Weaknesses of the ISO/IEC 14443 Protocol Regarding Relay Attacks

Wolfgang Issovits and Michael Hutter
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
Emails: Wolfgang.Issovits@gmail.com, Michael.Hutter@iaik.tugraz.at

***Abstract*—RFID and NFC are widely spread contactless communication systems and are commonly used in security-critical applications such as payment and keyless-entry systems. Relay attacks pose a serious threat in this context that are not addressed by most of the RFID applications in use today. The attacks circumvent application-layer security and they cannot be prevented by the usual cryptographic primitives. In this paper, we will present a practical implementation of a relay attack based on systems using the widely used ISO/IEC 14443 standard. We use an off-the-shelf mobile phone and a self-developed RFID-tag emulator that can forward RFID communication over a Bluetooth channel. We will show that the attack succeeded and discuss various methods how to exploit certain mechanisms of the ISO protocol to increase the chance for a successful attack. We will also give recommendations to protect against relay attacks in practice while still complying to the ISO standard which is not considered by most of the proposed countermeasures given in literature.**

I. INTRODUCTION

Radio Frequency Identification (RFID) is a contactless communication technology and includes a wide range of different applications. The technology differs in various characteristics such as physical appearance, frequency, reading range, operation mode, coupling method, and power supply of the transponder.

The basic concept of an RFID system can be seen in Figure 1. Every RFID system consists of a reader and a transponder. The reader creates an electric or magnetic field that allows a communication with transponders in the proximity. Next to the communication (data exchange), this field can be used to supply power and a clock frequency to transponders. Passive transponders, for example, make use of that field to extract the power whereas active transponders provide an own power source (*e.g.* a battery) [5].

With the wide distribution of RFID systems, attacks on those systems evolved. Among others there exist so called relay attacks. During a relay attack, an attacker establishes a channel between two legitimate parties, without them being aware of the relay. Relay attacks on RFID systems involve two devices. One device impersonates the reader to the transponder, and is called *mole*. The other device impersonates the transponder to the reader, and is called *proxy*. Those two devices are connected by a relay channel [7].

There exists a variety of different standards for RFID systems. One of the most common standards for proximity

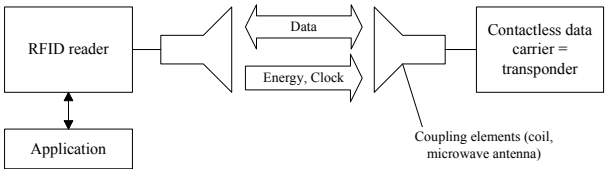

Fig. 1. Basic concept of an RFID system [5].

cards, which have a transmission range of approximately 15 cm [5], is the ISO/IEC 14443 specification. It is used by major RFID systems like MIFARE [18], Calypso [2], or electronic passports. NXPs MIFARE system, for example, is used for transit systems in over 650 cities worldwide and had an estimated market share of 75 % in 2010 [16]. Due to the wide distribution, this standard is a very interesting target for attackers.

However, the standard does not introduce any security measures against relay attacks. Moreover, it defines a number of mechanisms that can be exploited by such attacks. One of those is the Frame Waiting Time (FWT, the maximum response time for the RFID target), which can be chosen up to 4.95 seconds. Also it defines recovery functionality (Negative Acknowledges, NAKs), which gives an attacker additional time for a relay. Further it allows the target to request additional computation time using Waiting Time eXtensions (WTXs).

In this paper, we show that the exploitation of those mechanisms is possible and significantly increases the chances for the attacker. We have been able to perform successful relay attacks on the ISO/IEC 14443 standard, which is widely used especially for security-crucial applications, using low-cost hardware. Therefore, we conclude that countermeasures need to be developed. As the ISO/IEC 14443 standard is already widely used, we propose countermeasures that are compliant with the standard.

The paper is organized as follows. In Section II, related work is given. Section III describes the ISO/IEC 14443 protocol standard used throughout the paper. In Section IV, we introduce into relay attacks in general. The hardware setup of our experiments and implementation details are given in Section V and Section VI. Results are presented in Section VII. Section VIII contains a discussion to secure ISO/IEC 14443 systems before we finish with a conclusion in Section IX.

 DOI: http://dx.doi.org/10.1109/RFID-TA.2011.6068658

II. RELATED WORK

Kfir and Wool [14] already described a possible setup for a relay attack. One of the first practical attack implementations was done by Hancke in 2005 [7]. He implemented a relay attack connecting proxy and mole through an UHF antenna and relayed the analogue data between the two devices. For the relay channel, he reached an introduced delay of only 15-20 µs. Note that such small delays are only possible if the communication is relayed as analogue data. If the data is digitized and forwarded as binary data, the additional processing time introduces a significant additional delay requiring much more transmission time.

