Contact Tracing: De-mystifying How an App Designed to Track People Can Ensure User Privacy and Security

Many governments in many countries around the world recognise that contact tracing plays a very important part to reduce the spread of the deadly disease, COVID-19. In this article, we take a look at the conventional method of contact tracking and comparing it against how technology helps contact tracing and its pro's and con's.

Technology and Contact Tracing

With the evolution of technology in the past 10 years, more and more people have turned to using smart devices on a regular basis. Millions of people around the world, of various ages, have a smartphone with them most of the time, and by taking advantage of this fact, could help identify who someone has been in proximity with.

But how is this done securely without disclosing personal information and location data? Application developers and vendors have to tread a very careful path on ensuring the information is not misused or left insecure for hackers to obtain this very valuable data. There are two common data models that developers are using, a centralised model and a decentralised model.

Apple vs. Google – a Decentralised Model

Majority of the smartphone market is covered by either an Apple operating system smartphone or an Android operating system smartphone. Both Apple and Google often compete against each other with new handsets, new operating systems and new features to attract the consumer to invest into their eco-system.

However, on the 10th April 2020, Apple and Google made a joint statement that seemed to many, a common-sense approach. The two technology giants joined forces to enable the use of Bluetooth technology to help reduce the spread of COVID-19 through contact tracing, with user privacy and security core to the design.

Together, the two technology companies will deliver a two-phased exposure notification service. The first phase is to release and API (Application Programming Interfaces) to allow 3rd parties to utilise the new technology; the second phase will be embedding a notification service into the operating system itself without the need of an application installed on the phone.

Once enabled, the users' device will send out a beacon via Bluetooth on a regular basis. The beacon will consist of a random string of numbers that are not tied to any personal information about the user and will change every 10-20 minutes for additional protection and prevent tracking. Any devices in the area will be listening out for these beacons whilst broadcasting their own. The

received beacons are stored securely on the device. At least once a day, a list of keys for the beacons that have been verified as belonging to people confirmed as positive for COVID-19, are downloaded to the device. Each device will check the beacons it has recorded against this list. If a match occurs, the user is informed of what next steps are required and pass on medical advice.

If a user is positively diagnosed with COVID-19, they can work with the relevant health authority to report that diagnosis within the app, and with their consent their beacons will then added to the positive diagnosis list.

Downside of the "App-oogle" decentralised approach

Both Apple and Google designed this solution with user privacy at its core. There is no personal information or location data shared, just random numerical strings that change every 10-20 minutes.

As there is no centralised server to store any of this information, compromising this solution is virtually impossible. However, as there is no central server, no data analysis can be conducted, that could help predict hotspots, resource planning and other factors.

UK National Health Service (NHS) Contact Tracing – Centralised Model

The UK government have decided to not use Apple and Google's API in their contact tracing application, at the time of writing this article. There are rumours that they are reconsidering this decision though.

Instead, they have decided to develop and create their own solution, which uses a centralised model. At the time of writing, the application is being tested in a trial, restricted to an island off the south coast of England. The beta presented some valuable feedback and shortcomings to the solution by security researchers. NHS have made the source code open source.

By not utilising native support from the operating system vendors, 3rd party developers have to develop their own methods. One of the key challenges the developers will face is to create a solution to ensure the application runs smoothly in the background whilst not open, and not to drain the device's battery and resources at the same time. If the developers get this wrong, there will be a very low adoption of the solution and would be ineffective in tracing the virus.

The NHS developers have designed their application with privacy in mind. All information stored and shared with the NHS server is anonymous.

When the application is executed for the first time, the device generate assigns a unique random number (128 bit GUID). The application creates a random elliptic curve key pair daily, to encrypt the unique identifier of the device. The app asks the user the first part of their postcode (GU14 or W1A, for example, for NHS resource planning, mainly) and it records the model of the phone (for example 'Apple iPhone 10,1'). Nothing identifying and no personal data is captured from the device. This information is only available to the device and the NHS servers.

When a device comes in proximity of another device, it exchanges a package that contains the encrypted identifiers, the time, duration and transmission power used for the Bluetooth connection. During the time the devices are in touch with each other, the Bluetooth signal strengths every few seconds. By measuring the signal strength gives an idea of how close the two devices are and determine if it's a physical encounter.

A user can report on the application if they have symptoms similar to COVID-19. They have the choice to submit their anonymous records of proximity events to the NHS server. The servers can identify the devices that have been in contact with that device. There is a complex risk model that has been designed to determine if the devices have been in close physical encounter by analysing the duration and signal strengths. NHS can use their notification service to inform the devices of the potential encounter and offer medical advice.

Using this model provides the health service opportunities to conduct analysis of the data. The collected data can be used to prepare hospitals, predict hotspots, and create statistics and trend models that could help determine when the government will be able to relax lockdowns.

Upside and Downside to the NHS centralised model

Like any centralised model, there is a risk of information misuse and attacks on central systems. However, with the NHS application, assurances have been made that all information is anonymous, and no personal data is harvested from the devices.

The public health authority has anonymous data to help it understand how the disease appears to be spreading and has the anonymous contact graphs to carry out some analysis. So, the health authority could discover that a particular person seems to infect people really well. While the system wouldn't know who they are, encounters with them could be scored as riskier, and adjust the risk of someone being infected by a particular encounter appropriately. The NHS app uses this centralised model, but also protects your security and privacy strongly.

Conclusion

There are positive and negatives to both a centralised and decentralised model. But there is definitely an advantage of using an Operating System developed feature over a custom developed application. The marriage of software and hardware by Google and Apple means better performance, better battery life and resilience.

If a centralised model is required, then steps like NHS health authority have taken to ensure personal data is protected or not collected in the first place, must be a priority.

References:

- https://www.tripwire.com/state-of-security/healthcare/contact-tracing-ensure-user-privacy-security/
- https://securityboulevard.com/2020/06/contact-tracing-de-mystifying-how-an-app-designed-to-track-people-can-ensure-user-privacy-and-security/