Distance bounding

- Places an upper bound on physical distance
- Does not provide absolute location
- Operates on physical characteristics of the communication medium.
- Supplements existing security mechanisms
RFID devices

- Various applications
- Passive devices with low resources
- Limited range
- Used to link an item or person to a location
Relay attack

- Simple, well known attack
- Circumvents application layer security protocols
Relay attack demonstration

Proxy Token
- 14443 A/B test card circuit
- Signal processing with discrete components
- Duplex RF link

Proxy Reader
- Commercial reader module
- Reprogrammed with our firmware
- Price $100
Relay attack detection

- Delay
  - Could be reduced with complex hardware
  - Cannot be less than 3 ns/m

- Physical layer
  - High-resolution timing

- Application layer
  - Timing information lost

Timing difference between an actual token (top) and a Proxy token (bottom) response to a reader’s `REQA` command.
Our Protocol

Goals

- Suited to RFID environment
  - Verifier handles demanding processing functions
  - Prover performs simple functions
- Provide same level of security as other distance bounding protocols
  - Should not be worse because it has hardware constraints

Implementation

- Suggest practical ideas on how to implement our protocol
- Protocol should supplement current RFID standards, not suggest wholesale changes
Protocol assumptions

Security target

- Places an upper bound on the distance between Verifier and Prover
- Does not provide non-repudiation of location to a third party
- The Prover does not collude with an attacker

Crypto primitives

- Shared secret key, $K$
- Shared pseudorandom function, $h$
- Nonces $N_V, N_P$ are of sufficient length and will not be repeated
Protocol assumptions (2)

Time base

- Verifier is computationally strong
  - Perform accurate timing operations
- Prover is computationally weak
  - Cannot determine accurate timing information
  - Uses external clock signal (received carrier)
  - Prover can detect large deviations in clock frequency

Communication channels

- Low bandwidth error corrected channel
- High bandwidth rapid bit exchange channel
Protocol description

Verifier (RFID reader)
- Secret key $K$
- Function $h$
- Generate nonce $N_V$

Prover (RFID token)
- Secret key $K$
- Function $h$

$N_V$
Protocol description

Verifier (RFID reader)
- Secret key $K$
- Function $h$
- Generate nonce $N_V$
- Generate random bits $C_1, \ldots, C_n$

$$\langle C_i \rangle = 01001100$$

Prover (RFID token)
- Secret key $K$
- Function $h$
- Calculate $h(K, N_V) = R$
- Split $R = R_0 || R_1$
- $10011011 \leftarrow R^0$
- $01110110 \leftarrow R^1$
Protocol description

Verifier (RFID reader)
- Secret key $K$
- Function $h$
- Generate nonce $N_V$
- Generate random bits $C_1, \ldots, C_n$

\[
\langle C_i \rangle = 01001100 \\
\langle R_i^{C_i} \rangle = 1
\]

Prover (RFID token)
- Secret key $K$
- Function $h$
- Calculate $h(K, N_V) = R$
- Split $R = R_0 || R_1$

\[
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1
\end{array}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0
\end{array}
\end{array}
\end{array}
\end{array}
\]

\[
R_1^{C_1} = 1
\]
### Protocol description

**Verifier (RFID reader)**
- Secret key $K$
- Function $h$
- Generate nonce $N_V$
- Generate random bits $C_1, \ldots, C_n$

**Prover (RFID token)**
- Secret key $K$
- Function $h$

\[ N_V \]

**Calculate**
\[ h(K, N_V) = R \]

Split $R = R_0 || R_1$

\[ \begin{array}{l}
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0
\end{array} \]

\[ \begin{array}{l}
R_0 \\
R_1
\end{array} \]

\[ C_2 = 1 \]

\[ R_2^{C_2} = 1 \]

\[ \langle C_i \rangle = 01001100 \]

\[ \langle R_i^{C_i} \rangle = 11 \]
Protocol description

Verifier (RFID reader)
- Secret key $K$
- Function $h$
- Generate nonce $N_V$
- Generate random bits $C_1, \ldots, C_n$

$$ \langle C_i \rangle = 01001100 $$
$$ \langle R_i^{C_i} \rangle = 110 $$

Prover (RFID token)
- Secret key $K$
- Function $h$

Calculate
$$ h(K, N_V) = R $$
Split $R = R_0 || R_1$

$$ \begin{array}{c}
10011011 \\
01110110 \\
\end{array} \quad \begin{array}{c}
R^0 \\
R^1 \\
\end{array} $$

$$ C_3 = 0 $$
$$ R_3^{C_3} = 0 $$
Protocol description

Verifier (RFID reader)
- Secret key $K$
- Function $h$
- Generate nonce $N_V$
- Generate random bits $C_1, \ldots, C_n$

\[
\langle C_i \rangle = 01001100
\]
\[
\langle R^C_i \rangle = 1101
\]

