BIAS: Bluetooth Impersonation AttackS

Daniele Antonioli (EPFL), Nils Tippenhauer (CISPA), Kasper Rasmussen (Oxford Univ.)
Bluetooth standard

- Bluetooth standard
  - Specifies **Bluetooth Classic (BT)** and Bluetooth Low Energy (BLE)
  - 1 vulnerability in the standard = billions of exploitable devices
Contribution: Bluetooth Impersonation AttackS (BIAS)

- Bluetooth Impersonation AttackS (BIAS)
  - Exploiting standard-compliant vulnerabilities in Bluetooth authentication
  - To impersonate any Bluetooth device without having to authenticate

![Master Impersonation](image)

![Slave Impersonation](image)
Contribution: Bluetooth Impersonation AttackS (BIAS)

- **Bluetooth Impersonation AttackS (BIAS)**
  - Exploiting standard-compliant vulnerabilities in Bluetooth authentication
  - To impersonate any Bluetooth device without having to authenticate
Bluetooth Threat Model

Alice
slave

Bob
master
Bluetooth Threat Model

\( K_L \) Alice slave \( \leftrightarrow \) Pairing \( \leftrightarrow \) Bob master \( K_L \)
Bluetooth Threat Model

Alice slave  

Session Establishment  

Bob master  

$K_L$  

$K_L$
Bluetooth Threat Model

Alice slave  \( K_L \)  Bob master  \( K_L \)  Pairing key Authentication
Bluetooth Threat Model

Session key Negotiation

Alice slave

Bob master

$K_L$

$K'_C$

$K_L$

$K'_C$
Bluetooth Threat Model

Alice slave

Secure session

Bob master

$K_L$ $K'_L$

$K_C$ $K'_C$
Bluetooth Threat Model

Charlie as Alice

NO secure session

Bob master

$K_L$

$K'_C$
Bluetooth Threat Model

Alice slave

\[ K_L, K'_C \]

NO secure session

Charlie as Bob
## BIAS Attacks on Bluetooth Session Establishment

<table>
<thead>
<tr>
<th>BIAS Attacks</th>
<th>Master Impersonation</th>
<th>Slave Impersonation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy Secure Connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Connections</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### BIAS Attacks on Bluetooth Session Establishment

<table>
<thead>
<tr>
<th>BIAS Attacks</th>
<th>Master Impersonation</th>
<th>Slave Impersonation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legacy Secure Connections</strong></td>
<td>Alice slave (Bob)</td>
<td>Charlie as Alice</td>
</tr>
<tr>
<td>BIAS</td>
<td>Charlie as Bob</td>
<td>Bob master</td>
</tr>
<tr>
<td>Secure Connections</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**BIAS: Bluetooth Impersonation Attack**
# BIAS Attacks on Bluetooth Session Establishment

<table>
<thead>
<tr>
<th>BIAS Attacks</th>
<th>Master Impersonation</th>
<th>Slave Impersonation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legacy Secure Connections</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alice slave</td>
<td>BIAS</td>
<td>Charlie as Alice</td>
</tr>
<tr>
<td>Charlie as Bob</td>
<td></td>
<td>Bob master</td>
</tr>
<tr>
<td><strong>Secure Connections</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alice slave</td>
<td>BIAS</td>
<td>Charlie as Alice</td>
</tr>
<tr>
<td>Charlie as Bob</td>
<td></td>
<td>Bob master</td>
</tr>
</tbody>
</table>
Legacy Secure Connection (LSC) Authentication

Alice (slave)

Bob (master)

\[ R_A = H(C_B, A, K_L) \]

R_A check
1. LSC authentication is **not used mutually** for session establishment.

2. A device can **switch authentication role**.

![Diagram of LSC authentication process]

- Alice (slave)
- Bob (master)
- $A, LSC$
- $B, LSC$
- $C_B$
- $R_A = H(C_B, A, K_L)$
- $R_A$ check
BIAS Attack on LSC: Master Impersonation

Alice (slave)

A

B, LSC

A, LSC

C

C

R_A = H(C, A, K_L)

Skip R_A check

Charlie as Bob (master)

C
BIAS Attack on LSC: Slave Impersonation

Charlie as Alice (slave)

C

B, LSC

A, Role Switch, LSC

Accept Role Switch

Charlie is the master (verifier)

C_C

R_B = H(C_C, B, K_L)

Skip R_B check

Bob (master)

B

Daniele Antonioli (@francozappa)
Secure Connections (SC) Authentication

Alice (slave) \( A \)

Bob (master) \( B \)

\[ R_B, R_A = H(C_B, C_A, B, A, K_L) \]

\[ R_A \]

\[ R_B \]

\[ R_B \text{ check} \]

\[ R_A \text{ check} \]
Standard-Compliant Issues with SC Authentication

1. SC negotiation is not integrity-protected
2. SC support is not enforced for pairing and session establishment

![Diagram showing the SC handshake process](image)
BIAS Attack on SC: Master Impersonation

Alice (slave)

A

Charlie as Bob (master)

C

B, LSC

A, SC

SC downgraded to LSC

BIAS master impersonation on LSC
BIAS Attack on SC: Slave Impersonation

Charlie as Alice (slave)

B, SC

A, LSC

SC downgraded to LSC

BIAS slave impersonation on LSC

Bob (master)
Very Secure Connections (VSC) ?!

