RFID Wormholes

The Case of Contactless Smartcards

Tomáš Rosa

crypto.hyperlink.cz

SmartCard Forum 2011, Prague

Abstract

- This presentation is a summary of research activity aimed to prove the following hypothesis:
  - *Using generally available computing devices and program codes, it is practically easy to mount a wormhole (or relay) attack in a typical system accepting ISO 14443 contactless smartcards.*
- We emphasize, that a negation of this hypothesis is still very often used as an argument supporting security of many contactless smartcard applications.
- This research is, besides the others, directly linked to physical access control systems, electronic passports, and contactless identity cards.

Part ONE
Contactless Smartcard Recalled

Contactless Smartcard

- In this presentation, the term *contactless smartcard* refers to any RFID transponder compatible with ISO 14443, level 1 to 4.
  - Usually, ISO 7816-4 and higher is further encapsulated into ISO 14443, level 4 packets.
  - ISO 7816-4 often serves as unifying platform for both contact and contactless smartcards.
  - We, however, do not rely on such assumption in experiments described here.

Contact(less) Smartcard

<table>
<tr><td>Application layer</td><td colspan="3">ISO 7816-4 and higher</td></tr>
<tr><td>Transport layer</td><td rowspan="3">ISO 7816-3</td><td colspan="2">ISO 14443-4</td></tr>
<tr><td>Data link layer</td><td>ISO
14443A-3</td><td>ISO
14443B-3</td></tr>
<tr><td>Physical layer</td><td>ISO
14443A-2</td><td>ISO
14443B-2</td></tr>
<tr><td>Electromechanical properties</td><td>ISO 7816-1, 2</td><td colspan="2">ISO 14443-1</td></tr>
</table>

contact interface

contactless interface

PCD, PICC

- According to ISO 14443
  - The card is referred to as a **PICC** (proximity integrated circuit card).
    - We will also use the term **application transponder** to denote the PICC together with a significant application code (access card, electronic passport, etc.).
  - The terminal part responsible for the RFID communication itself is referred to as a **PCD** (proximity coupling device).

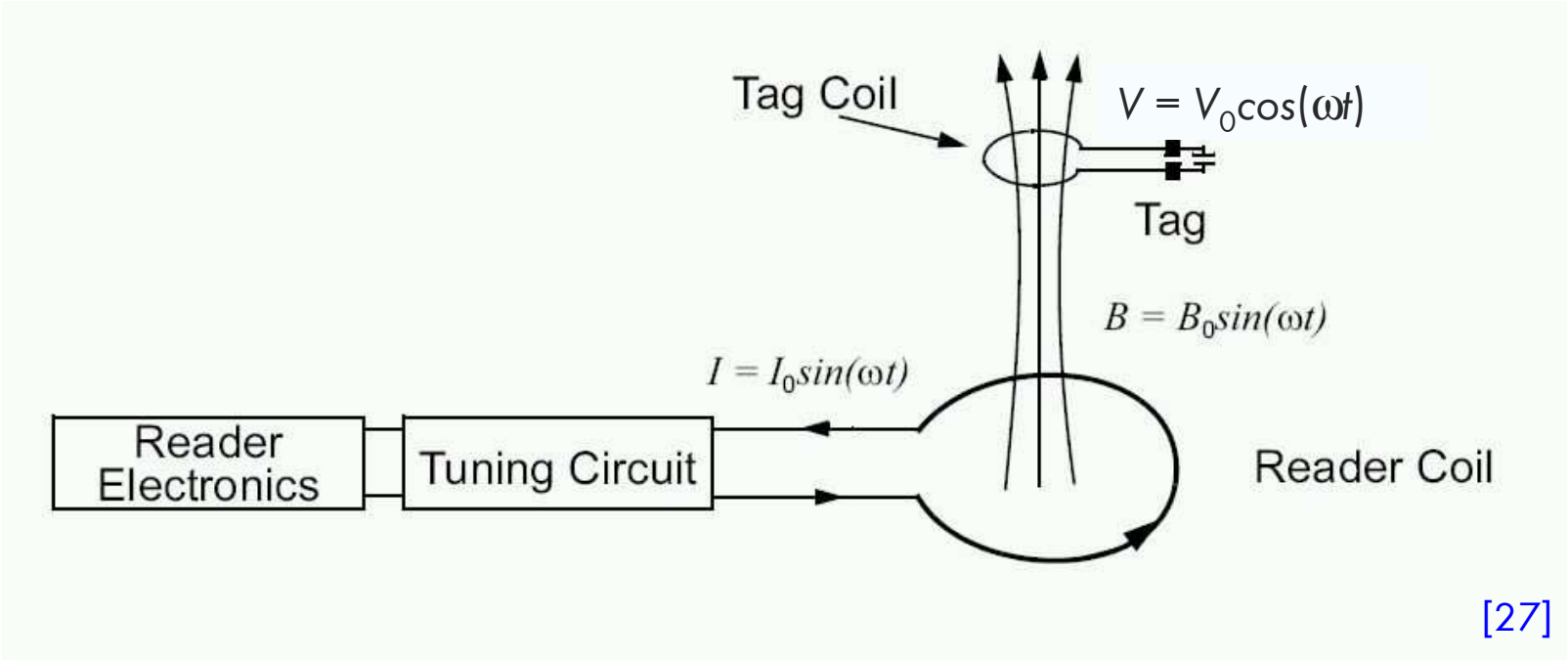
ISO 14443 Physical Layer

- Employs inductive coupling in so-called near field of the transmitter at **13.56 MHz** (HF band)**.**
  - Field equations are reduced considerably, especially wave effects can be omitted [7], [11], [31], [41].
    - This is true for an ordinary operation. An attacker trying to expose limits of this communication may be facing a “different” physics.
    - Threshold is approx. $\lambda/2\pi$, $\lambda \cong 300/f$ [m, -, MHz]
  - Arrangement „PCD antenna – PICC antenna“ can be viewed as a high frequency transformer.
    - Comprehensive description is given in [11].
    - Such a setup differs from UHF RFID [7], [11] significantly, so care must be taken when interpreting distance ranges experiments, etc.

ISO 14443 – Variants A and B

- They differ in levels 2 and 3 of the standard.
  - Different modulation index, modulation encoding, and packet framing.
- Level 4, however, stays the same for both of them.
  - Usually both variants are supported by the PCD, but they are unified at level 4 of the standard.
  - Therefore, from the application viewpoint, the communication difference vanishes.
  - Furthermore, from the application viewpoint the difference in between contact/contactless smartcard usually vanishes as well (cf. the table given before).

PCD – PICC Coupling (Energizing)



[27]

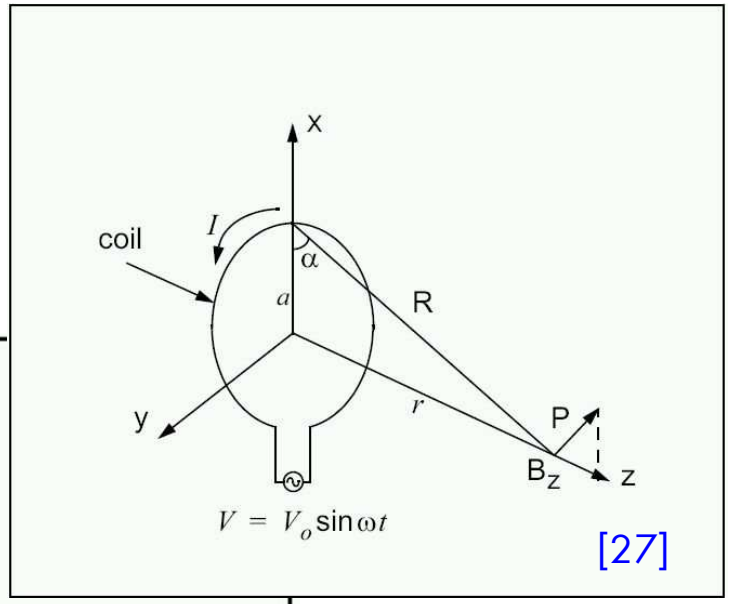
The tag itself is assumed to have no autonomous power source. It gets the energy for computation solely from the terminal's field.

