Bluetooth Tracking Privacy Bubble

Sophie Walker

5 October 2023

1 Introduction

Bluetooth Low Energy (BLE) 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 disruptive, whilst true stalking is prevented. This can also prevent annoyances from false positive stalker detection that picks up tags owned by friends, family or colleagues, 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

My project does not aim to create new tags or hardware, instead, I want to alter the system used to interact with tags, so this could be implemented without users requiring a new or altered tag. So, this project will involve two key items:

- **The App:**This will be modified from a current app (I am looking into the most suitable one at the moment for my final proposal, - e.g.: this) that can scan for BLE tags and obtains their Received Signal Strength Indicator (RSSI) to calculate the location of tags. I will then modify this to communicate with the server by passing the locations of found tags to it. This can be further modified in extensions to improve locating tags and provide security.
- **The Server:** I will build this using Python Flask and MySQL to create a database which stores the tag IDs, which mode they are registered as, their location and if they are inhibited. It will also calculate which tags are in range of inhibitors and block these. Additionally, it will share the last known location of trackers back to the user.

  I will also have to solve difficulties regarding the imperfect BLE system and create one that can cope with the interference of the BLE signal through people, multipath fading and other spurious results [2]. This will also have to ensure if tags are in range of each other, but detected by separate devices, or if a tracking tag is detected before the nearby inhibitor is. These are a few of the issues my system should aim to be robust against.

  I can evaluate the system based on the false positive rates, false negative rates, and any other stats of interest for various settings and scenarios. I could potentially design an experiment based on the usability of this system, and whether introducing these inhibitor tags is an effective way to reduce the risk/impact/ease of stalking.

3 Success Criteria

- An app must be modified that can register BLE tags in two modes, locate tags based on RSSI and the phone's location. It needs to 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 the 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 what settings could reasonably cover a person from stalking.

4 Possible Extensions

- Explore tag type being set by the detecting phones. This adds flexibility later so tags can be changed from one type to another, even historically. The owner of the inhibitor will likely be carrying their phone and inhibitor together, so this can be used to set the mode locally and then update the server. I can investigate if this is a feasible implementation likely to be used.
- Implementing the same security procedures used by Apple to cycle IDs regularly and encrypt data in the server.
- Improving methods for locating tags, this can be based on an epoch of measurements[3] or use one of the smoothing algorithms suggested [4].
- Identifying stalkers even if they have been blocked, so those that have been blocked for a long period can be found by those being stalked and how other stalking detection tools can interact with inhibiting tags.
- Implementing local finding, if the devices are in range so we can allow genuine tags to be found only if their owner is in range. use case For example, so a user does not stop neighbours from finding their items while at home. This can also prevent the malicious use of inhibitor tags that can block an area of tags to prevent owners from finding items.

5 Starting Point

This will be completed in Java/Kotlin (based on the most appropriate app chosen) which I have used in the OOP 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.

6 Work Plan

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 and limitations that could affect this project. Write up an understanding of the modifications and requirements for app.
3-4	30/10/2023	Decide structure of database and server functionality to ensure correct inhibiting.	Specification of full Solution
5-6	13/11/2023		Implement modifications to app
7-8	27/11/2023		Implement web server and inhibiting
9-10	11/12/2023		Evidence of successful 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 and Presentation. An evaluation plan.
15-16	22/01/2024		Record data for inhibiting and perform any required experiments
17-18	05/02/2024		Optional: Recorded data/experiments for implemented extensions. Any Previous unfinished deliverables.
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	Any appendixes	Full Completed Dissertation

7 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 its 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] K.I. Turk, A. Hutchings, A. Beresford, "Can't Keep Them Away: The failures of anti-stalking protocols in personal item tracking devices" to appear in the proceedings of the Security Protocols Workshop, March 2023

[2] Faragher, R., Harle, R., "An Analysis of the Accuracy of Bluetooth Low Energy for Indoor Positioning Applications," Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014), Tampa, Florida, September 2014, pp. 201-210.

[3] 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.

[4] Mustafa, Abdul and Sykes, Edward. (2021). A high fidelity indoor navigation system for users in motion using BLE with beacons