RADIO ASPECTS OF NFC SECURITY

Tomáš Rosa

http://crypto.hyperlink.cz
ANTENNA ESSENTIALS WITH NEAR AND FAR FIELDS DISCUSSION
START WITH SOMETHING FAMILIAR

[Buddipole QRV by 5B8AP]
THE IDEAL ELECTRIC DIPOLE

- Electrically small, i.e. \( \Delta z \ll \lambda \), uniform amplitude current element.
  - Ordinary dipole is covered by integration over these elements.
- In the far field, a donut-like pattern bearing the vertical polarisation is produced.
- In general, its field has the following components.

\[
\begin{align*}
\vec{E}_{edp}(I^{(e)}) &= E_{edp,\theta}(I^{(e)}) \cdot \hat{e}_\theta + E_{edp,r}(I^{(e)}) \cdot \hat{e}_r \\
\vec{H}_{edp}(I^{(e)}) &= H_{edp,\phi}(I^{(e)}) \cdot \hat{e}_\phi
\end{align*}
\]
HAVE YOU SAID DONUT?
The Small Loop

- Electrically small, i.e. $2\pi a < \lambda/10$, uniform amplitude current loop.

- Can be modelled as an ideal magnetic dipole which is the theoretical dual of the ideal electric dipole.

- The duality equations follow.

$$\vec{E}_{mdp}(I^{(m)}) \equiv -\vec{H}_{edp}(I^{(m)}), \quad \vec{H}_{mdp}(I^{(m)}) \equiv \vec{E}_{edp}(I^{(m)})$$

$$\mu_{mdp} \equiv \varepsilon_{edp}, \quad \varepsilon_{mdp} \equiv \mu_{edp}$$

$$\beta_{mdp} = \omega \sqrt{\mu_{mdp} \varepsilon_{mdp}} = \omega \sqrt{\varepsilon_{edp} \mu_{edp}} = \beta_{edp}$$

Note also $\beta = \frac{2\pi}{\lambda}, \quad v = \lambda f$
The duality with the ideal electric dipole tells us the far field has the donut-like form.

The polarisation is reversed (!) - i.e. horizontal in place of vertical, now.

In the near field, however, there is a significant radial component (cf. below).
\[ \vec{E}_{mdp}(I^{(m)}) = -\frac{I^{(m)} \Delta z}{4\pi} j\beta(\frac{1}{r} + \frac{1}{j\beta r^2})e^{-j\beta r} \sin \theta \cdot \hat{e}_\phi \]

\[ \vec{H}_{mpd}(I^{(m)}) = \frac{I^{(m)} \Delta z}{4\pi} j\omega\varepsilon(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r} \sin \theta \cdot \hat{e}_\theta 
+ \frac{I^{(m)} \Delta z}{2\pi} j\omega\varepsilon(\frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r} \cos \theta \cdot \hat{e}_r \]
MAGNETIC CURRENT OF THE SMALL LOOP

\[ I^{(m)} \Delta z = j \omega \mu I S \]

\[ S = \pi a^2 \]

(based on far field equivalence)
Basing on the dominating $E$, $H$ field terms, it is useful to distinguish:

- **Reactive near field (XNF)**, where the terms with $1/r^2$ and $1/r^3$ dominate. Energy is mainly stored and exchanged between $E$ and $H$.

- **Radiating near field (Fresnel region)**, where the $1/r^2$ terms start to dominate, i.e. $r > \lambda/2\pi$. Energy is mainly radiated with unstable patterns, however.

- **Far field (Fraunhofer region)**, where the $1/r$ terms remain to dominate and the plane wave model can be used. Several conditions shall be met: $r > 2D^2/\lambda$, $r > 5D$, $r > 1.6\lambda$, where $D$ is the largest antenna dimension. Energy is radiated with a distance-independent field pattern.
WHEREVER YOU ARE
The input impedance $Z_A$ describes the antenna from the lumped circuit parameters viewpoint.

- $R_r$ is the equivalent radiation resistance representing the energy emanated through the radio waves
- $R_o$ describes the dissipative energy loss
- $X_A$ reflects the energy exchanged back-and-forth with the reactive near field
RADIATION OF THE SMALL LOOP

\[ P = 10I^2(\beta^2S)^2 \]

\[ R_r = \frac{2P}{I^2} = 20(\beta^2S)^2 \approx 31171\left(\frac{S}{\lambda^2}\right)^2 \]

\[ \approx 31171\left(\frac{NS}{\lambda^2}\right)^2 \), for a small N-turn loop}
• For the radiation efficiency analysis, $R_o$ shall also cover any damping resistor $R_q$ used.

• Especially for NFC, a nonzero $R_q$ is often inserted serially to lower the antenna $Q$ to achieve the required bandwidth.