Field Induction Estimation

...using even stationary field equations

Biot-Savart: $d\boldsymbol{B} = \mu_0 NI(\boldsymbol{R} \times d\boldsymbol{c})/(4\pi|\boldsymbol{R}|^3)$

circular coil integration



[27]

$$B_z = \frac{\mu_o I N a^2}{2(a^2 + r^2)^{3/2}}$$

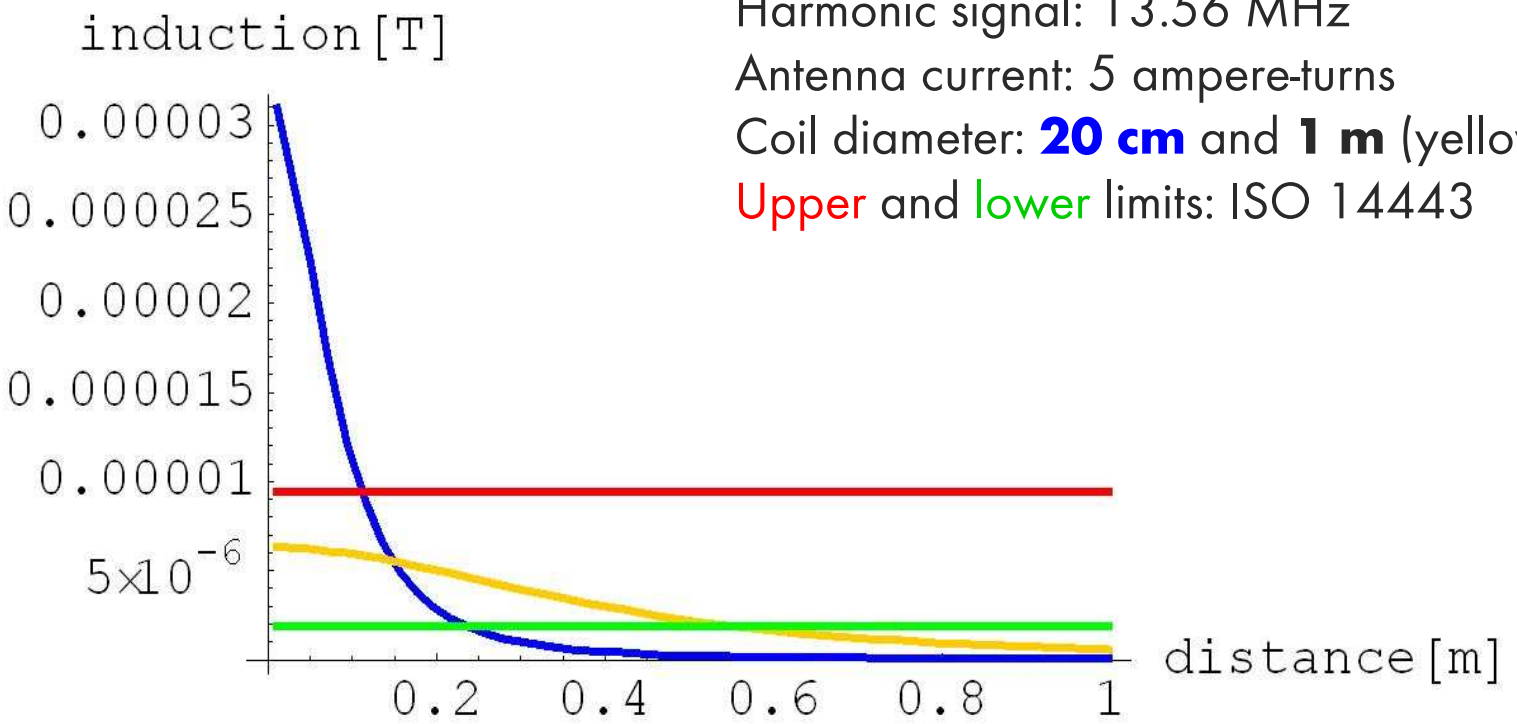
$$= \frac{\mu_o I N a^2}{2} \left(\frac{1}{r^3}\right) \quad \text{for} \quad r^2 >> a^2$$

[27]

note $|d\boldsymbol{c}| = a * d\varphi$

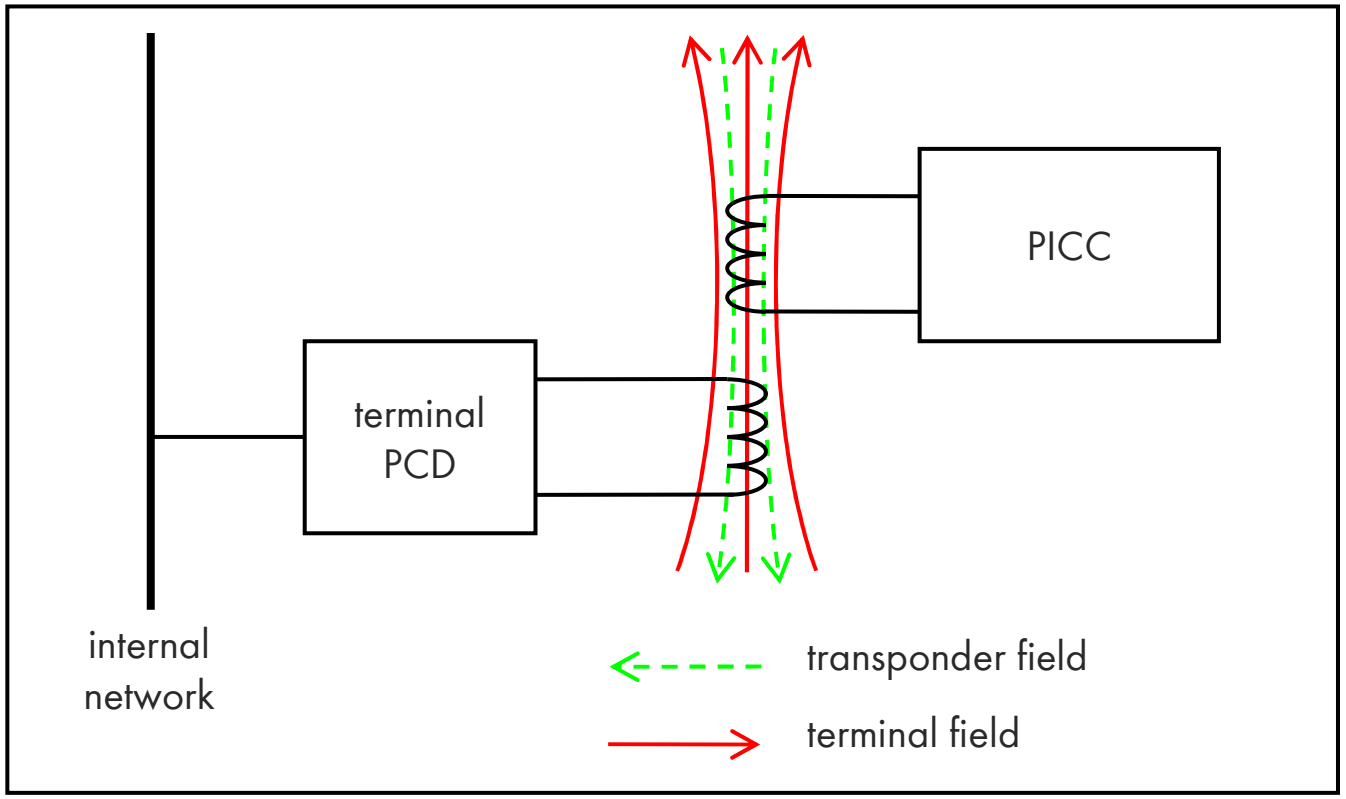
Optimum antenna diameter: $a = r*\sqrt{2}$, where r is the communication distance.