Recently, Francis et al. [6] presented a practical relay attack on NFC mobile phones. They used two NFC mobile phones as proxy and mole and established a Bluetooth link in order to relay data in the 2.4 GHz frequency band. However, although the attack worked as a proof of concept, it lacks in the fact that the required Unique Identifier (UID) from off-the-shelf mobile phones cannot be changed which restricts the attack to only a limited number of applications.

Weiss [23] obtained similar results during his experiments. He implemented a relay attack using NFC mobile equipment in the course of his master's thesis and reached delays of about 50 ms. His setup includes a USB-based NFC device as a relay proxy that requires the connection with a PC, which might not be practical for a real life scenario. Moreover, he did not exploit protocol mechanisms for his attack.

Next to attacks, a number of countermeasures against relay attacks have been proposed so far where distance-bounding techniques seem to be one of the most promising solutions. Hancke and Kuhn [8] proposed a distance-bounding protocol based on a single-bit challenge-response scheme. The protocol makes use of an additional ultra-wide band (UWB) channel because Hancke and Kuhn stated that accurate distance bounding is not possible over the 13.56 MHz communication link. However, an additional UWB channel is not available in current RFID systems and would cause significant additional costs.

Other proposals have been made by Reid et al. [21] and Munilla et al. [15]. Their proposed protocols expect the response in predefined clock cycles. This approach is vulnerable to overclocking attacks [9] and might cause problems with compatibility issues with existing standards. Implementations on the transponder may vary significantly and sending the response within a defined clock cycle might not always be possible.

So far no one has addressed the security issues of the ISO/IEC 14443 standard and performed a relay attack by exploiting those issues. Furthermore, to the authors knowledge, no one has proposed countermeasures that are compliant with the standard.

III. THE ISO/IEC 14443 STANDARD

The ISO/IEC 14443 standard describes the operation method and parameters for proximity-coupling smart cards. Those cards operate in a range of up to approximately 15 cm.

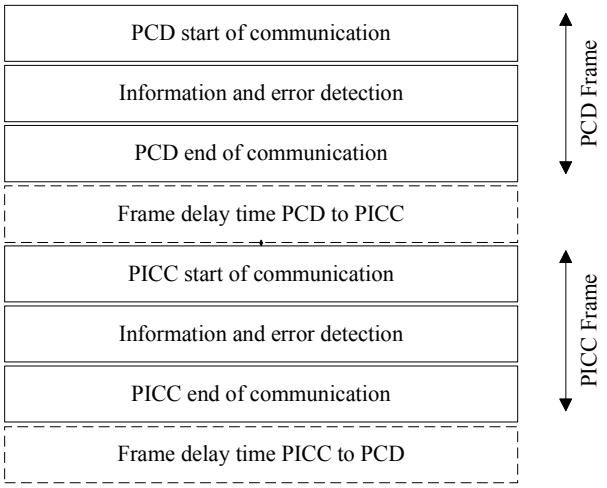

Fig. 2. Sequence of a frame pair as defined by ISO/IEC 14443.

We will refer to the standard only as ISO/IEC 14443 and will describe the newest version of the standard released in 2010.

The standard labels the reader as a Proximity Coupling Device (PCD) and the transponder as a Proximity Integrated Circuit Card (PICC). We will use the terms PCD and PICC whenever we refer to the reader and the transponder of an ISO/IEC 14443 system.

The standard is split into four parts. The first part covers the physical characteristics of the PICC [10]. The second part specifies the characteristics of the fields to be provided for power and bi-directional communication between the PCD and the PICC [11]. The third part defines the routines for the initialization of the PICC as well as an anticollision routine for multiple PICCs [12]. The fourth and last part defines a half-duplex block transmission protocol satisfying special needs for contactless environments. It also defines the activation and deactivation sequence of this transmission protocol [13]. Note that the higher parts are designed to be used in conjunction with the lower parts.

The ISO/IEC 14443 standard does not define any security mechanisms as the protocol stack is completely transparent. For our implementation only layer 3 and layer 4 are relevant. We will describe the important characteristics briefly in the following subsections.

A. ISO/IEC 14443 Part 3: Initialization and Anticollision

The third part of the standard first defines how the polling for new PICCs in range is handled. It also specifies the initial phase of the communication and methods to deal with multiple PICCs within the reading range (anticollision). The standard defines two types of PICCs, namely A and B. We will only deal with type A cards for the rest of the paper.

