CovidCard Pre-Trial Assessment

Defence Technology Agency

October 2020

1 Background

At request of Ministry of Health (MoH), the Defence Technology Agency (DTA) carried out a rapid assessment of the cards and software for the CovidCard Bluetooth contact tracing system, to ascertain whether the system was satisfactory for a short field trial involving several hundred participants.

The CovidCard system supplied to DTA for testing consisted of:

- Five Bluetooth Low Energy contact logging cards,
- A Windows 10 PC application for secure card data download,
- Access to a website providing an interface to uploaded card data.

Specific system requirements for the field trial are:

1. Encryption on the cards to protect the interaction logs in the event a card is lost,
2. A rotating random identifier, unique to each card, so that the cards cannot be tracked,
3. Firmware tested and guaranteed to be stable for the duration of the trial,
4. A means for secure over-the-air download and decryption of data from cards at the conclusion of the trial.

2 Assessment

2.1 Encryption on the cards to protect the interaction logs in the event a card is lost

CovidCards store records of interactions with other cards. The precise details of the metrics used and thresholds were not finalized in the CovidCard specifications released to DTA in the July CovidCard technology review. DTA made several recommendations following that review, including changes to the recording of RSSI data, contact duration and consequently the contact record format. We have not received any further communication from Virscient regarding any changes following the review, but it is possible that Virscient have made some changes relating to our suggestions. Virscient has not released any further update to the July specifications.

According to the July firmware specification, all data on the cards is stored in an encrypted format and is not decrypted until it is uploaded to the server. Also note that we have verified that the cards transmit 96-bit random identifiers.

We conclude that CovidCard satisfies requirement (1) for the trial.

2.2 A rotating random identifier, unique to each card, so that the cards cannot be tracked

We have observed that the Bluetooth Low Energy (BLE) transmissions from the cards ‘rotate’ (change) their random identifier and MAC address every 15 to 25 minutes. The random identifier is transmitted in the BLE packet payload and is a 96-bit random number, as in the specification.

As the MAC address and card identifier change simultaneously, tracking the card over long periods of time by associating users to identifiers becomes extremely difficult.

We conclude that requirement (2) is satisfied for the trial.

2.3 Firmware tested and guaranteed to be stable for the duration of the trial

We have operated all five cards supplied and tested the interaction with other cards and uploading of contact data to the server. This involved one scenario with two test subjects wearing the cards on lanyards, and a test in which two cards were suspended from hooks about 0.5 m apart from 6pm 14th October until about 12pm 16th October (about 40 hours of continuous operation).

In the latter test the two cards were kept awake continually by using a floor fan to induce movement (CovidCards have an accelerometer which is used to detect motion. The cards enter a sleep mode after a prolonged period of inactivity to reduce power consumption, hence the need to maintain movement for this test).

All cards remained responsive to button presses, and we were able to successfully upload data from all cards to the test server using the Windows application. No errors or unexpected states were encountered.

Based on this test we believe the card firmware is stable enough to proceed with a week-long trial. Hence, we conclude that requirement (3) is satisfied.

2.4 A means for secure over-the-air download and decryption of data from cards at the conclusion of the trial

The system is provided with a Windows PC based application that downloads card data using a Bluetooth connection, and uploads data to the server. Data is encrypted during over-the-air download and cannot be decrypted on the Windows application. Contact data is decrypted on the server, was resolved to the correct card number, and is accessible via a web interface with Username/Password access control.

For the purposes of the trial, we suggest that any personally identifiable information is not added to the server (there is a text box in the web interface into which notes can be added). All personally identifiable information should be held on a separate MoH controlled server with strictly limited access.

We conclude that requirement (4) is satisfied.

3 Conclusion

Based on the testing conducted, and additional technical specifications provided, the security, privacy and stability requirements of the CovidCard system for the field trial have been met.

Nathaniel de Lautour
Logan Small
Austin Chamberlain

16th October 2020