B_z Induced by a Circular Coil



Harmonic signal: 13.56 MHz
Antenna current: 5 ampere-turns
Coil diameter: **20 cm** and **1 m** (yellow)
Upper and lower limits: ISO 14443

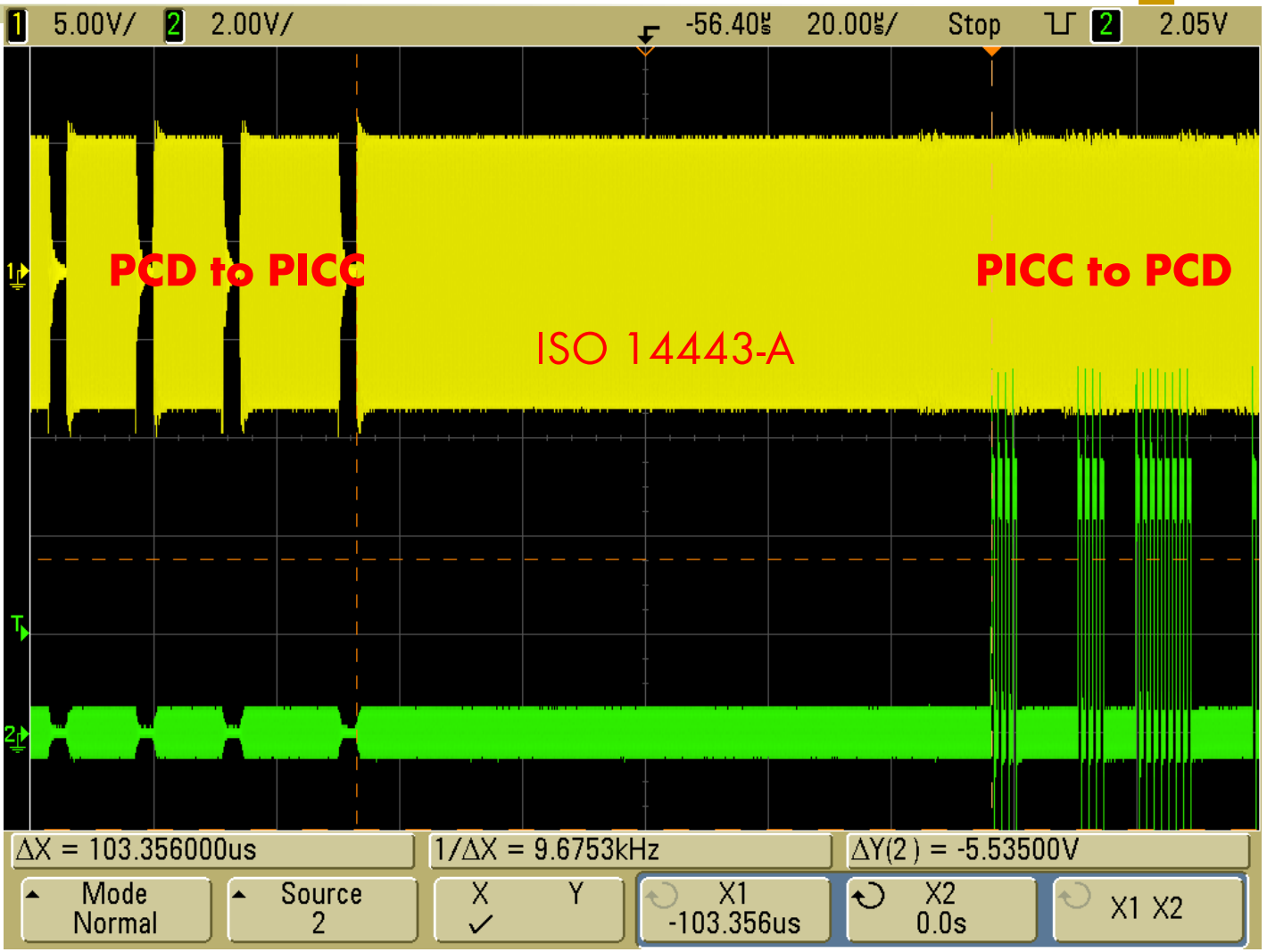
PCD – PICC Coupling (Data Communication)



PCD: direct amplitude modulation of the basic carrier
PICC: load modulation resulting in indirect amplitude/phase modulation of the basic carrier

Communication Oscillograph

- Yellow trace: basic carrier
- Green trace: AM detector with 847.5 kHz filter



When the Distance Matters

Method	Distance
Active communication with PICC	dozens of cm
Passive reception – PICC and PCD	units of m
Passive reception – PCD only	dozens of m
Active communication with PCD	dozens of m

- Table summarizes attacker's objectives and ranges for ISO 14443 (HF band).
- Note that in wormhole attacks, we are usually not challenging these distances, expect possible extension of active communication with the original PICC.

Part TWO
Wormhole Attack - Cryptography Viewpoint

Wormhole (Relay Channel)

- *Let the wormhole be any method enabling communication in between an out-of-range application transponder and the terminal.*
  - The term *wormhole* is getting used in place of *relay channel* to mimic the parallel with (yet hypothetical) 4D-spacetime “shortcuts”.
    - However, no 4D-spacetime shortcut (even hypothetical) actually occurs here, this just a fancy name.

Wormhole Attack (WA)

- *Let the wormhole attack be any attack strategy based on using a wormhole to make the terminal to accept and process the out-of-band application transponder.*
  - The main risk of this attack is coming from the fact, that, in many contactless applications, the presence of a transponder at the terminal is directly linked to somebody's intension to e.g. open door, pay a bill, undergo electronic passport check, etc.

Wormhole vs. MITM Attacks

- The key difference in between the wormhole attack and the more widely known man-in-the-middle approach is in the primary objective:
  - MITM is a-priori aimed at data interception and/or manipulation.
  - Wormhole attack is a-priori aimed at enabling certain unwanted communication to occur.
    - The communication itself, however, is not necessarily being modified or even understood by the attacker.
    - Therefore, conventional cryptographic techniques aimed at a pure data protection [30] are totally useless against WA.

Cryptography Viewpoint of WA

- WA (as defined here) is a particular instance of so-called *mafia fraud* [2], [4], [5].
  - It is also related to the famous game-theoretic story of a little girl Anne-Louise, who played against two Chess Grandmasters (Fisher, Spassky) and managed to win one of the games. She did so by mounting a “wormhole” in between Fisher and Spassky who then played against each other. Provided there is no stalemate, Anne-Louise shall win one of these games.

Old Problem's New Face

- Wormhole attack is definitely not such a new threat as RFID sellers (sometimes even researchers) try to pretend.
  - In cryptology, it is known at least since 1987 [5].
  - The reference [5] also gives an interesting story on how the *mafia fraud* term originated.
  - It is rather long-time overlooked than a brand new problem.
- On the other hand, thanks to RFID, its importance is becoming adequately recognized.
  - We note, however, that the viewpoint stated in [5] foresees certain issues that are somehow out of scope basing on the distance bounding paradigm accelerated by RFID.

Terrorist Fraud

- This is a variant of mafia fraud, such that the legitimate transponder owner would willingly cooperate with the fraudster to perform the wormhole attack [4].
- There are, of course, certain limits to keep this model sound.
  - The legitimate transponder owner will not simply lend their transponder to the fraudster.
  - Nor will the fraudster know secret keys of the transponder.
  - So, the owner is willing to somehow cooperate, but not too much.
- In this presentation, however, we will not pay attention to distinguish mafia vs. terrorist fraud.
  - Since we are not interested in comparison of various distance bounding protocol schemes here.
  - We emphasize, however, that designers building countermeasures against wormhole attacks shall be fully aware of this distinction.
  - In access control systems, for instance, terrorist fraud may be used to assure alibi for a person who “cannot be in both places simultaneously”.

