RFID Security

Selected Areas of LF and HF Applications

Tomáš Rosa

crypto.hyperlink.cz

Soom – Hacking & Security 2012, Prague

Part ONE
RFID Physical Layer Recalled

Radio Classification of Transponders

Band	Sub-class	Typical sort	Typical deployment	Operation Distance (order)
LF (100 to 150 kHz)	-	Memory card	Access control, immobilizer, implant, loyalty card	cm to m(*)
HF (13.56 MHz)	Vicinity ISO 15693	Memory card	Access control, skipass, loyalty card	cm to m
	Proximity ISO 14443	Contact-less smartcard	Access control, payment card, e-passport	cm
UHF (430– 2450 MHz)	-	Memory card	Stock control	cm to 10s m

(*) rare configurations with low consumption read-only cards and high power, high dimension readers

Contact(less) Smartcard

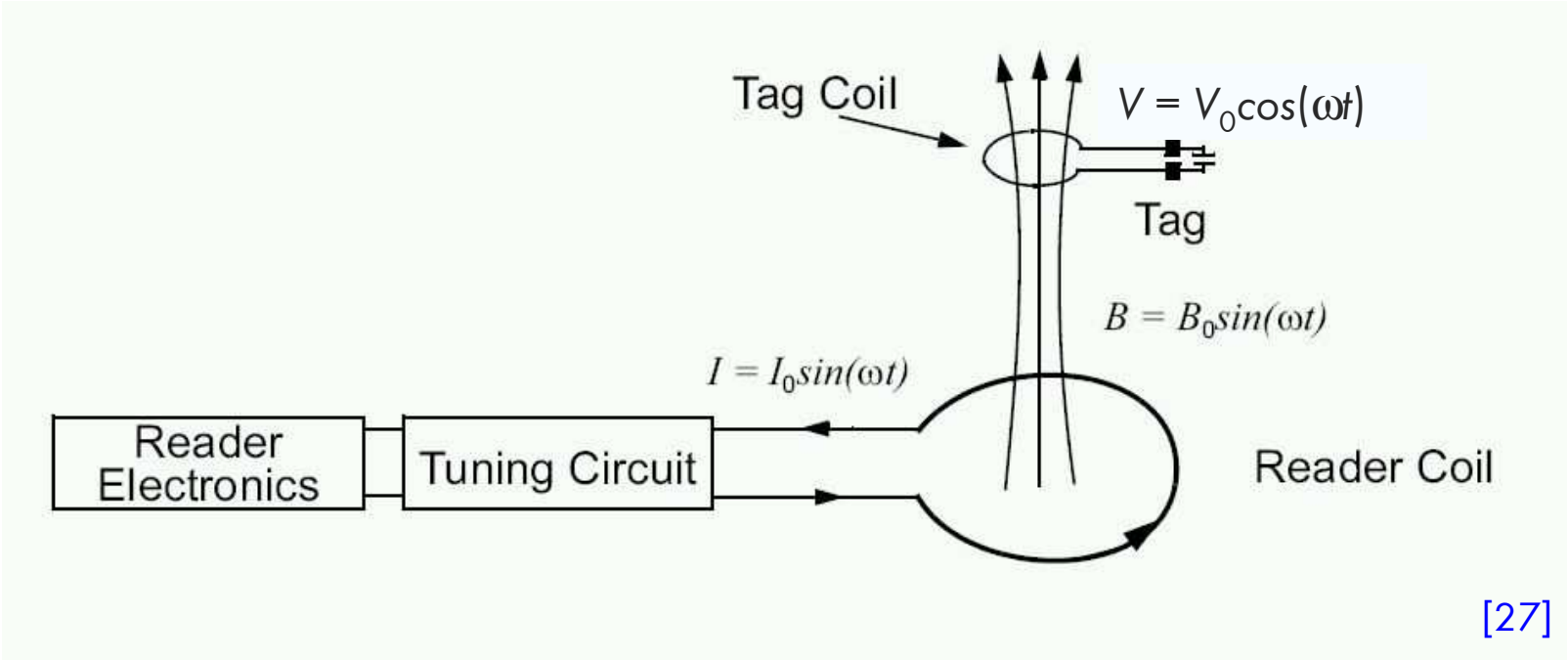
<table>
<tr><td>Application layer</td><td colspan="3">ISO 7816-4 and higher</td></tr>
<tr><td>Transport layer</td><td rowspan="3">ISO 7816-3</td><td colspan="2">ISO 14443-4</td></tr>
<tr><td>Data link layer</td><td>ISO
14443A-3</td><td>ISO
14443B-3</td></tr>
<tr><td>Physical layer</td><td>ISO
14443A-2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

LF & HF Physical Layer

- Employs inductive coupling in so-called near field of the transmitter at circa **125 kHz** (LF) or **13.56 MHz** (HF)**.**
  - 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 „transponder antenna – terminal 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.

Terminal – Transponder In LF/HF
Energizing



[27]

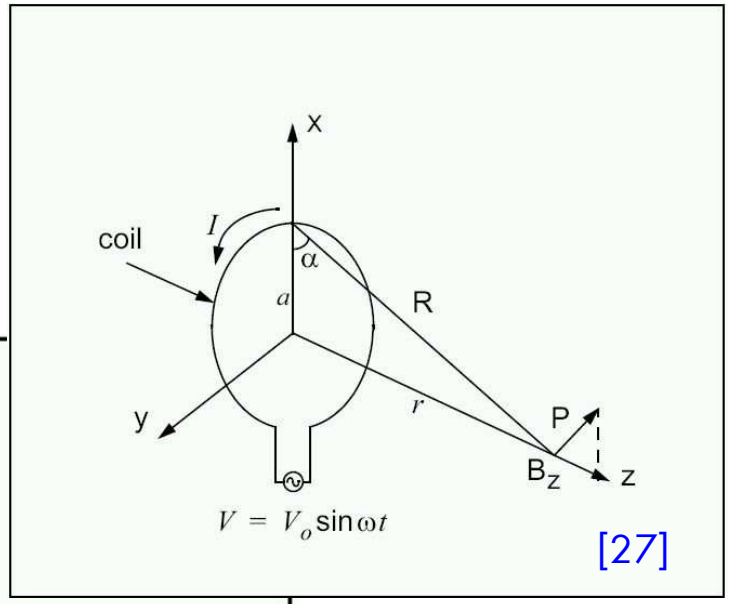
The tag itself is assumed to have no autonomous power source. It gets the energy for computation solely from the terminal's field.

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]

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

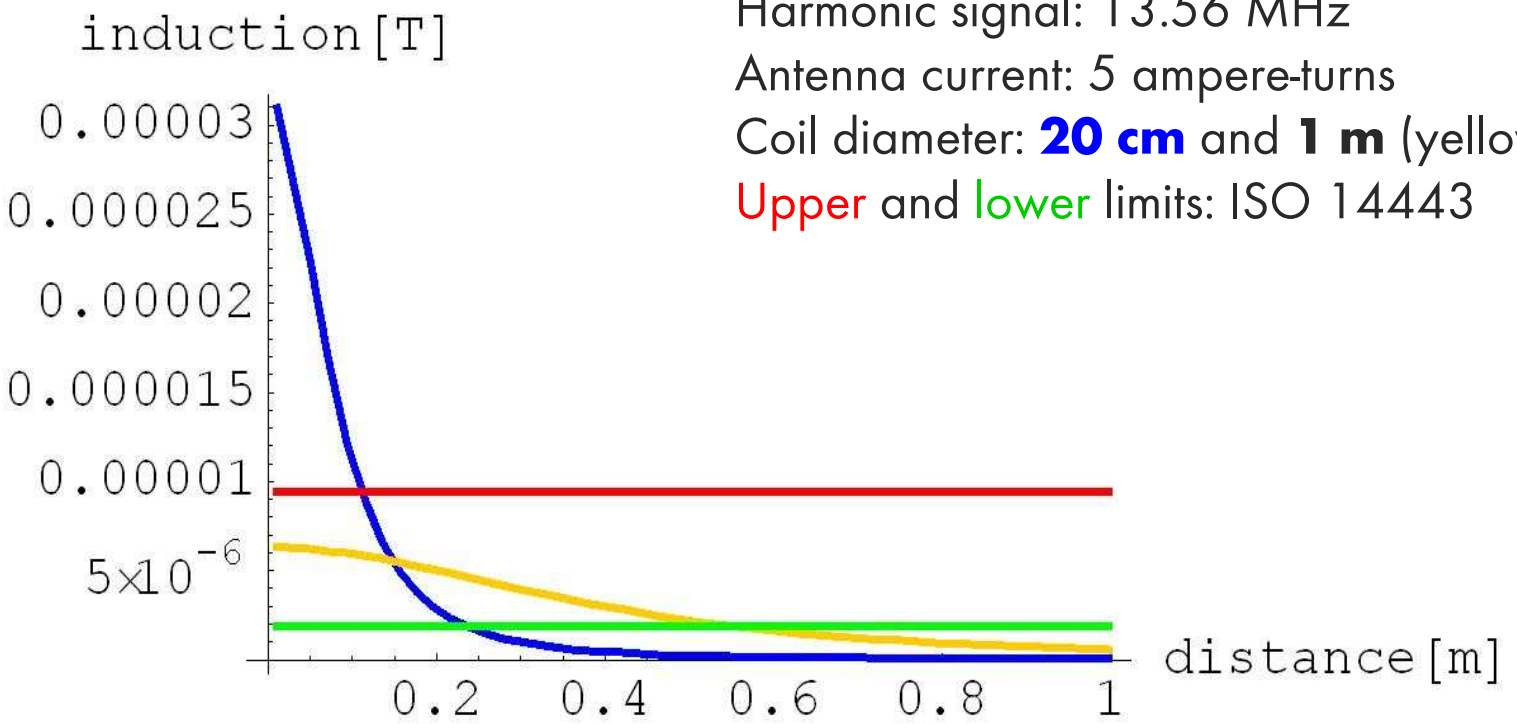
$$= \frac{\mu_o I N a^2}{2} \left(\frac{1}{r^3}\right) \quad \text{for} \quad r^2 >> a^2$$

[27]