- Let’s define Very Secure Connections (fictional security mode)
  - Use SC authentication (mutual)
  - Not vulnerable to SC downgrade

- Are we safe against impersonation attacks on VSC?
  - No, VSC is vulnerable to master and slave reflection attacks
  - See the paper for the details
Implementation of the BIAS Attacks

Linux Laptop

USB

CYW920819

https://github.com/francozappa/bias
## Evaluation: BIAS Attacks on 31 Devices (28 BT Chips)

<table>
<thead>
<tr>
<th>Chip</th>
<th>Device(s)</th>
<th>LSC</th>
<th>SC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bluetooth v5.0</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple 339S00397</td>
<td>iPhone 8</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>CYW20819</td>
<td>CYW920819EVB-02</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Intel 9560</td>
<td>ThinkPad L390</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Snapdragon 630</td>
<td>Nokia 7</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Snapdragon 636</td>
<td>Nokia X6</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Snapdragon 835</td>
<td>Pixel 2</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Snapdragon 845</td>
<td>Pixel 3, OnePlus 6</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td><strong>Bluetooth v4.2</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple 339S00056</td>
<td>MacBookPro 2017</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Apple 339S00199</td>
<td>iPhone 7 Plus</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Apple 339S00448</td>
<td>iPad 2018</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>CSR 11393</td>
<td>Sennheiser PXC 550</td>
<td>●</td>
<td>-</td>
</tr>
<tr>
<td>Exynos 7570</td>
<td>Galaxy J3 2017</td>
<td>●</td>
<td>-</td>
</tr>
<tr>
<td>Intel 7265</td>
<td>ThinkPad X1 3rd</td>
<td>●</td>
<td>-</td>
</tr>
<tr>
<td>Intel 8260</td>
<td>HP ProBook 430 G3</td>
<td>●</td>
<td>-</td>
</tr>
</tbody>
</table>
## Evaluation: BIAS Attacks on 31 Devices (28 BT Chips)

<table>
<thead>
<tr>
<th>Chip</th>
<th>Device(s)</th>
<th>LSC</th>
<th>SC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth v4.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CYW4334</td>
<td>iPhone 5s</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>CYW4339</td>
<td>Nexus 5, iPhone 6</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>CYW43438</td>
<td>RPi 3B+</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Snapdragon 210</td>
<td>LG K4</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Snapdragon 410</td>
<td>Motorola G3, Galaxy J5</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Bluetooth v≤ 4.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCM20730</td>
<td>ThinkPad 41U5008</td>
<td>●</td>
<td>O</td>
</tr>
<tr>
<td>BCM4329B1</td>
<td>iPad MC349LL</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>CSR 6530</td>
<td>PLT BB903+</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>CSR 8648</td>
<td>Philips SHB7250</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Exynos 3470</td>
<td>Galaxy S5 mini</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Exynos 3475</td>
<td>Galaxy J3 2016</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Intel 1280</td>
<td>Lenovo U430</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Intel 6205</td>
<td>ThinkPad X230</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Snapdragon 200</td>
<td>Lumia 530</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
BIAS + KNOB: Break Bluetooth Session Establishment

Alice (master) — A — Bob (slave) — B

Phase 1: pairing key authentication
Phase 2: session key negotiation
Phase 3: secure session
BIAS + KNOB: Break Bluetooth Session Establishment

Alice (master)

Phase 1: pairing key authentication (BIAS attack)

Charlie as Bob (slave)

Phase 2: session key negotiation

Phase 3: secure session

Daniele Antonioli (@francozappa)

BIAS: Bluetooth Impersonation AttackS
BIAS + KNOB: Break Bluetooth Session Establishment

Phase 1: pairing key authentication (BIAS attack)
Phase 2: session key negotiation (KNOB attack [SEC19])
Phase 3: secure session
BIAS + KNOB: Break Bluetooth Session Establishment

Alice (master) \( \overset{A}{\leftrightarrow} \) Charlie as Bob (slave) \( \overset{B}{\leftrightarrow} \)

Phase 1: pairing key authentication (BIAS attack)

Phase 2: session key negotiation (KNOB attack [SEC19])

Phase 3: secure session (Charlie is Bob)
BIAS + KNOB: Break Bluetooth Session Establishment

Charlie as Alice

Bob (slave)

Phase 1: pairing key authentication (BIAS attack)

Phase 2: session key negotiation (KNOB attack [SEC19])

Phase 3: secure session (Charlie is Alice)
BIAS Attacks Countermeasures and Disclosure

• We propose a set of countermeasures
  ▶ Use LSC authentication **mutually** during session establishment
  ▶ **Integrity-protect** session establishment with the pairing key
  ▶ **Enforce SC support** across pairing and session establishment

• We disclosed the BIAS attacks, and the Bluetooth standard has been updated
  ▶ However, most of the devices are still vulnerable
  ▶ E.g., no user or device updates, no device recalls
Conclusion: Bluetooth Impersonation AttackS (BIAS)

- **Bluetooth Impersonation AttackS (BIAS)**
  - Exploiting standard-compliant vulnerabilities in Bluetooth authentication
  - To impersonate any Bluetooth device without having to authenticate
  - Website: [https://francozappa.github.io/about-bias/](https://francozappa.github.io/about-bias/)
  - Code: [https://github.com/francozappa/bias](https://github.com/francozappa/bias)