Distance Bounding Protocols

- These are special kind of cryptographic protocols, that can in theory protect against wormhole attacks [3].
  - They are, however, seldom known and even more rarely used in practice.
- Their cornerstone principle is really nicely illustrated by the excellent, two-sentence-long conclusion of Beth and Desmedt [2] (1990).
  - "*Because the speed of light is finite and constant we have provided a practical solution to the mafia and terrorist fraud. Its applications go beyond identification.*"

Distance Bounding Implementation

- The cornerstone principle of distance bounding protocols (DBP) suggests they are, besides classic cryptography algorithms [30], based on certain physical measurements.
  - Actually, it is the (propagation delay) time that has to be measured.
  - The more accurate measurement we have, the finer the distance bounding can be (even one meter and less).
  - To estimate the time measurement accuracy needed note that light can travel about 30 cm in 1 ns.
  - The measurement, with the aforesaid accuracy, is to be performed by PCD.

DBP Practice

- Practical variants of DBP [18] usually proceed in the following phases:
  1. Protocol initialization
     - randomness generation, etc.
  2. Rapid data exchange
     - randomized challenge-response with precise time-delay measurement
  3. Data authentication
     - use conventional cryptography to confirm that data in step 2 were sent from the authentic transponder and terminal
  - Protocol fails if either of steps 1 to 3 fails.
    - Otherwise, it is expected that the distance in between the transponder and terminal is bounded by a certain limit measured in step 2.
    - It is then left on the application layer, whether it will accept the distance upper-limit measured by the protocol or not.

DBP Security Considerations

- To get secure DBP, we have to ensure at least that:
  - (Pseudo) random values being used are fresh and cannot be circumvented by the attacker.
  - The time-delay measurement is accurate and cannot be tampered by the attacker.
  - The cryptographic mechanisms and keys used for data authentication are secure.
  - The terminal and application transponder cannot be tampered by the attacker.

RF Considerations of DBP

- Using elementary signal theory, the time-delay resolution achievable at the terminal side can be estimated as:

$$\Delta t = 2 / B,$$

  where B is the RF channel bandwidth. Here, we assume the transponder is using the load modulation of the terminal basic carrier signal [11].

- The distance measurement then has an accuracy no better than:

$$\Delta d = c*\Delta t / 2 = c / B,$$

  where c is the speed of light (*celeritas*). This simple formula agrees with the one presented in [18].

DBP and ISO 14443 I

- There is no DBP which would be an implicit part of ISO 14443.
  - Actually, this standard rather enhances the wormhole attacks [19].
  - Unfortunately, there are also physical limits imposed by the relatively narrow bandwidth of at most 2 MHz.

$$\Delta d \cong 150 \text{ m}$$

DBP and ISO 14443 II

- There are claims saying the natural range limitations of the inductive coupling interface employed in ISO 14443 *is an implicit countermeasure against wormhole attacks*.
  - Well, this can be considered as a kind of protection – against spontaneous accidents.
  - It was shown (cf. here and references) that such a measure fails to provide adequate protection against intentional attacks.

DBP and ISO 14443 III

- Despite the bad starting position, it is nevertheless worth trying to mount some DBP into this standard.
  - We can, at least, prevent the most severe wormholes based on widespread available NFC devices discussed in this presentation.
  - Special devices like [16], [24], will, however, pass undetected bellow the limit stated before. This is a risk to be accepted or mitigated in other ways.
- There are, however seldom tries do to that at all.
  - The author is aware of one and only PICC declaring explicit support of certain DBP. This is the MIFARE Plus X card.
  - Note that to get DBP working, both PCD and PICC must provide certain active support for it.

Part THREE
Practical Approaches To Wormhole Attack

Wormhole Attack Scenario

- Typically, there would be two attackers (**A**, **B**), one card holder – victim (**V**), and one accepting terminal **T**.
  - **A** stays near (< 0,5 m) to **V** with a hidden device called *leech*. The leech establishes (hidden) RFID connection with **V**'s card.
  - **B** is at accepting terminal **T** with a masked device called *ghost*. Ghost establishes an RFID connection with **T**.
  - There is a network connection (via wifi, bluetooth, GSM, etc.) in between **A** and **B** allowing transient data exchange in between **T** and **V**'s card.
  - Now, **T** thinks it has **V** at its front while **V**'s card thinks it is at **T**.
  - Transaction data are exchanged, and the action linked to the transaction is granted. Action can be door entry, goods payment, aircraft boarding, etc.
  - The distance in between **A** and **B** can vary from several meters to even thousands of kilometers. It only depends on the kind of network connection used and wormhole strategy employed.

Wormhole Attack Illustrated

Victim

Attacker A

near field inductive coupling
in between the *leech* and V's card (passport)
distance < 0,5 m (cf. following discussion)

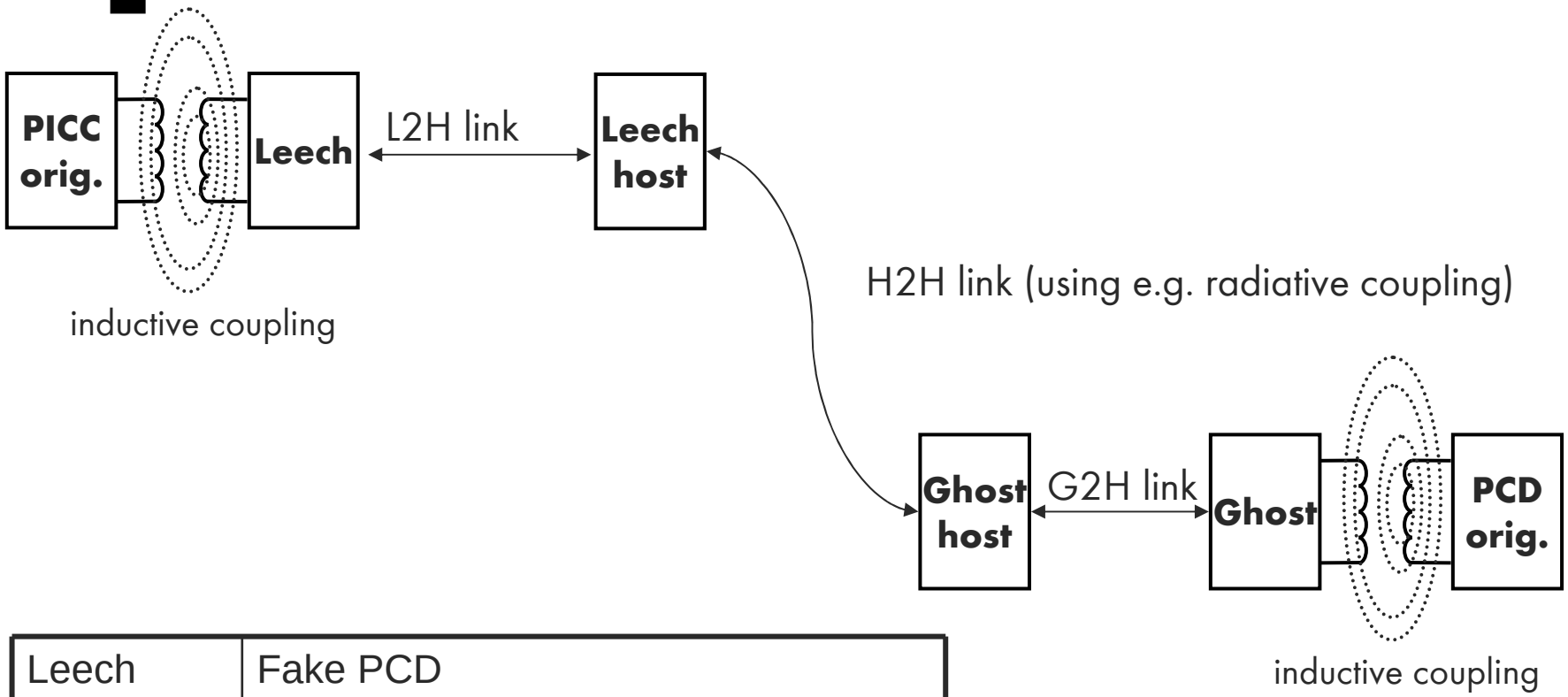
interconnection network

far field radiative coupling
(wifi, bluetooth, GSM, etc.)

