Weekly Blog 5

This week I discovered Altbeacon. An off-the-shelf library that supports contact tracing. Altbeacon's documentation shows that the library can be used as a GATT service (similar to GAEN) to announce its presence and advertise the data. The GAEN payload is of the following format:

1. A 16 bit UUID formatted as 0xfd6f. This UUID is responsible for tagging the advertisement as an Exposure Notification.
2. A 16 byte RPI which is used for matching potential exposures.
3. A 4-byte AEM containing information about the strength of the BLE signal.

Here, Altbeacon also uses a similar structure and also supports GATT service. Consider the following code:

```
BeaconParser beaconParser = new BeaconParser()
    .setBeaconLayout("s:0-1=fd6f,p:-:-59,i:2-17,d:18-21");
```

In this code, the library explicitly allows us to set the format for sending out an Exposure notification payload.

1. Here bytes 0-1 represents the 16 bit UUID 0xfd6f representing the Exposure Notification Service.
2. P:-:-59 represents the library's default to using a 1-meter reference of -59 dBm for its built-in distance estimates.
3. I:2-17 represents the 16 byte RPI which can be used as part of the payload.
4. D:18-21 represents the 4-byte AEM.

As of now, I have integrated this as part of the Exposure Notification Service and tested it out to check if my app is sending out beacons. Using BeaconScope (Beacon Scope), I was successfully able to detect beacons broadcasted from my foreground service. The corresponding code commit can be found at AltBeacon Commit Link.

I have successfully integrated my generated RPIs to be broadcasted as beacons.

Apart from this, I have also added checks to alert the user to turn on Bluetooth and location services prior to using the application.

Privacy Guidelines for Contact Tracing Applications

What question does the research paper address?

The paper mainly addresses certain privacy guidelines from various points of view. We will be analysing our approach based on these guidelines through hypothetical or factual opinions. They are as follows:

1. Related to Personal Data

   The paper suggests that no personal information should be requested from the user regarding contact tracing. It suggests any information such as GPS or Bluetooth should not be sent across in its raw format. Further, no identifiable information should be requested by the apps as well.
   a. In our approach, we conform to these guidelines.
   b. We do not ask for personal information.
   c. We do not send across raw data.
   d. We do not store or process identifiable information.

2. Informed Consent
   a. In this, the choice of an infected user uploading her TEKs for informing her contacts about COVID exposure is totally up to the user.
   b. There is also trust and transparency as explained in my previous paper following fact sheets.

3. Guidelines for Patient Privacy
   a. The only data that is uploaded from the patient’s side is TEKs, that does not contain any personal information for identification.
   b. It is just used for generating RPIs for matching purposes. Again, the user has consent to do so.

4. Guidelines for the Non-User Privacy

   As per the guidelines provided by the paper, our app conforms to the following:
   a. Identity and location of non-users are not public. We do not collect any location data.
   b. It provides consent for non-users to upload their RPIs if they were to be infected.

5. Guidelines for Business Confidentiality
    a. Data Collection and Processing
        i. The paper suggests that the data for processing should reside in the user's device and not go out. This is applicable to our case as well where the contact matching processing happens locally on the user's device.
            1. As such we maintain the confidentiality and integrity of the data
            2. Decentralized architecture
    b. Privacy-Preserving Analytics
        i. For processing the data, very little computation is performed. Only the TEks is used for regenerating the RPis to check if they have been matched with the RPIs stored locally.
    c. Transparency and Explainability:
        i. For this, I have created a factsheet document in the previous weekly blog. Following that, the trust and transparency of our application will be prominent. (Weekly Blog 4: MWS)
    d. Usability.
        i. The overall UI is very minimal, with only two screens. One for the initial launch and the next for the user to submit his TEKs as and when he is diagnosed with COVID.

CONTAIN: privacy-oriented contact tracing protocols for epidemics

The paper primarily explains certain privacy principles to preserve the privacy of users. They are:

1. No dependency on WiFi access points and GPS.
2. No disclosure of PII
3. Users should not be able to understand the identity of users they have come in contact with
4. Information needed for contact tracing must be anonymised.

Of the two protocols proposed (encrypted beacons and random beacons), our project is similar to the first one that is the encrypted beacons approach. We derive beacons with anonymised identifiers through cryptographic secure algorithms like HKDF and AES. As such, no PII is revealed. Moreover, as suggested in the paper, the identifiers are periodically refreshed as well. The entire approach is similar to GAEN protocol, which we are following.

We also compare the privacy analysis with ours:

P1. Beacons emitted by a user do not reveal any personally identifying information or location information about that user to other users.

Our approach does not reveal any PII or location information. It uses anonymised identifiers along with BLE for contact matching.

P2. Users that are not infected are not required to upload any information to the verification server.

No personal information is requested or uploaded to the server. Only anonymised identifiers generated from cryptographic random generators and algorithms are used.

P3. Users will not be notified by the verification server about or receive any data from the verification server that can help them verify potential contact with users that are not infected

This is currently part of our to-do list. We intend to match the RPIs locally following a decentralised approach and notify the users if they have been in contact with COVID positive cases.

P4. Users that are infected must opt-in in order for other users to determine if they have been near that infected user.

The app does provide consent for upload feature to infected users.

P5. Users can check if they have been near an (opted-in)an infected user without revealing any personally identifiable information about themselves.

Same as P3

REFERENCES

1. Shukla, M., Lodha, S., Shroff, G. and Raskar, R., 2020. Privacy Guidelines for Contact Tracing Applications. arXiv preprint arXiv:2004.13328.
2. Hekmati, A., Ramachandran, G. and Krishnamachari, B., 2020. CONTAIN: privacy-oriented contact tracing protocols for epidemics. arXiv preprint arXiv:2004.05251.