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

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

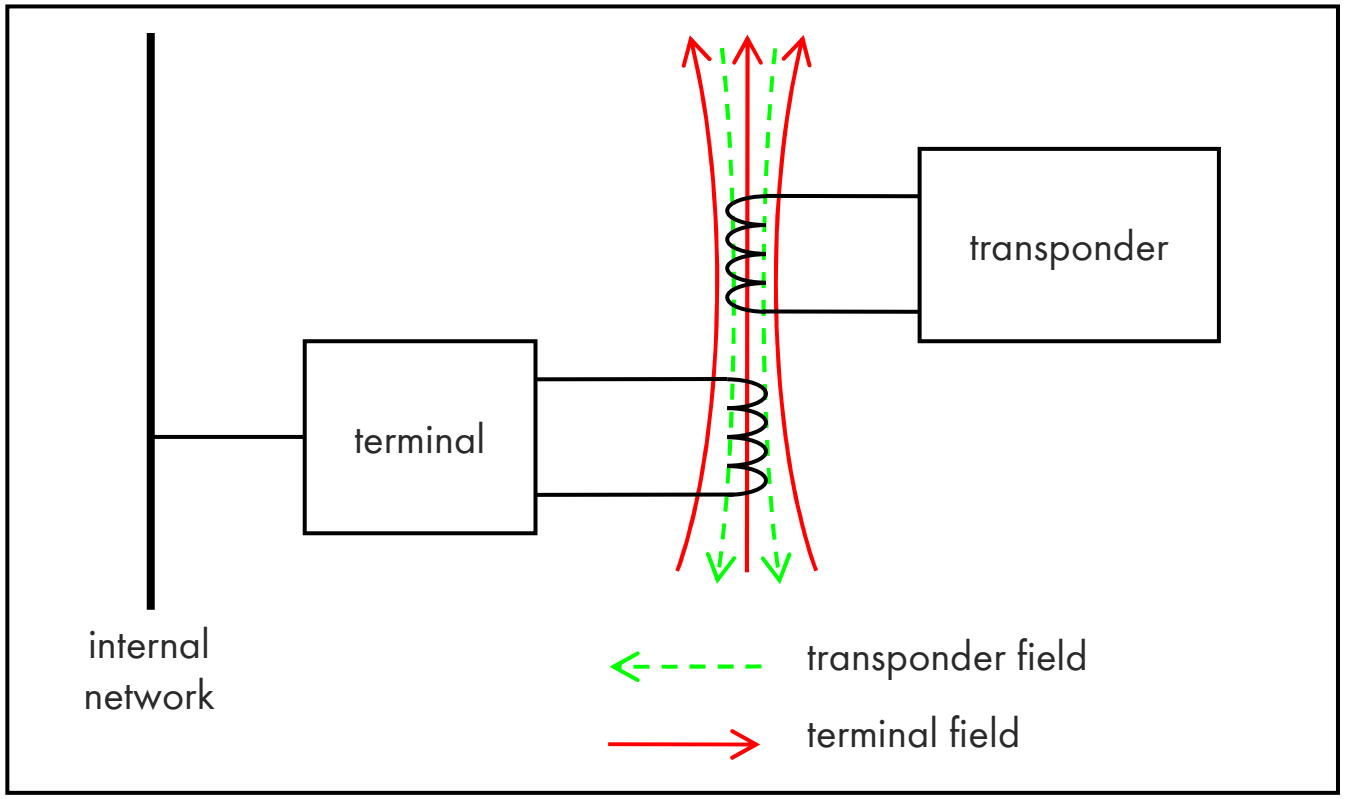
B_z Induced by a Circular Coil



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

Terminal – Transponder In LF/HF

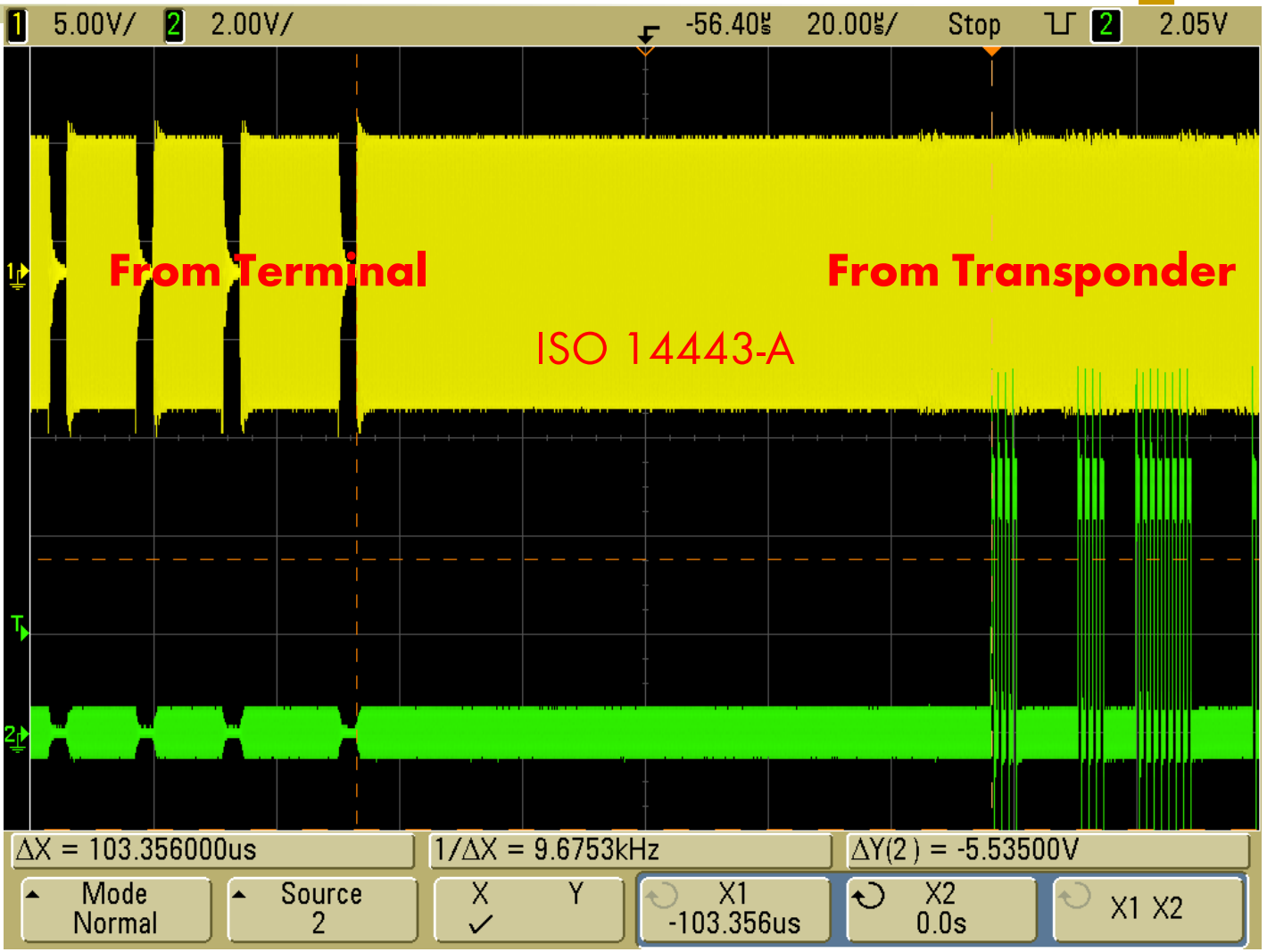
Data Communication



Terminal: direct amplitude modulation of the basic carrier
Transponder: 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 (LF/HF)

Method	**Distance**
Active communication with transponder	dozens of cm
Passive reception – both ways	units of m
Passive reception – terminal only	dozens of m
Active communication with terminal	dozens of m

Part TWO
Access Control Systems

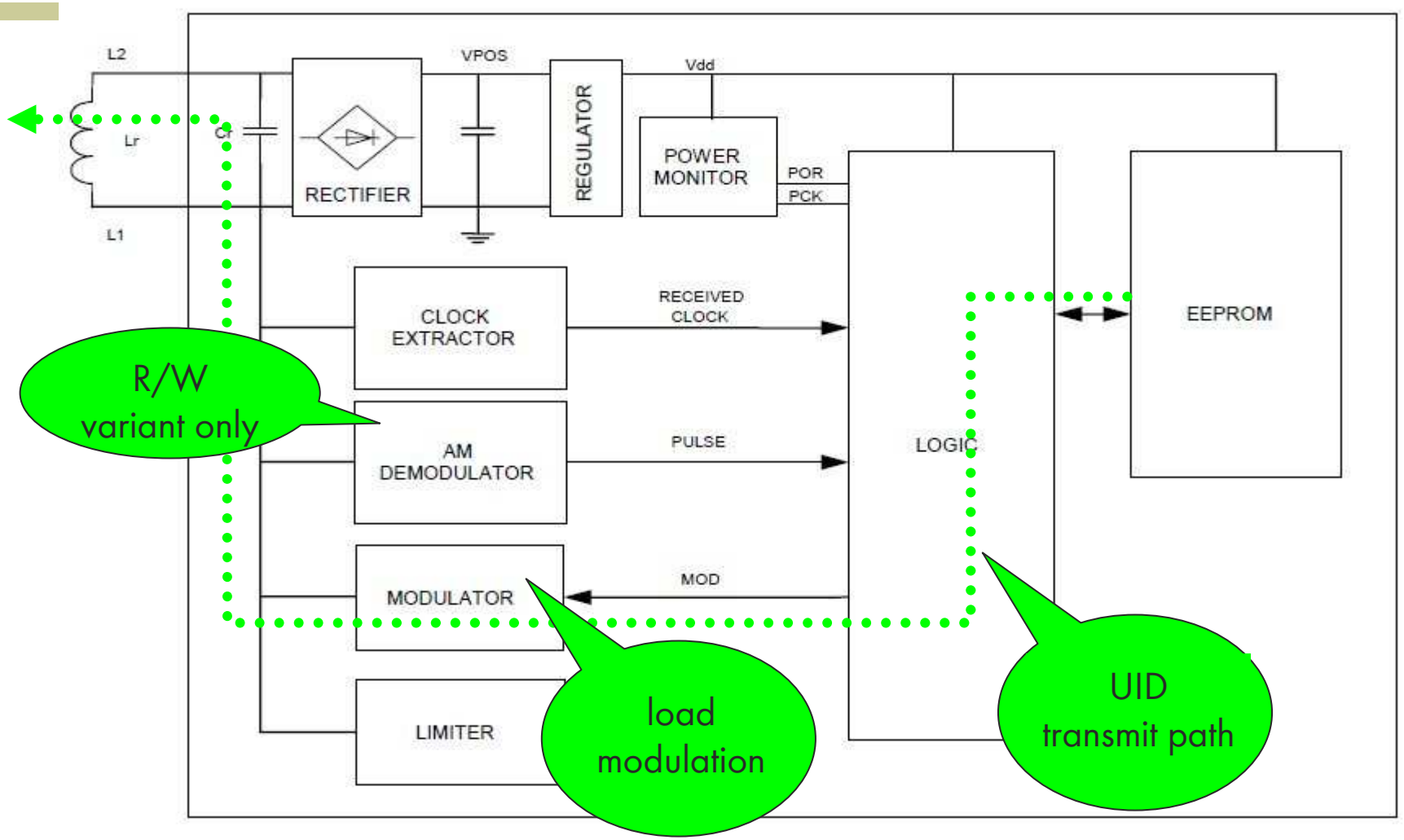
Penetration Test Scope

- The aim was to try to make a functionally equivalent duplicate of an existing access control card.
  - That is a theft of identity of some employee or temporary worker or an external supplier, etc.
  - See [49] for particular cases reported (CZ).

