Formal Analysis and Patching of BLE-SC Pairing

Min Shi, Jing Chen, Kun He, Haoran Zhao, Meng Jia, Ruiying Du

Wuhan University, China
BLE-SC Pairing

Bluetooth Low Energy (BLE)

Connecting devices with minimal energy overhead.

Pairing

BLE Secure Connection (BLE-SC) is the latest pairing protocol in BLE.
Motivation

Broken

- Tschirschnitz et. al. disclosed the Method Confusion Attack (MCA).
- Their countermeasures have backward compatibility issue.

Questions

- How to formally analyze the security of the BLE-SC pairing protocol and disclose the design flaws?
- How to fix the found design flaws while maintaining backward compatibility?
BLE-SC Pairing

Pairing Feature Exchange

LTK Generation

Transport Specific Key Distribution

IO, MitM, OOB, KSize

Public Key

JW, NC, PE, or OOB

Confirmation

Specific Keys

Public Key Exchange

Auth. Stage 1

Auth. Stage 2
Association Models

**Numeric Comparison (NC)**

- Input: 764511
- Compares: 764511

**Passkey Entry (PE)**

- Input: 764511

**Just Work (JW)**

- Protocol flows are most like NC, but do not need user to confirm.
- Not Prevent MITM.

**Out Of Band (OOB)**
Comprehensive Formal Model

- We use *Tamarin Prover* (symbolic modeling and analysis of security protocols.)
- Dolev-Yao adversary with an **additional capability of brute forcing low entropy keys**.

Model Covers:

- Pairing Feature Exchange
- LTK Generation
- Transport Specific Key Distribution
- NC
- PE
- OOB
- JW

General-Specific Models

General Model

29 Cases

Results

Tamarin Prover

29 Specific Models
Analysis Results

We verified

- Four authentication properties.
- MitM Protection.
- LTK Confusion Protection.
- Secrecy of Authenticated LTK.

Verification was fully automatic.

Attacks:

- Confirms two existing attacks.
- Discloses a new attack.

<table>
<thead>
<tr>
<th>No.</th>
<th>Pairing Cases</th>
<th>Exe. P1</th>
<th>P2</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DisplayYesNo-DisplayYesNo</td>
<td>NC</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>2</td>
<td>DisplayYesNo-KeyboardDisplay</td>
<td>NC</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>3</td>
<td>KeyboardDisplay-KeyboardDisplay</td>
<td>NC</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>4</td>
<td>KeyboardDisplay-DisplayYesNo</td>
<td>NC</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>5</td>
<td>DisplayOnly-KeyboardOnly</td>
<td>PE</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>6</td>
<td>DisplayOnly-KeyboardDisplay</td>
<td>PE</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>7</td>
<td>DisplayYesNo-KeyboardOnly</td>
<td>PE</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>8</td>
<td>KeyboardOnly-DisplayOnly</td>
<td>PE</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>9</td>
<td>KeyboardOnly-DisplayYesNo</td>
<td>PE</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>10</td>
<td>KeyboardOnly-KeyboardOnly</td>
<td>PE</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>11</td>
<td>KeyboardOnly-KeyboardDisplay</td>
<td>PE</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>12</td>
<td>KeyboardDisplay-DisplayOnly</td>
<td>PE</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>13</td>
<td>KeyboardDisplay-KeyboardOnly</td>
<td>PE</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>14</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>14-25 Other Pairs (12)</td>
<td>JW</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>26</td>
<td>No-OOB-No-MITM</td>
<td>JW</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>27</td>
<td>Uni-direction OOB (I→R)</td>
<td>OOB</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>28</td>
<td>Uni-direction OOB (I←R)</td>
<td>OOB</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>29</td>
<td>Bi-direction OOB (I←→R)</td>
<td>OOB</td>
<td>✓</td>
<td>x</td>
</tr>
</tbody>
</table>

➤ Models & Results: [https://github.com/luojiazishu/BLE-SC-Pairing-Model](https://github.com/luojiazishu/BLE-SC-Pairing-Model)
➤ Or Browser Results Only: [https://luojiazishu.github.io/BLE-SC-Pairing-Model/](https://luojiazishu.github.io/BLE-SC-Pairing-Model/)
Method Confusion Attack

Method Confusion Attack

Affected Cases found \textit{automatedly}

<table>
<thead>
<tr>
<th>IOCap\textsubscript{R}</th>
<th>DisplayYesNo</th>
<th>KeyboardOnly</th>
<th>DisplayKeyboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayYesNo</td>
<td>N/A</td>
<td>MCA-PN</td>
<td>MCA-PN</td>
</tr>
<tr>
<td>KeyboardOnly</td>
<td>MCA-NP</td>
<td>N/A</td>
<td>MCA-NP</td>
</tr>
<tr>
<td>DisplayKeyboard</td>
<td>MCA-NP</td>
<td>MCA-PN</td>
<td>MCA-NP*</td>
</tr>
</tbody>
</table>

\textit{MCA-PN: Initiator PE, Responder NC.}

\textit{MCA-NP: Initiator NC, Responder PE.}

*: There should be MCA-PN & MCA-NP, but Tamarin only give one Counterexample.

Countermeasures

- Enforcing Pairing Method
- User Interface Design Hotfix
- Authenticating Association Model

“Currently \textbf{there is no fix} available that would not massively affect backwards compatibility to older Bluetooth devices.”
Key Negotiation Downgrade Attack

Countermeasures
- Higher Minimum Entropy
- Remove Entropy Negotiation

“We agree that the described scenario is a plausible means for a MITM to affect the establishment of a pairing or bonding between LE devices supporting and using LE Secure Connections pairing when the stored LTKs are generated and confirmed but nevertheless do not match because of different masked lengths.”
Patching

Original NC

Displays a number $V_I$, user confirms

Displays a number $V_R$, user confirms

Displays a number $H_I = g_3(V_I||req||rsp)$, user confirms

Patched NC

Original PE

User inputs passkey

Displays passkey

User inputs $D_R$, checks $H = g_3(passtext||req||rsp) = D_R$

Patched PE

The countermeasures had been verified under symbolic model.

Bluetooth SIG’s Response

“As the described notification method occurs via information available at the host layer or above, implementations would be free to instigate this or similar notification method for users.”
Thank you!

Contact: Min Shi, itachi@whu.edu.cn