Detecting Unwanted Location Trackers

BoF Presentation
July 27, 2023
System Architecture

(How Bluetooth Crowdsourcing and Unwanted-Tracking Detection Work)
Near-owner mode

- Phone physically close to accessory
- Persistent or periodic BT connection keeps accessory in near-owner mode
Separated mode

Owner’s tag

Separated Mode
- Phone physically far away
- OR could be powered off or have dead battery
Separated mode + Bluetooth (BT) crowdsourcing

Crowdsourcing
- Finders observe BT advertisement
- Finders encrypt their own location using key in advertisement
- Finders upload encrypted locations to server
- Owner’s phone queries locations from the server, decrypts them, and computes best-estimate of location
Architecture: Unwanted tracking

- Tag is separated from owner
- Tag has been moving with non-owner over time and distance
- Background scans detect tag multiple times
- Alert is shown on non-owner’s phone

**UT detection and alerting**

- Advertise over Bluetooth
- Non-owner traveling with the tag
- Query capabilities, play sound, etc.
- Fetch tag info over HTTP/HTTPS

Non-owner’s phone

**Server**

TBD
Architecture: BT crowdsourcing + unwanted tracking

- Owner's tag in non-owner's backpack
- Non-owner's phone
- Owner's tag in non-owner's backpack
- Non-owner's phone
- Finder
- Owner's phone

**UT detection and alerting**
- Tag is separated from owner
- Tag has been moving with non-owner over time and distance
- Background scans detect tag multiple times
- Alert is shown on non-owner's phone

**Server**
- c. Fetch locations over HTTPS
- b. Publish locations over HTTPS
- e. Fetch tag info over HTTP/HTTPS
- d. Query capabilities, play sound, etc.

**Owner's phone**
- a. Advertise over Bluetooth
- b. Publish locations over HTTPS
- c. Fetch locations over HTTPS

**Finder**
- Non-owner traveling with the tag

**Non-owner's phone**
- Owner's tag in non-owner's backpack

**TBD**
- Non-owner traveling with the tag

**Encrypted locations**
- Owner's phone

**Finder**
- Non-owner's phone

**Non-owner's phone**
- Owner's tag in non-owner's backpack
Comparison of some existing systems

<table>
<thead>
<tr>
<th>Surface</th>
<th>Deterrence at pairing</th>
<th>Proactive alerts (background scanning)</th>
<th>Learn about accessory</th>
<th>Non-owner play sound</th>
<th>Serial number look-up</th>
<th>Accessories detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS UT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>AirTags + AirPods + Apple FMN accessories</td>
</tr>
<tr>
<td>Android UT</td>
<td>N/A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>AirTags + Google FMD accessories</td>
</tr>
<tr>
<td>Airguard app</td>
<td>N/A</td>
<td>Android: yes iOS: Tile + Samsung tags</td>
<td>❌</td>
<td>✓</td>
<td>❌</td>
<td>All accessories?</td>
</tr>
<tr>
<td>Tile app</td>
<td>Under consideration</td>
<td>Under consideration</td>
<td>✓</td>
<td>Under consideration</td>
<td>✓</td>
<td>Tile tags and Tile partner’s accessories</td>
</tr>
</tbody>
</table>
Threat Model
<table>
<thead>
<tr>
<th>Persona</th>
<th>Threat</th>
<th>Proposed Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stalker</td>
<td>Uses location-enabled accessory for unwanted tracking</td>
<td>Enable target to find and trace accessory (below)</td>
</tr>
<tr>
<td>Target</td>
<td>Target unaware of unwanted tracking</td>
<td>24 hour BT address stability</td>
</tr>
<tr>
<td></td>
<td>Target unable to find tracking accessory</td>
<td>Play sound on item</td>
</tr>
<tr>
<td></td>
<td>Target didn’t receive alert soon enough</td>
<td>Alternate finding hardware</td>
</tr>
<tr>
<td></td>
<td>Target unable to receive unwanted tracking alert</td>
<td>Scan for items</td>
</tr>
<tr>
<td></td>
<td>Target unable to identify known stalker</td>
<td>Obfuscated Owner Information</td>
</tr>
<tr>
<td></td>
<td>Target or Other working on Target’s behalf unable to trace stalker</td>
<td>Serial no. visible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serial no. over NFC/BT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pairing Registry</td>
</tr>
<tr>
<td></td>
<td>Target unable to disable location share</td>
<td>Can disable finding</td>
</tr>
<tr>
<td>Third-Party Scanner</td>
<td>Owner tracked across physical space with BT address</td>
<td>BT MAC randomization + 30 min address rotation</td>
</tr>
<tr>
<td></td>
<td>Target tracked across physical space with BT address</td>
<td>BT MAC randomization + 24 hour address rotation</td>
</tr>
<tr>
<td></td>
<td>Owner tracked across physical space with serial no. broadcast</td>
<td>Action required for broadcast + encryption</td>
</tr>
<tr>
<td>Accessory Hacker</td>
<td>Firmware overwritten to eliminate unwanted tracking protections</td>
<td>-</td>
</tr>
<tr>
<td>Non-Adherent Manufacturers</td>
<td>Accessory manufacturers implement spec incorrectly, incompletely, or not at all</td>
<td>-</td>
</tr>
</tbody>
</table>
Scope
Architecture: BT crowdsourcing + unwanted tracking