Prover (RFID token)
- Secret key $K$
- Function $h$
- Calculate $h(K, N_V) = R$
- Split $R = R_0 \parallel R_1$

\[
\begin{array}{c}
1 0 0 1 1 0 1 1
\end{array}
\]
\[
\begin{array}{c}
0 1 1 1 0 1 1 0
\end{array}
\]

An RFID Distance Bounding Protocol – p. 10
Protocol description

Verifier (RFID reader)
- Secret key $K$
- Function $h$
- Generate nonce $N_V$
- Generate random bits $C_1, \ldots, C_n$

Prover (RFID token)
- Secret key $K$
- Function $h$

Calculate $h(K, N_V) = R$

Split $R = R_0 || R_1$

$\langle R_i C_i \rangle = 11010$

$\langle R_i^C_i \rangle = 01001100$

$C_5 = 1$

$R_5^{C_5} = 0$

$R^0 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$

$R^1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$
Protocol description

Verifier (RFID reader)
- Secret key $K$
- Function $h$
- Generate nonce $N_V$
- Generate random bits $C_1, \ldots, C_n$

Prover (RFID token)
- Secret key $K$
- Function $h$

Calculate
$h(K, N_V) = R$
Split $R = R_0 \parallel R_1$

$\langle C_i \rangle = 01001100$
$\langle R_i^{C_i} \rangle = 110101$

$C_6 = 1$
$R_6^{C_6} = 1$

$\begin{array}{c}
1 0 0 1 1 0 1 1 \\
0 1 1 1 0 1 1 0
\end{array} \leftarrow R^0$
$\begin{array}{c}
1 1 \\
1 0
\end{array}$
Protocol description

Verifier (RFID reader)
- Secret key $K$
- Function $h$
- Generate nonce $N_V$
- Generate random bits $C_1, \ldots, C_n$

\[
\langle C_i \rangle = 01001100 \\
\langle R_i^{C_i} \rangle = 1101011
\]

Prover (RFID token)
- Secret key $K$
- Function $h$

Calculate
\[
h(K, N_V) = R
\]
Split $R = R_0 || R_1$
\[
\begin{array}{c}
1 0 0 1 1 0 1 1 \\
0 1 1 1 0 1 1 0
\end{array}
\]

\[
\begin{array}{c}
C_7 = 0 \\
R_7^{C_7} = 1
\end{array}
\]
Protocol description

Verifier (RFID reader)
Secret key $K$
Function $h$
Generate nonce $N_V$
Generate random bits $C_1, \ldots, C_n$

\[
\langle C_i \rangle = 01001100
\]
\[
\langle R^C_i \rangle = 11010111
\]

Prover (RFID token)
Secret key $K$
Function $h$

Calculate
$h(K, N_V) = R$
Split $R = R_0 || R_1$

\[
\begin{align*}
\begin{array}{cccccc}
1 & 0 & 0 & 1 & 1 & 0 \leftarrow R^0 \\
0 & 1 & 1 & 1 & 0 & 1 \leftarrow R^1
\end{array}
\end{align*}
\]

$C_8 = 0$
$R_8^{C_8} = 1$
Protocol description

Verifier
Secret key $K$
Function $h$

\[ \langle C_i \rangle = 01001100 \]

Expected $\langle R_{C_i} \rangle$
1 1 0 1 0 1 1 1

Received $\langle R_{C_i} \rangle$
1 0 1 0 0 1 0 1

Attacker
Secret key $K$
Function $h$

\[ N_V \]

$C_i$

\[ R_{C_i} \]

\[ 1 0 1 0 1 0 0 1 \leftarrow R^0 \]
\[ 1 0 1 0 0 1 1 0 \leftarrow R^1 \]

\[ \text{Verifier} \leftrightarrow \text{Attacker} \]

\[ \frac{1}{2} \] chance of guessing a response bit correctly
Protocol description