  • Finally, we can expect a very small radiation efficiency for a typical NFC antenna.

  • Interestingly, we may investigate on how to design a yet-usable NFC antenna that is, however, a very poor radiator anyway.

  • *Nevertheless, it does not mean the radiation is zero.*
To get a better overview, we can compute the radiation efficiency $e_r$ that can be further used for e.g. gain estimation, etc.

We do that by comparing the equivalent real resistances from the circuit model of $Z_A$.

\[ R_s = \sqrt{\frac{\omega \mu}{2\sigma}} \]

\[ R_o = \frac{a}{c} R_s, \ a \sim \text{loop radius}, \ c \sim \text{wire radius} \]

\[ e_r = \frac{R_r}{R_q + R_o + R_r} \]
From the security viewpoint, we shall recognise it may not be the primary antenna only that can radiate sensitive data.

In general, any spatial distribution of a time-varying current modulated (or sensed!) by the internal processing unit is a potential backdoor.

- We are getting to the well-known phenomenon of the electromagnetic side-channels.
- Here, we have an extremely high chance this mechanism is exploitable by attackers.
- In principle, applying anti-RFI techniques for all those patch cables and power lines is a good idea to start with.
NEAR FIELD COMMUNICATION
PASSIVE NFC COUPLING

[Finkenzeller, K., 2011]
INITIATOR SPEAKING
NFC-A
INITIATOR SPEAKING
NFC-A
INITIATOR SPEAKING
NFC-B

<table>
<thead>
<tr>
<th>Mode</th>
<th>Source</th>
<th>Υ</th>
<th>Χ1</th>
<th>Χ2</th>
<th>ΔY(1)</th>
<th>ΔX = 9.44000us</th>
<th>1/ΔX = 105.93kHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>1</td>
<td></td>
<td>-94.4500us</td>
<td>-85.0100us</td>
<td>13.5000V</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agilent Technologies

WED MAY 13 12:20:53 2015

ΔX = 9.440000us

1/ΔX = 105.93kHz

ΔY(1) = 13.5000V

Mode Manual

Source 1

X Y

X1 -94.4500us

X2 -85.0100us

X1 X2

SOS || WUPB || EOS
Lenz’s Law Illustrated

Short Circuit Switch

NFC Initiator
Lenz’s Law Illustrated

Short Circuit Switch

NFC Initiator

probe

OFF
Lenz's Law Illustrated

Short Circuit Switch

NFC Initiator

ON

OFF

probe
TARGET RESPONSE
NFC-A
IF U LIKE IT HOT
(THE WHOLE QUIZ)
IF U LIKE IT HOT
(THE WHOLE QUIZ)
## NFC Overview

### NFC Forum Overview Table

<table>
<thead>
<tr>
<th>Activity</th>
<th>Technology / Device Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen, RF Collision</td>
<td>NFC-A Section 4</td>
</tr>
<tr>
<td>Avoidance, Technology</td>
<td>NFC-B Section 5</td>
</tr>
<tr>
<td>Detection, Collision</td>
<td>NFC-F Section 6</td>
</tr>
<tr>
<td>Resolution</td>
<td></td>
</tr>
<tr>
<td>Device Activation</td>
<td>Type 1 Tag Platform Section 8</td>
</tr>
<tr>
<td></td>
<td>Type 2 Tag Platform Section 9</td>
</tr>
<tr>
<td></td>
<td>Type 4A Tag Platform Section 11</td>
</tr>
<tr>
<td></td>
<td>Type 4B Tag Platform Section 12</td>
</tr>
<tr>
<td></td>
<td>Type 3 Tag Platform Section 10</td>
</tr>
<tr>
<td>Data Exchange</td>
<td>NFC-DEP Protocol Section 14</td>
</tr>
<tr>
<td></td>
<td>Type 1, 2, and 3 Tag</td>
</tr>
<tr>
<td></td>
<td>Half-duplex Protocol Section 7</td>
</tr>
<tr>
<td></td>
<td>ISO-DEP Protocol Section 13</td>
</tr>
<tr>
<td></td>
<td>Type 1, 2, and 3 Tag</td>
</tr>
<tr>
<td></td>
<td>Half-duplex Protocols Section 7</td>
</tr>
<tr>
<td>Device Deactivation</td>
<td>NFC-DEP Protocol Section 14</td>
</tr>
</tbody>
</table>

*Source: NFCForum-TS-DigitalProtocol-1.0, 2010*
NFC RADIO ATTACKS

(With the focus on the passive NFC mode.)
• Allows RF skimming or wormhole (relay) attacks.

• Due to very low $e_r$ and very high power consumption, it is practically limited to the reactive near field region (XNF).