ISO/IEC 14443 communication follows a request-answer scheme, which makes it mandatory that frames are always transmitted in pairs. The first frame is sent by the PCD to the PICC, and the second frame by the PICC to the PCD. The delay between those two frames is defined as the frame

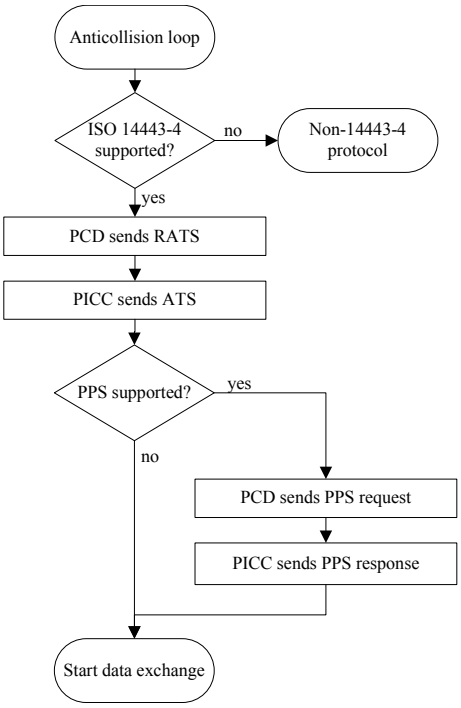

Fig. 3. Activation sequence of Type A PICC after anticollision [5].

delay time (FDT). Figure 2 illustrates the basic communication concept.

During anticollision, the commands REQA, SELECT, and ANTICOLLISION are used by the PCD. Those commands request a FWT of 91.15 µs or 86.43 µs, depending on the last bit of the command. Those low FWT only apply during anticollision. The FWT for the transmission protocol is agreed on during the protocol activation sequence. For more details on initialization and anticollision we refer to part 3 of the ISO/IEC 14443 specification [12].

B. ISO/IEC 14443 Part 4: Transmission Protocol

1) Protocol Activation: The ISO/IEC 14443 standard defines a half-duplex block transmission protocol, which considers special needs for contactless environments. Type A PICCs need to be activated before starting the transmission of data. This activation sequence can be seen in Figure 3 and is in detail described in part 4 of the standard [13], [5].

The activation sequence consists of several message exchanges between the PCD and the PICC to agree on the used parameters. The most important parameter for our implementation is the Frame Waiting Integer (FWI). The PICC defines which FWI it supports. The resulting FWT is calculated by

$$FWT = (256 \times 16/f_c) \times 2^{FWI}. \quad (1)$$

The FWI is defined in the range of 0 to 14 which results in a minimum FWT of 302 µs and a maximum FWT of 4.95 seconds.

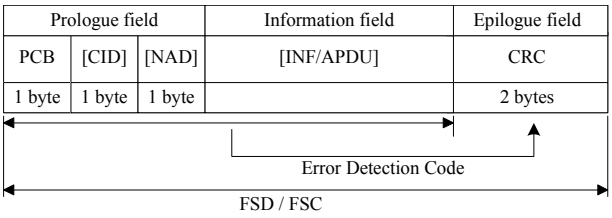

Fig. 4. Structure of an ISO/IEC 14443-4 block [13].

2) Protocol Blocks: The protocol defines three types of blocks that are exchanged. I-blocks are used to send information for the application layer, R-blocks are used to send positive or negative acknowledgments, and S-blocks are used to exchange control information between PCD and PICC. The basic structure of a block can be seen in Figure 4. FSC (Frame Size Card) and FSD (Frame Size Device) denote the size of the complete block.

a) Prologue Field: The prologue field contains the mandatory Protocol Control Byte (PCB) and the two optional bytes for CID and NAD. The CID field is used to address one of multiple active PICCs. It also contains two bits that can be used as power level indicator. The NAD field is used to build up and address multiple logical connections. The PCB byte defines which of the 3 block types is following.

b) Information Field: The information field is optional and of variable length. It contains application data for I-blocks and non-application data and status information for S-blocks. The length is calculated as the total number of bytes minus the prologue and the epilogue field.

c) Epilogue Field: The epilogue field contains a two byte error detection code (CRC_A) for the transmitted block. It is used to detect errors that occurred during the transmission. The exact calculation of the CRC_A is defined in the appendix of the ISO/IEC 14443-3 specification.

3) Waiting Time Extensions: Waiting time extensions (WTXs) are a way for the PICC to request additional time for complex or time consuming computations. They are sent as an S-Block with a one byte information (INF) field. The INF field contains two bit as power level indicator and six bit for the waiting time extension multiplier (WTXM). The standard defines the WTXM in the range 1-59 [13]. Given the WTXM, the PCD grants a temporary FWT calculated by

$$FWT_{tmp} = FWT \times WTXM. \quad (2)$$

However, the temporary FWT can never exceed the maximum FWT of 4.95 seconds. Note that it is possible to request several WTXs in a row. Every WTX request, if received correctly, is answered with a WTX response.

4) Error Detection and Recovery: The standard also defines a recovery procedures using Negative Acknowledges (NAKs). Whenever the PCD receives an erroneous response from the PICC, or does not receive a response in time, it can request a retransmission by sending a NAK. Note that this recovery

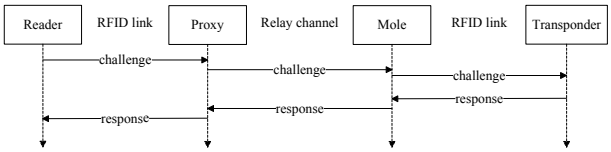

Fig. 5. Possible scenario for a relay attack on an RFID system.

mechanisms is optional and the number of retransmission tries depends on the implementation of the PCD.