Verifier
Secret key $K$
Function $h$

$\langle C_i \rangle = 01001100$

Expected $\langle R_i^{C_i} \rangle$
1 1 0 1 0 1 1 1

Received $\langle R_i^{C_i} \rangle$
1 0 1 0 0 1 0 1

Malicious Prover
Secret key $K$
Function $h$

$\langle R_i^{C_i} \rangle$

Verifier $\leftrightarrow$ Malicious Prover

$\frac{1}{2}$ chance of guessing a response bit correctly
Protocol description

Verifier
Secret key $K$
Function $h$

$\langle C_i \rangle = 01001100$

Expected $\langle R_{Ci}^i \rangle$
1 1 0 1 0 1 1 1

Received $\langle R_{Ci}^i \rangle$
1 1 0 0 0 1 0 1

Attacker
Secret key $K$
Function $h$

1 0 0 0 1 0 0 1 $R^0$
0 1 0 1 0 1 0 0 $R^1$

Prover
Secret key $K$
Function $h$

$\text{Veriﬁer} \leftrightarrow \text{Attacker} \leftrightarrow \text{Prover}$

$\frac{3}{4}$ chance of guessing a response bit correctly
Protocol description

Verifier
Secret key $K$
Function $h$

\[
\langle C_i \rangle = 01001100
\]

Expected $\langle R_{C_i}^C \rangle$
11010111

Received $\langle R_{C_i}^C \rangle$
11010111

Attacker
Secret key $K$
Function $h$

\[
\begin{align*}
01001011 &\rightarrow R^0 \\
01111010 &\rightarrow R^1
\end{align*}
\]

\[
\begin{align*}
10011011 &\rightarrow R^0 \\
01110110 &\rightarrow R^1
\end{align*}
\]

Prover
Secret key $K$
Function $h$

\[
\begin{align*}
N_V &\rightarrow A_C \\
R_{AC} &\rightarrow A_C
\end{align*}
\]

\[
\begin{align*}
h(K, N_V) &= R \\
01110110 &\rightarrow R^1
\end{align*}
\]

\[
\begin{align*}
10011011 &\rightarrow R^0 \\
01110110 &\rightarrow R^1
\end{align*}
\]

- Overclocking attack
  - Prevented in hardware e.g. Bandpass filter
## Protocol description

<table>
<thead>
<tr>
<th><strong>Verifier (RFID reader)</strong></th>
<th><strong>Prover (RFID token)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret key $K$</td>
<td>Secret key $K$</td>
</tr>
<tr>
<td>Function $h$</td>
<td>Function $h$</td>
</tr>
<tr>
<td>Generate nonce $N_v$</td>
<td>Generate nonce $N_p$</td>
</tr>
<tr>
<td>Generate random bits $C_1, \ldots, C_n$</td>
<td>Calculate $h(K, N_v, N_p) = R$</td>
</tr>
</tbody>
</table>

\[
\langle C_i \rangle = 01001100 \\
\langle R_i^{C_i} \rangle = 1
\]

\[
\begin{align*}
N_v & \quad \rightarrow \quad N_p \\
C_1 & = 0 \\
R_1^{C_1} & = 1
\end{align*}
\]

- **Overclocking attack**
- **Alternative to hardware solutions**
Noise

Bit errors will probably occur on the rapid exchange channel

- Accept if at least $k$ bits out of $n$ are correct
  - False accept:
    $$p_{FA} = \sum_{i=k}^{n} \binom{n}{i} \cdot \left(\frac{3}{4}\right)^i \cdot \left(\frac{1}{4}\right)^{n-i}$$

- False reject:
  $$p_{FR} = \sum_{i=0}^{k-1} \binom{n}{i} \cdot (1 - \epsilon)^i \cdot \epsilon^{n-i}$$

where $\epsilon$ is the bit-error probability.
Example of parameter tradeoffs in the presence of noise
Related work

\[ t_m = 2 \cdot t_p + t_d \]

\[ d = v_p \cdot \frac{t_m - t_d}{2} \]

- \( t_m \) = round trip time
- \( t_p \) = one-way propagation time
- \( t_d \) = processing delay
- \( d \) = distance
- \( v_p \) = signal propagation speed

Distance Bounding Protocols
- Beth and Desmedt (1991)
- Brands and Chaum (1993)
Brands and Chaum

<table>
<thead>
<tr>
<th>Verifier (RFID reader)</th>
<th>Prover (RFID token)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate random bits $C_1, \ldots, C_n$</td>
<td>Generate random bits $m_1, \ldots, m_n$</td>
</tr>
<tr>
<td>Verify commit</td>
<td>$R_i = C_i \oplus m_i$</td>
</tr>
<tr>
<td>Verify sign($M$)</td>
<td>message $M =$</td>
</tr>
</tbody>
</table>

- Time round trip of single bit exchange
- Processing with variable delay done beforehand
- Minimal processing delay during bit exchange
Brands and Chaum

