program. We adapted the NEDAP model to the parameters of the ISO 14443 standard, and used it to explore the reading range if the ghost ignores any regulatory limitations and does not use the standard load modulation.

We used two possible noise scenarios: Man-Made Noise and RFID system interferences (details may be found in the appendix). Under the "Man-Made-Noise" model, we calculate that the ghost can be about 50m away from the reader. Under the "RFID system interference" model the reader needs to be approximately three time closer

to the ghost than the interference device. Details about the noise models can be found in the appendix. We note that these distances agree with anecdotal empirical evidence [Fin04] and with the findings of the NIST experiment [All05].

B. From the Ghost to the Reader

In RFID systems, the card communicates with the reader using load modulation. Effectively, the card varies the impedance of a resistor, which slightly perturbs the current in the reader's antenna. (see Figure 11 in the appendix). However, load-modulation signals can only be received at very short ranges. Therefore, it seems as if the leech can hear the reader from a large distance—but how can it "talk back"?

However, in ISO 14443, the card uses a sub-carrier frequency to modulate. A key observation is that an active, powered, ghost can transmit directly on the sidebands with DSB (Dual Side Band modulation). From the reader's perspective, DSB modulation is indistinguishable from normal load modulation—however, DSB modulation does not rely on near-field effects and can be performed from a much larger distance. Thus, using DSB, the ghost-to-reader communication is subject to precisely the same distance limitations as the reader-to-ghost direction we saw in Section IV-A: Therefore, the distance between the ghost and the reader can be up to 50 meters, allowing bi-directional communication.

Note that a well-made ghost should synchronize its DSB transmit signal with the reader's carrier, so synchronous receivers would not reject the DSB transmissions.

C. How to build a Ghost?

Building a ghost with a low budget is a fairly simple task. The inventory list includes: wires, copper tubes (like the tubes used for cooking gas), a few hardware components and some basic knowledge of electronics.

Our design sketch (Figure 4) is a "souped-up" NFC device connected to a larger antenna using

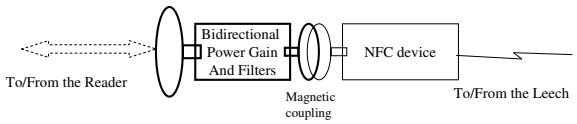

Fig. 4. Building a ghost using an NFC device.

amplifier components. Conveniently, there is no need to open the NFC device's casing. Instead, we can wrap a wire loop around the NFC device, to create a full magnetic coupling with its internal antenna. This wire loop is connected to a filter (to eliminate the carrier frequency), an amplifier, and a home-made copper tube antenna according to the recipe in [TI03a], [TI04], and [TI03b].

Alternatively, the attacker can build a ghost without using a NFC device, from readily available RFID hardware components. Such a custom construction will probably produce a superior ghost device. However, we speculate that (1) future NFC devices will probably have more advanced hardware/software development kits available, and (2) the rapid NFC technology development will make NFC-based ghosts more cost effective.

V. Increasing the Leech to Tag Distance

We saw in the previous section that the distance between the reader and the ghost can be 500 times larger than the system's nominal range. In this section we explore the distance between the leech and the victim card. As we shall see, a significant, but more modest, distance increase can be achieved, with various levels of effort. We shall see that the leech can be up to 40-50 cm away from the smartcards: a 5-fold increase.

As before, we adapted the NEDAP software to our needs and used it to simulate the physical layer communication. The inputs to the model were chosen for typical ISO-14443 parameters. The external noise was calculated as follows: We assume a second (external) RFID system that transmits at the maximum regulation limits ([CEP04], [FCC01] and [ITU00b]) from a distance of 100 meters. This external noise obeys the following formula:

$$Ext_{\text{noise}} = H_{\max} + 51.5 - 10\log_{10}\text{Distance} - 10\log_{10}\text{Bandwidth}$$

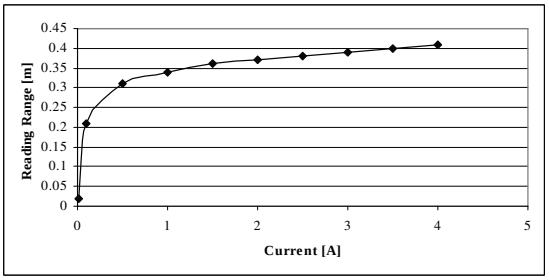

Fig. 5. Leech-to-Card distance as a function of current.