Unique-ID LF Transponders

- Serial memory programmed during the chip manufacturing or personalization phase
- When in the terminal (reader) field, they transmit the memory content automatically in a cycle
- There is no communication origin authentication
  - The transponder talks to anybody
  - The terminal listens to anybody
- Examples: EM Unique, HID Prox, INDALA

Unique-ID Transponder Overview



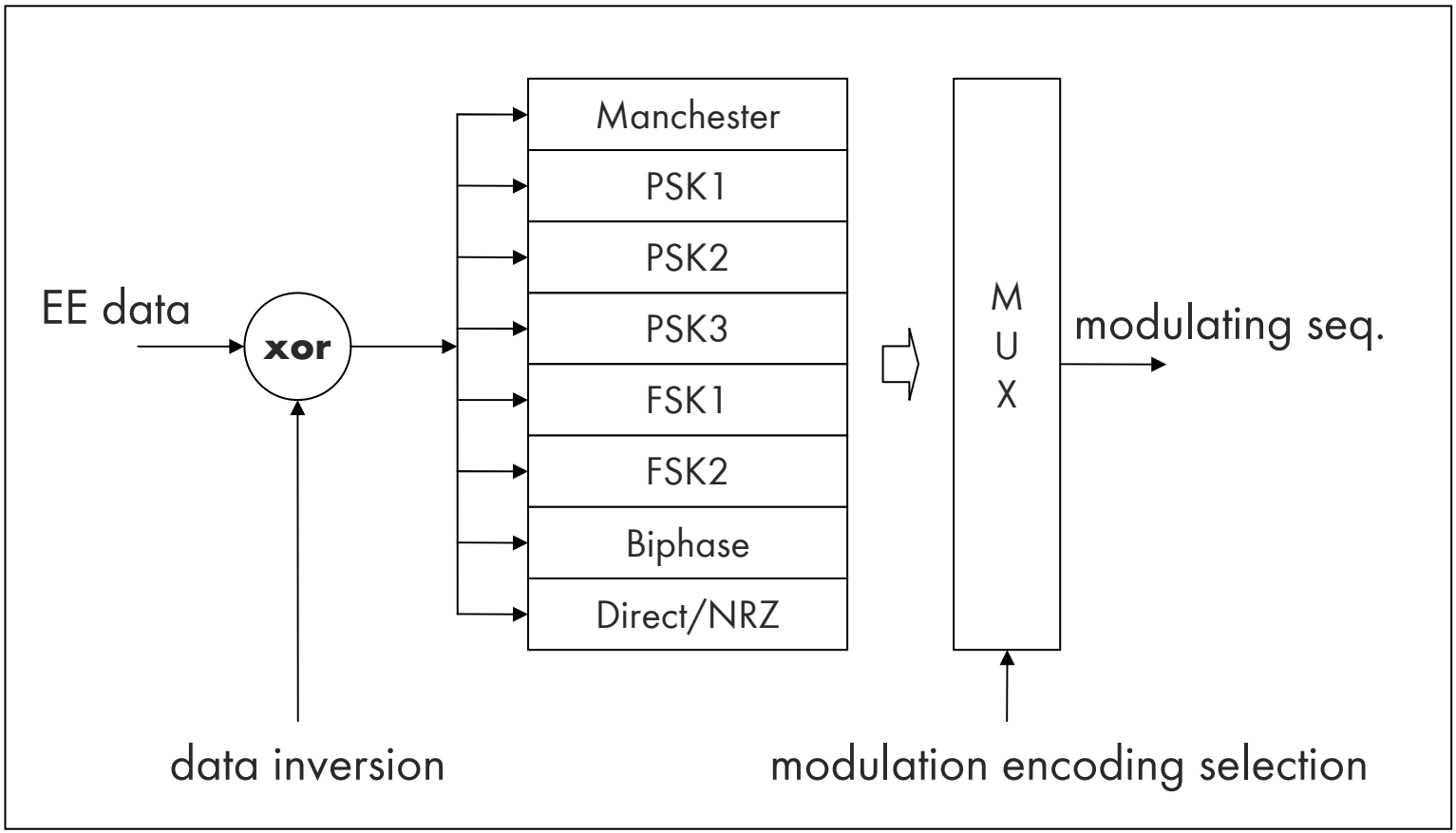
Where the Security Comes From

- It is important to note what the attacker really does **not** have to do:
  - To understand the meaning of the data stored in the transponder memory. The data can even be encrypted (and it still does not matter here).
- Necessary and sufficient condition to make the duplicate of the transponder is:
  - To effectively describe the control sequence driving the load modulator and to repeat this action in the terminal (reader) field later on.

Q5 – Queen of the LF Band

- Programmable LF transponder called “Q5”
  - 224 user defined EEPROM bits (330 b in total)
  - wide support of modulation and encoding schemes
- Variable chip packing – key fob, ISO card, etc.
- It was able to emulate all those LF “Unique-ID” transponders tested, so far
- Widely available on the market ☺
  - E.g. http://www.therfidshop.com/product_info.php?products_id=373

