

# Weekly Blogs - Week 1

Amal Sailendran	a1783111
-----------------	----------

- Weekly Blog 1:

a. ***So what have you done this week? (note that marks are allocated based on demonstrable outcomes)***

Some of the main things I had undertaken this week:

- I researched the various available sources concerning COVID-19 contact tracing.
- Read briefly about "Privacy-Preserving Automated Exposure Notification" <https://eprint.iacr.org/2020/863.pdf>.
- Created the wiki underlying the essential concepts from the paper in the above point:  
<https://github.cs.adelaide.edu.au/2020-Mobile-and-Wireless-Systems/CovidGuard-F/wiki/Privacy-Preserving-Automated-Exposure-Notification-Wiki>
- Learned about Exposure Notification API by Google and Apple (Gapple:  
<https://developers.google.com/android/exposure-notifications/exposure-notifications-api>)
- We created a Trello board for tracking our team's progress.
- Jotted down a wiki of essential links for later purposes:  
<https://github.cs.adelaide.edu.au/2020-Mobile-and-Wireless-Systems/CovidGuard-F/wiki/Important-Links>
- Co-ordinated and conducted team meetings on Zoom.
- Noted down the questions to be discussed with our supervisor on the weekly catchup meetings

b. ***What are your outcomes (what have you learned? What have you implemented? what have you read?)***

Some of the main things I learned this week:

- i. From the various sources related to COVID contact tracing, I learned the main reason people hesitate to download contact tracing apps is because of privacy concerns.
- ii. I learned about how Gapple (Exposure notification API by Google and Apple) is better when compared to other approaches because of the following reasons:
  1. Bluetooth metadata is encrypted leading to enhanced privacy of a person making it difficult to retain identity-related information by a hacker.
  2. Does not use location data.
  3. Ability to turn off and on as desired.
  4. Identity is not shared with Google or Apple.
- iii. After reading the paper on "Privacy-Preserving Automated Exposure Notification", I learned about re-babbler and cleverparrot. Two decentralized approaches for contact tracing.
  1. I learned re-babbler ensures strong privacy in non-diagnosed individuals while lesser privacy for diagnosed individuals
  2. I learned cleverparrot ensures relatively more privacy for diagnosed individuals at the expense of efficiency.
  3. I learned the four main steps for manual contact tracing:
    - a. Case identification
    - b. Contact elicitation and identification
    - c. Contact notification
    - d. Contact follow-up
  4. I learned about the main steps for identifying a positive COVID-19 case:
    - a. Seed generation: Seeds randomly broadcasted chirps over Bluetooth. Sampling new seeds for each seed period ensured enhanced privacy
    - b. Chirp generation: Chirps were computed as a function of seed and time. For instance, for a seed  $s$ , chirp would be  $F(\text{chirp}, s)$ .
    - c. Listening: These chirps are heard by other users
    - d. Upload: Diagnosed users upload their data to the DB for other users to be notified.
    - e. Merge and check: Diagnosed users can check the chirps from the DB if they have become in contact with a diagnosed person

- iv. I researched whether to develop the app using Flutter, React Native, or JAVA.
  - 1. We ruled out Flutter since it was mainly for cross-platform development using the Dart programming language.
  - 2. We ruled out React Native as most of us were proficient in JAVA.

**c. Some of the questions I have for Zach are:**

- i. Ask about exposure notification API
- ii. Decentralized or centralized?
- iii. Should we be concerned about diagnosed individuals' privacy enhancement as mentioned in the paper?
- iv. Level of app development user-wise perspective expectation. Should we be primarily focussing on security or the user interface look and feel as well?
- v. Phone and BLEs for implementation?

**d. Does your blog and activity briefly and clearly describe your outcomes?**

Yes, I feel I have looked into the surface level concepts related to COVID contact tracing.

- i. I have mainly read about privacy and security related areas. I read the paper "Privacy-Preserving Automated Exposure Notification" and understood about two new approaches for ensuring security: re-babblar and cleverparrot.
- ii. I have also learned about the APIs that could be used for contact tracing.
- iii. We will focus on system-level architecture, data flow modeling diagram, and work on our proposal presentation next week with a deeper understanding.