In our case $H_{\max} = 42$ [dBμA/m/Hz] at 10 m, Distance is 100 m, Bandwidth is 106,000 Hz and the constant 51.5 is the air impedance, so the external noise is about 24 [dBμV/m/Hz].

All the results we present are for ISO-14443 [ISO00a] type B. The results for ISO-14443 type A are similar.

A. Distance limitations

The card to reader distance presents the most difficult challenge in any passive RFID system. The leech's task is to increase this distance. Building an effective leech must take into consideration three kinds of distances limitations.

1) The card activation range is the most obvious limitation, since card is powered up by the magnetic field emitted by the leech. However, if the leech can ignore regulatory limits and create a stronger magnetic field, it can activate the card from further away.
2) The leech's sensitivity places a limitation on how far the leech can "hear" the card. In near-field-communication the attenuation is 60dB/Dec, i.e., the signal strength drops by a factor of 1000 whenever the distance grows by a factor of 10. Therefore, having a more sensitive receiver allows us to increase the leech-to-card distance.
3) The third and the most unexpected difficulty is the environment noise in the attack area. The noise directly affects the SNR which the leech receives. The leech-to-card distance is dramatically affected by the SNR value and is fundamentally limited by the Shannon limitation.

B. Increasing the reading range by increasing the activation range

Before any communication can take place between the leech and the victim smartcard, the leech must supply enough energy to power up the card: i.e., the card has to be within the activation range. Note that, fundamentally, the activation range cannot be too large: the boundary between near-field and far-field behavior is given by $c/(2\pi f)$. When $f = 13.56$ MHz this distance is about 3.52 m, which gives us an upper bound on the activation range.

Even approaching this upper bound is difficult in practice. To do so, the leech has to generate a stronger magnetic field. This can be achieved by passing a stronger current though its antenna, or by using a larger antenna (or both). However, increasing the transmit power also increases the internal noise, which may drown the weak signal received from the contactless smartcard. Furthermore, a larger antenna picks up more external noise, which again drowns the received signal. In fact, for every fixed current value, there exists an antenna size that is optimal for that current. The NEDAP model accounts for the effects of these types of noise in its calculations.

In the following simulations, we limited the antenna's current by 4 A, which we believe is a reasonable limitation for a mobile leech device powered by batteries, operated in bursts.

Figure 5 shows the results of the amplified signal in the leech device. For each current value we used its optimal antenna size. The graph shows that, using a larger antenna and stronger current, the leech *can* increase the reading range by a factor of 3.5 over the nominal range. We found that when the current is $1 - 4$ A then the optimal antenna dimensions are about 40×40 cm^2: still allowing reasonable mobility of the leech device.

C. Strengthening the Tag Signal

Once the leech manages to increase the reading range, by transmitting a powerful signal, the bottleneck on any further range increase becomes the leech's ability to receive the card's signal above

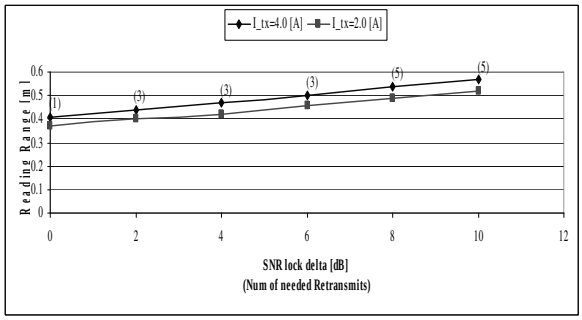

Fig. 6. Distance as a function of the locking ΔSNR, using software-based retransmissions, for two current values. The number of retransmissions appears in parentheses.

the noise.

The main tool we use here is retransmissions. The key idea is that if the leech causes the card to re-transmit every message multiple times, it effectively reduce the bandwidth and amplifies the signal. In the following subsections we suggest two methods of handling retransmissions.

Note that the ISO-14443 [ISO00a] standard allows the reader (the leech in our case) to request an unlimited number of retransmissions for each frame.

