STAYAWAY Covid: A Secure and Privacy Friendly Application Case Study

The Covid-19 pandemic was one of the biggest public health issues ever known, especially in the 21st century. Associated with this pandemic the Portuguese Health Authorities came up with the idea of developing the **STAYAWAY Covid**. An app for mobile devices so that the whole population could track if they were in contact with somebody who tested positive for Covid-19. The **main goal of this app** was to **mitigate the advance of the pandemic in Portugal**. At first it just seemed like a normal application for mobile phones but, after a while many people started questioning themselves if the app was safe.

In response to this pandemic, the **Decentralized Privacy-Preserving Proximity Tracing** (also known as **DP-3T**, or $\boldsymbol{dp^3t}$, which is an **open protocol** that makes digital contact tracing easier. In conformity to the recommendations of the European Union, instead of using the GPS (geolocation system), the dp^3t protocol bases itself on the **utilization of Bluetooth** to detect and log close contacts between users' devices, recording temporary anonymous **Ephemeral Identifiers** (*EphID*) to protect users' privacy. These identifiers are only exchanged between devices if the people are closer than a defined number of meters and are the only data that is transmitted to the other devices.

If one of the people you were in close contact tested positive for the Covid-19, you would get alerted with a notification and an advice to contact the Health Authorities so you could be advised by a professional. This app had several benefits such as:

- **Unknown Location**: The app uses the **Bluetooth LE** (Low Energy) technology instead of **GPS**, leading to no one being able to store or discover any user's location. This technology focuses on proximity unlike the GPS that is focused on location.
- **Data Minimization**: The authorities could only **collect data if the user consented** since the **app's focus** was **alerting the person** if they were exposed to the virus not to share the exact location of the contact.
- **Minimal Information**: By only receiving the Ephemeral IDs the **health authorities could never access more data** from the users.
- **Graceful Dismantling**: The **data on the server and the app** was only **saved for fourteen days** being removed afterwards. This **system dismantled itself** after the end of the pandemic.
- **Decentralization**: In this application there is not one central point for operations. All the **critical operations** like creating EphemeralDs every day and matching them were done **locally in each device**. The exiting of a backend server was only needed to ensure availability for all the users, making attackers not gain anything by compromising it. This allowed for **all the sensitive information** being **decentralized** and being in every **user's individual device**.

Despite all its good qualities, this app wasn't a major success because the potential users weren't convinced enough to download it and use it, being scared that their data would be made public.

References:

[1] https://github.com/stayawayinesctec/stayaway-app, last accessed on October 28th 2023
[2] https://github.com/DP-3T, last accessed on October 28th 2023
[3] https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing, last accessed on October 28th 2023
[4] https://www.deco.proteste.pt/tecnologia/telemoveis/noticias/stayaway-covid-como-funciona-a-app, last accessed on October 28th 2023