Attacker B

near field inductive coupling
in between the *ghost* and the inspection terminal

Wormhole Attack Scheme



Leech	Fake PCD
Leech host	Computing device driving the leech
Ghost	Fake PICC
Ghost host	Computing device driving the ghost

Practical Considerations

- In analytical step, several questions shall be answered.
  - What is the planned host-to-host distance?
    - Affects H2H (main link) selection as well as the ISO 14443 wormhole layer choice.
  - What is the planned leech-to-host or ghost-to-host distance?
    - Affects L2H and G2H (secondary links) selection.
  - What is the planned leech-to-victim distance?
    - Affects leech device selection and eventual power boosting.
  - What devices will play the roles of leech and ghost?
    - Of-the-shelf device or from-scratch design or something in between?
  - What protocol level will be used for the wormhole?
    - Physical, data link, transport or even application layer of ISO 14443 / 7816?
    - The higher level we choose, the more robust wormhole we get, since we can enjoy several fault recovery mechanisms or optimize the data transfer. We are, however, obviously more dependent on the particular application then.

Our Approach

- Since we are searching for a low-cost, of-the-shelf, straightforward, and yet-universal construction, we have made the following assumptions:
  - NFC device will be used for the leech and the ghost.
  - PC notebook will be used as the host for leech and ghost.
  - Wormhole will occur on data link layer of ISO 14443 with certain advice from transport layer.
    - NAK/ACK ping-pong according to PC/SC card presence polling [35] is handled locally, etc.
- This approach would be probably also chosen by a student who wants to make a demo attack in a couple of weekends.
  - Such a result could be enough to defame the whole system.
  - Cf. skimming (not wormhole) attack videos [21], [22].

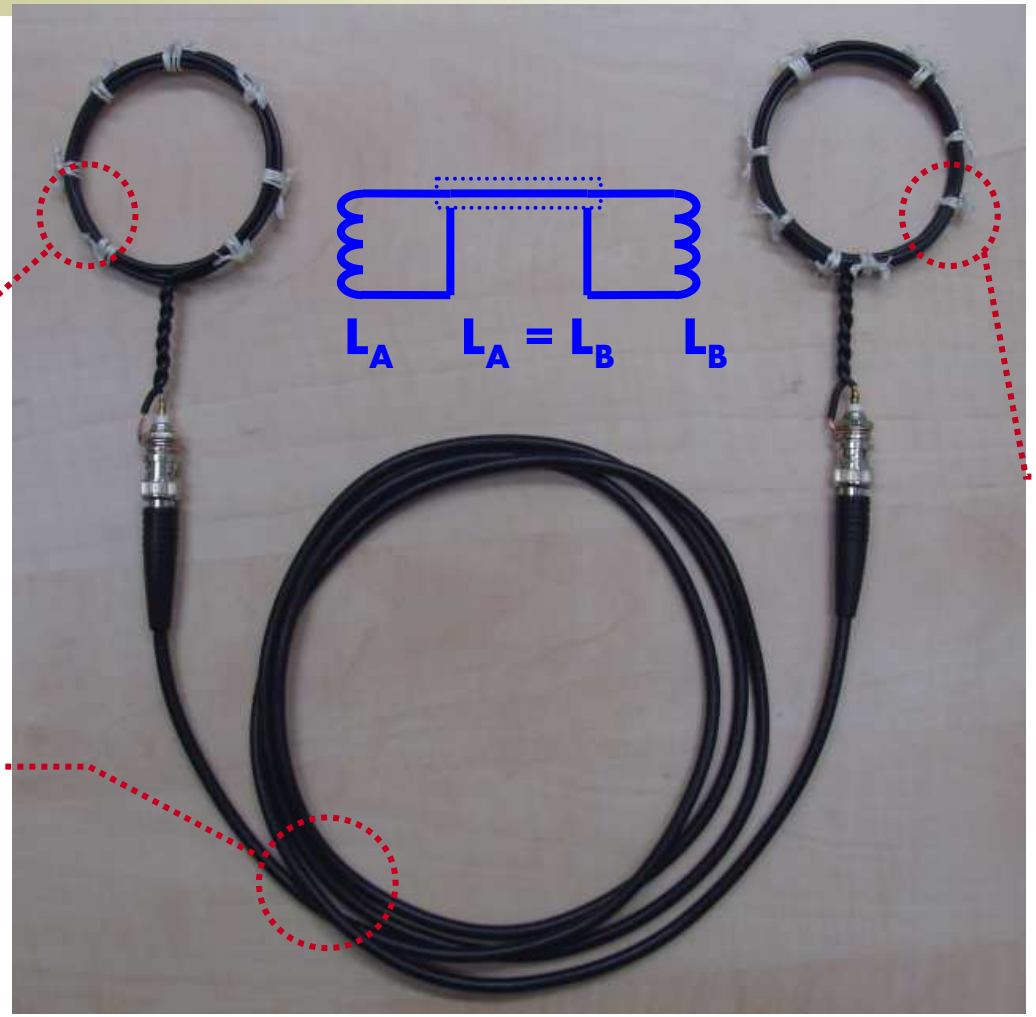
Other Approaches I

- In the diploma thesis [40], NFC-capable GSM phone usability is studied intensively.
  - Besides the others, this approach leads to highly inconspicuous and yet effective leech design.
  - Certain problems were encountered with the ghost side.
  - Anyway, once the next generation of NFC phones hits the market (1 or 2 years approx.), this is definitely a high way for majority of future attacks.

Other Approaches II

- Physical layer wormhole is discussed in [16], [24].
  - This approach assumes special devices playing the roles of leech (called mole) and ghost (called proxy here).
  - Distance of 50 meters was achieved using a cheap UHF radio link components for H2H connection [16].
  - L2H and G2H almost disappeared because of leech and ghost architectures and embedded host controllers.
  - Nevertheless, this kind of attacks is very interesting, since:
    - even 50 meters can be enough (to defame, at least),
    - this is the kind of attack that is bellow ISO 14443 physical distance resolution capability as discussed before.
  - Therefore, this is the kind of attack that shall be assumed to be almost always possible.

Do-It-Yourself Wormhole

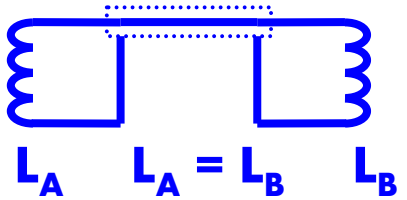


L_A: 4 turns of plain CUL wire, coil ∅ 75 mm

same as L_A

coax. RG 58 length < $\lambda'/2\pi$ (tested ≤ 2m)

DIY Demo Principle



- 1:1 transformer with a coaxial transmission line.
  - The impedance of PCD or PICC antenna circuit together with the particular coupling coefficient cannot be guaranteed.
  - Therefore, we cannot universally match the transformer for the coaxial line used.
  - Anyway, if we stay in the near field area, we can omit this matching (for a rigor analysis, note EM wavelength variance for the transmission line used - λ').
  - Therefore, the wormhole range is limited to (say) meters.
- Anyway, such a demo is sufficient for a wormhole existence demonstration in RFID.
  - It can be even shown in fundamental Maxwell equations [41].
  - It may, however, be also sufficient to defame the whole system by a carefully prepared demonstration for TV news…

Wormhole In Access Control

Picture shows a real successful experiment with the DIY wormhole.