1) Software-based retransmissions: The following assumptions form the basis for this method: (a) We assume that the leech hardware can lock-on the card signal at a lower SNR than needed for error-free data reception even with a bad BER (Bit Error Rate), (b) We assume that if the leech hardware locks-on the card signal, it will provide the frame to the driver software, even if the frame has errors and fails in the CRC or checksum test. If these assumptions hold, then the leech can compensate for the reception errors (poor BER) by using multiple copies of each bit. Using this fact, the leech causes the card to transmit each frame K times and takes the majority value for each bit.

In reality, the receiver's locking point, as a function of SNR, depends on the modulation method, the receiver architecture, and implementation. For any given device, this locking point is basically fixed and hard to optimize. It is our understanding that in most systems the receiver does in fact work at a higher SNR than it needs for signal-locking

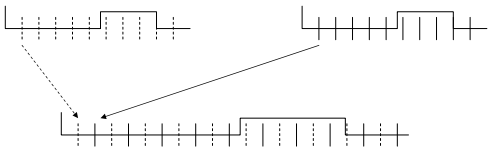

Fig. 7. Interleaving of two copies of the same incoming frame.

[Fin04], thus assumption (a) is reasonable.

Let ΔSNR denote the difference between the SNR needed for error-free communication and the SNR needed for signal lock on. Figure 6 shows how the reading distance increases as a function of the ΔSNR. The number of retransmissions appears in brackets. The number of retransmissions is determined by the minimum number of repetitions that give at least the same BER as that given by a 10dB signal. The formula to calculate BER as a function of SNR was taken from digital communication theory [Pro95]. The majority's calculations were done using elementary combinatorics.

Figure 6 shows that for a leech receiver with a ΔSNR of 10dB can increase the reading distance by another 30% over the distance achieved with a stronger current and larger antenna. The number of retransmissions that are needed is relatively small (at most 5). In case the ΔSNR is larger, better distances will be achieved.

Notes: 1) This method is only possible if the leech hardware supports our assumptions. 2) In order to implement this method, the attacker needs good programming knowledge, and access to the receiver driver (in the NFC device).

2) Signal-processing-based retransmissions: Our second method uses custom digital signal processing at the leech, and requires much more knowledge from the attacker. Again, the leech causes the card to retransmit each frame K times. The leech signal processing (hardware or software) interleaves the repeated frames into a jumbo frame, as shown in Figure 7. Filtering the jumbo frame with a new filter, which has a lower bandwidth, will improve the SNR.

Note that this technique works because the noise is a random process, and the sample times have no

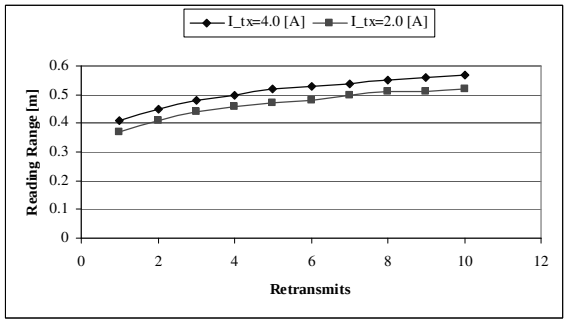

Fig. 8. distance as a function of interleave retransmit modification.

effect on such a process.

Figure 8 shows how using the interleaving methods with retransmitted frames can increase the reading range. We can see that with $K = 16$ retransmissions, the reading range increases by 40% to about $55cm$.

D. The Complexity of Building the Leech

Building a leech is quite similar to building a ghost. Figure 9 shows the basic schema structure of a leech using NFC device: wrap a magnetic coupling around the NFC device, using a looped wire. In transmission operations, the gain stage amplifies the outgoing transmitted signals to a high-power-signal. In receive operations the gain stage amplifies the weak received signals to the level required by NFC device and filters out-of-band noises. The gain stage is connected to an antenna with optimal size, which transmits and receives signals to/from the card.

E. A Comparison of Leech Designs

Table I summarizes the achievable leech-card range versus the effort, cost and attacker knowledge needed to build a leech using NFC device. [1]

The table clearly shows that the largest range increase is achieved by amplifying the current and

[1]The attacker can build a superior leech without using NFC device, by optimized the hardware and software algorithms. Although this option exist it's less time and cost to build a leech with NFC device.

