# Week 1 Blog

**Course:** COMP SCI 7092 - Mobile and Wireless Systems


| | |
|---|---|
| Sree Ram Boyapati | a1775690 |


## So what have you done this week?

As part of the suggestions, I have read the following papers -
1. Vetting Security and Privacy of Global COVID-19 Contact Tracing Applications
2. A Survey of COVID-19 Contact Tracing Apps
3. Zero Knowledge Proofs
4. Blue Trace Protocol

This allowed me to understand what kind of architecture and data needs to be supported. I framed the architecture of the systems we need to develop as part of our project and various considerations that we need to take.

The first paper helped me understand the functionality needed for the App to successfully address various functionality like taking permission to collect the data from infected users and concerns regarding false positive cases using signed chirps.

https://github.cs.adelaide.edu.au/2020-Mobile-and-Wireless-Systems/CovidGuard-F/wiki/Vetting-Security-and-Privacy-of-Global-COVID-19-Contact-Tracing-Applications---Paper-Review

From the second paper, Architecture of a decentralized system was much more detailed and many security attacks and privacy attacks were detailed. Battery Usage was noted as one of the major concerns. I have worked with the team to prepare for a meeting with the supervisor and other members who delved deeply into exposure notifications. I have provided a sketch on tools to use to gather results as required by the assessment rubric.

# What are your outcomes (what have you learnt? What have you implemented? what have you read?)

Decentralized solutions are highly private however, device security is a major issue. Given the fact that android is heavily fragmented and 90% of mobile devices use android. Security issues take over. Comparing chirps and doing a risk analysis on a completely decentralized system may be very consuming. I like the idea of generating seeds and temporary rotational IDs on the client side and storing the contact traces on the server side. Deanonymization strategies can be refined.

To authenticate the users, signed chirps can be used, however, we need to check if the signature can fit into the payload and further explore.

Handling denial of service attacks using rate-limiting (how many maximum people can be circle of 1.5 m) needs to be further explored. Traditional solutions like sqreen.io may not be useful as we are not storing IP addresses.

**Tools that can be used as  part of the project -**
1. Travis CI - https://travis-ci.org/ for continuously testing our android builds
2. For static analysis of the code  - https://deepsource.io/
3. For data flow analysis - Data Access Auditing
https://developer.android.com/preview/privacy/data-access-auditing#java
4. For Malware Analysis - https://github.com/MobSF/Mobile-Security-Framework-MobSF
5. Code obfuscators - DexGuard

**For addressing privacy concerns -**
1. Protecting identity of the user - Generate temporary tokens in periodic intervals in the mobile

Table 3 of the Survey of Covid-19 Tracing apps. provides a good overview on separation of concerns between each service can be useful.

**Things to be handled in the server side -**
1. Encrypted databases
2. TLS support
3. Privacy compliance support using helpshift - https://www.helpshift.com/
4. Rate Limiting with heuristics

**Few questions to take up in meeting with the supervisor -**

1. Hybrid and Bluetooth based systems? should we go ahead?
2. What is expected of the backend? Just notification of a positive case?
3. Can we send location (coarse location) of traces to increase efficiency ?? What will be the impact of privacy
4. Vetting privacy - false positives ? add cryptography? signed tokens? temporary signed tokens?
5. As part of vetting privacy and security - What do we want to present for week 3?
6. In Venue Trace, People who do not have the app can be notified and traced - Is that needed?
7. Can we make a demonstration through only android?
8. How can we integrate CI/CD with github enterprise, Did past teams try integrations?
9. Permission can be taken through OTP to publish traces from infected patients?

# Does your blog and activity briefly and clearly describe your outcomes?

In my blog, I feel I have addressed a lot of security concerns and most of the privacy concerns by selecting a hybrid approach. Detailed analysis of privacy concerns needs to be further taken up after discussion with my teammates. I was able to come up with actionable measures for addressing several aspects of security and privacy. In the next week, Efficiency of hybrid architecture needs to be measured and taken up. Venue Tracing required widespread adoption of Venue IDs so we are not sure if it is useful. Tagging places from trace data course locations may be better and notifying relevant people using RSSI.