New DH protocol based on distance-bounding technique for peer-to-peer wireless network

22\textsuperscript{nd} November, 2007
Seon-Yeong PARK, Ju-Young KIM and Hong-Yeop SONG
Yonsei University, Coding and Information Theory Lab
{sy.park, jy.kim, hysong} @yonsei.ac.kr
Some Pictures of Tor

Happy Birthday!
Contents

- Introduction
- Preliminary
  - Commitment scheme
  - MITM attack
  - DH protocol, distance-bounding protocol
- Existing DH-DB protocol
- Improved DH-DB protocol
- Result and Discussion
- Conclusion
Introduction

- Peer-to-peer key agreement protocol
  - Auto configuration of mobile router without shared secret
- DH (Diffie-Hellman) protocols
  - Vulnerability against the MITM attacks
  - Involvement of users
  - Needs of physical devices
- Design of improved DH-DB (Distance-Bounding)
  - Improvement of resistance to attacks
  - Optimization of protocol
## DH Protocol[^1]

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given $ID_A$, $g$</td>
<td>Given $ID_B$, $g$</td>
</tr>
<tr>
<td>Pick $X_A$, and calculate $g^{X_A}$</td>
<td>Pick $X_B$, and calculate $g^{X_B}$</td>
</tr>
<tr>
<td>Pick $N_A \in {0,1}^k$</td>
<td>Pick $N_B \in {0,1}^k$</td>
</tr>
<tr>
<td>$m_A \leftarrow 0</td>
<td></td>
</tr>
<tr>
<td>$(L_A, K_A) \leftarrow \text{commit}(m_A)$</td>
<td>$(L_B, K_B) \leftarrow \text{commit}(m_B)$</td>
</tr>
<tr>
<td>$L_A \rightarrow L_B$</td>
<td></td>
</tr>
<tr>
<td>$K_A \rightarrow K_B$</td>
<td></td>
</tr>
<tr>
<td>$m_B \leftarrow \text{open}(L_B, K_B)$</td>
<td>$m_A \leftarrow \text{open}(L_A, K_A)$</td>
</tr>
<tr>
<td>Verify 1 in $m_B$; $i_A \leftarrow N_A \oplus N_B$</td>
<td>Verify 0 in $m_A$; $i_B \leftarrow N_B \oplus N_A$</td>
</tr>
<tr>
<td>Verify $i_A = i_B$</td>
<td>Verify $i_B = i_A$</td>
</tr>
<tr>
<td>If $i_A = i_B$, Alice and Bob accept $m_B$ and $m_A$, respectively.</td>
<td></td>
</tr>
<tr>
<td>Generate $g^{X_B X_A}$</td>
<td>Generate $g^{X_A X_B}$</td>
</tr>
</tbody>
</table>

Commitment Scheme[2]

Commitment/opening pair

- \( L=(y, f) \) is a Locked box.
- \( K=(x) \) is a Key.

Commitment procedure
1. Pick universal hash function \( f \) and \( x \) at random so that \( f(x)=m \).
2. Compute \( y=h(x) \), where \( h \) is a collision-free hash function.
3. Send \( L=(y, f) \) to receiver.

Opening procedure
1. Send \( K=(x) \) to receiver.
2. Receiver computes \( f(x)=m \).

MITM Attack

She can collect $L_A, K_A$ (or $L_B, K_B$) and get secret DH key. She can use collected $L_A, K_A$ (or $L_B, K_B$) for replay attack.
Distance-bounding Protocol\[3\]

**Distance-bounding principle**

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha_i \in U{0,1}^k$</td>
<td>$\beta_i \in U{0,1}^k$</td>
</tr>
</tbody>
</table>

Starting of rapid bit exchange

$\alpha_i$ $\rightarrow$

$\beta_i$ $\leftarrow$

End of rapid bit exchange

- Single-bit challenge and rapid single-bit response
- Upper-bound the distance between two parties based on the maximum of the delay time for responses
- Two parties communicate when they are close by.

Environment

- **RF and sound capability**[^4]
  - For accurate estimation of the distance between two parties

- **Local verification protocol**[^5]
  - The measured distance appears on both device displays and the users then visually check whether there are other users/devices closer to them than the displayed distance bounds.