Leech Range Extension

- Usual of-the-shelf RFID reader allows communication with the victim's card at a distance < 10 cm.
  - For many attacks, this is quite enough (cf. [22]).
  - Especially, NFC phones tested had excellent reading range.
  - Some readers may need certain antenna re-tunning.

- An attacker who wants to extend this range will need to modify the of-the-shelf reader slightly.
  - This approach shall still be achievable for a reasonably skilled electronic engineer [26].
  - Naturally, RFID manufacturers also provide guidance on how to extend active range of their chipset [32].
  - Main parts of the leech or even whole kits can be bought on the internet. The main task is to assemble these things together appropriately.

Building Extended Range Reader

- For instance, the Melexis demo kit DEMO90121LR [29] seems to be a promising starting point.
  - The kit itself is aimed at ISO 15693 which is a different RFID standard.
  - It shall, however, be compatible with ISO 14443 as well, since its internal MLX90121 controller handles this standard as well.
  - The analog part is also similar enough, in fact it is right the power amplifier of Melexis design that was used to construct the low-cost extended range reader in [26].
  - Attention deserves the antenna part, which may require certain tuning adjustment (mainly because of different RF bandwidth).

Range Extension Limits

- The very principal limit is given by near/far field threshold, which is approximately

$$\lambda / 2\pi \cong 3.52 \text{ m}$$

- In [25], practically achievable limit is estimated to be 0.5 m (at cost < $100 in year 2005).
  - This is the distance we shall assume in risk assessments.
- Using of-the-shelf devices modification, communication at around 15-25 cm shall be achievable using home-grown development [13], [15], [26].
  - Basing on our own practical experiments, we agree with [13] results and conclusion stating that: "*That said, 15 cm or 20 cm is enough to execute an attack in a crowded area and easily allows reading of a token in somebody's pocket or bag.*"
  - See also skimming attack presentations [21], [22].

Part FOUR
Hacking Into & With NFC

NFC at Glance

- NFC stands for *Near Field Communication*
- Device equipped with an NFC controller can work in the following modes:
  - Passive-mode initiator (or just a “PCD”)
  - Passive-mode target (or just a “PICC”)
  - Active-mode initiator/target (or just “PCD-to-PCD”)

NFC Standards

- ISO 18092 specifies the **NFCIP-1** core protocol.
  - In fact, several parts duplicate the ISO 14443 A or FeliCa, but with a rather “innovative” wording.
  - Attention – the word “passive” does no longer equal to “without autonomous power source” here.
  - It is used to address those ISO 14443 A or FeliCa compatible modes in general (reader as well as tag).
- Furthermore, ISO 21481 addresses possible RF interference issues.
  - Handles coexistence of devices and operational modes following other standards occupying 13.56 MHz.
  - Those mainly are ISO 14443 and ISO 15693.

NFC and ISO 14443

- NFC-equipped device can address contactless smartcards world in two ways:
  - As a PCD
    - ISO 14443 A – passive-mode initiator
  - As a PICC
    - ISO 14443 A – passive-mode target

NFC and Mobile Phones

- At this moment, several incompatible architectures exist.
  - We can call them “generation zero” devices.
  - Interesting survey is given in [40].
- Approaching version of “generation one” devices shall:
  - Include special HW module called CLF (Contactless Front-end).
  - Interconnect CLF directly with SIM card, so the SIM will serve the role of a *secure element*.
  - Also provide certain monitor connection in between CLF and phone’s main processor.

CLF

- Provides SWP (Single Wire Protocol) interface.
  - Described in public standards:
    - ETSI TS 102 613 (physical and data link layer),
    - ETSI TS 102 622 (host controller interface - HCI).

- At present, CLF can be bought separately.
  - Cf. e.g. www.bladox.com
  - SWP<->USB interface converter is one of those wanted technical projects, since CLF seems to be a valuable tool for security analysts in itself.
  - On the other hand, it is still unclear what kind of benefit the stand-alone CLF could provide over NFC-equipped reader we have used in the our experiments.
  - As far as we can say, CLF is probably composed of certain NFC controller plus another microcontroller implementing the SWP and HCI.

NFC Controllers

- Handle NFCIP-1 protocol implementation.
  - Gradually replace previous generation of “PCD-only” RFID controllers used in contactless smartcard readers.
  - Therefore, we are slowly approaching the situation where almost any “reader” will be able to serve the role of a smartcard emulator as well.
- Several manufacturers provide NFC controllers.
  - NXP’s chipset seems to be the most popular.
  - ST and Inside Contactless provide similar chips, too.
  - Unfortunately, their interfaces are not compatible.

NXP's Controllers Overview

Chip	Interface	PCD Mode	PICC Mode	Level 4 Framing
PN531	I2C, SPI, USB	ISO 14443-A	ISO 14443-A	PCD only
PN532	I2C, SPI	ISO 14443-A/B	ISO 14443-A	PCD & PICC
PN533	USB	ISO 14443-A/B	ISO 14443-A	PCD & PICC

- Table presents summary of NFC controllers of PN53x family made by NXP [32].
  - Simplified viewpoint based on wormhole attacks on ISO 14443.
  - Further details can be also found in [28].
  - Although variant-A-only support in PICC mode seems to be a limiting condition, it is actually not the case (cf. elaboration given in part V).

NXP's NFC-WI/S2C Channel

- This interface allows direct connection to the physical layer of NFCIP-1 implemented in the NFC controller.
  - The controller handles solely "digital to RF" conversion and vice versa. The rest is left on the interfaced circuit (probably a microcontroller).
  - One of its intended applications is connection of certain *secure element* card [34].

- Despite not being used for this presentation, it is worth noting that this channel can be sensibly used for attacks requiring such low-level access.
  - The controller handles the "tricky" analog part while still allowing unlimited physical layer level access.
  - For instance, the designs of [16], [24] mentioned before can be further simplified using this interface.
  - Other exploitation is described in [36].

Hacking Into & With NFC

- When successfully mastered, an NFC-capable device is a vital tool for any security analyst.
  - Mainly the passive-mode target promises, obviously, many interesting applications.

- The whole approach has, however, two steps:
  - Hacking into NFC. While it is relatively easy to buy a device with an NFC controller, it is much harder to get full documentation for it.
    - Even the NFC controllers themselves try to somehow limit their usage for an attacking purpose – by e.g. UID setting obstacles.
    - Very important and useful project is www.libnfc.org [28].
  - Hacking with NFC. The NFC devices can be used to implement e.g. wormhole or MITM attack, etc.

Part FIVE
Experiments With libnfc

libnfc at Glance

- According to the libnfc authors:
  - "*…libnfc is the first free NFC SDK and Programmers API released under the GNU Lesser General Public License. It provides complete transparency and royalty-free use for everyone…*" [28].

- As far, as we can confirm, the aforementioned statement is true.
  - It is quite easy to (even unintentionally) buy an NFC-equipped device, while, on the other hand, it is considerably harder to get full programmer's documentation and support for it.
  - libnfc commendably dares to remove this barrier.

libnfc Version Alert

- libnfc is vital fast evolving project, so it is wise to consult [28] for the latest version available.
- The research part presented here was done in Autumn 2010 with libnfc v. 1.3.4.
- In time of presentation, however, even version 1.4.2 was available.
  - Besides the others, it also contains a sample code for a wormhole mounted on the top of the transport layer of ISO 14443.

libnfc Internals

NFCIP-1 API	Provide connection initialization an communication with an RF inductively coupled counterpart (ISO 18092).
NFC controller drivers	Provide monitor (firmware) commands wrappers for a particular NFC controller chipset.
device drivers	Provide monitor mode communication with an NFC controller embedded inside a particular peripheral device.
bus drivers	Provide data communication with an NFC-capable device (also cover L2H and G2H links).

