Eavesdropping Near Field Contactless Payments: A Quantitative Analysis

Thomas P. Diakos\textsuperscript{1} Johann A. Briffa\textsuperscript{1} Tim W. C. Brown\textsuperscript{2} Stephan Wesemeyer\textsuperscript{1}

\textsuperscript{1}Department of Computing, University of Surrey, Guildford
\textsuperscript{2}Centre for Communication Systems Research, University of Surrey, Guildford

Computer Laboratory, University of Cambridge, January 21, 2014
Outline

Introduction: Near Field Communications

Eavesdropping Antennas

Experimental Work

Results

Conclusions and Future Work
Near Field Communications

Near Field

- Distance \( \ll \) Wavelength (\( \approx 22m \))
- HF 13.56 MHz radio inductive coupling
- H-fields
- Reader and tag (passive)
- Short (‘from a touch to a few cm’) range of operation

NFC devices

- Reader and tag on the same device
- Power on-board
Near Field Communications

Near Field Contactless Payments

- Marketed as ideal for quick, convenient transactions
- Contactless Cards and NFC devices
- 23 million cards in the UK alone
- 13.32% of smartphones equipped with NFC
Near Field Communications

Near Field Contactless Payments

- Marketed as ideal for quick, convenient transactions
- Contactless Cards and NFC devices
- 23 million cards in the UK alone
- 13.32% of smartphones equipped with NFC

What’s the catch?

‘Because the transmission range is so short, NFC-enabled transactions are inherently secure.’

http://nfc-forum.org/what-is-nfc/nfc-in-action/
Motivation

Eavesdropping - Chosen attack

- Why eavesdropping?
## Motivation

### Eavesdropping - Chosen attack

- Why eavesdropping?
- ‘Inherently’ secure?
- Difficult to defend against
- ‘Contact world’ heritage
# Motivation

## Eavesdropping - Past work

- Expensive, cumbersome equipment
- No control over transmit power
- Traces on a scope?

## Our contribution
Motivation

Eavesdropping - Past work

- Expensive, cumbersome equipment
- No control over transmit power
- Traces on a scope?

Our contribution

- Relatively inexpensive, inconspicuous equipment
- Varying Magnetic field strength
- Quantitative analysis
Eavesdropping Antennas

Design Factors

The ideal eavesdropping antenna

- Maximise SNR
- Resonance
- Suitable Q factor
- Impedance matched
NFC antenna design principles

Ideal H-antenna

- H-field antenna
- $L$ constant
- $R$ (DC) negligible
NFC Antenna Design Principles

H-Antenna Receiver Mode

- In RX mode:
  \[
  \frac{V_L}{V_{in}} = \frac{1}{1 + \frac{j\omega L(\omega)}{R_L} - \omega^2 LC}
  \]  \hspace{1cm} (1)

- At resonance:
  \[
  \frac{V_L}{V_{in}} = \frac{R_L \sqrt{C}}{j \sqrt{L(\omega_0)}}
  \]  \hspace{1cm} (2)

H-Antenna Conclusions

- Low Inductance, high load Resistance
- Magnitude of 2 is equal to the Q-factor
Large Metallic structures

The shopping trolley

- Various distances
- Fixed Ground
- Network Analyser
The shopping trolley

Findings at 13.5 MHz

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Inductance at 13.5 MHz / $\mu$H</th>
<th>Resistance at 13.5 MHz / $\Omega$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Near End</td>
<td>0.42</td>
<td>1.31</td>
</tr>
<tr>
<td>Middle End</td>
<td>1.42</td>
<td>18.48</td>
</tr>
<tr>
<td>Leg End</td>
<td>3.73</td>
<td>70.66</td>
</tr>
<tr>
<td>Far End</td>
<td>2.59</td>
<td>7.67</td>
</tr>
</tbody>
</table>

Connection point dependence
Shopping Trolley antenna

Pros

- Ease of execution (variable C)
- High load resistance desirable
- Short connection points

cons

- Trolley resistance
- Loop size
Eavesdropping Antenna Benchmarks

Eavesdropping H-fields

- H-loop antenna used as a transmitter
- Controlled H-field through current
- Signal generator and power amplifier
- Three types of eavesdropping antennas
- Path Loss measurements
NFC Antenna Design Principles

H-Loop Antenna

- Matched to 50 Ω with a resistor (10 Ω) in series
Path Loss Measurements

Various H-fields for H-loop and trolley only

![Propagation range for various magnetic fields](chart.png)
Quarter Wavelength Antenna

$S_{11}$ Reflection Coefficients

Reflection Coefficient of a 5m wire

Thomas P. Diakos (t.diakos@surrey.ac.uk)
Quarter Wavelength Antenna

Worn over body

- Water content of body reduces efficiency
Path Loss Measurements

Trolley

![Trolley Path Loss](image_url)
Summary

- H-loop and trolley are most efficient
- Antenna orientation
- H-field strength
- Proceed with FER measurements
Eavesdropping Near Field Contactless Payments