Q5 – Output Encoder Part

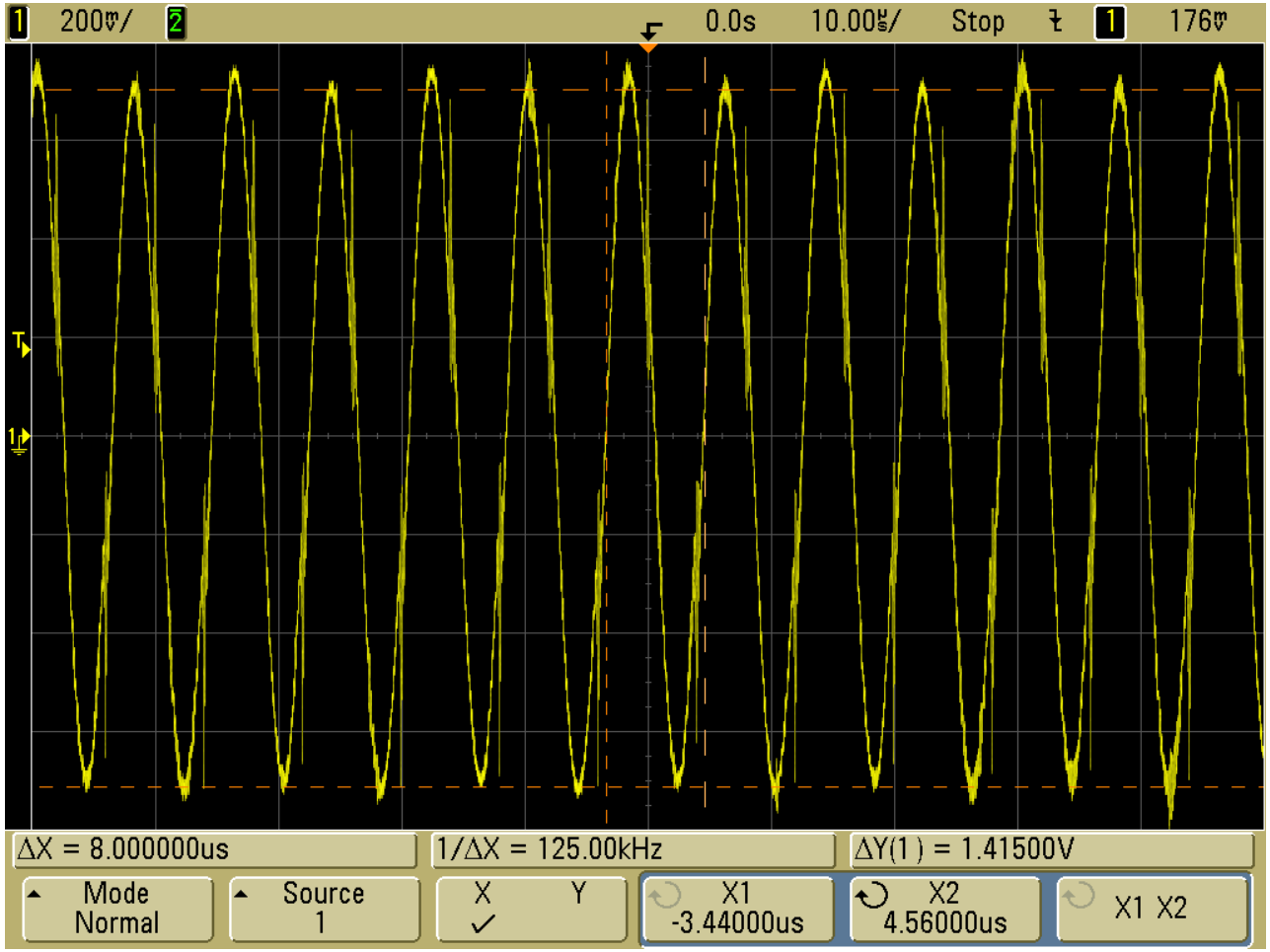


Using Q5 for an Attack

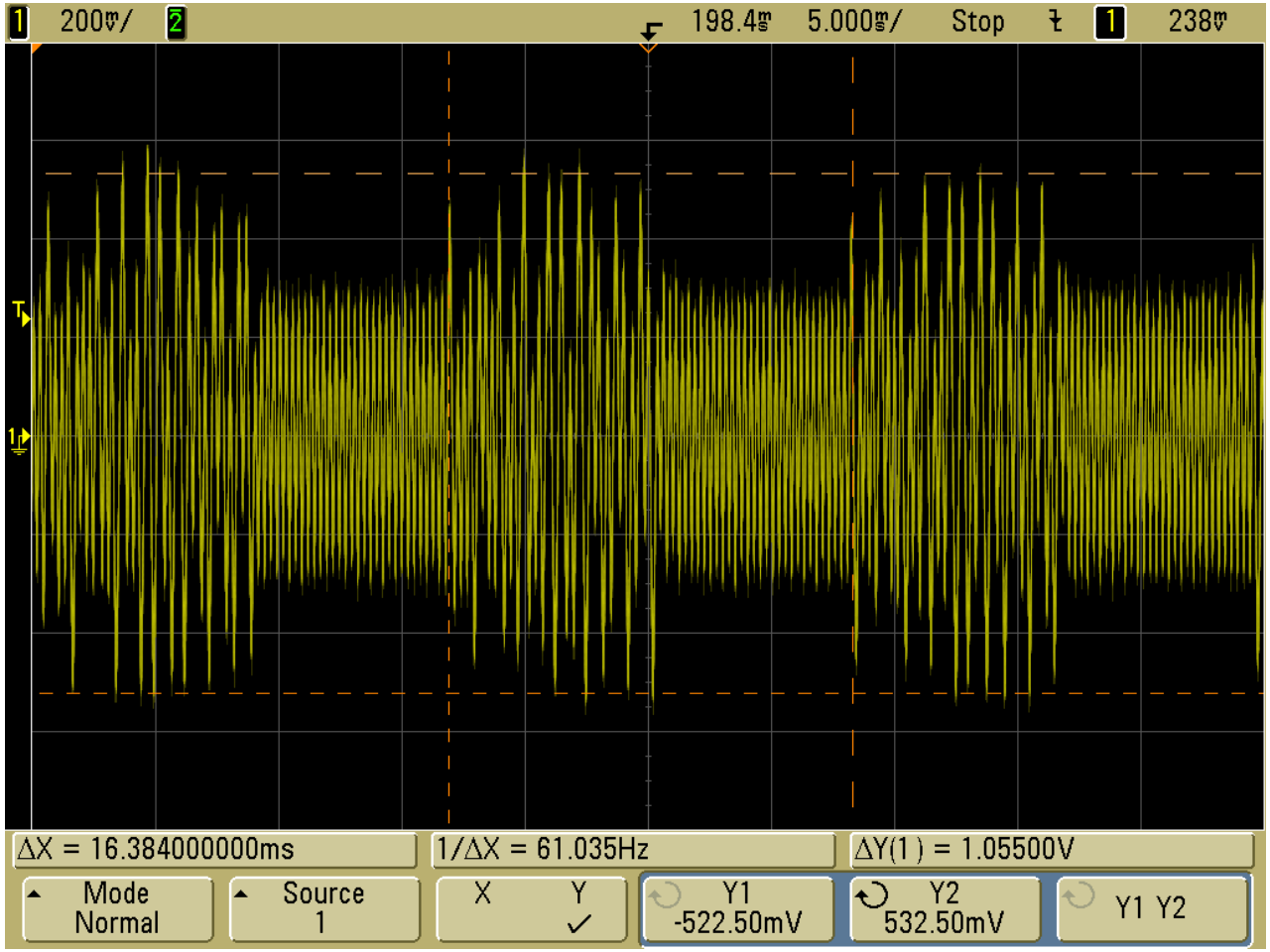
- Phase I – describing the modulating seq. of the original transponder
  - In theory, this can be a very hard problem, but…
  - … in practice, we seldom meet something "unique".
  - Let us be inspired by all those possible Q5 configurations!

- Phase II – making the duplicate
  - We store the modulating seq. into Q5 memory and program its output encoder/modulator…

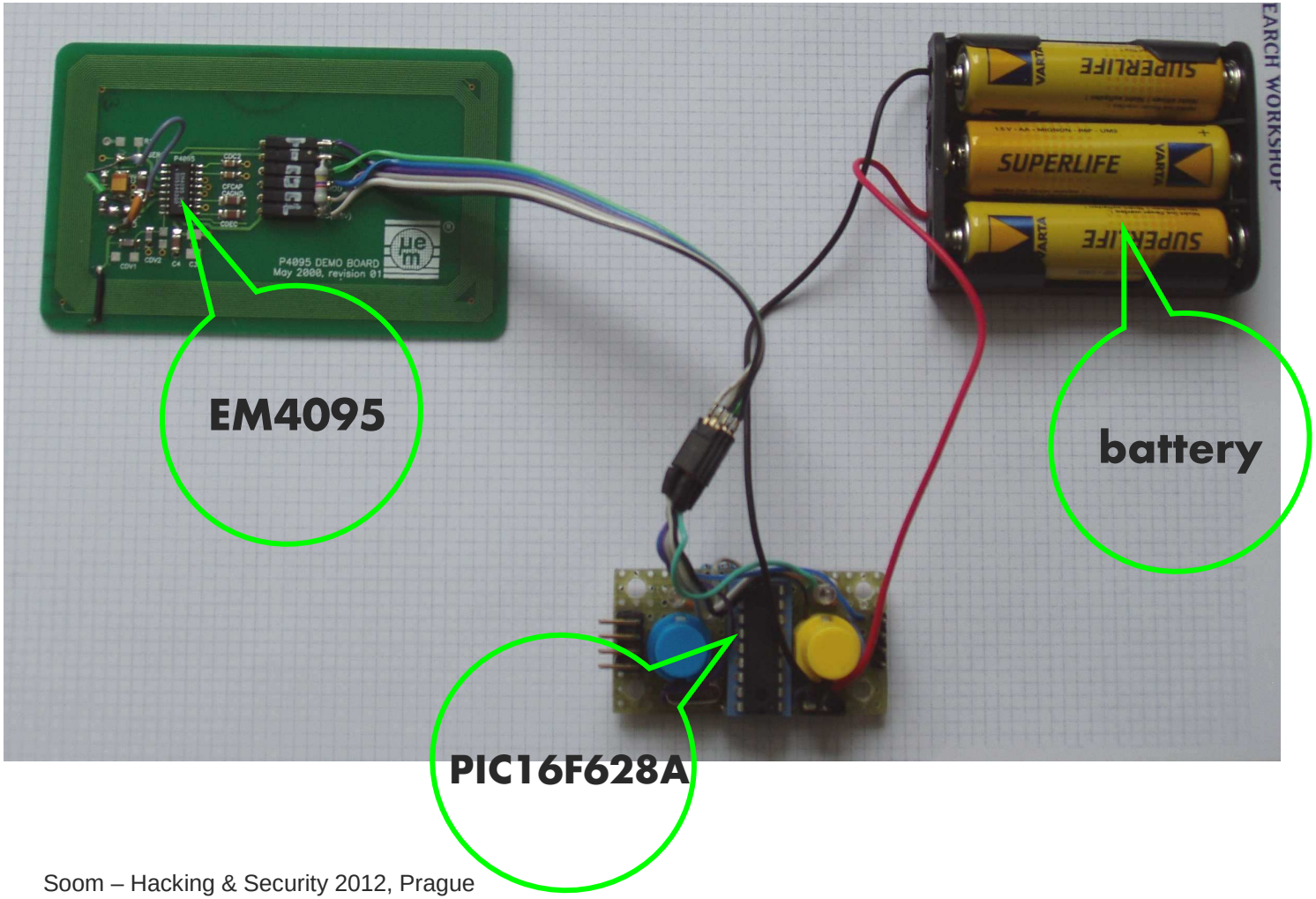
LAB: The Effect of Using a Subcarrier Frequency



