Theoritical Limits of ISO/IEC 14443 type A Eavesdropping Attacks

Florian Pfeiffer (perisens)
Klaus Finkenzeller (Giesecke & Devrient)
Erwin Biebl (Fachgebiet Höchstfrequenztechnik – TUM)
12.06.2012
Outline

- Motivation
- Theoretical approach
- Characterization of an exemplary transponder
- Uplink & Downlink results
- Conclusion
Eavesdropping is an unauthorized detection of the bidirectional data communication between reader and tag.
Motivation

Published practical and theoretical results show considerable differences in the eavesdropping range (ISO/IEC 14443 A)

- ~10cm range of a typical reader system
- Oscilloscope measurement [Finke 2004] 2 m
- Reading card ID [BSI 2008] 2.3 m
- Reading card ID [Hancke 2008] 1 to 3 m (different measurement locations)
- Reading card ID (SNR of 6dB) [Novotny 2008] 8 to 15 m (different tokens)
- Theoretical study (BER of 0.1%) [NXP 2007] 2.4 to 38.6m (different environments)
A successful attack requires that the attacker is able to detect the bidirectional data with a sufficient accuracy.

In a real environment, noise degrades the signal detection and causes bit errors with a certain probability. To ensure a reliable detection the bit error rate (BER) has to be low enough.
Required Bit Error Rate

Typical frame length in ISO/IEC 14443 systems require a Bit Error Rate of 0.01% for reliable detection.

Probability that a frame with N-bits arrives without any bit error = \((1 - BER)^N\)

<table>
<thead>
<tr>
<th>Data length</th>
<th>BER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 %</td>
</tr>
<tr>
<td>2 Bytes</td>
<td>85.1 %</td>
</tr>
<tr>
<td>4 Bytes</td>
<td>72.5 %</td>
</tr>
<tr>
<td>256 Bytes</td>
<td>0 %</td>
</tr>
</tbody>
</table>

No error correction considered here (according to ISO/IEC 14443), but...

- error detection (CRC, parity) could be used for error correction
- by forcing a frame retransmission (e.g. by interfering single bits) interleaving could be used to improve detection
A reliable eavesdropping with a defined bit error rate (BER) requires a certain signal-to-noise ratio (SNR).

ISO/IEC 14443 A
- Amplitude Shift Keying (ASK)
- Additive white Gaussian noise
- Coherent demodulation
- Matched filter
- Optimum threshold detector

\[
BER = \frac{1}{2} \text{erf}\left(\frac{1}{2} \sqrt{\frac{SNR_{HF}}{1}}\right)
\]

<table>
<thead>
<tr>
<th>BER</th>
<th>SNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01%</td>
<td>11.4dB</td>
</tr>
<tr>
<td>0.1%</td>
<td>9.8dB</td>
</tr>
<tr>
<td>2%</td>
<td>6dB</td>
</tr>
</tbody>
</table>
Minimum Signal Field Strength $H_{\text{min}}$

The minimum magnetic field strength $H_{\text{min}}$ of the desired signal (at the location of the attacker) can be derived from noise level and required SNR:

- **Signal:**
  \[ H_{\text{Signal,min}} \text{ [dBuA/m]} = H_{\text{Noise}} \text{ [dBuA/m]} + SNR \]

- **Noise:**
  \[ H_{\text{Noise}} \text{ [dBuA/m(rms)]} = F_{\text{am}} - 78.5 + 20 \log_{10} \left( \frac{B}{\text{Hz}} \right) \]

- **With matched filter:**
  \[ B = 1/T_{\text{Bit}} \]

  - Downlink $T = 3 \text{us} / B = 333 \text{ kHz}$
  - Uplink $T = 9.4 \text{us} / B = 106 \text{ kHz}$

Legend:
- $F_{\text{am}}$... Noise figure,
- $B$... Bandwidth, $T$... Bit duration
Noise Level in the HF-Band

In the HF-band the external noise normally exceeds the internal receiver noise

External noise sources:
- Man Made Noise (MMN) for
  - Business,
  - Residential,
  - Rural and quite rural environment
- Atmospheric noise
- Galactic noise

