RFID Penetration Tests
when the truth is stranger than fiction

Dr. Tomáš Rosa, tomas.rosa@rb.cz
Raiffeisenbank, a.s.

SmartCard Forum 2009
Agenda

- Technology overview
- Physical layer of LF and HF bands
- The „Unique ID “ phenomenon
- Penetration tests – selected aspects
  - Where the security of transponders comes from
  - The LF band – Q5 takes it all
  - The HF band – MIFARE: two ways to use, both of them bad
- Conclusion
### Radio Classification of Transponders

<table>
<thead>
<tr>
<th>Frequency band</th>
<th>Sub-class</th>
<th>Typical sort</th>
<th>Typical deployment</th>
<th>Operation Distance (order)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LF</strong></td>
<td>-</td>
<td>Memory card</td>
<td>Access system, immobilizer, implant, loyalty card</td>
<td>cm to m (*)</td>
</tr>
<tr>
<td>(100 to 150 kHz)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HF</strong></td>
<td>Vicinity card</td>
<td>Memory card</td>
<td>Access system, skipass, loyalty card</td>
<td>cm to m</td>
</tr>
<tr>
<td>(13.56 MHz)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proximity card</td>
<td>Contact-less smartcard</td>
<td>Access system, payment card, e-passport</td>
<td></td>
<td>cm</td>
</tr>
<tr>
<td><strong>UHF</strong></td>
<td>-</td>
<td>Memory card</td>
<td>Stock control</td>
<td>cm to 10s m</td>
</tr>
<tr>
<td>(430 – 2450 MHz)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) rare configurations with low consumption read-only cards and high power, high dimension readers
Employs the behavior of so-called near field of the transmitter
- Threshold is approx. $\frac{\lambda}{2\pi}$, $\lambda = \frac{300}{f}$ [m, -, MHz]
- Uses the well known effect of inductive coupling
- Arrangement „terminal antenna – chip antenna“ can be viewed as a high frequency transformer
Feeding Up a LF/HF Transponder

\[ V = V_0 \cos(\omega t) \]

\[ I = I_0 \sin(\omega t) \]

[lee: AN710, Microchip 2003]
Biot-Savart: \( \mathbf{dB} = \mu_0 N I (\mathbf{R} \times \mathbf{dc}) / (4\pi |\mathbf{R}|^3) \)

Solution for an ideal circular loop antenna.

\[
B_z = \frac{\mu_0 I N a^2}{2(a^2 + r^2)^{3/2}}
\]

\[
= \frac{\mu_0 I N a^2}{2} \left( \frac{1}{r^3} \right) \quad \text{for} \quad r^2 >> a^2
\]

[Lee: AN710, Microchip 2003]
$B_z$ vs. Distance vs. Loop Diameter

HF band: 13.56 MHz
Current: 5 ampere-turns
Loop diameter: 20 cm a 1 m
Intensity bounds: ISO 14443
Talking with the LF/HF Transponder

Terminal: direct amplitude modulation of the basic carrier

Chip: load modulation resulting in indirect amplitude/phase modulation of the basic carrier
### When the Distance Matters

<table>
<thead>
<tr>
<th>Method</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active communication with the chip</td>
<td>dozens of cm</td>
</tr>
<tr>
<td>Passive reception – chip and terminal</td>
<td>units of m</td>
</tr>
<tr>
<td>Passive reception – terminal only</td>
<td>dozens of m</td>
</tr>
<tr>
<td>Active communication with the terminal</td>
<td>dozens of m</td>
</tr>
</tbody>
</table>
A huge majority of access control systems in Czech Republic uses:

- either so called Unique ID transponders in LF band,
- or MIFARE (Classic) chips in HF band.
Unique ID 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
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 i.a. mutual authentication of transponder and terminal.
    - Broken totally in 2007-2009. At present, there are dozens of practically feasible devastating attacks.
Known weaknesses

- Insufficient key length of Crypto1 alg. (48 bits)
- Possibility to stabilize the PRNG state
- Non-linear filter tap symmetry in LFSR of Crypto1
- Conditional multidifferential property of Crypto1
- Fault side channel in the authentication protocol
- Inappropriate order of encryption and error control codes
- ...

SmartCard Forum 2009
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 Classic – What next?**

- **MIFARE DESFire**
  - Defeats number of attacks while (!) introducing large amount of another possible weaknesses.
  - Obviously spoiled interconnection in between cryptography and the application protocol.
  - There is a threat of attacks based on erred configurations (the architecture encourages them)...

- **MIFARE Plus**
  - Up to now (spring 2009) there is no technical documentation nor engineering samples available (should have been available in Q3 of 2008).
Despite no necessary dependence, the majority of applications offer the MF Classic profile only. Thus sharing a number of original weaknesses as well.

It is a question whether these profiles eliminate at least those weakness, that are possible to fix without a compatibility loss.

Weak PRNG and the fault side channel in the authentication procedure.
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.
Unique ID Transponder Overview

- R/W variant only
- Load modulation
- UID transmit path
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 😊
Q5 – Output Encoder Part

EE data → XOR → data inversion

Modulation encoding selection:
- Manchester
- PSK1
- PSK2
- PSK3
- FSK1
- FSK2
- Biphase
- Direct/NRZ

MUX → modulating seq.
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 led 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...
Examples of the Phase I follow...
LAB Example: The Effect of Using a Subcarrier Frequency
LAB Example: Subcarrier with Phase Modulation
LAB Example: Ad Hoc Spyware

EM4095
PIC16F628A
battery
LAB Example: 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 „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
- Only one obstacle here – there is no Q5 analogue for the HF band...
  - We need to build our own emulator – e.g. PicNic.
PicNic: HF Band Transponder Emulator

For details cf. crypto.hyperlink.cz/picnic.htm
On MF UID Interception

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

repetition

primary transfer

$\Delta X = 3.334788000 \text{ms}$

$\frac{1}{\Delta X} = 299.87 \text{Hz}$

$\Delta Y(2) = -5.53500 \text{V}$

$\text{Mode} \quad \text{Normal}$

$\text{Source} \quad 2$

$\text{X} \quad \text{Y}$

$X_1 \quad 13.9212 \text{ms}$

$X_2 \quad 17.2560 \text{ms}$
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. UID can be read clearly, still without any preprocessing (becomes necessary with increasing distance).
Besides paying in the canteen, the same card opens the office door. Of course...
So, let's feel the power of technology convergence – take a lunch and go for a walk around the office... 😊
Conclusion

- Huge majority of contemporary access control systems is vulnerable to an identity theft attack.
  - Transponders serve the role of subject identification only.
  - They do not provide any reasonable subject authentication!
- Huge majority of physical security managers is not aware of such risk.
  - Seeing the risk requires noting that computer systems play a crucial role (even) in the area of physical security.
  - Material engineering is just not enough for physical security risk assessment any more.
  - Common principles of information security have to be applied as well.
  - Especially, RFID systems shall be subject to the penetration testing.
Thank you for your attention...

For more cf.: crypto.hyperlink.cz/cryptoprax.htm

Dr. Tomáš Rosa
Raiffeisenbank, a.s.
tomas.rosa@rb.cz