Near Field Contactless Payments

- PHY layer based on ISO 14443 standard
- Half-duplex communication
- Type A and Type B
Near Field Contactless Payments

ISO 14443 type A communication

- 106kbps or 9.4 μs bit duration
- Manchester encoded baseband
- 847 kHz Subcarrier modulation (OOK)
- Standard / short frames
- SOF and EOF markers
Eavesdropping Near Field Contactless Payments

Computing Frame Error Rates

- A known (random), long sequence
- Transmitter / Receiver
- Processing and computation
Eavesdropping Near Field Contactless Payments

Transmitter arrangement

- Synthetic data, 60 bytes per frame
- Subcarrier generated in software
- External trigger signal at 1.7 MHz
Eavesdropping Near Field Contactless Payments

Sequence of 5 bits
Eavesdropping Near Field Contactless Payments

Transition between two PICC frames
Eavesdropping Near Field Contactless Payments

Receiver arrangement

- LNA maximises SNR
- Band Pass Filter 12.7-14.4MHz
- Logarithmic detector
Eavesdropping Near Field Contactless Payments

Receiver arrangement

[Image of receiver arrangement with labeled components: LNA, Band Pass Filter (BPF), RF AMP, NOTCH FILTER, PEAK DETECTOR]
Eavesdropping Near Field Contactless Payments

Receiver arrangement

- LNA maximises SNR
- Band Pass Filter 12.7-14.4MHz
- Logarithmic detector
- Capture card sampling at 1.7MS/s
Eavesdropping Near Field Contactless Payments

Noise corruption

- Frame synchronisation becomes challenging
Eavesdropping Near Field Contactless Payments

Noise corruption

- Frame synchronisation becomes challenging
- Variance computing sliding window
- Threshold crossing

Thomas P. Diakos (t.diakos@surrey.ac.uk)
University of Surrey

Eavesdropping Near Field Contactless Payments: A Quantitative Analysis
Eavesdropping Near Field Contactless Payments

Variance sliding window
Eavesdropping Near Field Contactless Payments

Variance smoothing and threshold

\[ \text{Gaussian smoothing} \]
Eavesdropping Near Field Contactless Payments

Robust Frame Synchronisation

▶ Frame length
▶ Rough estimate based on $\rho$ crossing
▶ $(EOF - SOF - 32) \pm Y \Rightarrow$ multiple of 144
▶ Cross correlation for bit decoding
Eavesdropping Near Field Contactless Payments

Experimental Set-up

```
Outside Chamber

PC → Data Card → IQ Modulator → 13.56 MHz carrier

Pre Amp → Step Attenuator

Inside Chamber

RF Amp → Tx Antenna → Rx Antenna → Receiver & Peak detector

Thomas P. Diakos (t.diakos@surrey.ac.uk)
University of Surrey
Eavesdropping Near Field Contactless Payments: A Quantitative Analysis
```
### Eavesdropping Near Field Contactless Payments

**Receiver circuit and antenna**

![Image of receiver circuit and antenna](image-url)
Eavesdropping Near Field Contactless Payments

Preliminary testing

- Anechoic chamber
- Controlled environment
- 500 frame tests
- Establish $\sigma$ and $\rho$ values
Eavesdropping Near Field Contactless Payments

\(\sigma\) and \(\rho\) selection at 7.45 A/m
Eavesdropping Near Field Contactless Payments

Experimental procedure

- 5000 frames (20 minutes per run)
- 20–170 cm, increments of 5 cm (2–30 cm for trolley)
- 1.5, 3.45, 7.45 A/m
- Experiments ran over 2 days
Results

H-Loop Antenna FER

- Normal approximation, 95% confidence interval levels

Thomas P. Diakos (t.diakos@surrey.ac.uk)
University of Surrey
Eavesdropping Near Field Contactless Payments: A Quantitative Analysis
Eavesdropping Near Field Contactless Payments

Shopping trolley eavesdropping arrangement
Eavesdropping Near Field Contactless Payments

Shopping trolley FER (σ = 10, ρ = 50)

- Trolley generates its own noise, lossy antenna
Conclusions and Future work

Conclusions

- Eavesdropping distance 45-90 cm in shielded environment
- Similar conditions to those found in underground stations
- Relatively inexpensive equipment, inconspicuous antennas
- Gaussian filtering and variance computation are reliable

Future work

- Real data with real devices
- Improve portability (FPGA), integrate a skimmer
- What does this mean for the user?
Eavesdropping Near Field Contactless Payments

Thank you for listening

Please forward any questions