Assuming a non-directional antenna the noise figure lies between:
- 26 dB for galactic noise and
- 45.4 dB for MMN in a business environment

Small Circular Loop Antenna

Magnetic field of a small loop antenna in dependence of the distance depends on the antenna orientation.

\[ H_r = j \frac{ka^2 I_L \cos \theta}{2r^2} \left( 1 + \frac{1}{jkr} \right) e^{-jkr} \]

\[ H_\theta = j \frac{(ka)^2 I_L}{4r} \sin \theta \left( 1 + \frac{1}{jkr} - \frac{1}{(kr)^2} \right) e^{-jkr} \]

\[ H_\phi = 0 \]

Legend:
a... loop radius,  \( I_L \) ... loop current,
\( k \)... wavenumber \( k = \frac{2\pi}{\lambda} \), \( r \)... distance.
Optimum Loop Placement

The optimum antenna placement depends on the distance between the two loops in relation to the wavelength.

**distance < 8.3m**
- Coaxial orientation
- Magnetic fields

**distance > 8.3m**
- Coplanar orientation

- Tx Loop
- Rx Loop
Uplink Eavesdropping

Contactless reader PCD

Contactless smartcard PICC

Downlink Data

Attacker

Uplink Data
Uplink: Reader / Transponder Model

Characteristic parameters of an exemplary tag (Mifare)

- L2, R2, C2 was measured using an impedance analyzer
- RL depends on the incident magnetic field and is calculated from the IC-voltage
- UQ2 depends on the incident magnetic field

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mifare tag</td>
<td>4.0</td>
<td>68x38</td>
<td>7</td>
<td>3</td>
<td>28</td>
<td>15.0</td>
</tr>
</tbody>
</table>
Uplink: Measuring the IC-Voltage

The IC-voltage $u_2$ was measured by applying a defined magnetic field, using the bridge according to ISO/IEC 10373-6.
Uplink Signal

To eavesdrop the uplink data, it is sufficient to detect the upper side band: ISO/IEC 14443A Manchester coded uplink signal with 847.5kHz subcarrier

<table>
<thead>
<tr>
<th>IC-Voltage U2 [V(rms)]</th>
<th>IC-Load R2 [Ohm]</th>
<th>Coil-Current I2 [A(rms)]</th>
<th>A_ssb [dBc]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5 A/m(rms)</td>
<td>3.5 / 1.5</td>
<td>426 / 175</td>
<td>11.7 / 9.1</td>
</tr>
<tr>
<td>4.5 A/m(rms)</td>
<td>4.3 / 3.0</td>
<td>169 / 117</td>
<td>27.4 / 26.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-24 dBc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-40.6 dB</td>
</tr>
</tbody>
</table>
Depending on the applied noise a eavesdropping distance between 3 and 8 m is calculated for $H = 1.5 \text{ A/m}$.
# Uplink Results (Coherent Demodulation)

Maximum Eavesdropping distance depending on the BER, applied noise and field strength

<table>
<thead>
<tr>
<th>Noise Source</th>
<th>Business</th>
<th>Residential</th>
<th>Galactic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BER =0.1%</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 A/m(rms)</td>
<td>3.2 m</td>
<td>3.9 m</td>
<td>9.4 m</td>
</tr>
<tr>
<td>4.5 A/m(rms)</td>
<td>2.2 m</td>
<td>2.7 m</td>
<td>5.5 m</td>
</tr>
<tr>
<td><strong>BER=0.01%</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 A/m(rms)</td>
<td>3.0 m</td>
<td>3.6 m</td>
<td>7.7 m</td>
</tr>
<tr>
<td>4.5 A/m(rms)</td>
<td>2.1 m</td>
<td>2.5 m</td>
<td>5.1 m</td>
</tr>
</tbody>
</table>

Eavesdropping range lies between
- 2.2 and 9.4 m for BER of 0.1%
- 2.1 and 7.7 m for BER of 0.01%
- With un-coherent demodulation the range decreases by 15 %
**Downlink Eavesdropping**

The downlink eavesdropping range can be derived directly from the magnetic strength at the reader’s position.

