Cryptographically Secure Contact Tracing

James Petrie

March 2020

This document describes a cryptographically secure mechanism for performing cellphone-based contact tracing. By generating a new random number for each contact event the system is able to operate without storing or transmitting any personal information. This method is designed so that only the phones involved in a contact event are able to identify messages on a public database.

The method works as follows:

1. Every time two phones are close they randomly generate a contact event number and share it privately. This number is saved locally on both phones
2. If one of the phone owners is diagnosed positive they are given a permission number by health authorities
3. This person sends a packet to the public database with the permission number and their history of contact event numbers
4. If the permission number is valid, the contact event numbers are stored in the database and transmitted to all other phones
5. Each phone compares the publicly posted contact event numbers against their own history. If there are any matches this means they were close to an infected individual and are given instructions on what to do next

The only authentication required is the permission number provided by a public health authority. This permission number is used so that malicious actors cannot send false alarms. After authentication the permission number is deleted from server memory.

The contact event numbers are random and only known by the message recipient and the message sender so the database can be made public without risk of sensitive information being discovered.