Bluetooth Tracking Privacy Bubble

Sophie Walker

5 October 2023

1 Introduction

Bluetooth Low Energy tags such as AirTags or Tile Trackers are useful tools for locating personal items. However, these can be used maliciously to stalk others. My project will involve creating a system to unobtrusively prevent stalking. This involves an inhibitor mode for tags that will create a ‘privacy bubble’ around them. Tags functioning in a normal mode, which can be located to find, are ‘tracking’ tags. A privacy bubble means any tracking tags near in time or distance to an inhibitor will not report their locations back to an owner. This has the potential to stop stalking as tags placed on a victim will be unable to be tracked.

Additionally this will give people peace of mind that stalking will be stopped, even before it is detected by other tools, as this will block any tracking tags nearby. Benign tags will go out of scope with their owners, so the blocking should not be diruptive, whilst true stalking is prevented. This can also prevent annoyances from false positive stalker detection that picks up tags owned by friends, family or collegues, as this mechanism works without requiring notifications.

Currently there are other stalking prevention features in similar devices, but typically detecting stalkers takes at least 4 hours [1] and can repetitively alert users to false positives if we are near a person with their own tag, for extended periods of time. This method of indiscriminately blocking nearby tags should not pose issues for people finding their own tags, but solves the issue other tools have where we cannot distinguish malicious from safe tracking.

2 Description of Project

This will involve creating my own system to track tags, register inhibitor/tracker mode and distribute locations or not within this. I will have to overcome....!!!! I wish to investigate the effectiveness and usability of such a system The main work items are different settings for the time bounds and distance bounds for two devices being co-located is introducing inhibitor tags to a BLE tracking system an effective way to reduce the risk/impact/ease of stalking" Received Signal Strength Indicator

3 Success Criteria

- An app must be modified that can register BLE tags in two modes, locate tags based on RSSI and the phones location. and communicate with the server to share the signal strength of any tags that can be detected and current location.
- A server must be built that can communicate with the app to identify inhibitor tags and find any tracking tags that are within time and distance bounds of a tracker tag.
- The time and Distance bounds should be able to be set and changed on the server. I will investigate the time and distance ranges that will be appropriate for this bubble, based on experiments centred on the accuracy for variable bounds, and how what settings could reasonably cover a person from stalking.

4 Possible Extensions

- Return uninhibited tags' locations to the owner. This is not required for the core investigation into whether we can have a functioning 'privacy bubble' as we can still mark those tags as (un)blocked. However for investigation into the usability, this is required.
- Tag type is determined is in the server alone in the main implementation, an extension may explore tag type being set by the detecting phones. This adds flexibility later (tags can be changed from one type to another, even historically.
- Implementing the same security procedures used by Apple to cycle IDs regularly and encrypt data in the server is a clear example.

- complex and accurate methods for locating tags based on an epoch of measurements
- identifying stalkers even if they have been blocked
- Implementing local finding, if the devices are in range - i.e. to allow genuine tags to be found only if their owner is in range. use case i.e. so you do not stop your neighbours finding their own items while at home. This can also prevent malicious use of inhibitor tags by thiefs that can block an area of tags to prevent owners finding items etc.

5 Evaluation

BLE is a suboptimal system and by implementing this test system we can establish the false positive rates, false negative rates, and any other stats of interest for various settings and scenarios.

This can include an experiment based on

. We will address the question ”is introducing inhibitor tags to a BLE tracking system an effective way to reduce the risk/impact/ease of stalking”.

6 Starting Point

This will be completed in Java/Kotlin (based on most appropriate app chosen) which I have used in the OP course/ which I have not used except for a basic tutorial this summer. I will also use Python Flask to build the webserver, which I have used briefly before in the Group Project last year. I have used SQL in databases, but not MySQL specifically. I have not previously used tools or libraries related to BLE tracking tags before.

7 Work Plan

8 Resource Declaration

The resources that this project requires are BLE tracking tags to test and create the inhibitor and tracking system and Android phones are required to detect the tags. Both of these will be provided by Dr Ramsey Faragher. In the case they are not provided, I will be able to simulate BLE beacons on my laptop and use my personal phone, although they have already been ordered so this should not be the case. I will use my personal laptop to build this, with another personal laptop as a contingency. I will backup all code to GitHub and use it's version control. Any documents created I will back up to GitHub. I am using TeXworks and Obsidian to write these. I accept full responsibility for this machine and I have made contingency plans to protect myself against hardware and/or software failure.

References

[1] "Can't Keep Them Away: The Failures of Anti-Stalking Protocols in Personal Item Tracking Devices"

[2] R. Faragher and R. Harle, "Location Fingerprinting With Bluetooth Low Energy Beacons," in IEEE Journal on Selected Areas in Communications, vol. 33, no. 11, pp. 2418-2428, Nov. 2015, doi: 10.1109/JSAC.2015.2430281.

Week	Start	Work Package	Deliverable
1-2	16/10/2023	Learn to use and edit BLE libraries. Set up and learn to use flask with MySQL.	Write up of completed experiments, limitations that could affect this project. Write up understanding of modifications and requirements of app.
3-4	30/10/2023		Full Specification of Solution
5-6	13/11/2023		Implement modifications to app and deviced based inhibiting
7-8	27/11/2023		Implement web server and web based inhibiting
9-10	11/12/2023		Evidence of succesful testing of both systems. Optionally Implement extension
11-12	25/12/2023	Part of this package will be spent on the Christmas Holiday. The rest will be used to continue working on any extensions or as slack for unfinished deliverables.	Any Previous Unfinished Deliverables.
	Lent Term	Lent Term	Lent Term
13-14	08/01/2024		Progress Report. An evaluation plan. Recorded Data for Device based inhibiting.
15-16	22/01/2024		Presentation for Progress Report. Recorded Data for server based inhibiting
17-18	05/02/2024		Optional: Recorded data/experiments for implemented extensions.
19-20	19/02/2024		Write up of data recorded and evaluation and conclusions.
21-22	04/03/2024		Any Previous Unfinished Deliverables.
23-24	18/03/2024		Introduction Chapter of Dissertation
25-26	01/04/2024		Preparation and Implementation Chapters of Dissertation
27-28	15/04/2024		Full dissertation Chapters
29-30	29/04/2024		Full Completed Dissertation