IV. RELAY ATTACKS

A relay attack is any attack, where the attacker relays information between two legitimate parties, without them being aware of the relay. The two parties are made believe that the information is exchanged on a legitimate RF channel, but it is actually forwarded through a relay channel of any transmission medium, created by the attacker.

The concept of relay attacks already exists for several decades and can be performed in many different environments. One of the first relay attacks was introduced by Conway as the grandmaster chess problem [3]. An unskilled chess player could play a game of correspondence chess against two grandmasters simultaneously. If he plays white in one, and black in the other game, he just copies every move of the grandmasters and let them play against each other. He would then either win one game, or draw both.

A. Relay Attacks on RFID Systems

Two devices are needed for our relay attack, a mole and a proxy, which are connected through a relay channel. A possible scenario of such an attack is presented in Figure 5. Transponder and mole as well as reader and proxy are connected through a conventional RFID link. Mole and proxy communicate through a relay channel. The reader sends a challenge to the proxy, that only the transponder can solve. The proxy immediately forwards the challenge to the mole which then sends it to the transponder. The transponder computes a correct response and sends it to the mole. Note that the transponder assumes that it is communicating directly with the reader. The mole then forwards the response to the proxy, which then sends it to the reader.

The scenario described above is a passive relay attack because no data is changed by the attacker. Especially for identification purposes, there is usually no need to change any of the data. An attack could make the reader presume that the genuine transponder is right in front of it, although it is actually in another room or even further away. This attack is very powerful because there is no need to deal with the cryptographic primitive itself. A protocol can be secure in a mathematical sense while a practical relay attack could still be performed, which makes such attacks powerful and hard to detect [9].

1) Introduced Delay: To see the additional delay introduced by a relay attack we look at Figure 6. The communication between the reader and the proxy, as well as the computation

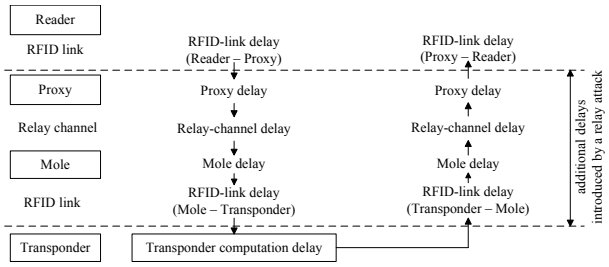

Fig. 6. Delays introduced during a relay attack.

time of the transponder, can be ignored as those delays would also occur during a "conventional" communication. For the introduced delay, we sum up the remaining delays, and multiply them by two, because the data needs to travel the distance twice.

$$\begin{aligned}\text{introduced delay} = (&\text{proxy delay} + \\ &\text{mole delay} + \\ &\text{relay-channel delay} + \\ &\text{RFID-link delay}) \times 2.\end{aligned} \tag{3}$$

V. HARDWARE SETUP

A. The Proxy

The proxy must impersonate the real PICC and therefore must be capable of operating as an RFID target. It has to be fast, flexible, and needs to support ISO/IEC 14443-A functionality.

1) RFID-Tag Emulator Platform: We decided to use an RFID-tag emulator that provides programming capabilities. This allows us to perform passive as well as active relay attacks by allowing the modification of relayed data by the proxy. The used tag emulator is shown in Figure 7. It is only about double the size of a regular ID-1 card and runs completely independent with a portable power source (9 V battery). This makes the tag inconspicuous and very practical as a proxy.

As a processor, it features an ATxmega256 microcontroller from Atmel [1]. The microcontroller implements the ISO/IEC communication protocol and allows the transmission of higher-level Application Protocol Data Units (APDUs). Furthermore, it consists of a Printed Circuit Board (PCB) antenna, an analogue front-end, and several interfaces like USB (for monitoring and powering the device) or JTAG (for programming the microcontroller). A library already implements support for several RFID protocols such as ISO/IEC 15693/18000-3, ISO/IEC 18092, and for our experiments most importantly ISO/IEC 14443-A. The library allows changes in layers two to four of the ISO/IEC 14443 protocol and therefore the UID of the tag can be changed to any value (4, 7, and 10 byte UIDs are supported).

The tag emulator also provides an additional interface for individual adaptors. It allows other boards to be attached to it and to communicate with the microcontroller. We made use of this interface and attached a board with a Bluetooth module.

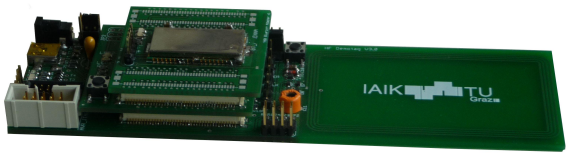

Fig. 7. Tag emulator used as a relay proxy.

