Unwanted Tracking Scenarios and Implications for DULT Protocol Design

Maggie Delano, Swarthmore College
Jessie Lowell, Safety Net Project, NNEDV

About us

Maggie Delano
Associate Professor of Engineering
Swarthmore College

Jessie Lowell
Technology Safety Specialist
National Network to End Domestic Violence

Talk Outline

1. **Motivation**
2. Common Unwanted Tracking Scenarios Involving BT Trackers
3. Limitations of Existing Protections
4. Proposed Next Steps

Motivation

- In order for the DULT protocol to be successful, the WG will need an understanding of the unwanted tracking landscape today
- We will share common unwanted tracking scenarios, along with limitations of the present protocols
- Our presentation aims to contribute to the following DULT WG goals:
  - Threat analysis
  - Documentation of the current state of tracker accessory platforms (Goal 1)
  - Standards-track protocol and guidance for preventing unwanted tracking (Goals 2, 3, 4)

Talk Outline

1. Motivation
2. **Common Unwanted Tracking Scenarios Involving BT Trackers**
3. Limitations of Existing Protections
4. Proposed Next Steps

Scenarios Background

- Composite cases based on experiences:
  - Working with survivors
  - Providing case consultations with community programs
  - Hearing reports from the field
- Intended to illustrate several different angles of the problem
  - Not only technological - meant to provide realistic insight into survivors' constraints
- **No** actual identifying info
  - Confidentiality requirements for US laws that fund these services are **very strict**

Scenario 1: Abuser plants location tracker on child

Malka and Anna have two young children. Malka left because Anna was abusive. She was homeless for a month, and the children have been living with Anna. She now has an apartment two towns away. She does not want Anna to know where it is, but she does want to see the children. She and Anna meet at a public playground. She gets there early so that Anna will not see which bus route she arrived on and keeps playing with the children on the playground until after Anna leaves, so that Anna will not see which bus route they get on. Two days later, Anna shows up at Malka’s door, pounding on the door and shouting.

Scenario 2: Survivor has reason to think there may be a location tracker but cannot find it

Safiya and Edward live together. Safiya has noticed that Edward has become excessively jealous – every time she goes to visit a friend by herself, he accuses her of cheating on him. To her alarm, over the last week, on multiple occasions, he has somehow known which friend she visited at any given time and has started to harass them. She eventually gets a notification that a tracker is traveling with her, and thinks it may be in her car, but she cannot find it. She lives in a car-dependent area and cannot visit friends without the car, and Edward controls all of “their” money, so she cannot take the car to the mechanic without him knowing.

Scenario 3: Survivor cannot use tech to scan for a location tracker or receive alerts

Hao-Yu and Ming have been dating for two years. Ming works for a tech company and often emphasizes how much more he knows about technology than Hao-Yu, who works at a restaurant. He insists on having access to Hao-Yu's computer and Android phone so that he can "make sure they are working well and that there are no dangerous apps." Ming hits Hao-Yu when he's angry and has threatened to out him as gay to his conservative parents and report him to Immigration & Customs Enforcement if Hao-Yu "talks back" to him. Hao-Yu met with an advocate at a local domestic violence program to talk about going to their shelter once a bed was available. The advocate did some safety planning with Hao-Yu, and mentioned that there is an app for Android that can scan for location trackers, but Hao-Yu did not feel safe installing this app because Ming would see it. The next time Hao-Yu went to see the advocate, he chose a time when he knew Ming had to be at work until late to make sure that he did not follow him, but when Ming got home from work he knew where Hao-Yu had been.

Real advocates, real survivors, real comments

- “If I get an alert for an AirTag, how long has it been following me? Where can I see this?”
- “Is there a way to find an AirTag/tracker immediately, before someone enters a certain place?”
- “Can I find out who owns a tracker if I **can't physically find it**?”
- “It would be helpful for me as an advocate to have a clear, concise explanation for why it is a random value between 8 hours- 24 hours; e.g. I see the advantage of it being not predictable, but how was the window size chosen?”

Quotes courtesy of the Clinic to End Tech Abuse at Cornell Tech, used with permission

Talk Outline

1. Motivation
2. Common Unwanted Tracking Scenarios Involving BT Trackers
3. **Limitations of Existing Protections**
4. Proposed Next Steps

Unwanted Tracking Affordances and Constraints

- **Active** and **passive** scanning options are needed
- Some individuals being tracked without their consent may not be able to take proactive measures to protect themselves
  - They may not be able to install software
  - Their accounts may be compromised
  - They may not own a smartphone

Current Unwanted Tracking Landscape

Manufacturer	Network	Active Scanning	Passive Scanning
Apple (AirTags)	Find My	Android only	Android iOS
Tile	Tile	Android iOS	Not available
Chipolo	Find My	Not available	iOS only
Samsung (Smart Things)	SmartThings Find	Android iOS (beta)	Not available

There is not only a need for standardization, but also active and passive scanning support on both Android and iOS for all trackers that implement the protocol.

