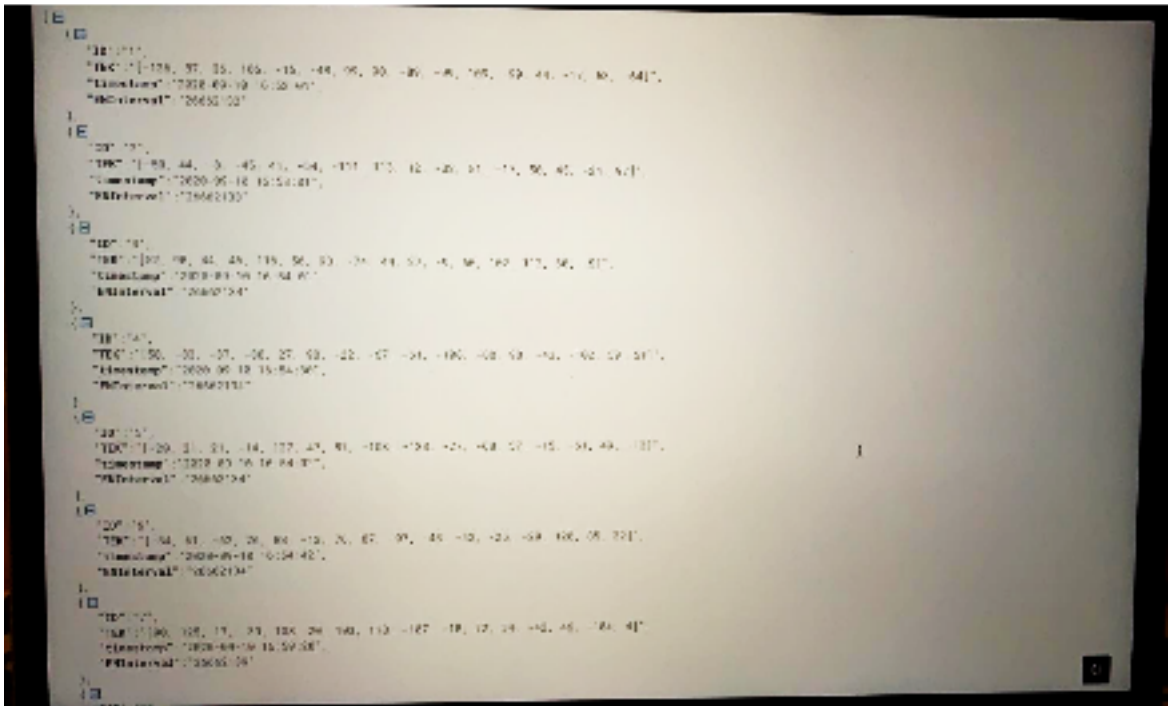
Weekly Blog 7

This week I mainly worked on the first stage of sending the TEKs upon the click of the submit button in our app. Commit link: https://github.cs.adelaide.edu.au/2020-Mobile-and-Wireless-Systems/CovidGuard-F/commit/fe4ef1fa74d9357405aaf78eafd672eae40f387e. The following steps were employed:

1. Incorporate clickSubmitHandler() function as part of the diagnosis_fragment to trigger the conversion of TEK data stored in SQLite (prior to upload, TEKs are stored locally in the following format: ID, TEK, Created_At and ENIN) as a JSONArray.
2. Converted the data stored in SQLite to the format of JSONArray as shown below in the screenshot:



3. The above data is now prepped to be received as a response by the server, following which it can be uploaded to the diagnosis key server for the next stage which is the fetching of data from diagnosis key server for regenerating RPIs and

perform notification toast.

Summary of Bluetooth Contact Tracing Options

What research question does the paper address?

The paper provides a summary of BLE contact tracing options comparing the most widely use BlueTrace protocol with the newer one, Google/Apple Exposure Notification (GAEN) API. The authors compare the two based on the following paradigms:

1. Performance:

   The authors highlight the fact of a decentralized approach, keeping human-out-of-loop implementation where no user data is collected for social graphing using GAEN. Contrastingly, BlueTrace follows a centralized paradigm wherein the details of users are used for social graphing.

   In our project, we perform a decentralized approach with no collection of any PPI

2. Privacy

   The authors compare the approach of GAEN wherein privacy of infected users are strongly guaranteed with comparatively less privacy for infected users. On the other hand, BlueTrace's approach requires processing and matchmaking of contacts in a central server leading to lesser privacy overall.

3. Data access

   GAEN is explained on the basis of not having to access any data or identify any PPI. As IDs are derived from cryptographically secure random number generators, the GAEN is having an advantage over the BlueTrace

4. User Friction

   Some of the main aspects are the advantage of having no GPS information needed for GAEN and its background working indefinitely. Furthermore, there is no connection required for broadcasting packets and can happen without the internet.

What was the conclusion of the research?

The conclusion of the project is how GAEN resolves most of the shortcomings of other widely used protocols. However, wide-scale adoption of GAEN, in the long run, would either make or break the protocol.

How can you apply this knowledge to your own project?

Some of the previous weekly blogs focused on privacy and security related papers concerning GAEN. I believe i could leverage these weekly blogs during the privacy assessment of our app and while I write my research paper as well.

REFERENCES

1. Small, L., Harris, J., Hopkins, M. and de Lautour, N., 2020. Summary of Bluetooth Contact Tracing Options.