Existing DH-DB Protocol\(^{[6]}\) (1/3)

### Initialization phase

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Given</strong> (\text{ID}_A, g^{x_A})</td>
<td><strong>Given</strong> (\text{ID}_B, g^{x_B})</td>
</tr>
<tr>
<td>Pick (N_A, R_A \in {0,1}^k)</td>
<td>Pick (N_B, R_B \in {0,1}^k)</td>
</tr>
<tr>
<td>(m_A \leftarrow 0</td>
<td></td>
</tr>
<tr>
<td>((L_A, K_A) \leftarrow \text{commit}(m_A))</td>
<td>((L_B, K_B) \leftarrow \text{commit}(m_B))</td>
</tr>
<tr>
<td>((L'_A, K'_A) \leftarrow \text{commit}(0</td>
<td></td>
</tr>
<tr>
<td>(m_B \leftarrow \text{open}(L_B, K_B))</td>
<td>(m_A \leftarrow \text{open}(L_A, K_A))</td>
</tr>
<tr>
<td>Verify 1 in (m_B; i_A \leftarrow N_A \oplus N_B)</td>
<td>Verify 0 in (m_A; i_B \leftarrow N_B \oplus N_A)</td>
</tr>
</tbody>
</table>

Eve can collect \(c_A, d_A\) (or \(c_B, d_B\)) and get secret DH key.
Existing DH-DB Protocol[6](2/3)

**Distance-bounding phase**

**Alice**

The bits of $R_A$ are $R_{A1}, \ldots, R_{Ak}$
The bits of $i_A$ are $i_{A1}, \ldots, i_{Ak}$

$\alpha_1 \leftarrow R_{A1} \oplus i_{A1}$

Measure delay between $\alpha_i$ and $\beta_i$

$\alpha_i \leftarrow R_{Ai} \oplus i_{Ai} \oplus \beta_{i-1}$

**Bob**

The bits of $R_B$ are $R_{B1}, \ldots, R_{Bk}$
The bits of $i_B$ are $i_{B1}, \ldots, i_{Bk}$

$\alpha_1 \rightarrow \beta_1 \leftarrow R_{B1} \oplus i_{B1} \oplus \alpha_1$

Measure delay between $\beta_{i-1}$ and $\alpha_i$

$\beta_i \leftarrow R_{Bi} \oplus i_{Bi} \oplus \alpha_i$

$\beta_i \rightarrow \alpha_i \leftarrow \ldots$

$\alpha_k \leftarrow R_{Ak} \oplus i_{Ak} \oplus \beta_{k-1}$

Measure delay between $\alpha_k$ and $\beta_k$

$\alpha_k \rightarrow \beta_k \leftarrow R_{Bk} \oplus i_{Bk} \oplus \alpha_k$

$\beta_k \rightarrow \ldots$
## Verification phase

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K'_A$</td>
<td>$0</td>
</tr>
<tr>
<td>$K'_B$</td>
<td>$i_{A1} \leftarrow \alpha_1 \oplus R_{A1}$</td>
</tr>
<tr>
<td>$1</td>
<td></td>
</tr>
<tr>
<td>$i_{Bi} \leftarrow \alpha_i \oplus \beta_i \oplus R_{Bi} \ (i = 1, \ldots, k)$</td>
<td>Verify $i_B = i_A$</td>
</tr>
<tr>
<td>Verify $i_A = i_B$</td>
<td>Why here?</td>
</tr>
</tbody>
</table>

Alice and Bob visually verify that there are no other users/devices in their integrity region.

---

Analysis of Existing DH-DB

- **Verification phase**
  - Vulnerable to the MITM attack
  - Insecure in reuse of DH public parameter

- **Distance-bounding phase**
  - Complicated procedures to hide verification string

- **Initialization phase**
  - Generate unnecessary random string for distance-bounding
New Design (Improved)

- Commitment/opening triplet \((f, y, x)\)
  - \(f\) is an index of universal hash function
  - \(x\) is a random string such that \(f(x) = m\) where \(m\) is a message
  - \(y\) is a \(k\)-bit output of the collision-free hash function \(h(x)\), used for measuring RTT

- Reordering of procedure
Security

- **Resistance against the MITH attack**
  - Eve cannot open $m$ without $x$.
  - $h$ is a one-way hash function: Eve cannot find $x$ easily even though she knows $y$, where $h(x)=y$.

