Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices

Hadi Givehchian, Nishant Bhaskar, Eliana Rodriguez, Héctor López, Christian Dameff, Dinesh Bharadia, Aaron Schulman

UC San Diego
BLE smart devices are constantly beaconing

<table>
<thead>
<tr>
<th>Smart Device</th>
<th>#adverts/min</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 10</td>
<td>872</td>
</tr>
<tr>
<td>Google Pixel 5</td>
<td>510</td>
</tr>
<tr>
<td>Thinkpad X1 Carbon</td>
<td>864</td>
</tr>
</tbody>
</table>
BLE beacons are a privacy risk
Tracking prevention at MAC layer

Attacker can track using MAC address

Bluetooth introduced MAC randomization
An underlying threat at PHY layer

- CFO
- I/Q imbalance
- I/Q offset
BLE has short known sequence

- **Training Samples**
  - Known bits (preamble)
  - Variable bits

- **WiFi**
  - 512
  - Payload

- **BLE**
  - 8
  - Payload
Utilizing the full BLE packet as a known sequence

We can decode the packet
• Don’t need high precision estimates

Use the full packet as a known sequence
Optimization approach

• Start with clean signal from decoded bits
• Iteratively add imperfections
• End goal – Get close to received signal
Improvement in imperfection estimation

We use all samples of signal
  • High resolution of estimation
  • Reduced impact of noise

It is feasible to get fine grained fingerprint
Is it feasible to do tracking in real world conditions?

Wireless environment can change

Physical environment can change
BLE devices may have similar fingerprints

Device fingerprints may be close
- Likely to confuse with each other

Device fingerprints vary by chipset
- Small range of I/Q offset for smartphone
- Large range in low-end devices
- Some devices have no I/Q offset
Fingerprints may drift with temperature

Device CFO can vary due to device and ambient temperature
1. BLE transmit power varies across smart devices and applications

2. Low cost SDRs may have imperfections that impact measurement

3. Location or speed of target device may change

How successful will an attacker be in real world?
How is the tracking performed?

Fingerprinting Stage
Repeat for 50 packets
(mean, variance)

Tracking Stage
Statistical distance
Repeat for 10 packets
distance < threshold
Packet from device
Overview of Field Evaluation

BLE beacon data collected from uncontrolled mobile devices
- coffee shops, library, food court, large facility

Our analysis

1. How accurately can we track target devices?
2. Is a smart device distinguishable among hundreds?
3. Is it feasible to track a person?
Evaluating accuracy of tracking

Fingerprinting
Office (Day 0)

False Negative
Food-court (Day 2-7)

False Positive
Coffee Shop (Day 8)
Evaluating accuracy of tracking

17 distinct target devices
  • Smartphones, watches, laptops

Average FPR 3.5%, FNR 3.2%

Most devices have distinguishable imperfections
Are these imperfections unique at scale?

647 unique devices observed
• Receiver placed at exit of a room
• 2 days, 10 hours a day

47.1% devices had distinct fingerprints
• Another 15% had one overlap

Even at scale, many devices are uniquely distinguishable
Is it feasible to track a person?
Tracking is feasible in real world situations, even in presence of other devices.
Possible defenses to tracking

1. Hardware/firmware modification to add a time-varying CFO or I/Q offset

2. Software runs time-varying computation, causing temperature changes
Conclusion

For many smart devices, physical layer BLE tracking is a real threat.

A number of real world devices have distinguishable imperfections, and are vulnerable.