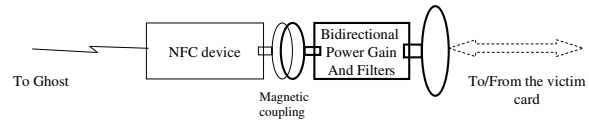

Fig. 9. Building a Leech using an NFC device.

using an optimum antenna size. The "Current + Antenna" method is fairly simple and leads to a very simple attacker profile: medium knowledge in RFID technology, a very small budget and easily obtained components.

The two other methods, which build on retransmitting the frame over and over, require a more sophisticated attacker and a substantial budget for the signal processing method. These methods can be the differentiation to wider leech usability in much more public places, although the benefits are not as great as the improvements achieved by "Current + Antenna" method

VI. Weaker attacks and Counter measures

A. Weaker attacks

The relay attack shows how the security and privacy assumptions of the near-field-communication break despite strong protocol protection mechanisms (like challenge-response authentication and data encryption). However, contactless smartcards are much more vulnerable in case these mechanisms are not used.

The worst attack is when there is no protection at all and the attacker can modify, copy, or do whatever he likes with the card without any notification to the card holder. A close second is an off-line card duplication attack: In case the card doesn't use reasonable authentication mechanisms, the card's data can be easily copied (e.g., using RFDump [GW04]) into the attacker's NFC device and used by the attacker. Another possible attack is replay: using sniffer techniques the attacker can record the traffic between the reader and the card and replay the data when needed.

Method	Property			
	Max Distance	Extra Cost (beyond NFC)	Availability	Attacker Knowledge
Standard	10 cm	0$	High	Low
Current + Antenna	40 cm	$< 100$$	High	Medium
Current + Antenna + Software	50 cm	$< 100$$	Medium	High
Current + Antenna + Signal-Processing	55 cm	$> 5000$$	Low	Very High

TABLE I

SUMMARY: LEECH TO TAG EFFORT AND BENEFIT

B. Possible Counter measures

We can classify the counter measures into two main kinds of protections: protecting the card owner and protecting the system.

A Faraday-cage approach to shield the contactless smartcard against malicious attackers can be used by the card holder as a protection method. At least one company already offers a Faraday-cage-based product for privacy purposes [mCl04]. A home-made Faraday cage can be created by wrapping the card in aluminum foil.

Activation by the card holder is an alternative method. In this method the card is active only when a the card owner takes some action, using an on-card mechanical or biometric actuator (e.g., an on-card push button or fingerprint scanner). Having an on-card input mechanism would force the card owner to take action to activate the card—and eliminate the attacker's ability to silently use a victim card.

System protections can be based on a Two-Factor-Authentication architecture, i.e., (a) something you have and (b) something you know (or something you own). For instance, besides presenting the smartcard, the user would need to type in a PIN code on the reader. Unfortunately such a system eliminates some of the convenience the contactless system can offer.

VII. RELATED WORK

A broad overview of RFID technology can be found in T.A.Scharfeld's thesis [Sch01]. This thesis analyzes RFID theory, standards, regulations, environment influence, and implementation issues.

Free attack/analysis tools that detect RFID cards and show their meta information are available from the RFDump web site [GW04]. These tools are able to display and modify the card data, such as the card ID, card type, manufacturer etc.

A discussion of smartcard operation in hostile environments is presented in [GSTY96]. The article describes interactions between the smartcard and a point-of-sale system, focusing on privacy and trust issues.

The trust model between the smartcard and the reader is described in [SS99]. The article discusses the security model of a smartcard system, independently of its application.

Much of the effort in the smartcard industry, and in the research community, is focused on privacy issues in RFID technology (See [McC03]). The Smart Card Alliance white-paper [All03] describes how smartcard technology can help to protect privacy and ensure security in a ID system. Methods to protect users' profiles can be found at Eurosmart's website [EUR] for contact and contactless smartcards. A set protection profile for smartcard security, based on the ISO/IEC 15408 [ISO99] standard, is the product of the Smart Card Security User Group [SCS01], with members like: American Express, Europay International, JCB Co Ltd, MasterCard International, Mondex International, Visa International etc.

Juels, Rivest and Szydlo [JRS03] propose a blocking tag approach that prevents the reader from connecting with the RFID tag. Their method can also be used as malicious tool: In order to disrupt the Reader-to-Tag communication, their blocker tag actually performs a denial-of-service attack against the RFID reader protocol by using the "Tree-Walking Singulation Algorithm" in the anti-collision mechanism. Juels and Brainard

[JB04] propose a variant on the blocker concept which involves software modification to achieve a soft blocking tag.

