Weekly Blog 11

1. **Testing Procedure Scenario 1:**
    a. Seated scenario:
        i. 3 devices for 3 people
        ii. Test subjects 1 and 2 held their phones in hand
        iii. Test subject 3 had their phones in a pocket
        iv. Each run was for 5 minutes
        v. Test subjects did not change their positions
    b. The moving scene in a queue fashion:
        i. 3 devices for 3 people
        ii. Test subjects 1 and 2 held their phones in hand
        iii. Test subject 3 had their phones in a pocket
        iv. Test subjects moved forward to the checkout counter as it progressed
        v. The infected test subject is the last one in line, the third person.
    c. Testing at a distance of 1.5 metres or social distancing criteria
        i. 3 devices for 3 people
        ii. Test subjects 1 and 2 held their phones in hand
        iii. Test subject 3 had their phones in a pocket.
        iv. An infected person could be anyone amongst the three
        v. The app should not notify infected due to social distancing.
    d. Test for false positives:
        i. Infected and non-infected users are separated by a concrete wall.
        ii. Test subjects do not change their positions for 5 minutes.
        iii. Phones could either be on hand or in the pocket.
        iv. False-positive if the app detects infection even with the separation of a concrete wall.
2. **Testing procedure scenario 2:**
    a. Changing TxPower to HIGH, advertising mode to LOW_LATENCY similar to COVID Safe.
    b. Changing TxPower to ULTRA_LOW, advertising mode to LOW_POWER similar to Arogya Setu.
    c. Switching TxPower to MEDIUM, advertising mode to BALANCED similar to Etheraz.

Component-Based Comparison of Privacy-First Exposure Notification Protocols

The paper mainly performs a comparison of various components in different privacy first contact tracing protocols. I will be mainly focusing on the GAEN related parts which covers the attack mitigation and the privacy side of users.

What are the different types of attacks?

Linkability: In this type of attacks, the identifiers used for transmitting to other devices should no be linkable to the primary key used for deriving those IDs. In GAEN, the IDs are anonymised through cryptographic secure random algorithms. Furthermore, the IDs are constantly rotated which would make it difficult to link it back ot the primary key, which in our case is the Temporary Exposure Key.

Replay Attacks: Replay attacks are attacks where a user would observe and re-broadcast another user's identifier triggering an exposure notification. In GAEN, we have not incorporated a timestamp which would notify about the validity of a received identifier. Hypothetically, if there are three people A, B and C. Let B be the malicious user. B attempts to observe and re-broadcast an identifier of A to C. Now if A becomes COVID positive. C would get a false exposure notification even though A and C have never met. As such, our GAEN is vulnerable to replay attacks.

Broadcast IDs Anonymity: In our case, since cryptographic secure random functions are used for deriving the anonymised IDs, there is complete broadcast ID anonymity.

Re-identification: In this case, the ability to identify which user has been diagnosed as COVID positive is studied. In GAEN, these have been implemented to the possible extent where no privacy information is collected or transmitted. As such, it could be nearly impossible to identify the infected user.

Hypothetical scenario: In a case where a user A has only been in touch with another user B. Following which, if user A receives exposure notification, then user A would be able to recollect from memory whom he/she had been in contact with. However, these kinds of vulnerabilities are impossible to implement and hypothetically unrealistic to happen.

Privacy of Non-Infected Users: In GAEN, the data of non-infected users never leave the device. Unless and until a user is infected, should he/she voluntarily upload her keys for matchmaking and exposure notification.

Location Privacy: Our implementation does not collect any location data and completely relies on BLE for transmission, reception, matchmaking and exposure notification of IDs. However, owing to Android limitations, location permissions will need to be given.

REFERENCES

1. Daw, E., Coalition, T.C.N. and Vista, C., 2020. Component-Based Comparison of Privacy-First Exposure Notification Protocols. IACR Cryptol. ePrint Arch., 2020, p.586.