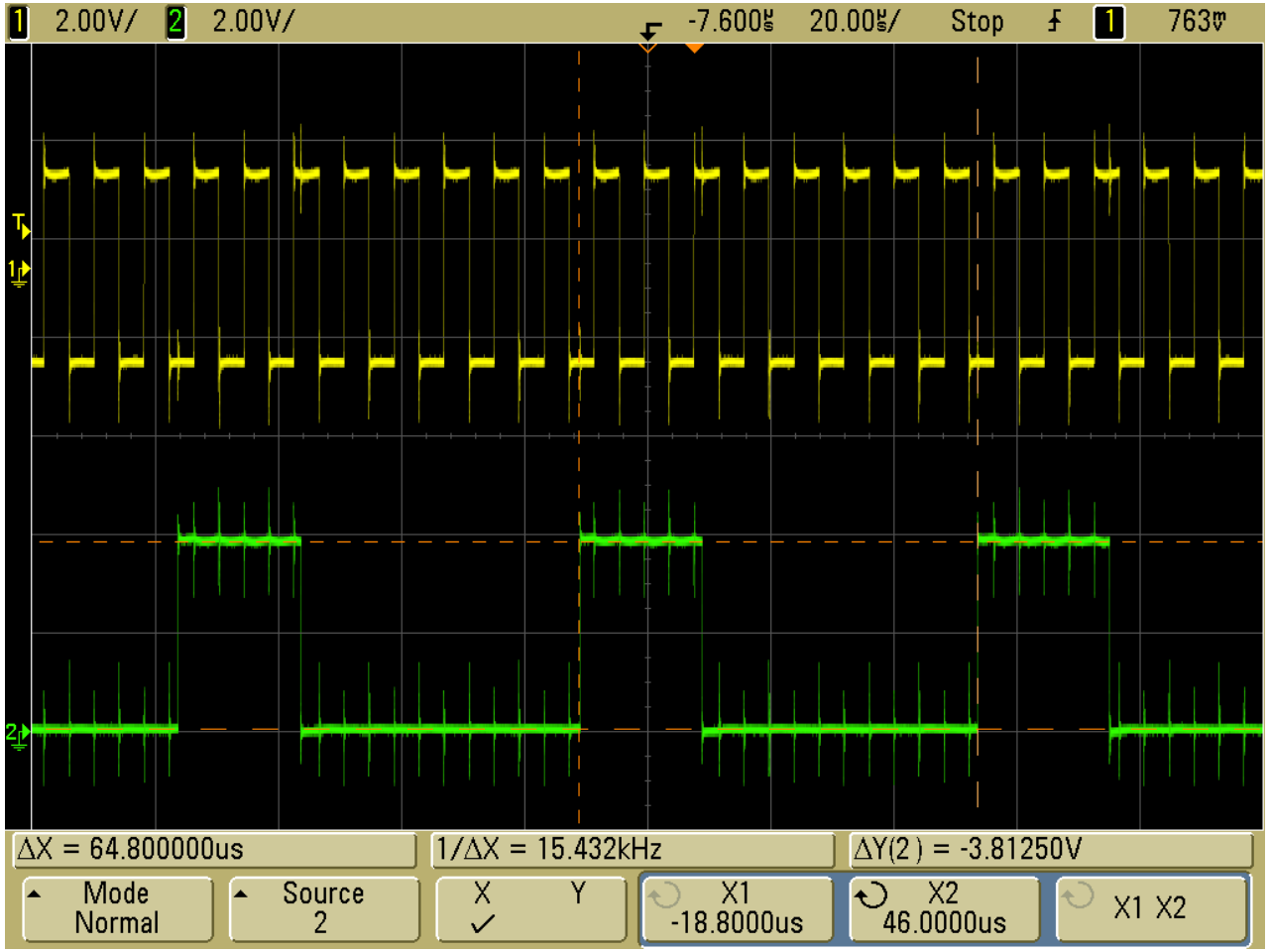
LAB: Subcarrier with Phase Modulation



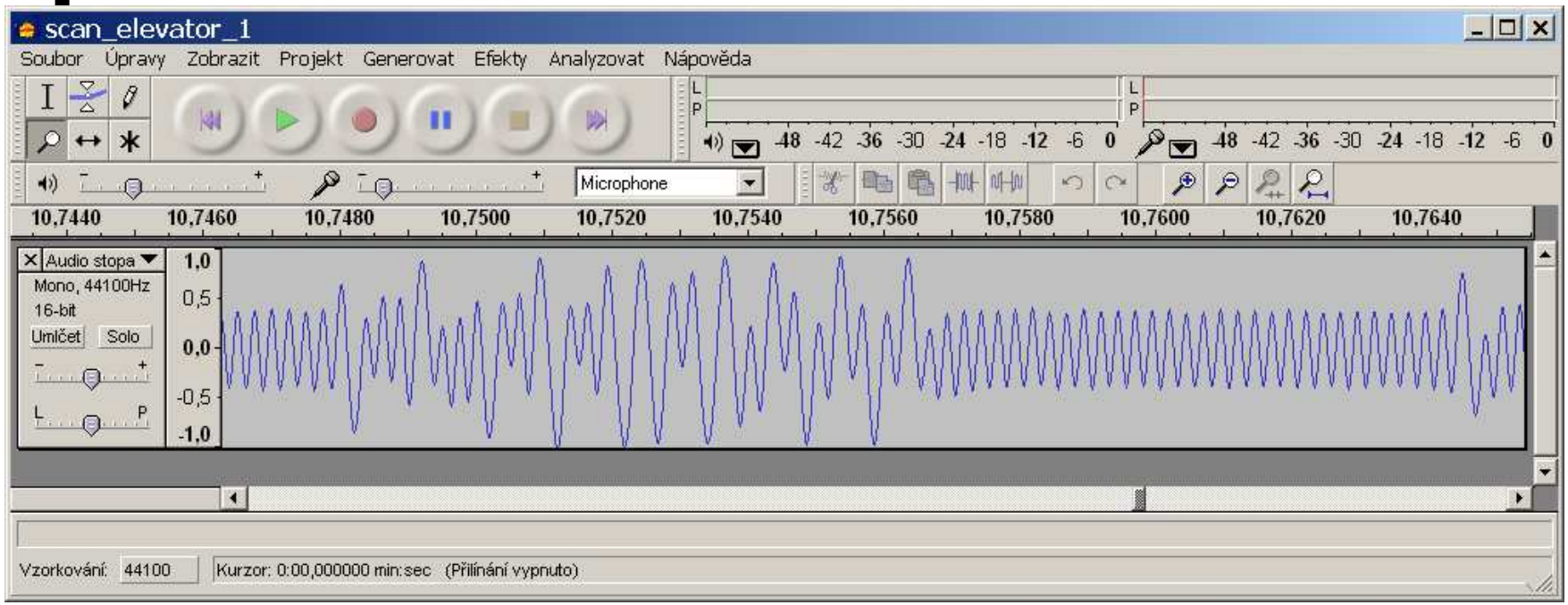
LAB: Ad Hoc Spyware



LAB: Frequency Modulation Disclosed by EM4095 (green)



Another Practical Scenario:
Eavesdropping in Elevator



LF band transponder data intercepted while its holder was authenticating to the reader in an elevator.
Distance: cca 0,5 m.
Receiver: Sangean ATS 909W.

Disclosing “The Secret”…

- EM Unique
  - direct manchester encoding, bitrate *f*/64, 64 bits in total
  - Q5 configuration word: 60 01 F0 04
- INDALA (1 particular setup)
  - subcarrier *f*/2 with phase shift keying, modulating sequence length of 64 bits
  - Q5 configuration word: 60 00 F0 A4
- HID Prox (1 particular setup)
  - 2 subcarriers *f*/8 and *f*/10 with frequency shift keying, modulating sequence length of 96 bits
  - Q5 configuration word: 60 01 80 56

MIFARE Classic

- Two basic ways of usage:
  - So-called „UID only“ mode which is functionally equivalent to the unique-ID transponders.
    - Easy to break using a transponder emulator.
  - So-called “cryptographic” mode that uses e.g. mutual authentication of transponder and terminal.
    - Broken totally in 2007-2009. At present, there are dozens of practically feasible devastating attacks.

MF Classic Cryptanalysis

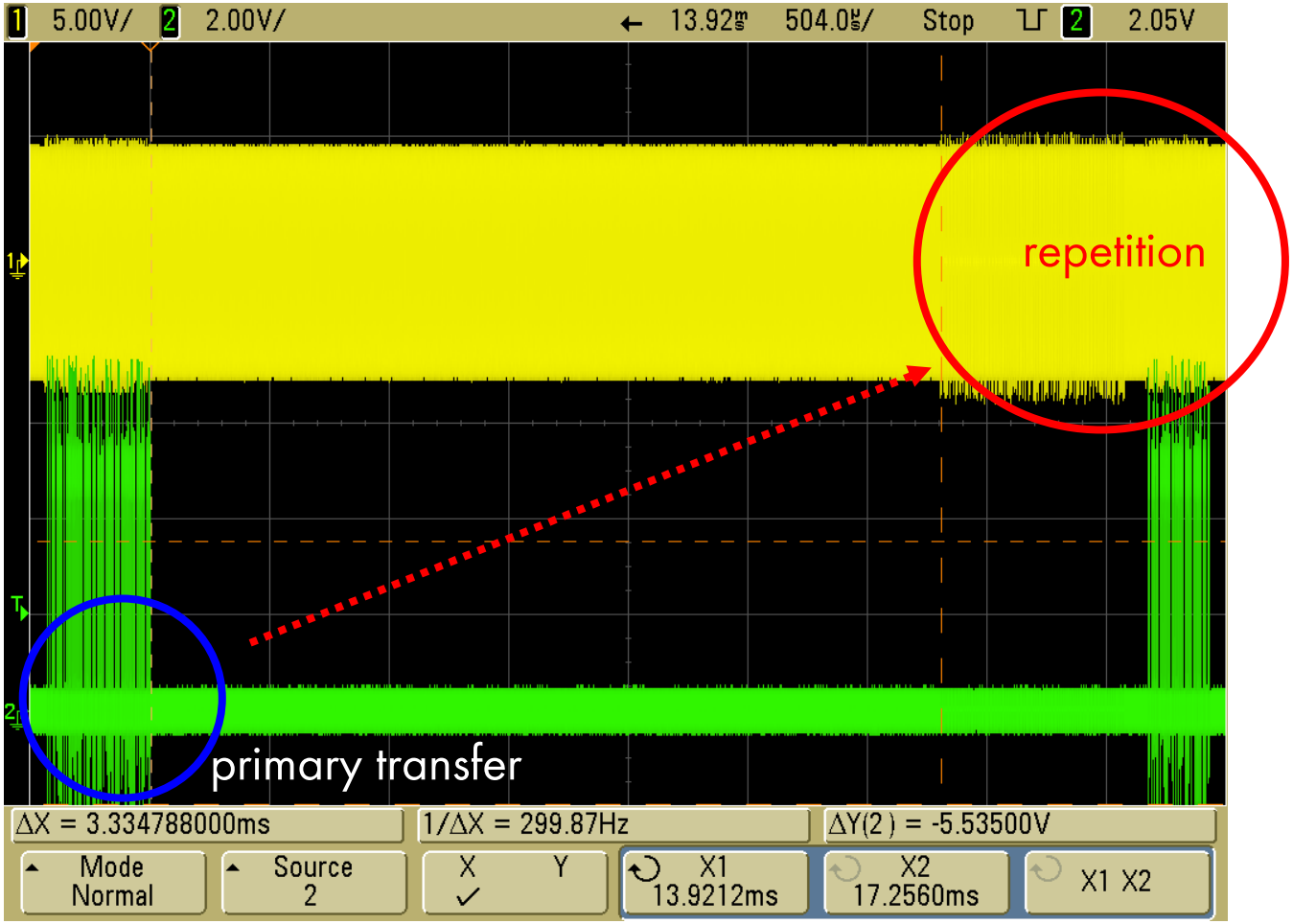
- Implications
  - Secret key recovery basing on an interaction with the terminal (reader) only
  - Secret key recovery from an intercepted terminal-transponder relation (it is enough to hear the terminal part only – feasible dozens of meters away)
  - Secret key recovery basing on an interaction with the transponder only
    - Totally devastating for a huge amount of micro-payment and public transportation applications.