[Wei03] and [SWE02] offer a "Hash-Lock" approach to low cost RFID devices which use a "lock/unlock" mechanism to protect against retrieving the RFID ID number. In the simplest scenario, when the tag is locked it is given a value (or meta-ID) y, and it is only unlocked by presentation of a key value x such that y = h(x) for a standard one-way hash function h.

Juels and Pappu [JP03] discuss the privacy implications of RFID-tags embedded in banknotes, with a scheme where banknote tag serial numbers are encrypted with a law-enforcement public key.

Juels [Jue04] proposed a formal security model for authentication and privacy in RFID tags, with a small amount of rewritable memory and very limited computing capability, in which a tag carries multiple, pre-programmed pseudonyms.

Recently, Bono et al. [BGS+05] showed a security analysis of an RFID device known as a Digital Signature Transponder (DST), which is used in car immobilizers and payent transponders. The authors have been able to reverse engineer a proprietary 40-bit cryptographic function embedded in these devices, to build an FPGA-based brute-force cryptanalysis system, and to emulate the DST's RF behavior.

VIII. Conclusions

In our opinion, this work describes a real threat on contactless smartcard systems. The "Relay attack" causes the reader to identify a remote card, which is not the device that is presented. This fact breaks the hidden assumption that the physical medium is secure and that the identified card must be very close to the reader device.

Extending the reader to card range using our ghost and leech devices allows the victim card to be at an unlimited distance. Additionally, extending the reader to ghost range and the leech to card range significantly increase the attacker's options: Larger distances mean no physical contact and no eye contact or security-camera exposure.

We believe that attackers will appear when the financial gain is high enough. Low cost NFC technology will be on the shelves soon, and upcoming credit cards based on contactless smartcard present a real temptation and high gain for attackers. The combination of high availability, low cost and easy profits may well cause the "Virtual Pick Pocket" attack to appear "in the wild" before long.

References

[All03] Smart Card Alliance. Privacy and secure identification systems: The role of smart cards as a privacy-enabling technology. A Smart Card Alliance White Paper, February 2003. http://www.smartcardalliance.org/ .

[All04a] Smart Card Alliance. Press releases, 2003–2004. http://www.smartcardalliance.org/about_alliance/alliance_press.cfm .

[All04b] Smart Card Alliance. Industry news, 2003-2004. http://www.smartcardalliance.org/industry_news/industry_news.cfm .

[All05] Smart Card Alliance. Nist report, 2004-2005. http://www.smartcardalliance.org/alliance_activities/rfid_FAQ.cfm item 17.

[Atm02] Understanding the requirements of ISO/IEC 14443 for type B proximity contactless identification cards. Atmel Corporation: Application Note 2056A-RFID-08/02, 2002. http://www.atmel.com .

[BGS+05] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. http://rfid- analysis.org/DSTbreak.pdf , 2005.

[CEP04] Relating to the use of short range devices (SRD). CEPT 70-03, October 2004. http://www.ero.dk/documentation/docs/doc98/official/pdf/REC7003E.PDF .

[Com04] Nokia launches mobile RFID kit, 19 March 2004. http://www.computerweekly.com/Article129304.htm .

[ECM04] Near field communication (NFC). ECMA/TC32-TG19/2004/28; ECMA/GA/2004/67, June 2004. http://www.ecma- international.org .

[Eco02] Security technology: Where's the smart money? The Economist, pages 69–70, 7 February 2002.

[EEt04] Tests reveal e-passport security flaw, 30 August 2004. http://www.eetimes.com/sys/news/showArticle.jhtml?articleID=45400010 .

[ERC99] ERC report 69: Propagation model and interference range calculation for inductive systems 10 KHz - 30 MHz. European Radiocommunications Committee (ERC) within the European

Conference of Postal and Telecommunications Administrations (CEPT), February 1999.

[EUR] EUROSMART. The voice of the smart card industry. http://www.eurosmart.com/ ; http://www.eeurope- smartcards.org/ .

[FCC01] Radio frequency devices. FCC Part 15, 2001.

[Fin03] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons, 2003.