This Bluetooth module can be accessed through an Universal Asynchronous Receiver Transmitter (UART) interface.

2) The BTM-222 Bluetooth Module: We used the BTM-222 Bluetooth module from Rayson [20]. It is a class 1 (+18 dBm) module that supports Bluetooth version 2.0, Enhanced Data Rate (EDR) by providing up to 3 Mbps, and several interfaces including USB and UART. As soon as any device connects to the BTM-222, it forwards all the data that is received through Bluetooth to its interfaces and vice versa.

The BTM-222 has a Serial Port Profile (SPP) firmware that supports AT commands to configure the device. Most importantly we increase the baud rate to of the BTM to 115 200 bits/sec to get shorter delays over the Bluetooth channel. The complete set of AT commands and settings can be found in the datasheet of the BTM-222 [19].

B. The Mole

As a mole, we used the Nokia 6212 NFC mobile phone [17]. In fact, a mobile phone is a very likely mole for a real life scenario because it is inconspicuous. The Nokia 6212 runs Java applications using the Java Micro Edition (Java ME) platform. Java ME already includes libraries for Bluetooth and NFC communications and therefore makes the implementation easy to perform.

For the Bluetooth connection with the proxy we used the *javax.bluetooth* package. It provides all necessary listeners for device and service detection, as well as functionality for communication over the Bluetooth link.

For the NFC connection with the PICC we used the *javax.microedition.contactless* package. The available listeners support different target types, one of them being *ISO14443_CARD*, which we used for our experiment. After the target discovery, we used the *ISO14443Connection* class for the data exchange.

VI. IMPLEMENTATION

A. Testing Environment

We used an ISO/IEC 14443 compliant reader and tag to implement our testing environment. The reader was set to query for new tags every second (as it is *e.g.* in the case of access control applications) and sends a simple byte-size command after activating a tag. The used devices can be seen in Figure 8.

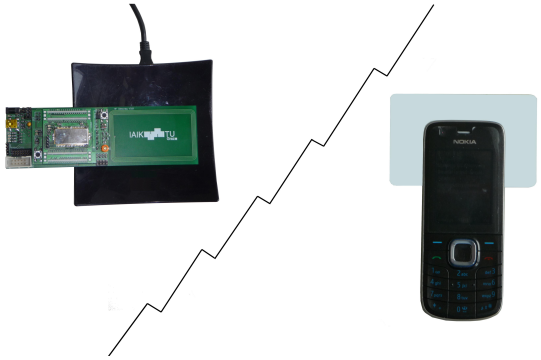

Fig. 8. Devices and setup of our relay-attack experiment.

B. Basic Concept

As we use high-level relay equipment, we introduce a delay in the region of milliseconds. Therefore, it is not possible to relay the anticollision and the activation sequence with our setup. However, in a real-world scenario this is not a stringent requirement since we can set the correct UID of the PICC on the tag emulator before starting the communication with the PCD. Thus, the initialization between PCD and the emulator is done without relaying communication which can be done very fast and within the given time margins (about 86 µs) of ISO/IEC 14443.

Figure 9 shows the basic concept of our implementation. The proxy is the commanding device (or master) of our relay attack. First, he requests the mole to fetch the UID of the PICC beforehand and stores the received UID. Note that the mole will keep the PICC activated after retrieving the UID, hence avoiding to perform the activation again afterwards. Second, the proxy emulates the PICC using the emulated UID in order to get activated by the PCD. After the initialization, the PCD will send ISO/IEC 14443 layer 4 commands to the proxy.

The transport protocol of layer 4 allows an FWT value between 302 µs and 4.95 seconds. According to the standard, the proxy can choose the value of FWI. Thus, an attacker has enough time to relay the application data even if the used relay channel provides slow data rates.

As a relay channel, we used Bluetooth in our experiments. Basically we send single characters over the Bluetooth interface from the proxy to the mole. In order to structure the communication, we defined a simple Comma Separated Value (CSV) based protocol to exchange commands and data between the two devices.

C. Exploiting the Waiting Time Extension (WTX)

The ISO/IEC 14443 standard defines a Waiting Time Extension (WTX) command. This command can be used by a PICC to request more time to prepare the response. In view of relay attacks, the command can be exploited to obtain more time to relay the data.