• Antenna diversity separating downlink and uplink channels may help significantly.

• **Distance:** Decimetres (confirmed), reliably working at around 20 cm. Principal upper limit $\approx \lambda/2\pi$, i.e. circa 3.5 m, is infeasible to achieve practically. So, we are limited to a kind of *bumping attack*. 
TARGET RANGE EXTENSION

- Allows covert communication with NFC terminal.

- Combines the techniques for a long range sniffing with the reciprocal problem of an extended-range signal injection into the RF front-end of the terminal.

- Based on direct DSB (Double Side Band) or even SSB (Single Side Band) injection, basing on the particular terminal signal processing.

- Principally possible even from the Fraunhofer region.

- The terminal antenna gain together with its input sensitivity limits the distance.

- **Distance**: Metres (confirmed). Working from the Fraunhofer region is practically very hard.
SNIFFING

- Sensitive data capture, identity theft.

- Works over all zones, from XNF to Fraunhofer region.

- **Often, this scenario induces the most serious risks.**

- For regions outside XNF, the important idea is to look for higher harmonics of the 13.56 MHz carrier.

- Furthermore, antenna design and orientation varies through the regions.

- **Distance:** Metres to dekametres. Confirmed for both downlink and uplink channels.
ALL YOU NEED IS LOOP
SPYING IN THE LANE (STILL IN XNF)

[https://www.youtube.com/watch?v=9QjxwejBPHs]
TRAFFIC INJECTION

- Allows Man-In-The-Middle scenarios.

- Due to the linear superposition in the EM field, the attacker does not have to be geometrically right in the middle, neither to break the original channel spatially.

- Again, a few turns of a wire around the original reader can be enough.

- Note we can also spoof the Initiator packets, besides the Target responses.

- Covering the path to the Target (downlink) requires XNF. One sided injection can work from the Fresnel or Fraunhofer regions as well.

- **Distance:** Decimetres (downlink TX covered) up to metres (TX for uplink only). Confirmed indirectly by other experiments together with own observations (cf. below).
LENZ’S LAW BASED “PASSIVE” DOWNLINK TX FOR NFC-B
LENZ’S LAW BASED “PASSIVE” DOWNLINK TX FOR NFC-B
LET’S FACE IT

Original NFC-B Initiator

Lenz-style Fake TX
• Allows searching for active terminals - for instance, exposing passengers inspection, etc.

• Carrier detection at 13.56 MHz or higher harmonics, possibly also with the communication footprint.

• Distance: Dekametres. Indirectly confirmed by the eavesdropping experiments that can serve as a lower bound.
TARGET LOCATION

- Allows searching for potentially valuable assets.
- Searching based on radio characteristics without querying the higher protocol layers.
- Electronic Article Surveillance (EAS) style to search for the particular resonant circuits.
- **Distance**: Decimetre (confirmed by the range extension experiments) to metres (estimated).
JAMMING

- Allows DoS attacks at airport, office entry, market centre etc.

- We can use reciprocity theorems to estimate the effect an attacker’s (measurement) antenna would have on the terminal input.

- **Distance:** Metres (confirmed by the range extension experiments) to dekametres (estimated).
DEVICE DESTRUCTION

- Allows selective DoS on the terminal or transponder.
- In principle, it requires a strong power pulse, so a near field approach is assumed.
- **Distance:** Decimetres.
CONCLUSIONS

- After all, **there is only one electromagnetic field out there**. NFC devices do not live in a separate universe. It is just a *different approach to the same theory*.

- Besides the wanted near field effects, there is always a plenty of other, possibly unwanted characteristics that can be exploited.

- We shall analyse the whole picture when designing NFC components to eliminate those undesired RF effects as much as possible.
  
  - Communication protocol engineers shall be fully aware of the residual threats then.

- We shall look for the remaining EM footprint carefully during security analysis and-or penetration tests.
POST SCRIPTUM
REFERENCES
(BESIDES THE BOOKS NOTED ABOVE)

Strengths in NFC Standards, 2013
 quantitative analysis, 2013
using Higher Harmonics, 2013
6. Finkenzeller, K.: Known attacks on RFID systems, possible countermeasures and upcoming standardisation
 activities, 2009
8. Finkenzeller, K., Pfeiffer, F., and Biebl, E.: Range Extension of an ISO/IEC 14443 type A RFID System with Actively
Emulating Load Modulation, 2011
Using NFC Mobile Phones, 2011
REFERENCES
(BESIDES THE BOOKS NOTED ABOVE)

15. NXP: AN1445 - Antenna design guide for MFRC52x, PN51x, and PN3x, 2010
REFERENCES
(BESIDES THE BOOKS NOTED ABOVE)