[Fin04] K. Finkenzeller, 2004. Personal communication.

[Foc00] T. W. H. Fockens. NEDAP - system model for inductive ID systems. NEDAP R&D, Groenlo, The Netherlands, October 2000. http://www.autoid.org/2001_Documents/WG3_SG1/WG3SG1_0533_LblTstr_Model.doc , http://www.rfid- handbook.de/downloads/ .

[GSA04] U.S. government smart card handbook. Office of Governmentwide Policy, General Services Administration, February 2004.

[GSTY96] Howard Gobioff, Sean Smith, J. Doug Tygar, and Bennet Yee. Smart cards in hostile environments. In *Proc. Workshop on Electronic Commerce*, 1996.

[Gua04] Guardian Unlimited. The magic of touch, 15 July 2004. http://www.guardian.co.uk/online/story/0, 3605, 1260978, 00.html .

[GW04] Lukas Grunwald and Boris Wolf. RFDump, 2004. http://www.rf- dump.org/ .

[ISO95] Identification Cards-Integrated Circuit(s) with Contacts - Part 4: Interindustry Commands for Interchange. ISO/IEC 7816-4, September 1995.

[ISO99] Common criteria for information technology security evaluation. ISO/IEC 15408; CCIMB-99-031, CCIMB-99-032, CCIMB-99-033, August 1999. http://www.csrc.nist.gov/cc .

[ISO00a] Identification cards – contactless integrated circuit(s) cards – proximity cards - part 1 to 4. ISO/IEC 14443, 2000.

[ISO00b] Identification cards – contactless integrated circuit(s) cards – vicinity cards. ISO/IEC 15693, 2000.

[ITU00a] ITU-R recommendation P.372-7 "RadioNoise". The International Telecomunication Union Radiocommunication sector, 2000.

[ITU00b] Technical and operating parameters and spectrum requirements for short-range radiocommunication devices. ITU-R 213/1, 2000.

[JB04] A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap, April 2004. http://theory.lcs.mit.edu/~rivest/ .

[JP03] A. Juels and R. Pappu. Privacy protection in RFID-enabled banknotes. In R. Wright, editor, *Proc. Financial Cryptography*, 2003.

[JRS03] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *Proc. 8th ACM Conf. Computer and Communications Security (CCS)*, pages 103–111, May 2003. http://theory.lcs.mit.edu/~rivest/ .

[Jue04] Ari Juels. Minimalist cryptography for low-cost RFID tags. In *Fourth Conference on Security in Communication Networks*, Amalfi, Italy, September 2004.

[McC03] D. McCullagh. RFID tags: Big brother in small packages. CNet, January 2003. http://news.com.com/2010- 1069- 980325.html .

[mCl04] mCloak: Personal / corporate management of wireless devices and technology, 2004. http://www.mobilecloak.com .

[Pro95] John G. Proakis. Performance of the optimum receiver for memoryless modulation. In *Digital Communications*, pages 257–282. McGraw-Hill, 1995.

[Sch01] Tom A. Scharfeld. An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, August 2001.

[SCS01] Common criteria for information technology security evaluation. Smart Card Security User Group - Smart Card Protection Profile (SCSUG-SCPP), September 2001.

[Shu01] A. Shukla. Feasibility study into the measurement of man-made noise. Radiocommunications Agency (DERA), UK Ministry of Defence, AY 3952, March 2001.

[SS99] B. Schneier and A. Shostack. Breaking up is hard to do: Modeling security threats for smart cards. In *First USENIX Symposium on Smart Cards, USENIX Press*, October 1999.

[SWE02] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES), LNCS 2523*, pages 454–470. Springer-Verlag, 2002.

[TI03a] Constructing a 1000 x 600 HF antenna. Technical Application Report 11-08-26-007, Texas Instruments, August 2003. http://www.ti- rfid.com .

[TI03b] HF antenna design notes. Technical Application Note 11-08-26-003, Texas Instruments, September 2003. http://www.ti- rfid.com .

[TI04] HF antenna cookbook. Technical Application Report 11-08-26-001, Texas Instruments, January 2004. http://www.ti- rfid.com .

[TI05] Rfid homepage. Texas Instruments, 2005. http://www.ti- rfid.com .

[Wei03] Stephen A. Weis. Security and Privacy in Radio-Frequency Identification Devices. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, May 2003.