We therefore implemented a timer at the proxy that starts when the request of a PCD is received. This timer will expire before the default FWT expires and the PCD would assume an

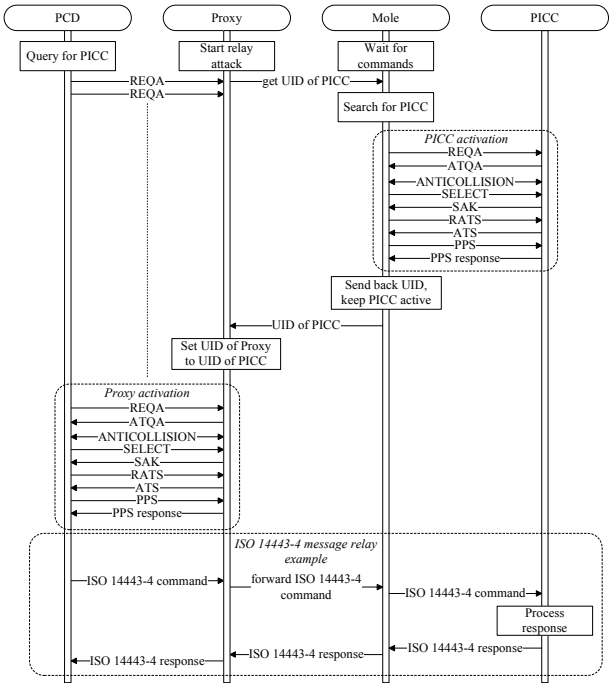

Fig. 9. General concept of our relay-attack implementation.

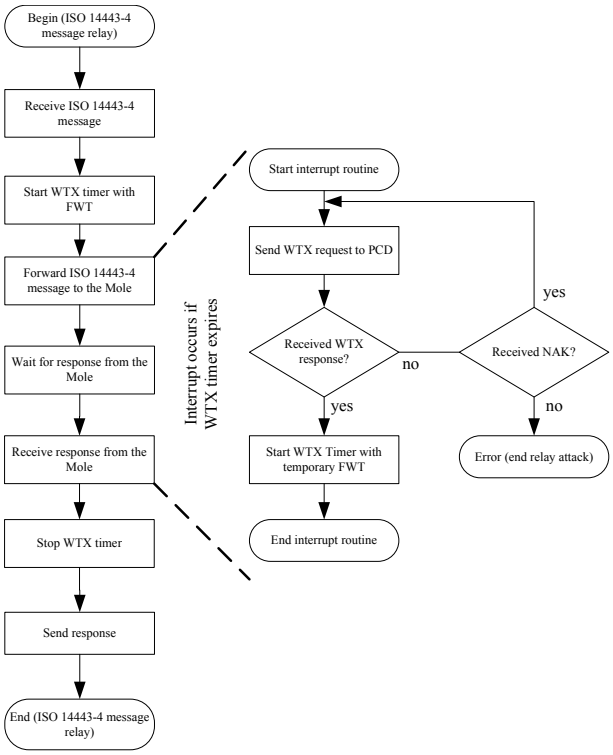

Fig. 10. Implementation of the utilization of WTXs on the proxy.

error. If the relayed answer of the PICC is received before the timer expires, the timer is stopped and the answer is forwarded to the PCD. If the timer expires before an answer is received, an interrupt routine is executed.

Within this interrupt routine, the proxy requests for a WTX to the PCD. The answer should be a WTX response, in which case the WTX request was received correctly. In case the answer is a NAK (Negative Acknowledge), the WTX request was not received correctly by the PCD. In this case, the proxy tries to retransmit the WTX command. If the PCD does not answer with the WTX response, for example with a DESELECT command, an error occurred and the relay attack is aborted. A flowchart of this procedure is shown in Figure 10.

D. Negative Acknowledge (NAK)

The recovery mechanism of the ISO/IEC 14443 protocol can also be utilized to increase the chance of a successful attack. If the PCD receives no response within the default FWT, it sends a NAK to the PICC (assuming the PCD implements a recovery mechanism). After that NAK, the PCD waits another FWT, before he expects a response. Figure 11 shows how an attacker can utilize this behavior.

The gain for an attacker depends on the number of recovery tries a PCD supports (NAKs sent). Therefore, the additional time can be calculated by

$$t_{additional} = FWT * NAK_{Sent\ by\ the\ PCD}\ . \qquad (4)$$

The exploitation of the ISO/IEC 14443 recovery mechanism is very straight forward. Because the PCD sends a NAK after the default FWT is over, the proxy simply ignores every message from the PCD until it receives the response from the mole. If the PCD is still sending NAKs (tries to recover the connection), the proxy can forward the response and the PCD will accept it.

VII. RESULTS

We have been able to successfully attack the described RFID system and could relay various data over the implemented Bluetooth channel. The distance between the PCD and the PICC has been several meters and can be performed theoretically up to 100 meters. In the following, we will describe the most significant results of our experiments.

A. Analysis of the Introduced Delay

For our experiment we used a data rate of 106 kbit/s. We sent a one byte challenge to the card, which answered with a one byte response.

In order to get a reference value of the given communication delay, we placed the genuine tag (PICC) directly on top of the reader antenna and measured the delay of 1000 challenge-response messages. The average delay for a challenge-response pair (after activation) was at 3 ms. This time was measured in C, which we used to control our PCD. It includes the time between the first bit sent and the last bit received, plus a slight overhead of the used C library.