MIFARE „UID only“

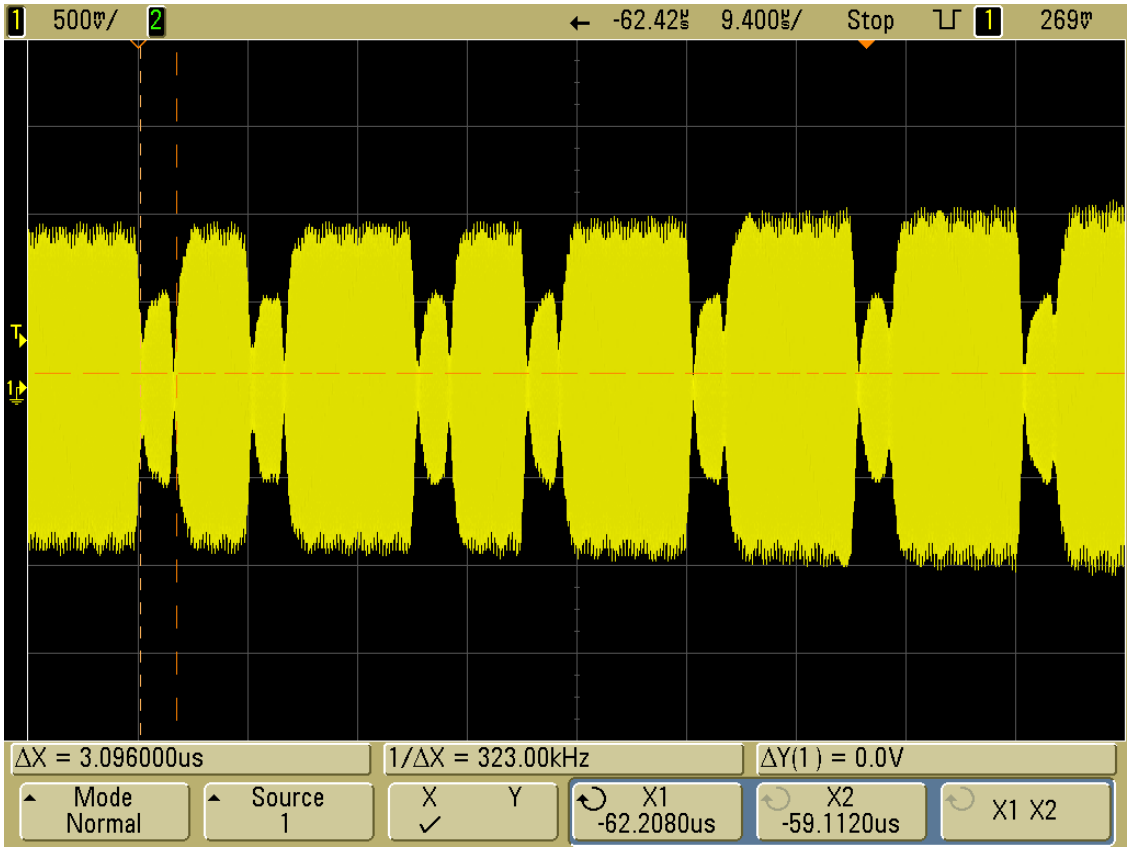
- In practice, huge amount of MF installations use this approach.
- In many aspects, the security of this approach is even worse than of the transponders in LF discussed before.
  - The communication protocol is standardized (ISO14443A).
  - UID interception is possible up to dozens of meters away.
  - Interestingly, similar security problem is already solved for UHF transponders [7].
- Only one obstacle here – there is no Q5 analogue for the HF band...
  - We need to build our own emulator – e.g. PicNic.

HF UID Interception

- Yellow trace: basic carrier
- Green trace: AM detector

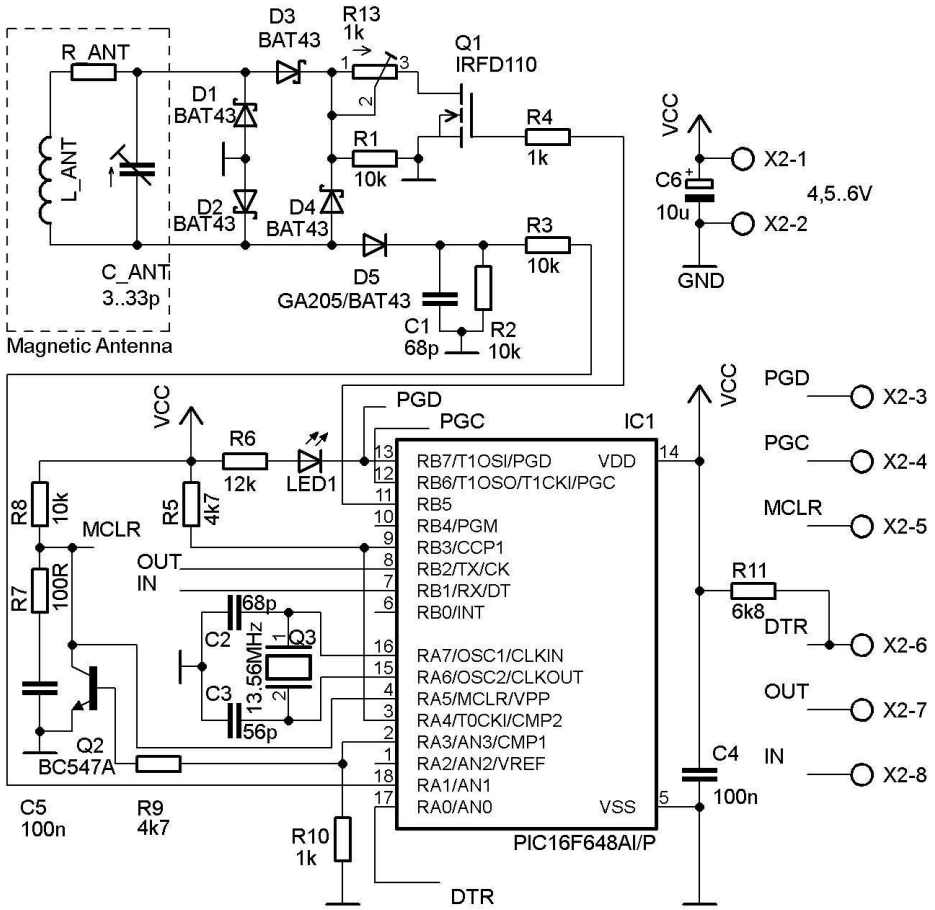


Real Life Experiment



Receiver AOR AR8600MK2, HF output at i.f. 10,7 MHz.
Distance cca 2 m, at least two readers in the field.

PicNic
HF Transponder Emulator



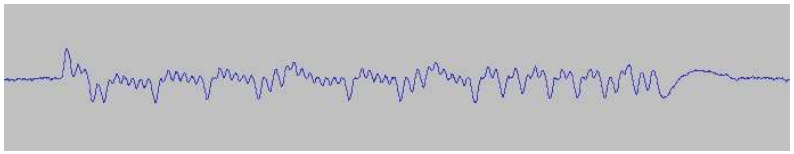
Details at http://crypto.hyperlink.cz/picnic.htm

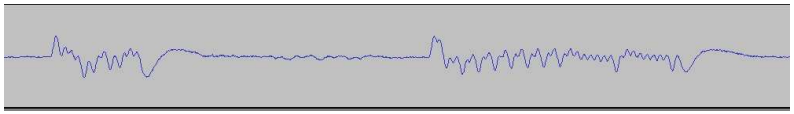
PicNic & CPLD Coprocessor

Another Real Life Scenario

Besides paying in the canteen, the same card opens the office door. Of course...
So, lets feel the power of technology convergence – take a lunch and go for a walk around the office... ☺

Immobilizers – Next Target?





125 kHz/WFM
receiver AOR AR8200MK3
co-driver's seat position

It concerns almost any car of any manufacturer.

Part THREE
RFID Wormholes

Wormhole (Relay Channel)

- *Let the RFID wormhole be any method enabling communication in between an out-of-range application transponder and the terminal.*
  - However, the sole presence of a transponder at the terminal is often directly linked to somebody's intension to e.g. open door, pay a bill, undergo electronic passport check, etc.

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.*"

Wormhole Attack Illustrated

Victim

Attacker A

near field inductive coupling
in between the *leech* and V's card (passport)
distance < 0,5 m (cf. [48])