Table illustrates libnfc internal structure in a layered model form. Despite not being an official picture provided by libnfc core team, we assume it is quite accurate – with respect to source code structure at least.

libnfc Drivers Available

- In v. 1.3.4, used for these experiments, the following NFC controllers are supported:
  - PN531
  - PN532
  - PN533
- Furthermore, the following device interfaces are supported:
  - PN53x direct connection (e.g. SCL3710 or SCL3711)
  - ACR122U connected through PC/SC (uses certain pseudo-APDUs interpreted in ACR122U firmware to get direct access to the PN532 embedded inside).
- The bus driver layer is ready to support:
  - USB (through libusb 0.1)
  - UART (through a serial line operating system device)

Principal Obstacles

- There are two obvious obstacles regarding usage of PN53x controllers.
  1. UID of the ghost device cannot be set to an arbitrary value.
  2. The ghost device cannot work under ISO 14443 – variant B standard.
- The following discussion shows how to overcome these potential issues.

UID of the Ghost I

- Aiming to perhaps limit abusing PN53x for straightforward attacks against simple UID-only access control systems, there is a certain UID mask that must be obeyed.
  - Actually, only 4-byte long UID of the following form can be set: 08 *X Y Z*, where *X*, *Y*, and *Z* are arbitrary byte values.
  - This rule is enforced by the innermost microcode of PN53x which is responsible for anticollision and PICC selection procedure handling.
  - Despite being out of scope for this presentation, we have to note that UID-only access control systems can be attacked in other simple ways, cf. [36].

UID of the Ghost II

- Now, the decision must be made on how to cope with the UID rule.
  1. Should this be an issue, we have to apply certain workaround.
     - These are known, but must be somehow tailored for the particular setup [28], [38].
  2. If this is not an issue, we can proceed with the existing UID mask without any intervention.

UID of the Ghost III

- Recall we are aimed at wormhole attacks on **smartcards**.
- Applications of these cards seldom care about UID at all, because of several reasons.
- Furthermore, the application developers shall assume UID is constructed at random.
  - So, they shall not rely on its particular constant value.
  - Nevertheless, UID still could have been incorporated into cryptographic protocols (as a kind of randomness), but this is often not the case.

UID of the Ghost IV

- Recall the UID mask enforced by PN53x conforms with a PICC using a dynamic value for UID according to ISO 14443.

- Several major applications already do expect and allow dynamic UIDs.
- Moreover, they do not use the (supposedly) random value for any cryptographic protocol computation.
  - Especially, electronic passports of ICAO [20] and EMV contactless cards [9] belong to this set.

UID of the Ghost V

- Since we are talking about smartcards with certain accent on e-passports, we can conclude that the UID mask is not an issue here.
  - Therefore, in our attack verification, we proceeded using the built-in anticollision microcode of PN53x with no special workaround.
  - On the other hand, we emphasize that should this be an issue, it can solved [40]. It may, however, involve even HW modification of the ghost then - using, for instance, NFC-WI/S2C interface mentioned in part IV before.

Ghost and ISO 14443 – B I

- It may happen that the original card being relayed is of standard variant B instead of A.
  - PN53x, however, can only emulate variant-A PICC.
  - On a first sight, this may seem to be an issue.

Ghost and ISO 14443 – B II

- Recall, however, that any substantial difference in between variant A and B vanishes from the application viewpoint.
  - Since we are focused on smartcard applications, we can simply let the leech to operate according to variant B while the ghost will stay with A.
  - This only means we shall perform anticollision and card selection independently for both leech and ghost sides and start relaying the data packets just after the selection phase is done.
  - Therefore, this is not an issue for our approach.

Experimental Achievements

- Using libnfc, we have successfully realized wormhole attack on the electronic passport application.
  - In place of an inspection terminal, we have used a demo application reading a BAC-equipped passport on PC with a popular dual smartcard reader CardMan 5321.
  - The passport was chosen as a typical contactless smartcard application.
- For a robust and fault-tolerant practical attack, we, however, suggest mounting the wormhole on the transport or application layer.
  - Nevertheless, this is still easily achievable, especially by using PN532 or PN533 which have built-in firmware support for transport layer framing.
  - libnfc v. 1.4.2. already provides certain sample application support for this approach.

Wormhole Core Details I

- Again, we tried to proceed in as simplest way as possible.
  - We, therefore, started with an interesting relay sample code being distributed right with libnfc.
  - It is located in **`src/examples/nfc-relay.c`**.
  - We did, however, certain modifications of this code aimed to improve its robustness and follow the general wormhole scheme mentioned before.
  - We, however, have stayed at the same protocol level – on the top of the data link layer.
  - We have verified, that even this straightforward approach leads to a satisfying result.
    - Now, things can only get better…

Wormhole Core Details II

- We mainly incorporated:
  - Independent anticollision and selection procedures running on leech and ghost hosts, respectively.
    - Furthermore, these fully employ the internal microcode of PN53x on the leech as well as the ghost sides to increase robustness of this procedure.
  - NAK/ACK ghost presence ping-pong [35] is handled locally by the ghost host.
  - Improved RF field checking procedure to allow faster wormhole recovery after reset condition.
  - The whole design is transaction-eager trying to re-establish the wormhole whenever it seems to be broken.

Wormhole Core Details III

- We also made modest changes to libnfc itself.
  - Improved USB [1] polling procedure to increase the whole throughput while preventing unintentional internal microcode restarts in PN53x.
  - Automatic SCL3710 power consumption calm down [37].
  - Vinculum-I serial-driven embedded USB host controller [39] support incorporated (experimental).
    - Employs VDAP Vinculum-I firmware [39].
    - Simplifies L2H or G2H link creation using bluetooth or wifi embedded serial-profile modules. Using Vinculum, there is no need to modify the leech or ghost HW to change its interface from USB to UART (or something else).

Wormhole Core Details IV

- Experimental setup used:
  - Leech:
    - ACR122U v203 (featuring PN532 v1.4)
    - SCL3710 (featuring PN531 v4.2)
    - Note: ACR122U v201 or v206 is recommended instead of v203.
  - Ghost:
    - SCL3710 (featuring PN531 v4.2)
  - Host (shared):
    - Compaq Evo N610c, Pentium 4M @ 2.00 GHz, 1 GB RAM
    - Linux Ubuntu 9.04, kernel 2.6.28-19-generic, running in terminal mode
    - libnfc 1.3.4 (plus its dependencies) (obsolete now!)
    - Note the ancient HW platform to figure out that the host part is really not demanding computational power too much.

Experimental Setup

Timing Constraints I

- We combined the leech and ghost host codes to run on a single PC.
  - This was to simplify the experimental setup.
- We have, however, deliberately induced parametric delays to mimic the existence of H2H main link channel.
- Furthermore, we also studied the timing constraints of L2H and G2H links respectively.
  - This was to study possibility of using one combined host controller while allowing remote RF (in radiative far field) connection with either leech or ghost.

Timing Constraints II

- We can summarize the results as follows:
  - For the H2H link: Even the internet connection is sufficient, provided there is a roundtrip delay (ghost to leech and back) less than several seconds.
  - For the L2H and G2H links: Local roundtrip must be less than approx. 20 ms. Otherwise, the PCD may reject late responses to RATS.
    - Nevertheless, this allows using short range bluetooth or wifi links, which may be enough to perform the attack demonstration in e.g. airport lobby.