After that, we measured the total delay for data transmission using our relay attack setup. For this, we measured 1000 challenge-response pairs. Furthermore, we measured the delay at the mobile phone, starting when receiving the first byte of the proxy and ending after sending the last byte of the

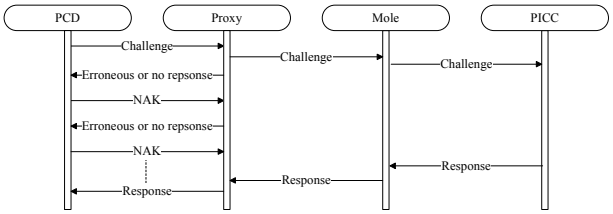

Fig. 11. Utilization of Negative Acknowledges (NAKs) for a relay attack.

response. Therefore, the mobile phone delay includes also the RFID delay and the computation time of the PICC. In addition, we measured the delay of the Bluetooth channel (including the delay of the Bluetooth modules at proxy and mole) by using a dedicated timer on the microcontroller. We started the timer before sending the first byte to the Bluetooth module and stopped it when receiving the last response byte. To adjust the results we subtracted the corresponding delays on the mobile phone. The results can be seen in Table I.

The results show that the main delay during the attack is introduced by the Bluetooth modules and the Bluetooth channel. The processing delay of the mobile phone and the proxy only introduce a rather small delay. We also observe that the total delays during a relay attack are significantly higher than those during a regular communication. However, even without any speed optimizations we achieved response times that succeed attacks we performed using various cards that are available and commonly used in many RFID systems.

In addition, note that the FWT can be chosen by the attacker and therefore the delay is not a crucial factor when attacking an ISO/IEC 14443 compatible system (that does not implement any countermeasures against these attacks). We could request a FWT of up to 4.95 seconds from the PCD which would give us plenty of time to perform the relay even on channels that allow a much farther communication distance such as given by GSM networks or the Internet.

B. Relay Attacks using WTX

We performed relay attacks by exploiting the WTX command as described in Section VI. For this attack, we introduced an artificial delay at the mobile phone of ten seconds. In a real scenario this delay could be caused through a large distance, a slow relay-channel medium, or bad connection between the mole and the PICC.

As expected, our ISO/IEC 14443 compliant reader accepts multiple WTX requests and grants new temporary FWTs. That way the PCD was stalled long enough for the mobile phone to send the response of the PICC. Theoretically an attacker could stall the PCD for an arbitrary long time by sending WTX requests.

Note that even if the PCD does not implement a recovery mechanism for timeouts (which is usually the case for Negative Acknowledges, for instance), our implementation will prevent timeouts by sending a WTX request before the default FWT times out.

TABLE I
MEASURED DELAYS FOR OUR RELAY ATTACK SETUP.

Delay Source	Average Delay [ms]	Minimum Delay [ms]	Maximum Delay [ms]
Mole (incl. RFID link + PICC)	9.7	9.0	38.0
Bluetooth Channel (incl. BT modules)	73.5	46.0	106.0
Proxy (incl. RFID link)	2.1	1.9	6.4
Total	85.3	57.6	150.4

C. Relay Attacks using NAK

We tried different numbers of recovery tries for our experiments and the PCD behaved as expected. Therefore, we gained additional time for our relay attack. The crucial factors here are the default FWT and the number of recovery tries performed by the PCD. As this additional time for the attacker may range up to several seconds, we conclude that the plain support of NAKs makes a system more vulnerable to relay attacks.

VIII. ISO/IEC 14443 Compliant Countermeasures

We already described some countermeasures against relay attacks in the Section II. None of those countermeasures are compliant with the ISO/IEC 14443 standard which is one of the most widely used RFID protocols in the field of access control, ticketing, electronic payment, and e-passports. In the following, we propose countermeasures to make such attacks more difficult to perform. Note that we are aware that none of the presented countermeasures will lead to full security. It should significantly increase the effort for possible adversaries to make an attack unattractive to perform. One requirement of all proposed countermeasures, however, is that it should be compliant to the standard so that an integration into existing solutions can be made with minimal costs.

A. Check Transmission Parameters

During the activation sequence of the protocol, a number of parameters are agreed on between PCD and PICC. Those parameters include for example the block size, the Frame Waiting Integer (FWI), and the data rate. As the protocol stack is transparent, the attacker can manipulate those parameters at both ends of the attack.

We assume that both, PCD and PICC, apply an encryption scheme (based on symmetric or asymmetric primitives) and the attacker cannot read or change the application data. In this case, the PCD and PICC can check if both agreed on the same parameters for the transmission. This wouldn't allow the attacker to use and manipulate different block sizes, frame waiting integers, or data rates necessary to perform a successful relay attack. Note that security-related tags already implement such encryption schemes for authentication purposes so that they can be simply reused to make relay attacks harder to perform.