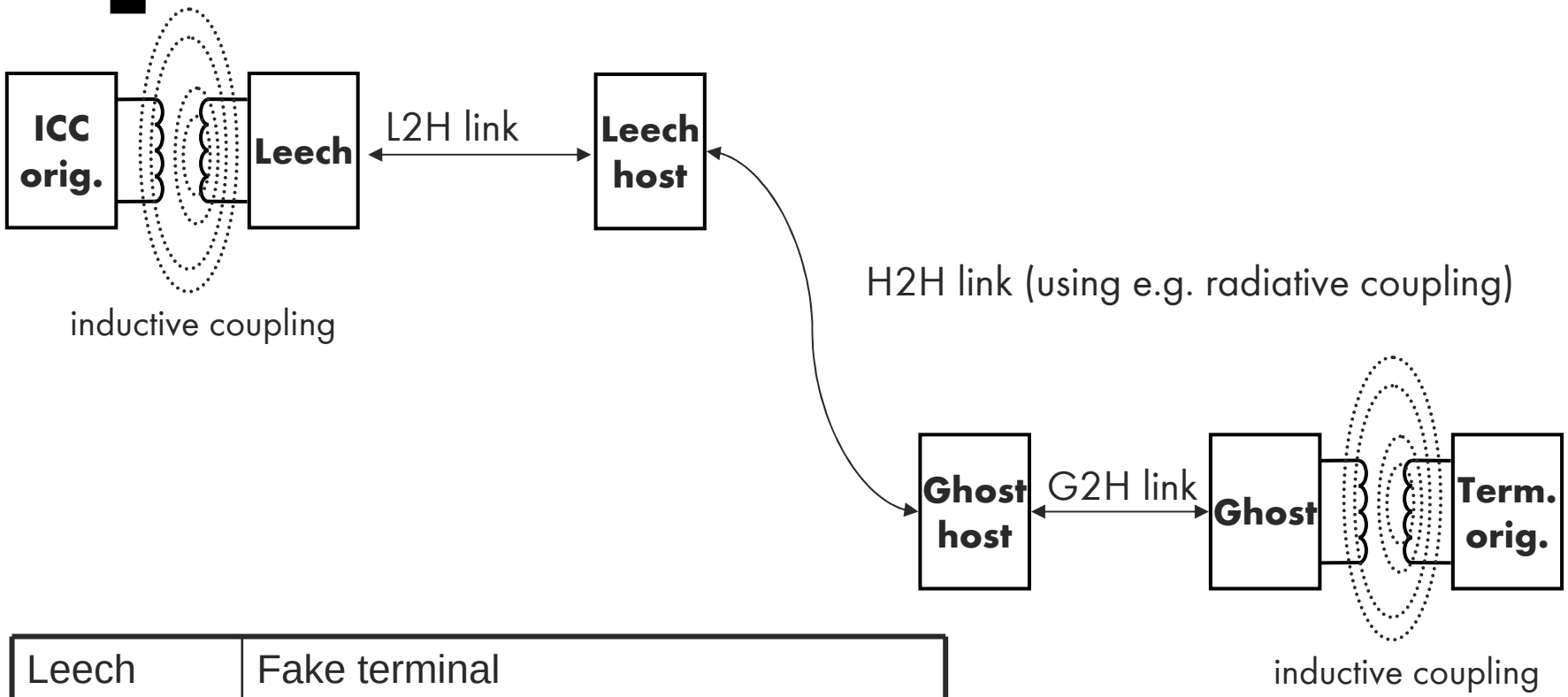
interconnection network

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

Attacker B

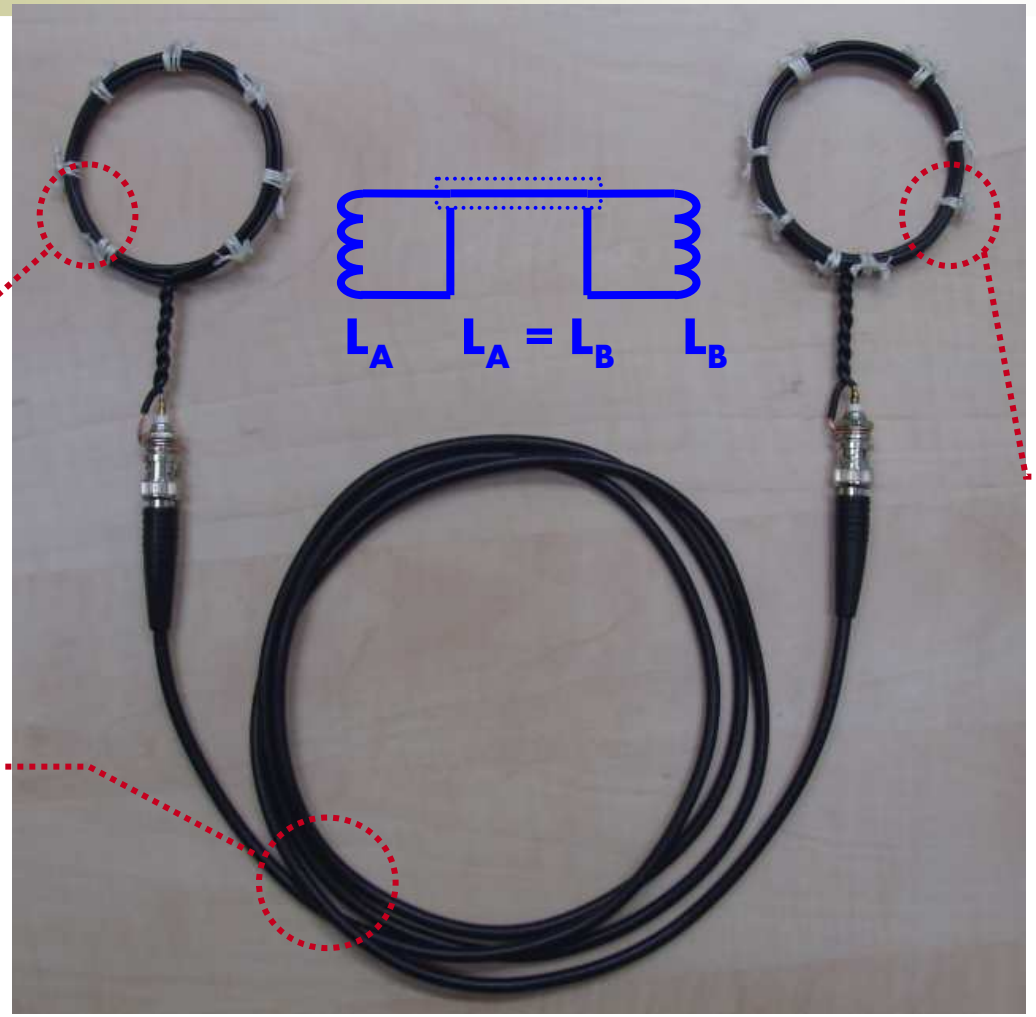
near field inductive coupling
in between the *ghost* and the inspection terminal

Wormhole Attack Scheme



Leech	Fake terminal
Leech host	Computing device driving the leech
Ghost	Fake transponder
Ghost host	Computing device driving the ghost

Do-It-Yourself HF Wormhole



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

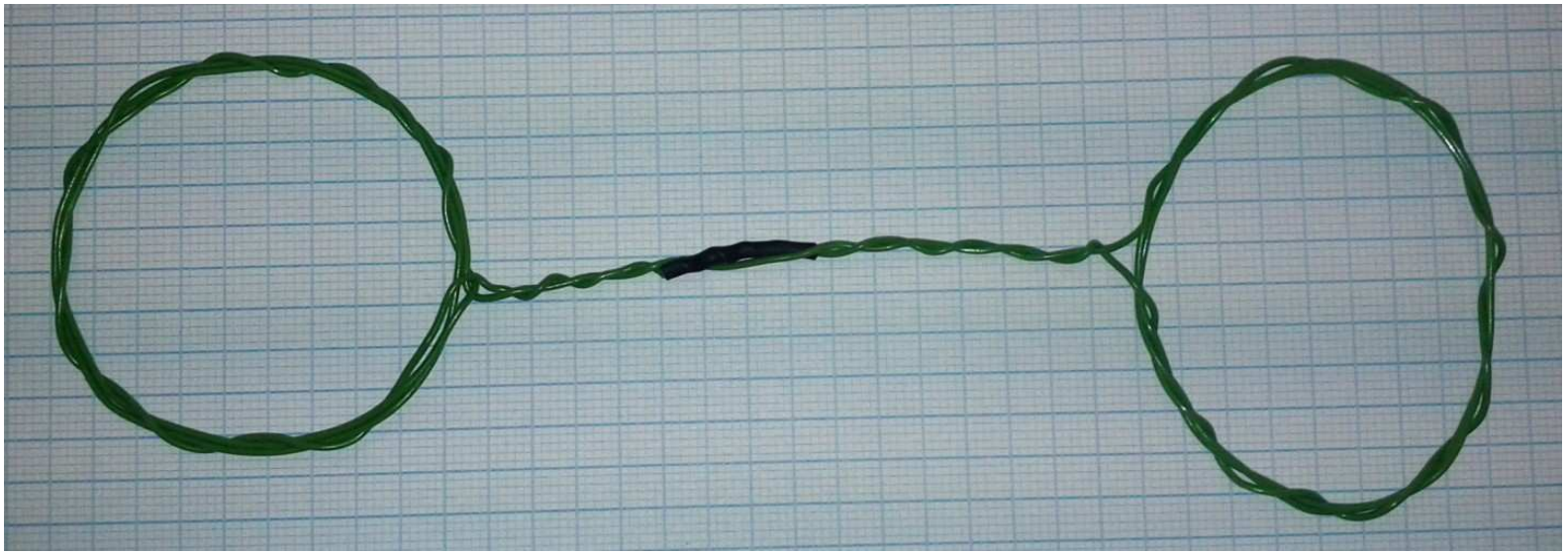
same as L_A

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

Wormhole In Access Control

Real successful experiment with the DIY wormhole in HF RFID access control.

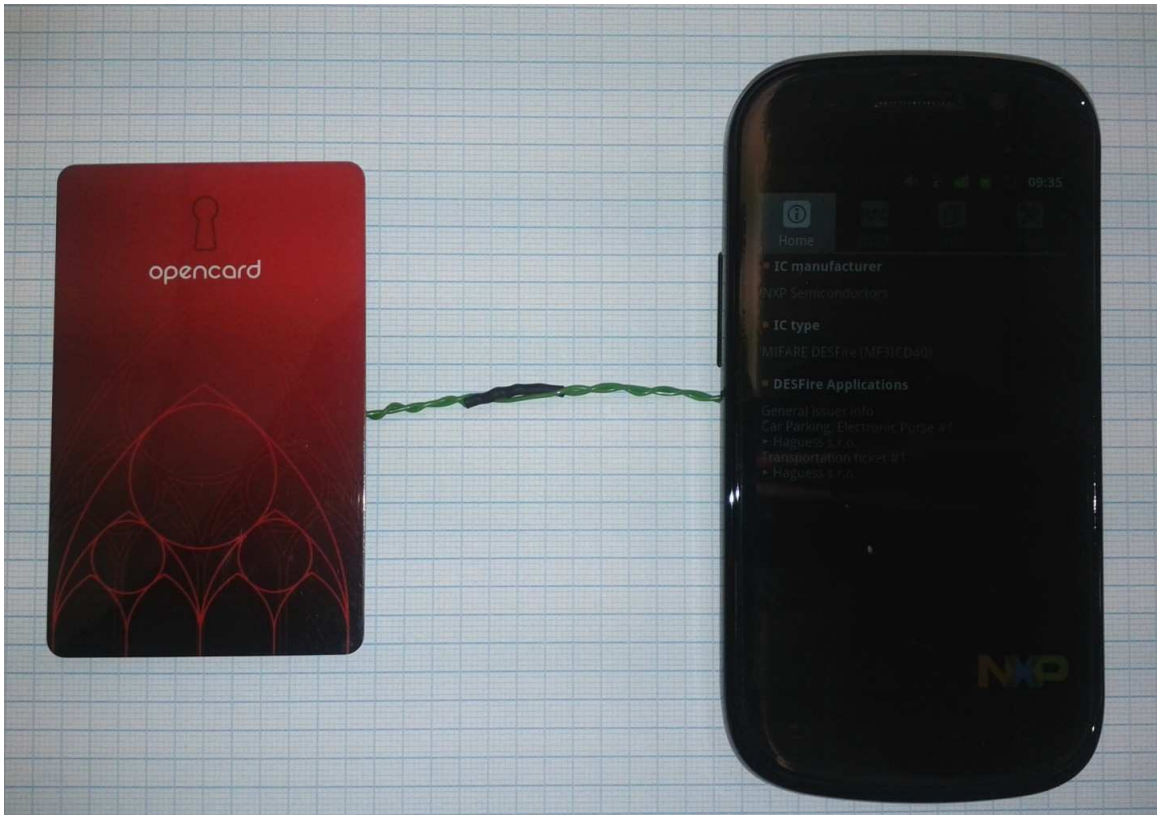
Wormhole for NFC Debugging



- Principal idea: Symmetric coils of 3 – 5 turns of CUL wire.
  - Later on, the coils can be deformed slightly on purpose to fit e.g. the NFC antenna geometry of a smart phone (cf. bellow).