[WSRE04] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Computing, LNCS 2802*, pages 201–212. Speinger-Verlag, 2004.

[Yos05] J. Yoshida. Euro bank notes to embed RFID chips by 2005. EE Times, 19 December 2005. http://www.eetimes.com/story/OEG20011219S0016 .

APPENDIX

A. Near Field Communication (NFC) - Operating Principle

As we have mentioned before, contactless smartcards are powered by the reader. The smartcards communicate with the reader via an inductive magnetic coupling of the reader's antenna to the card's antenna. The two loop antennas effectively form a transformer ([Atm02]). This type of communication is known as "Near Field Communication", or NFC. Figure 10 illustrates the magnetic field in the NFC inductive coupling devices.

The reader produces an alternating magnetic field by generating a sinusoidal current through the reader's antenna loop. When the tag enters this alternating magnetic field, an alternating current (AC) is induced in the tag's loop antenna. The tag's integrated circuit (IC) contains a rectifier and a power regulator to convert the AC into direct current (DC), which powers the integrated circuit.

The reader modulates the RF field to send information to the tag. The tag contains a demodulator to convert the modulation into digital signals. The data from the reader is decoded and processed by the tag's integrated circuit (IC).

The tag transmits information back to the reader by modulating the loading on the tag's antenna (e.g., by varying the impedance of a resistor). This load modulation, as it is called, causes changes to the current in the reader's antenna. Assuming that the tag is close enough—the reader can sense the tag's load modulation and demodulate. The tag uses a sub-carrier frequency for the load modulation, which allows the reader to filter the sub-carrier frequency off its antenna and decode the data.

B. Simulation Parameters

As mentioned before, we used the NEDAP model to estimate the leech performance. The NEDAP model is controlled by a large number of system parameters that need to be set.

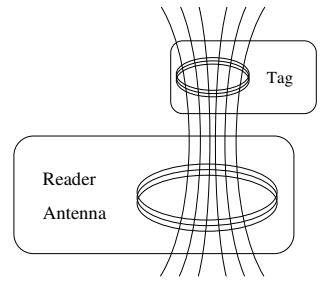

Fig. 10. Near Field Communication via Inductive coupling.

The parameters are divided into four groups: (1) global system parameters, (2) reader parameters, (3) tag parameters, and (4) environment parameters. Below we describe the parameters which we used in the leech simulations whose values are different from the default NEDAP-supplied values.

1) Global System Parameters:

- The magnetic field limit at a distance of 10 m was set to -4.34 [dBμA/m], which is generated by a reader with transmit power of 100mA.
- The data bandwidth was set to 212 KHz. This was derived from the load modulation parameters: ISO 14443 Type A uses ASK modulation and Manchester coding. ISO 14443 Type B use BPSK modulation and NRZ-L coding.
- The sub-carrier frequency was set to 847KHz, according to[ISO00a].

2) Reader Parameters: The dimensions of the rectangular reader antenna loop were set to 10 cm$\times$10 cm. We assumed that the reader antenna loop consists of a single winding.

3) Tag Parameters: The dimensions of the rectangular tag antenna were set to 5 cm$\times$8 cm, which are the sizes of typical credit card.

4) Environment Parameters: The external noise level was set to 24 [dBμV/m/Hz], flat over the receiver bandwidth (See also Section C below).

We set the parameter controlling the precision of the results to 1cm.

C. Noise Models for Ghost-to-Reader D Estimation

1) Man-Made-Noise: Standard noise are available from several sources su [ITU00a], [ERC99] and [Shu01]. Using the [ITU00a] model, the RMS[2] field strength i by:

$$F_{am}(f_{\mathrm{MHz}}) = c - d\log_{10} f$$

and

$$Ext_{\mathrm{noise}}(f_{\mathrm{MHz}}) = F_{\mathrm{am}} - 95.5 + 20\log_{10} f_{\mathrm{MHz}} + 10\log_{10} B_{\mathrm{Hz}}$$

For a "Business" environment the model gives parameter values of $c = 76.8$ and $d = 27.7$. Note that many parameters effect the estimated man made noise (location, time, etc). This calculation uses average values, which are assumed to be reasonable for a "typical" business environment. Using the ISO 14443 center frequency of $f = 13.56$ MHz and bandwidth of $B = 1$ Hz we compute that the estimated man-made-noise is:

$$Ext_{\mathrm{noise}} = -27.41[\mathrm{dB}\mu\mathrm{V/m/Hz}]$$

A practical contactless smartcard system, with a few centimeters reading range, and an antenna current of up to 100 mA gives a maximum field strength of $H_{\max} = -4.3$ [dBμA/m/Hz] at 10 m [TI05].