Non-owner's phone

Non-owner's phone

Finder

Non-owner's backpack

Non-owner traveling with the tag

Non-owner's backpack

Owner's tag

Owner's phone

Partially in scope

Owner's tag in non-owner’s backpack

Tag is separated from owner

Tag has been moving with non-owner over time and distance

Background scans detect tag multiple times

Alert is shown on non-owner’s phone

TBD

Server
c. Fetch locations over HTTPS
b. Publish locations over HTTPS
a. Advertise over Bluetooth
d. Query capabilities, play sound, etc.
e. Fetch tag info over HTTP/HTTPS

In scope

In scope

Owner's tag in non-owner’s backpack

Owner’s phone

In scope

Finder

Non-owner's backpack

Non-owner's phone

Encrypted locations

Owner’s phone

12
Scope of Charter Proposal – Goals

The goal of the DULT WG is to standardize a protocol for information exchange between location-tracking accessories and nearby devices, along with actions that these accessories and devices should take once unwanted tracking is detected. The intent of this WG is to make it easier for arbitrary devices to detect unwanted tracking by these accessories. The protocols and interactions between devices may be limited to certain states or modes, such as the accessory being separated from a paired/owner device.

The privacy goals of the WG solution are that:

- The owner of the tracking accessory must not learn information about nearby devices that discover or interact with the tracking accessory
- The interactions between tracking accessories and nearby devices are secure
- Actions available to a nearby device (e.g., playing a sound on a tracking accessory) can be limited to certain states or modes

The WG protocol design will be guided by an intent to:

- Minimize hardware changes needed in tracking accessories to implement this protocol; and
- Not preclude adoption by manufacturers of larger devices whose primary purpose is not location tracking, but have location tracking capabilities (e.g., headphones, bicycle, smartphone)
Scope of Charter Proposal – Program of Work

The WG is expected to:

1. Standardize a protocol between tracking accessories and nearby devices, which may:
   - Allow a tracking accessory to identify & advertise its presence when in a detectable mode
   - Allow a nearby device to trigger behavior on an unwanted tracking accessory to aid in determining its physical location
   - Allow nearby devices to fetch additional information about a tracker accessory

2. Specify practices that accessory manufacturers can implement to deter malicious use of tracking accessories and support the implementation of the WG-specified protocol.

3. Specify guidance for non-owner device platforms necessary to support implementation of the WG specified protocol
Not in Scope for This Spec

The WG will **not** standardize an end-to-end platform-based unwanted tracking detection system or define requirements for interactions between accessory manufacturers and law enforcement. In addition, these items are out-of-scope:

- Mechanisms for detecting tracking accessories that do not implement the protocol specified by the WG, and
- Mechanisms for detecting whether a tracking accessory implements the protocol or allowing a tracking accessory to attest that it implements the protocol
Apple Licensing Commitment

- Apple has timely submitted IPR disclosures under the rules of the IETF IPR Policy, RFC 8179, committing to license under RAND terms, for the purpose of implementing the Detecting Unwanted Location Trackers specification, any patent claims that would necessarily be infringed by implementation of such specification.
- Apple has made similar RAND commitments over the years and has publicized its commitment to RAND licensing principles to advance interoperability and give consumers confidence that products will interact reliably with each other.
Questions?
Back-up
Proactive Alert

- Proactive alert shows
  - Tag image
  - Text description
  - Play sound button
  - Disablement text instructions (potentially including diagram/video)
  - Etc.

This is a small location tracker made by Acme Inc.

Learn how to disable
Proposed BT advertisement header in Internet Draft

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Description</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-5</td>
<td>MAC address</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>6-8</td>
<td>Flags TLV; length = 1 byte, type = 1 byte, value = 1 byte</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td>9-12</td>
<td>Service data TLV; length = 1 byte, type = 1 byte, value = 2 bytes (TBD value)</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>13</td>
<td>Protocol ID (TBD value)</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>14</td>
<td>Near-owner bit (1 bit) + reserved (7 bits)</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>15-36</td>
<td>Proprietary company payload data</td>
<td>OPTIONAL</td>
</tr>
</tbody>
</table>

More discussion needs to be had on how to best limit privacy-violating uses of the proprietary data. Proposal: analysis and discussion of this part should be in scope of charter.