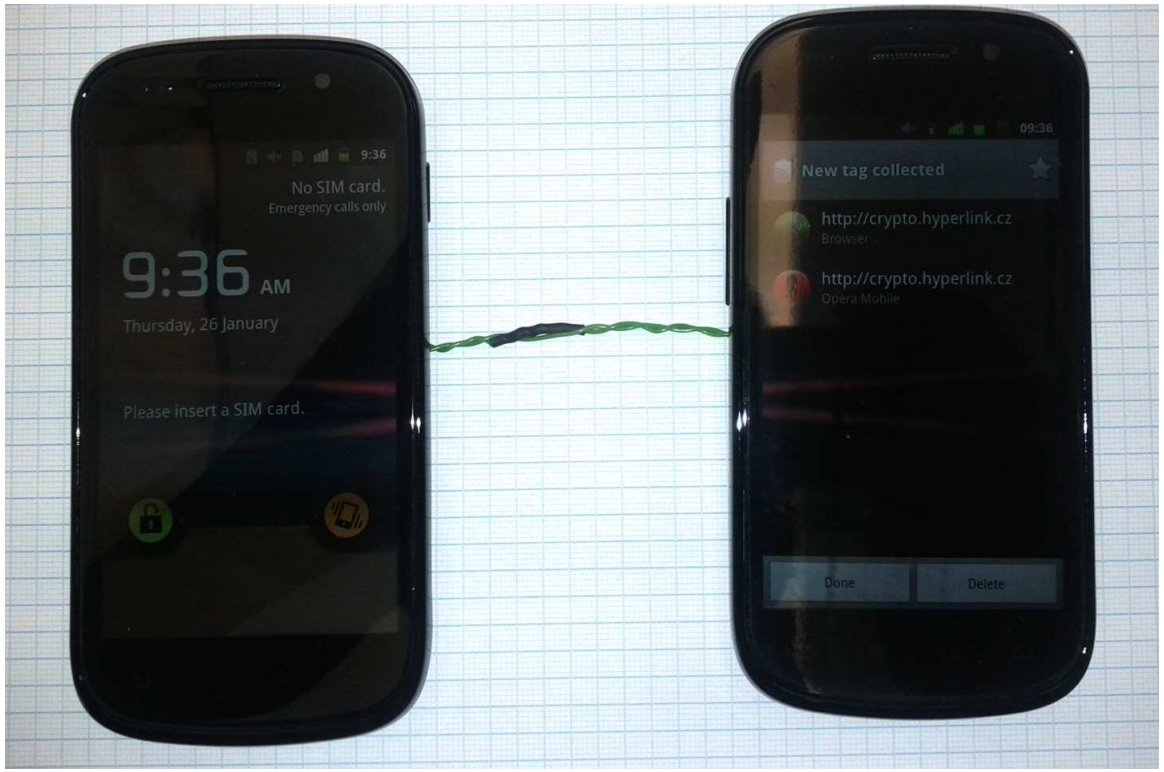
Simple Antenna Extender

Just Put the Stuff As-Is on Our Coils



- Google Nexus S (I9023) with Android 2.3.6 and TagInfo app working as passive-mode initiator with Prague's citizen card Opencard.

No More “96” Positions!



- Two Google Nexus S (I9023) with Android 2.3.6 working in reader-to-reader mode (user tag transfer).

Wormhole In Car Entry

- Interesting practical attack on keyless entry and start systems of modern cars was published in [12].
  - Focus on combined semi-passive LF/UHF transponder.
- By using LF wormhole, an attacker convinced the original transponder to send door opening request in UHF band.
  - The LF band circuit can be seen as a kind of implicit distance bounding protocol that should have ensured proximity distance between the key and the car.
  - Attack [12] shows, however, that this simple arrangement is weak.

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 “reader”)
  - Passive-mode target (or just a “transponder”)
  - Active-mode initiator/target (or just “reader-to-reader”)

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.
- Besides ISO, there is a lot of industry standards available at http://www.nfc-forum.org/specs/.

NFC vs. RFID I

- Correct to say NFC is an inductively coupled communication interface that shares many technical features with HF RFID.
  - This goes such far that NFC devices can directly play the role of certain HF RFID transponders or terminals (readers).
  - Of course, NFC also shares the general security properties related to communication interception, wormhole phenomenon, etc.

NFC vs. RFID II

- NOT correct to say that NFC directly equals to HF RFID.
  - There is, for instance, the reader-to-reader communication mode and a huge amount of protocols of upper layers [57] that are far beyond the established HF RFID.

- NEITHER correct, on the other hand, to say that NFC has nothing in common with RFID.
  - This is something Google tries to pretend to perhaps make NFC more sexy and harmless marketing word [42].
  - Such a view would, besides the others, hide the applications of HF RFID physical security analyses whose generalizations do (of course!) apply to NFC as well.
  - Perhaps, Google also wanted to emphasize NFC differs from **UHF** RFID significantly, which is true (in the same way as for HF RFID).

NFC and ISO 14443

- NFC-equipped device can address contactless smartcards world in two ways:
  - As a terminal (“reader”)
    - ISO 14443 A – passive-mode initiator
  - As a transponder emulator
    - ISO 14443 A – passive-mode target

NFC Controllers

- Handle NFCIP-1 protocol implementation.
  - Gradually replace previous generation of “terminal-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 [48].
  - 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 [48]).

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:
  - 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.
  - As far as we can say, most CLFs will be based on the next generation of NFC controllers - e.g. PN544 that seems to be further encapsulation of widely accessible PN53x family cores.

NFC In Smart Phone OS
(as of January 2012)

- The most systematic treatment can be found in Google Android.
  - Especially since Ice Cream Sandwich (4.0), but it already started with Gingerbread 2.3.3 [43].
  - Clearly, Google strives to become the leader in this area.
- Also interesting support in some BlackBerry devices (e.g. BB 9900 with BB OS API v7.0.0 [47], [59]).
- Apple seems to wait with iOS on how Google will eventually do [44], [45].
  - External NFC modules can be attached as accessories to iPhone [46].
    - This should principally work for iPad as well.

Android NFC

- The good points
  - Easy to learn, simple to use API.
  - Encapsulates even the communication with ISO 15693 transponders (initiator mode only).
- What is not so good
  - There is no support for passive-mode target.
  - Neither does it seem Google is willing to release it in public.
  - Apparently, this mode is "reserved" for first class citizens like banks, etc.
  - RIM, on the other hand, managed to provide this interface even to ”common naughty” programmers [47], [59].

Mobile + NFC + Malware = RISK

- Cf. Security and Privacy in Smartphones and Mobile Devices (SPSM) 2011 [58].
  - Malware running on a smart phone scans for RFID cards in its neighborhood.
    - Link occurs e.g. when a payment card and the mobile device are carried in the same pocket…
  - When it finds an interesting card, it interconnects that card with a remote controlling server.
  - Depending on the card type, the server decides on how to utilize the relayed connection – e.g. for making a contactless payment transaction.

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.

Experimental Setup [48]

Wormholes in Practice

- 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.*

Conclusion

- RFID security still deserves great attention across all frequency bands.
  - Security mechanisms employed for UHF are roughly comparable with LF. Furthermore, there is considerably increased threat of remote attacks [7].

- Hopefully, the following initiatives might contribute:
  - Low power microcontrollers,
  - Lightweight cryptography,
  - Business behind NFC and contactless payments,
  - Worldwide privacy protection effort.

Thank You For Attention

Tomáš Rosa
crypto.hyperlink.cz

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.

References VI

42. Pelly, N. and Hamilton, J.: *How to NFC*, Google I/O 2011, http://developer.android.com/videos/index.html#v=49L7z3rxz4Q
43. http://developer.android.com/guide/topics/nfc/index.html
44. Ankeny, J.: *Apple forgoes NFC m-payment integration with new iOS 5*, October 4, 2011, http://www.fiercemobilecontent.com/story/apple-forgoes-nfc-m-payment-integration-new-ios-5/2011-10-04
45. Evans, J.: *NFC: How Apple's iPhone gains on 'Google Wallet' plan*, October 26, 2011, http://blogs.computerworld.com/19162/nfc_how_apples_using_google_for_the_iphone_wallet
46. http://www.icarte.ca/
47. Francis, L., Hancke, G., Mayes, K., and Markantonakis, K.: *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*, Cryptology ePrint Archive: Report 2011/618
48. Rosa, T.: *RFID Wormholes – the Case of Contactless Smart Cards*, SmartCard Forum 2011
49. http://crypto.hyperlink.cz/cryptoprax.htm

References VII

50. Courtois, N.-T.: *The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime*, rev. May 2009, http://eprint.iacr.org/2009/137
51. Garcia, F.-D., et al.: *Dismantling MIFARE Classic*, ESORICS 2008, pp. 97-114, 2008
52. Garcia, F.-D., et al.: *Wirelessly Pickpocketing a Mifare Classic Card*, IEEE S&P 09, May 2009
53. MIFARE MF1 IC S50, Philips Semiconductors, Rev. 5.1, May 2005
54. Nohl, K., et al.: *Reverse-Engineering a Cryptographic RFID Tag*, USENIX 2008
55. http://code.google.com/p/crapto1/
56. Specification Q5B – ASIC for RFID, SID TAG Switzerland, SOKYMAT s.a., 2001
57. http://www.nfc-forum.org/specs/
58. Felt, A.-P., Finifter, M., Chin, E., Hanna, S., and Wagner, D.: *A Survey of Mobile Malware in the Wild*, SPSM'11, October 17, 2011
59. http://www.blackberry.com/developers/docs/7.0.0api/