Private Location Tracing

Benny Pinkas and Eyal Ronen

We propose a simple and private method for enabling users to identify co-location with COVID-19 positive persons. The method is particularly applicable for indoor usage, where GPS-based location is inaccurate. The system is distributed: All private information is locally stored on users' phones, rather than in a centralized database.

The basic structure of the proposal is as follows:

- Locations, such as stores, restaurants, schools or even buses and trains, will be assigned an identity code which is also represented as a QR code. This identity can be in any desired resolution (a school can assign a different identity per room, and a train can be assigned a different identity per coach).

  Let us denote a location which has an assigned identify as an i-location. An i-location will display in its entries exits clear copies of its identity QR code.

- Users will install a special application on their phone. When they enter or leave an i-location they will be asked to scan the QR code with this application.

  Ideally, the phone will give an audible confirmation for a successful scan, and will show a clear notification of whether it is in a state recording an entrance to an i-location.

- The application will keep a log of all i-locations which were visited and scanned in the last 14 days, together with the times of entry and exit from these places.
- When a user is identified as being COVID-19 positive, she will be given the option of uploading her log of i-location visits in the last 14 days.
- The Ministry of Health will publish on a regular schedule lists of all i-locations visited by new COVID-19 positive persons,
- The application will download these lists and will check for intersection between the locations and times visited by its user and the visits of COVID-19 positive persons.

Discussion The system is very similar to the Hamagen application of the Israeli Ministry of Health. The main difference is that Hamagen keeps a log of the GPS locations visited by the user, whereas the new system keeps a log of the i-locations based on QR codes that it scans.

- Advantages:
  - The new system will be more accurate than GPS tracking in tracking indoor locations (which are more relevant than outdoor locations with regards to corona virus infections).
  - The new system does not require users to use location or bluetooth services.

  - Simplicity: Deployment is very easy, since locations only need to register once and then receive a QR code to present. This can be done using a special version of the application, or in many other forms.

- Disadvantages:
  - The new system requires an active participation of users who are required to scan QR codes. This process must be made as smooth as possible.
  - Stores and other locations will also have to monitor visitors to make sure that they indeed scan when entering and leaving the place.

Privacy The system takes exactly the same approach as the first version of the Hamagen application. All data is stored locally at the application. No external server learns the locations visited by a user unless the user is COVID-19 positive and is willing to share her location.

Usability The main bottleneck in using the application is the need to scan QR codes, which might take a few seconds. It is crucial that the scanning operation will be quick and “fun”. (As an example consider the Bit payment application. The payment procedure in this application gives a very appealing experience to the user.)

Improving usabiliy by using other methods of communication QR scanning can be replaced by wireless communication via BLE or NFC (or maybe even wifi?). In particular, when Hamagen 2 is deployed then locations can use a beacon that sends fixed values over BLE. These values will be recorded on the users’ copies of the application.

Another option is for the application to use location and network data to suggest to the user to register as entering nearby businesses. Users can “check in” as entering the location, and then appropriate information will be displayed on the phone. Personnel at the entrance to the location can check that entering users has check in appropriately (this option is also available at the Singaporean SafeEntry application).

Protecting local data In order to protect users from having their visit history revealed to anyone who gets hold fof their phone, that information can be stored encrypted with a key which is generated by a slow process from a user password. For example, the password can be salted with a random 30 bit nonce which is then erased, and this value is then used as a seed for generating a private/public key pair. All information is encrypted with the public ley. when the user wishes to use the system she enters the password, and the system runs a search over the 30 bit nonce space to find the private key.

Similar Applications

The SafeEnrty application from Singapore has a similar functionality `https://support.safeentry.gov.sg/`, and seems to be widely deployed (the android version was downloaded by 50,000 businesses). It enables businesses to scan QR codes of users, enables users to scan QR codes of businesses, or to check-in online as entering a place. However, that application is centralized, and all visits made by users are stored in a government database.