Example Limitations

- Lack of active scanning for AirTags on iOS
- Lack of customization for detecting unwanted tracking

Some BT Trackers are easy to find using BT scanners

A scan in a busy urban area can detect more than 100 devices.

Tiles can be found very easily by filtering for the name “Tile” in any free BT scanning app.

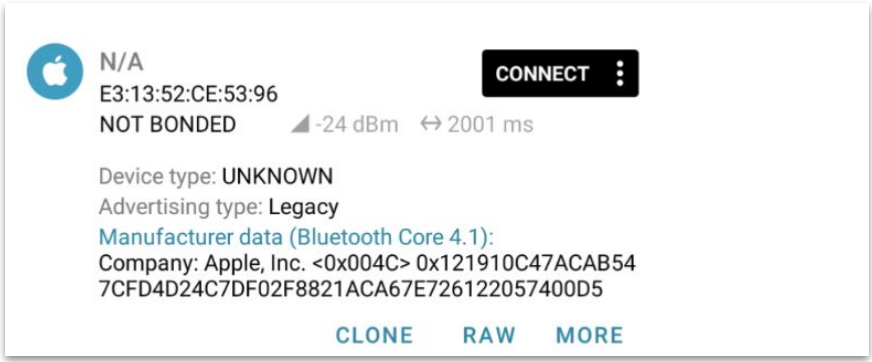
Source: How To Search Your Environment For Bluetooth Tracking Devices

AirTags are difficult to uniquely identify, esp. on iOS

iOS

AirTags on iOS can only be identified by signal strength and advertisement interval.

Android



AirTags on Android include the same information as iOS, plus manufacturer data.

Apple AirTags are not easy to detect on iOS because they 1) have no name, and 2) strip advertisement data from the iOS CoreBluetooth API that could be used to identify the manufacturer.

Source: How To Search Your Environment For Bluetooth Tracking Devices

Missing BT Advertisement Data On iOS

AirTag:

```
2021-08-27 14:36:49.372856-0400 BTLEViewer[371:11269] didDiscoverPeripheral succe
2021-08-27 14:36:49.373259-0400 BTLEViewer[371:11269] advertisementData: {
 kCBAdvDataIsConnectable = 1;
 kCBAdvDataRxPrimaryPHY = 0;
 kCBAdvDataRxSecondaryPHY = 0;
 kCBAdvDataTimestamp = "651782209.370573";
}
2021-08-27 14:36:49.373396-0400 BTLEViewer[371:11269] RSSI: -16
```

Bose SoundLink:

```
2021-08-27 14:36:49.614290-0400 BTLEViewer[371:11269] didDiscoverPeripheral succe
2021-08-27 14:36:49.614497-0400 BTLEViewer[371:11269] advertisementData: {
 kCBAdvDataIsConnectable = 1;
 kCBAdvDataLocalName = "LE-Bose Revolve SoundLink";
 kCBAdvDataManufacturerData = {length = 9, bytes = 0x01060206c575479a41};
 kCBAdvDataRxPrimaryPHY = 0;
 kCBAdvDataRxSecondaryPHY = 0;
 kCBAdvDataServiceUUIDs =     (
 FEBE
 );
 kCBAdvDataTimestamp = "651782209.612992";
 kCBAdvDataTxPowerLevel = 10;
}
2021-08-27 14:36:49.614562-0400 BTLEViewer[371:11269] RSSI: -82
```

Source: Enough with the beeping

While AirTags have no name on any platform, Manufacturer Data is missing on iOS only, and is readily available on Android and Mac.

How to address this issue for the DULT Protocol

Advertised manufacturer data, or some other identifying information, should be available to third party developers regardless of device OS.

Additionally, and especially if this is not possible/feasible, active scanning should be implemented by the OS.

Lack of Customization For Unwanted Tracking

In addition to active scanning, customizability in settings for how stringent the unwanted tracking algorithm is would be helpful. Maggie tracked themselves from Philadelphia to Boston and an alert was only triggered hours after they arrived.

Individuals should be able to customize their alerts, for example:

- Decreasing or increasing the “traveling with you” duration before a passive notification
- Decreasing or increasing the number of sounds before a device goes dormant, and/or sending notifications for each time a sound is played

Smart defaults can be used to avoid false positives while respecting the autonomy of individuals concerned for their safety.

Talk Outline

1. Motivation
2. Common Unwanted Tracking Scenarios Involving BT Trackers
3. Limitations of Existing Protections
4. **Proposed Next Steps**

Proposed Next Steps

We propose a number of next steps, including:

- Generation of additional scenarios based on real world experiences
- A more detailed evaluation of the affordances of current unwanted tracking approaches (passive, active) and how they can best address the real world scenarios
- Development of requirements for algorithms accordingly, especially considering the need for both active and passive tracking
- Evaluating the affordances of the near-owner state, especially for active scanning

Acknowledgements

Thank you to Alana Ramjit, Nick Doty, Alexis Hancock, and Andrew Crawford for their input on this presentation.