Magnetic field strength between 1.5 and 7.5 A/m (rms) specified in ISO/IEC 14443A.
# Downlink Results (Coherent Demodulation)

Maximum Eavesdropping distance depending on the BER, coil radius, applied noise and field strength

<table>
<thead>
<tr>
<th>BER = 0.1%</th>
<th>Business</th>
<th>Noise Source</th>
<th>Galactic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5 A/m(rms) / 3cm coil radius</td>
<td>10.9 m</td>
<td>18.4 m</td>
<td>107.8 m</td>
</tr>
<tr>
<td>7.5 A/m(rms) / 7.5cm coil radius</td>
<td>ca. 0.9 km</td>
<td>ca. 1.5 km</td>
<td>ca. 8.5 km</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BER = 0.01%</th>
<th>Business</th>
<th>Noise Source</th>
<th>Galactic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5 A/m(rms) / 3cm coil radius</td>
<td>8.8 m</td>
<td>15.2 m</td>
<td>63.4 m</td>
</tr>
<tr>
<td>7.5 A/m(rms) / 7.5cm coil radius</td>
<td>ca. 0.7 km</td>
<td>ca. 1.2 km</td>
<td>ca. 7 km</td>
</tr>
</tbody>
</table>

- Eavesdropping range lies between
  - 10.9 m and 8.5 km for BER of 0.1%
  - 8.8 m and 7 km for BER of 0.01%
  - With un-coherent demodulation the range decreases by 30%
Uplink & Downlink Eavesdropping

Contactless reader PCD

Contactless smartcard PICC

Uplink Data

Downlink Data

Attacker
Our Results Compared to Literature

- Oscilloscope measurement [Finke 2004] - 2 m
- Reading card ID [BSI 2008] - 2.3 m
- Reading card ID [Hancke 2008] - 1 to 3 m (different measurement locations)
- Reading card ID (SNR of 6dB) [Novotny 2008] - 8 to 15 m (different tokens)

**BER of 0.1%**
- [NXP 2007] - 2.4 to 38.6 m (different environments)
- [Our Results] - 2.2 to 9.4 m (different environments)
- [Our Results] - 2.1 to 7.7 m (different environments)

- \(\text{SNR of } 9.8\text{dB} \) instead of only 6dB in the measurements (with 6dB we calculate a maximum distance of 15m)
- Simplified assumptions like free space propagation against nearly undefined measurement conditions (as it is in a real environment)
## Older Studies vs. this Study

Differences between older studies and this study

<table>
<thead>
<tr>
<th></th>
<th>Older Studies</th>
<th>This study</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required BER</strong></td>
<td>0.1 %</td>
<td>0.1% / 0.01%</td>
</tr>
<tr>
<td><strong>Noise floor</strong></td>
<td>Man Made Noise in rural environment</td>
<td>Galactic noise</td>
</tr>
<tr>
<td><strong>Noise bandwidth</strong></td>
<td>= 1.5 / (Bit duration)</td>
<td>= 1 / (Bit duration)</td>
</tr>
<tr>
<td><strong>Tag’s loop current</strong></td>
<td>= (Modulation voltage) / (Loop inductance)</td>
<td>Full circuit model</td>
</tr>
</tbody>
</table>
| **Physical model**   | Near field: Biot-Savart law  
                        Far field: Radiation (using radiation resistance) | Near & far field:  
                        Formulas for small loop antenna |
Conclusion

- Bottleneck of the eavesdropping range is the detection of the uplink signal

- A higher magnetic field of the reader reduces the detection range of the uplink signal due to the control behaviour of the IC chip

- Theoretic range lies between 2.2 and 9.4m (for BER of 0.1%) and 2.1 and 7.7m (for BER of 0.01%) – both with coherent modulation

- Calculation are performed under simplified assumptions as free space propagation & pure Gaussian noise

  ➔ range limits can only give an indication for measurements (coupling into pipes/wires could also cause excessive range)