The above estimated man-made-noise and maximum field strength are the inputs for the range calculations. In order to calculate the range from which a ghost can operate, two formulas are used: The first formula answers the question how strong must the received signal be with a given SNR and noise level. The second formula is used to calculate the signal attenuation [3] depending on the distance from the reference point.

The calculations are based on the NEDAP [Foc00] model. The model takes into account three kinds of noise: external, internal and narrow-band

[2]Root Mean Square

[3]Due to the fact that the device transmit power give by his magnetic field strength at a distance of 10 meters, the calculation use far-field attenuation model.

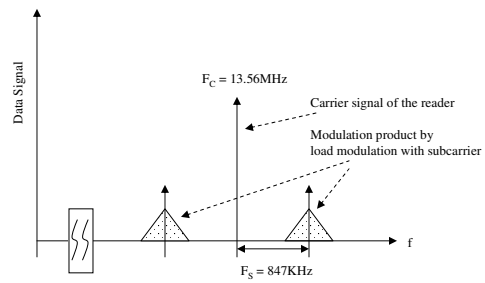

Fig. 11. Load Modulation - side band.

noises. The internal noise is created by the internal reader component and mostly affects the reader. The narrow-band noise is generated by external devices and has relatively low energy comparing to the external noise. Using only the external noise, which is the dominant noise in the model, gives the following formula:

$$H_{\mathrm{eff}}(SNR_{\mathrm{ext}}, BW, Ext_{\mathrm{noise}}) = SNR_{\mathrm{ext}} + (Ext_{noise} - 51.5) + 10\log_{10} BW,$$

where SNR_{ext} is the requested Signal to Noise Ratio in dB, Ext_{noise} is the external noise in dBμV/m/Hz, BW is the bandwidth in Hz and H_{eff} is the minimal magnetic field strength in dBμA/m. The constant 51.5 is equal to $20\log_{10} 375$, 375Ω is the air impedance (the ratio between electronic-field and magnetic-field is the air impedance, in standard conditions).

The physical behavior of the far field electromagnetic wave defines the second formula. In the far field, the attenuation is log-linear with a slope of $20\frac{dB}{Dec}$. The H_{max} parameter is a point on the log-linear line at a distance of $10m$. The following formula is the result of the linear-slope and point, after pulling out the log:

$$Distance(H_{eff}) = 10^{\frac{(H_{max}+20)-H_{eff}}{20}}$$

Given these formulas and setting $SNR_{ext} = 10[dB]$, $BW = 106,000[Hz]$ (receiver bandwidth), and $Ext_{noise} = -27.41[dB\mu V/m/Hz]$ shows that the maximal distance between the reader and the ghost can be more then 50 meters. Weis et al. [WSRE04] note that the threat on RFID technology is to monitor reader-to-tag

broadcast from a long-range, which may be picked up from hundred of meters away. Such results can only be archived under the following conditions: higher transmission power (above $H_{max} = 42[dB\mu A/m/Hz]$ at 10 m, which is the regulation limit), a low noise environment, and using a sensitive receive antenna. Since the ghost-to-reader distance is not the main challenge for the attacker, we did not suggest using special equipment to increase the ghost range beyond 50 m.

2) RFID system interferences: An alternative noise model is based on interference from other RFID sources transmitted in the same magnetic strength power. Assume that the ghost is trying to communicate with a reader, R1, which is at distance $x1$. A second reader, R2, is located at distance $x2 > x1$. The question is what is the relation between $x1$ and $x2$ which still allows the ghost to communicate with R1, which needs an SNR of 10 dB, despite the interference from R2. Assuming that both $x1$ and $x2$ are in the far-field, the attenuation is $20\frac{dB}{Dec}$. The difference between the received signals power, ΔP, should be at least the required SNR, 10 dB. These inputs give a ratio of: $x2 = x1 \times 10^{\frac{10}{20}} \approx 3.16x1$.