B. Distance Bounding Protocols

Hancke and Kuhn [8] proposed that a secure distance measure is not possible using the ordinary RFID communication channel. We propose to use their, or any other secure distance bounding protocol, on layer 4 of the ISO/IEC 14443 protocol. Although we will not get accurate distance measurements, we certainly would be able to detect a number of relay attack implementations. Our experiment for example could easily be detected using a very simple distance bounding because of the high difference in regular and relay attack delays.

Those protocols could be implemented to still be compliant with the standard. Although the standard defines certain communication procedures, it does not state how to handle the application-layer data. Therefore, the PCD can measure the response time for the distance bounding protocol and handle the transfer according to the ISO/IEC 14443 standard. Afterwards, the PCD can decide if the answer was received in time or not and therefore distinguish between regular communication and an attack. The threshold for the response time should be chosen to reach a reasonable number of false rejections and false positives.

IX. CONCLUSION

In this paper, we showed that ISO/IEC 14443 compliant systems are especially vulnerable to relay attacks. The protocol stack is transparent and the transmission protocol offers mechanisms that highly increase the chance for a successful attack.

The attacking hardware used in our implementation is low-cost, inconspicuous, and practical for a real-life attack. Both proxy and mole are equipped with a portable power source and are connected through a Bluetooth channel that works up to 100 meters. As we also are able to change the UID of our proxy (which is not possible using conventional NFC-enabled mobile phones), the PCD cannot determine if it is communicating with the PICC itself or with an emulator introduced by an attacker.

ISO/IEC 14443 systems by default do not implement countermeasures against relay attacks or even strict timing constrains. By using the standard compliant WTX commands, we were able to stall a PCD for several seconds, which is easily enough time for even very slow or complex relay channels. Using this attack, it is also possible to stall the PCD for minutes if necessary.

We also proposed a number of possible countermeasures that are compliant with the ISO/IEC 14443 standard. Although those countermeasures do not provide 100 % security, they would give a reasonable protection against relay attacks while being standard compliant.

ACKNOWLEDGEMENTS.

The work has been supported by the Austrian government founded project PIT, grant no. 825743.

REFERENCES

[1] Atmel, *Atmel ATxmega 256A3*, http://www.atmel.com, 2011.
[2] Calypso Network Association, http://www.calypsonet-asso.org, 2011.
[3] J.H. Conway, "On Numbers And Games", *The Academic Press*, 1976.
[4] S. Drimer and S.J. Murdoch, "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks", *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, Boston, MA, 2007.
[5] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, John Wiley & Sons, Ltd., Chippenham, UK, 2010.
[6] L. Francis, G. Hancke, K. Mayes, K. Markantonakis, "Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones", *6th International Workshop, RFIDSec*, Istanbul, 2010.
[7] G.P. Hancke, "A Practical Relay Attack On ISO 14443 Proximity Cards", http://www.rfidblog.org.uk/hancke-rfidrelay.pdf, 2005.
[8] G.P. Hancke and M.G. Kuhn, "An RFID Distance Bounding Protocol", *International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Los Alamitos, CA, 2005.
[9] G.P. Hancke, K. Mayes and K. Markantonakis, "Confidence in Smart Token Proximity: Relay Attacks Revisited", *Computers & Security*, vol. 28, pp 615 - 627, 2009.
[10] ISO/IEC, "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical Characteristics", 2010.
[11] ISO/IEC, "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface", 2010.
[12] ISO/IEC, "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and Anticollision", 2010.
[13] ISO/IEC, "Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission Protocol", 2010.
[14] Z. Kfir, A. Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems", *International Conference on Security and Privacy for Emerging Areas in Communications Networks*, Athens, Greece, 2005
[15] J. Munilla, A. Peinado, "Enhanced low-cost RFID protocol to detect relay attacks", *Wireless Communications and Mobile Computing*, vol 10: pp 361 371, 2009
[16] NFC Times, "Vendor Group Seeks to Crack Mifare Dominance", http://www.nfctimes.com/report/vendor-group-seeks-crack-mifare-dominance, 2010.
[17] Nokia, Nokia 6212 classic, http://www.nokia.at/produkte/alle-modelle/nokia-6212-classic, 2011.
[18] NXP Semiconductors, MIFARE, http://www.mifare.net, 2011.
[19] Rayson, *BTM-222 datasheet*, 2005.
[20] Rayson, www.rayson.com, 2011.
[21] J. Reid, J. Gonzalez Nieto, T. Tang, B. Senadji, "Detecting Relay Attacks with Timing-Based Protocol", *2nd ACM Symposium on Information, Computer and Communications Security – ASIACCS*, 2007
[22] D. Singelée, B. Preneel, "Distance Bounding in Noisy Environments", *4th European Conference on Security and Privacy in Ad-hoc and Sensor Networks – ESAS*, 2007
[23] M. Weiss, "Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment", *Master's Thesis*, Munich, 2010.