Verifier (RFID reader)
Generate random bits $C_1, \ldots, C_n$

Verify commit
Verify sign($M$)

Prover (RFID token)
Generate random bits $m_1, \ldots, m_n$

commit($m$)

$C_i$

$R_i = C_i \oplus m_i$

open commit

sign($M$), $C,R$

message $M =$

$C_i | R_i | \ldots | C_n | R_n$

- Additional commit and sign operations
- Additional bits on slow channel
- In presence of noise $C$ and $R$ need to be transmitted
Performance vs Brands and Chaum

For $\text{EER} = 10^{-4}$ and $\epsilon = 0.1$
Assume bit exchange rate $= \frac{f_{\text{carrier}}}{4}$

<table>
<thead>
<tr>
<th>Standard</th>
<th>Time (B and C) $n = 70$</th>
<th>Time (Our protocol) $n = 360$</th>
</tr>
</thead>
<tbody>
<tr>
<td>15693 ‘fast’ 26.4 kbp/s, 13.56 MHz</td>
<td>5.3237 ms</td>
<td>0.1062 ms</td>
</tr>
<tr>
<td>15693 ‘long’ 6.62 kbp/s, 13.56 MHz</td>
<td>21.1687 ms</td>
<td>0.1062 ms</td>
</tr>
<tr>
<td>14443 A/B 106 kbp/s, 13.56 MHz</td>
<td>1.3414 ms</td>
<td>0.1062 ms</td>
</tr>
</tbody>
</table>
For $\text{EER} = 10^{-10}$ and $\epsilon = 0.05$

Assume bit exchange rate $= \frac{f_{\text{carrier}}}{4}$

<table>
<thead>
<tr>
<th></th>
<th>Standard</th>
<th>Time (B and C)</th>
<th>Time (Our protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$n = 125$</td>
<td>$n = 440$</td>
<td></td>
</tr>
<tr>
<td>15693 ‘fast’</td>
<td></td>
<td>9.5066 ms</td>
<td>0.1298 ms</td>
</tr>
<tr>
<td>26.4 kbp/s, 13.56 MHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15693 ‘long’</td>
<td></td>
<td>37.8012 ms</td>
<td>0.1298 ms</td>
</tr>
<tr>
<td>6.62 kbp/s, 13.56 MHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14443 A/B</td>
<td></td>
<td>2.3954 ms</td>
<td>0.1298 ms</td>
</tr>
<tr>
<td>106 kbp/s, 13.56 MHz</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Positioning technology

Positioning Technology used today

- Radio Frequency
  - Secure but complex

- Ultrasound
  - Appear closer by relaying data with faster RF link

- Received Signal Strength
  - Amplified signal appears closer
Resolution

Estimate \( r \approx \frac{c}{B} \), where \( B \) is the channel bandwidth

- RFID communication inadequate
  - e.g. for ISO 14443 at 106 kbp/s, \( r \approx 3 \) km

- Ultra Wideband Pulses
  - Higher bandwidth equals better resolution

- RFID implementation issues
  - Error free operation requires high resources
    - e.g. synchronization, bit placement
  - Crude implementation possible but would allow bit errors
  - Sufficient for bit exchange channel
  - Not to be used for normal communication
Proposed bit exchange channel

Use carrier for loose synchronization
e.g. Zero crossing
Proposed bit exchange channel

Reader (Verifier) adjusts $t_t$ to match sampling delay $t_r$ in the token (Prover)
Proposed bit exchange channel

- Carrier wave
- Challenge pulse $C_i$
- Response pulse $R_{i}^{C_i}$
- $t_d$ is a predictable hardware delay
Proposed bit exchange channel

\[ d = c \cdot \left( t_s - t_t - t_d \right)/2 \]
Conclusion

- Few more bit exchanges to achieve same cryptographic security
  - Chance of attacker guessing correct response $\frac{3}{4}$ vs $\frac{1}{2}$

- Faster operation
  - Extra bits transmitted on faster bit exchange channel
  - Much less data transmitted on slow error corrected channel

- Practical implementation suited for RFID
  - Low power and processing requirements for Prover
  - Timing-sensitive measurements and adjustments done by the Verifier
  - Faster completion of protocol suited for RFID environment
Future work

- Practical implementation
  - Pseudorandom functions suited for RFID device
  - Rapid bit exchange channel
  - UWB antennas for card form factor

- Mutual distance bounding protocol
  - For applications where illegitimate reading attempts are more common e.g. e-Passports