  We can use $y$ for measuring RTT without any loss in security!

- **Secure reusability of DH public parameter**
  - The protocol is broken if Eve exists in integrity region before Alice and Bob exchange $x_A$ and $x_B$. 
Improved DH-DB (1/3)

- Initialization phase

<table>
<thead>
<tr>
<th></th>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given</td>
<td>$\text{ID}_A$, $g^{x_A}$</td>
<td>$\text{ID}_B$, $g^{x_B}$</td>
</tr>
<tr>
<td>Pick</td>
<td>$N_A \in _U {0, 1}^k$</td>
<td>$N_B \in _U {0, 1}^k$</td>
</tr>
<tr>
<td>$m_A \leftarrow 0</td>
<td></td>
<td>\text{ID}_A</td>
</tr>
<tr>
<td></td>
<td>$(f_A, y_A, x_A) \leftarrow \text{commit}(m_A)$</td>
<td>$(f_B, y_B, x_B) \leftarrow \text{commit}(m_B)$</td>
</tr>
</tbody>
</table>

- Generate commitment/opening triplet
Improved DH-DB (2/3)

- **Distance-bounding phase**

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>The bits of $y_A$ are $y_{A1}, \ldots, y_{Ak}$</td>
<td>The bits of $y_B$ are $y_{B1}, \ldots, y_{Bk}$</td>
</tr>
</tbody>
</table>

The bits of $y_A$ are $y_{A1}, \ldots, y_{Ak}$

Measure delay between $y_{A1}$ and $y_{B1}$

Measure delay between $y_{A2}$ and $y_{B2}$

... (continues)

Measure delay between $y_{Ak}$ and $y_{Bk}$

The bits of $y_B$ are $y_{B1}, \ldots, y_{Bk}$

Measure delay between $y_{Bk-1}$ and $y_{Ak}$

Measure delay between $y_{Bi}$ and $y_{Ai}$ (Simplified distance-bounding)
Opening phase

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_A$</td>
<td>$x_B$</td>
</tr>
<tr>
<td>$m_B$←open($f_B$, $y_B$, $x_B$)</td>
<td>$m_A$←open($f_A$, $y_A$, $x_A$)</td>
</tr>
<tr>
<td>Verify 1 in $m_B$; $i_A ← N_A ⊕ N_B$</td>
<td>Verify 0 in $m_A$; $i_B ← N_B ⊕ N_A$</td>
</tr>
<tr>
<td>Verify $i_A = i_B$</td>
<td>Verify $i_B = i_A$</td>
</tr>
</tbody>
</table>

Alice and Bob visually verify that there are no other users/devices in their integrity region.

- Secure reuse of DH public parameter
Structure of Protocol (Summary)

- **Initialization and commitment**
  - Pick DH exponent
  - Commit messages (Send a locked box)

- **Distance-bounding**
  - Upper-bound the distance and make integrity region

- **Visual check**
  - Check the existence of attacker in the integrity region

- **Opening and verification**
  - Open messages (Unlock the box)
  - Check verification string for integrity
Analysis of Performance

- **Assumption**
  - Same universal and collision-free hash function
  - Only consider XOR operation
  - 3-DES random generator

- **Result**

<table>
<thead>
<tr>
<th></th>
<th>Message (success)</th>
<th>Message (fail)</th>
<th>Parameters</th>
<th>XOR Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing</td>
<td>2k+6</td>
<td>2k+4</td>
<td>18</td>
<td>-</td>
</tr>
<tr>
<td>Proposed</td>
<td>2k+6</td>
<td>2k+2</td>
<td>14</td>
<td>Reduce ((7682^*(k/64)-64)*2) operations</td>
</tr>
</tbody>
</table>

- When \(k=64\), the number of reduced XOR operation is 15,236.
Conclusion

- Contribution
  - Provide improved DH-DB to the fundamental problem of key agreement over a radio link
  - Appropriate for devices which have limited power, limited memory, and limited computational power.