BLE-Guardian: Protecting the Privacy of BLE Users

Kassem Fawaz*, Kyu-Han Kim†, Kang G. Shin*

*Computer Science and Engineering, University of Michigan
†Hewlett Packard Labs
What is Bluetooth Low Energy?

- Attractive communication technology
  - Short range
  - Low energy footprint
  - Supported by most hosts

- Currently:
  - 74K unique products with BLE support

- 2013:
  - 1.2 billion BLE products shipped

- 2020:
  - 2.7 billion BLE products expected
BLE Primer

- **Standby**: Low Power Mode. Receiver and transmitter switched ‘off’

- **Advertising**: Used by low power ‘Server’. Only transmitter required.

- **Scanning**: Used by ‘Client’. Receiver listens to advertising channels.

- **Initiating**: ‘Server’ sends connection request

- **Connection**: After scanning, ‘Client’ responds to ‘Server’ advertisement
BLE Advertisements

• 3 dedicated advertising channels:
  • 2402 MHz (37), 2426 MHz (38), 2480 MHz (39)

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADV_DIRECT_IND</td>
<td>Connect to a particular device only</td>
<td>3.75 ms, but only for 1.28 seconds</td>
</tr>
<tr>
<td>ADV_IND</td>
<td>General presence known + connections</td>
<td>20ms – 10.24s</td>
</tr>
</tbody>
</table>

\[ \mathcal{r} \in [0, 10] \]
BLE Security and Privacy

• Pairing & bonding
  • Prevent unauthorized access to device or secured services

• Address randomization
  • Prevent user tracking

• Direct Advertisements
  • Prevent user tracking and profiling
BLE Privacy & Security Effectiveness

• *Passively* scan for BLE advertisements
• Collect:
  
  <Timestamp, BT Address, advertisement content, RSSI>

<table>
<thead>
<tr>
<th>Site</th>
<th>Participants</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hewlett Packard Labs</td>
<td>1</td>
<td>40 days</td>
</tr>
<tr>
<td>Ann Arbor</td>
<td>13</td>
<td>2 months</td>
</tr>
<tr>
<td>Phone LAB/ SUNY Buffalo</td>
<td>86</td>
<td>2 months</td>
</tr>
</tbody>
</table>
BLE Privacy & Security Effectiveness

- **Indirect Advertisements**
  - Detected 214 different unique *types of* devices

- **Address Randomization**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Device</th>
<th>Days observed</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ihere</td>
<td>key finder</td>
<td>One</td>
<td>37</td>
<td>00:17:E9:CB:F3:61</td>
</tr>
<tr>
<td>DEXCOMRX</td>
<td>Glucose monitor</td>
<td>Flex</td>
<td>37</td>
<td>00:17:E9:CB:F5:01</td>
</tr>
<tr>
<td>Frances’s Band ea:9d</td>
<td>smartband</td>
<td>Zip</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>Otbeat</td>
<td>heart rate monitor</td>
<td>Forerunner 920</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>JS00002074</td>
<td>digital pen</td>
<td>Basis Peak</td>
<td>25</td>
<td></td>
</tr>
</tbody>
</table>

**Revealing Names**

**Consistent Addresses**

**Poor Randomization**
BLE Privacy & Security Effectiveness

• Device Pairing

Advertise and accept connections

Battery level

Unique identifiers
It all starts with the advertisements...

Tracking User

Consistent addresses, poor randomization, unique device names and identifiers
It all starts with the advertisements...

Attacker BLE device

Tracking User

Profiling User

Health situation, user’s lifestyle, behavior, preferences, and personal interests
Fingerprinting of and unauthorized access for sensitive systems and devices

It all starts with the advertisements...

Tracking User

Profiling User

Harming User

Fingerprinting of and unauthorized access for sensitive systems and devices
Research Questions

Can we effectively fend off the threats to BLE-equipped devices

(1) in a device-agnostic manner,

(2) using COTS (Commercial-Off-The-Shelf) hardware only, and

(3) with as little user intervention as possible?
BLE-Guardian
BLE-Guardian

- Ubertooth One
  - Programmable BT radio
  - Open source firmware
  - Rx/Tx on each BT channel

- User-level app
  - Control BLE-Guardian
  - Update firmware seamlessly
High-level Description

BLE-Guardian running

Owner chooses target BLE device

New client

Authorized client

Attacker detected

Access Control Module

Client Authorization

Access denied

Access granted

Authorized Client List

Device Hiding Module

Connection Enabling

User Alert

Authorized client

Authorized Client List

Please choose a device to hide:

GALAXY Gear (CE00)

Device: GALAXY Gear (CE00)

Authorized Client List

1CBA:8C2F:18:28

Charge HR

1CBA:8C2F:18:28

2015jump

-88

-91

-93
Device Hiding

- Jam BLE device advertisements to hide its existence
- Need to learn device advertising Sequence
  - Otherwise jamming will be ineffective or inefficient
Device Hiding

Estimate advertising interval:

\[ \text{adv}' = E(t_i) - 5 \]

Max delay
Device Hiding

- Detect RSSI (received signal strength indication) increase
- Apply jamming and follow advertising sequence
At this point, the target BLE device is hidden.

How to enable access to it?
Access Control

Authorization:

Bluetooth classic as an OOB channel.

Client

BLE-Guardian

Target BLE device

Attacker

Bt_addr, UUID

Attempt connection

Send pairing request

User completes pairing

Client authorized by user

jamming

adv

Connection request

User completes pairing

Client authorized by user
Access Control

Connection Enabling:

Connection parameters to distinguish legitimate connection request.
Evaluation
Evaluation

Cut-off Distance

[Diagram showing an attacker, a BLE device, and a BLE-Guardian with a cut-off distance marked by 'd']
Evaluation

Cut-off Distance

Adversary has to be within 1 m of BLE device to read its advertisements
Evaluation

Impact on Advertising Channels

1. Protect single device at advertising intervals:
   • 20ms, 960ms, and 10.24 sec
2. Two devices advertising at 20 ms
3. 15 other devices
   • With varying advertising frequencies

The number of unnecessary jamming instance is minimal
Evaluation

Energy Overhead

1. BLE-device and authorized clients
   • No overhead

2. Smartphone as a gateway
   • Idle power: 1370mW
   • Overhead: less than 16%
Conclusion

• **BLE-Guardian**
  • Privacy protection for BLE device users
  • Device agnostic and relies on COTS hardware
  • Low overhead on advertisement channels

• Future work
  • Explore other M2M protocols such Zigbee
  • Implement without needing external hardware (need firmware access)
Thank You

kmfawaz@umich.edu
kassemfawaz.com