Timing Constraints III

- Recall that ISO 14443 is quite “wormhole-friendly” [19] standard.
  - There is no distance bounding protocol.
  - There are mechanisms to (almost unlimitedly) increase frame waiting time.

- There are actually two ways on how PICC (ghost) can request extra delays.
  1. Using FWI parameter of ATS string.
  2. Using S(WTX) service packet.

- Attacker is mainly concerned about the ghost side, since according to this standard, time constraints are imposed by PCD only.

Timing Constraints IV

- FWI can be limited in some applications.
  - By [9], for instance, the card shall set FWI ≤ 7 resulting in maximum response delay approx. 38.66 ms.
- Should we need more, we can, however, use S(WTX) service packet for ad hoc frame waiting time extension.
  - Despite being still possibly limited to 38.66 ms, we can invoke S(WTX) repeatedly to gradually increase the frame waiting time as we need.
  - Furthermore, PN532/533 firmware fires such S(WTX) automatically when working in ISO 14443 – level 4 PICC mode!

Antenna Geometry I

- Sometimes, the PCD requires the card to be inserted inside an aperture similar to a contact card reader.
- There is a question on whether an of-the-shelf ghost device can be used to emulate the original card under such conditions.

Antenna Geometry II

- Inspiration can be found in the DIY wormhole presented above.
  - We simply use a suitable antenna transformer.
  - Its secondary coil is shaped to fit inside the PCD's aperture while the primary one is fastened at the ghost device.
  - We suggest considering PCB layout and 1:1 ratio for the transformer coils, although particular situation may require slightly different approach. Anyway, it is an easy and funny experimentation, not a rigid obstacle.
- So, using such apertures cannot be regarded as a countermeasure against wormhole attacks.

Conclusion

- Because of the wide availability of NFC controllers and libraries, the following is true:
  - *Using generally available computing devices and program codes, it is practically easy to mount a wormhole attack in a typical system accepting ISO 14443 contactless smartcards.*

References I

1. Axelson, J.: *USB Complete: Everything You Need to Develop USB Peripherals*, 3rd Ed., Lakeview Research LLC, 2005
2. Beth, T. and Desmedt, Y.: *Identification Tokens – Or: Solving the Chess Grandmaster Problem*, In Proc. of CRYPTO ’90, pp. 169-176, Springer-Verlag, 1991
3. Brands, S. and Chaum, D.: *Distance-Bounding Protocols,* In Proc. of EUROCRYPT ’93, pp. 344–359, Springer-Verlag, 1994
4. Desmedt, Y.: *Major Security Problems with the ‘Unforgeable’ (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them*, SecuriCom ’88, SEDEP Paris, pp. 15-17, 1988
5. Desmedt, Y., Goutier, C., and Bengio, S.: *Special Uses and Abuses of the Fiat-Shamir Passport Protocol*, In Proc. of CRYPTO ’87, pp. 16-20, Springer-Verlag, 1988
6. *Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technologies*, ICAO, ver. 1.7, 2004
7. Dobkin, D.: *The RF in RFID: Passive UHF RFID in Practice*, Elsevier Inc., 2008
8. Drimer, S. and Murdoch, S.-J.: *Relay Attack on Card Payment – Vulnerabilities and Defences*, Conference 24C3, December 2007

References II

9. EMV Contactless Specifications for Payment Systems, *EMV Contactless Communication Protocol Specification*, v. 2.0.1, July 2009
10. Finke, T. and Kelter, H.: *Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*, BSI - German Federal Office for Information Security, 2005
11. Finkenzeller, K.: *RFID Handbook – Fundamentals and Applications in Contactless Smart Cards and Identification*, John Willey and Sons Ltd., 2003
12. Francillon, A., Danev, B., and Čapkun, S.: *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*, IACR ePrint Report 2010/332, 2010
13. Hancke, G.: *Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens*, Journal of Computer Security, accepted to be published 2010
14. Hancke, G.: *Eavesdropping Attacks on High-Frequency RFID Tokens*, 4th Workshop on RFID Security (RFIDSec), July 2008
15. Hancke, G.: *Practical Attacks on Proximity Identification Systems (Short Paper)*, In Proc. of IEEE Symposium on Security and Privacy, pp. 328-333, 2006
16. Hancke, G.-P.: *A Practical Relay Attack on ISO 14443 Proximity Cards*, Tech. Report, 2005

References III

17. Hancke, G.: *Research Homepage*, http://www.rfidblog.org.uk/research.html
18. Hancke, G.-P. and Kuhn, M.-G.: *An RFID Distance Bounding Protocol*, In SecureComm '05, pp. 67-73, IEEE Computer Society, 2005
19. Hlaváč, M. and Rosa, T.: *A Note on the Relay Attacks on e-passports: The Case of Czech e-passports*, IACR ePrint Report 2007/244, 2007
20. ICAO - International Civil Aviation Organization, http://www.icao.int/
21. *Identity Theft - MIFARE Campus Card Skimming Attack (EN titles)*, http://www.youtube.com/watch?v=NW3RGbQTLhE
22. *Identity Theft - Prague Citizen Card Skimming Attack (CZ titles)*, http://www.youtube.com/watch?v=Yxvy_eGK5r4
23. Jelínek, L.: *Jádro systému Linux - Kompletní průvodce programátora*, Computer Press, a.s., Brno 2008
24. Kasper, T.: *Embedded Security Analysis of RFID Devices*, Diploma Thesis, Ruhr-University Bochum, July 2006

References IV

25. Kfir, Z. and Wool, A.: *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, IACR ePrint Report 2005/052, 2005
26. Kirschenbaum, I. and Wool, A.: *How to Build a Low-Cost, Extended-Range RFID Skimmer*, USENIX 2006
27. Lee, Y.: *Antenna Circuit Design for RFID Applications*, Application Note 710, Microchip Tech. Inc., 2003
28. libnfc.org - Public platform independent Near Field Communication (NFC) library, www.libnfc.org
29. Long range HF RFID demonstrator – DEMO90121LR, Melexis, http://www.melexis.com/General/General/DEMO90121LR_662.aspx
30. Menezes, A.-J., van Oorschot, P.-C., and Vanstone, S.-A.: *Handbook of Applied Cryptography*, CRC Press, 1996
31. Myslík, J.: *Elektromagnetické pole - základy teorie*, BEN - technická literatura, Praha 1998
32. *Overview of Technical NFC Documents,* includes PN53x documentation catalogue, NXP, March 2009, http://www.nxp.com/documents/other/nfc_documentation_overview.pdf

References V

33. *PKI for Machine Readable Travel Documents offering ICC Read-Only Access*, IACO, ver. 1.1, 2004
34. *S2C Interface for NFC*, Survey VI.0, Philips, 2005
35. PC/SC Workgroup Specifications, http://www.pcscworkgroup.com/specifications/overview.php
36. Rosa, T.: *PicNic - Yet Another Emulator/Spyware for HF RFID*, technical project 2008 – 2010, http://crypto.hyperlink.cz/picnic.htm
37. Rosa, T.: *SCL3710 USB Dongle Config-based SHORT-CIRCUIT Found*, libnfc developers forum, 2010, http://www.libnfc.org/community/topic/194/scl3710-usb-dongle-configbased-shortcircuit-found/
38. Rosa, T.: *Passive Target Mode Initialization *Without* Secondary Reader*, libnfc developers forum, 2010, http://www.libnfc.org/community/topic/200/passive-target-mode-initialization-without-secondary-reader/
39. Vinculum-I device datasheet, application notes, drivers, and prototyping boards, http://www.ftdichip.com
40. Weiss, M.: *Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment*, Master's Thesis in Computer Science, Fakultät Für Informatik, Der Technischen Universität München, May 2010
41. Fleisch, D.: *A Student's Guide to Maxwell's Equations*, Cambridge University Press, New York 2008.