Privacy Preserving Contact Tracing

Hack the Crisis [NL]

4 april 2020

Contents

1 Summary

This document is a report written during the **Hack the Crisis NL** online hacakthon[1]. We propose a system for secure and privacy-preserving contact tracing. Providing a technological foundation to help slow the spread of the SARS-CoV-2 virus.

Goals:

- Take advantage of existing implemented solutions to brake transmission chains and control the spread of the disease,
- Avoid Identity Driven solutions. We don't ask citizens to provide their identity,
- Inform the user if there is an infection in their contact chain,
- Automate the process of inferring the list of possible users that might have been exposed to an infected person in the 14 days preceding the test

The system aims to minimise single point of failure, privacy and security risks for citizens and communities and to guarantee data protection.

To achieve this goal, we use mobile applications to continuously track anonymous users (we do not ask them to provide email,name, surname or ID numbers) and ask them to report symptoms, if they are using Individual Protection Devices or Protective Clothing when they go out. The information is encrypted and stored in an ummutable decentralized digital ledger called Tangle. If a citizen is tested positive, verified Health Departments send his universal unique identifier (uuid) of the the application to the Tangle and flags it as an infected uuid.

As soon as a new infected uuid is published on the ledger a computer (no server is required, works with a personal computer as well) performs the contact tracing

task and uuids at risk are broadcasted.

If the application sees its uuid on the Tangle, the user is notified.

We use mobile applications to track the anonymous user and report his symptoms

2) Information is encrypted and stored in an immutable decentralized digital ledger called Tangle

3) If a citizen is tested positive, verified health departments broadcast the id on the ledger

4) As soon as a new infected id is available, the contact tracing is performed. Resulting ids and associated risk are broadcast

5) If the App sees its id then the user is notified

Additionally, the system enables users to voluntarily provide information to epidemiologists to enable studies of the evolution of disease in the region of interest and to assist in finding better policies to prevent further infections.

We provide a description about security aspects, privacy properties, architecture and the provided features.

The code is available on Github and released under the GNU GPL v3 license so that further protection mechanisms can be added if weaknesses are identified and additional features can be added by the community.

2 Contact Tracing

Contact tracing is a strategy for breaking transmission chains and controlling the spread of the disease. Contact tracing is most effective as a means of containing flareups. Applying this strategy can prevent exponential growth in new cases, protect health-care systems and potentially save lives.

2.1 Description

It involves identifying infected persons, finding those with whom the infected person may have been in close contact while infectious, locating and testing these close contacts. If a close contact is found to be infected, the disease-investigation process starts again.

It is extremely important to identify asymptomatic or paucisymptomatic because these cases can transmit the virus. This investigation helps public-health departments to draw lines of transmission accurately. Contact tracing could help find those people and ask them to self-isolate.

2.2 Current base approaches

The algorithm for the management of contacts of probable or confirmed COVID-19 cases issued by the European Center for Disease prevention and control is described below:

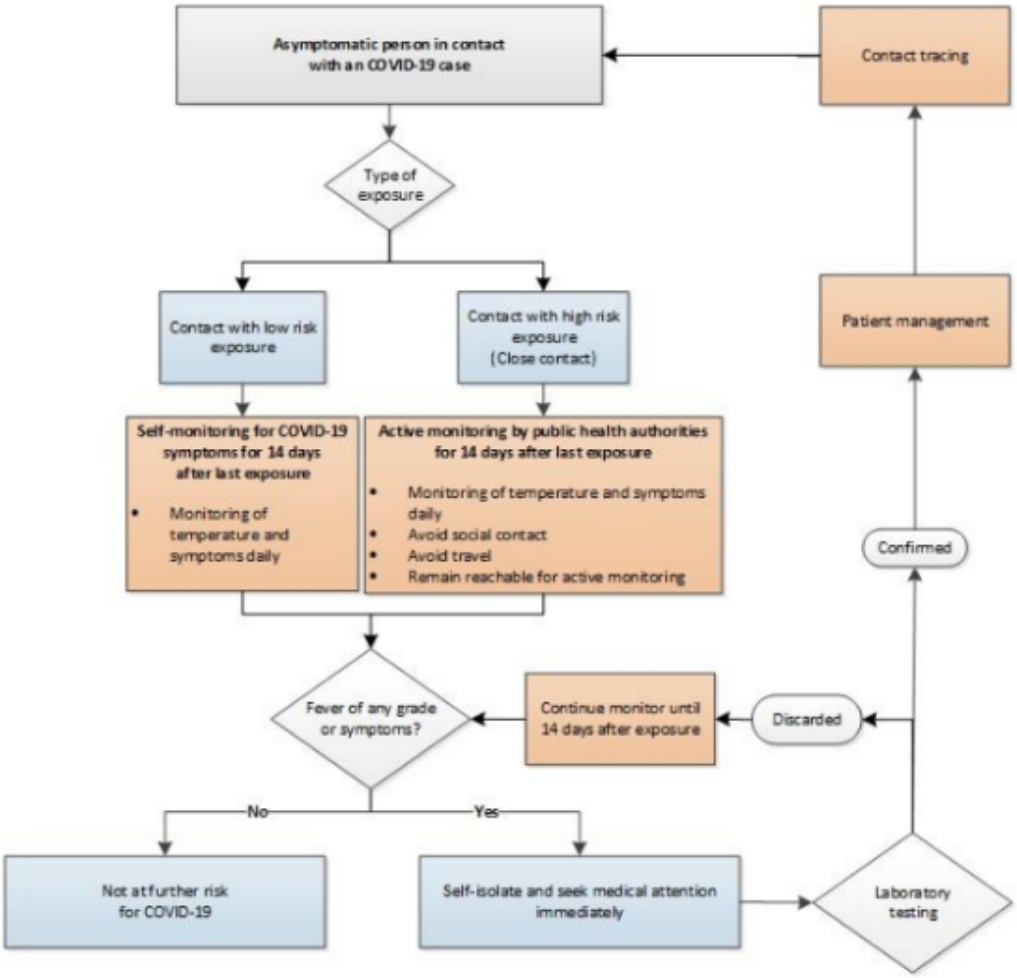

Figure 1: Algorithm for the management of contacts of probable or confirmed COVID-19

During the contact investigation, the IDD makes a distinction between high-risk and low-risk contacts.

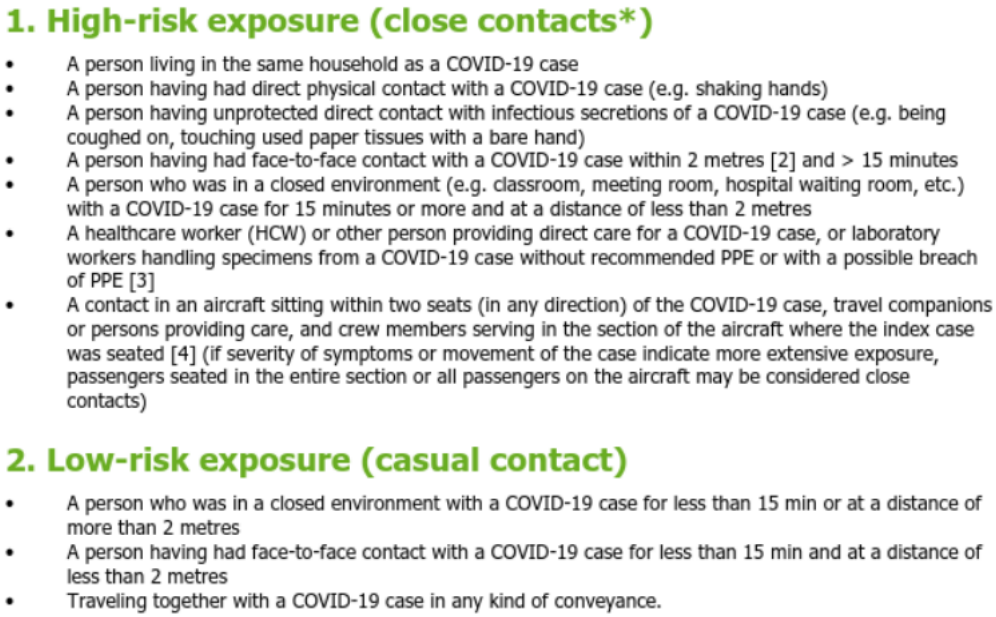

Figure 2: Distinction between high and low-risk contacts

Current modes of operation in the Netherlands[3] and in Italy are described in the following sub sections.

2.2.1 The Netherlands

If a person tests positive for the coronavirus, the Infectious Disease department (IDD) of the municipal or regional Health Service will be notified. The IDD contacts the patient or another designated contact person and maps out who the patient has been in contact with during the contagious period. From the first day of illness of the patient - the day someone starts to cough or develop symtoms - until the last moment of contact that the patient has had with someone.

2.2.2 Italy

In Italy, we rely on covid patients' past memories. They ask if they remember who they have been in contact with. If they miss someone, the forgotten citizen will be potentially the next patient 0 and the deadly will loop strike back.

3 The race to new methods

In this section we quickly discuss the methods used by other countries to improve contact tracing.

3.1 Main idea

Researchers and technologists all around the world are developing several mobile based solutions that alert users when they have come into contact with someone with coronavirus. Proximity or location data are used to notify someone who has recently been near to an infected individual, so that they can then take preventive action such as self-isolating.

These solutions could safely help transition out of national lockdowns and relax social distancing rules while defending against a second wave of infections. Medical researchers and bioethicists at the University of Oxford found that digital contact tracing had the potential to achieve epidemic control if used by enough people.

3.2 Bluetooth based methods

One of the most popular formats to emerge have been bluetooth based apps. By taking advantage of th low energy protocol, bluetooth identifiers and signal strength from other nearby phones they keep a record of them for a set period of time. This approach allows both outdoor and indoor tracking and is considered by privacy advocates as the least intrusive form of mobile tracking. Several solutions have been released under free software or less restrictive open source licences. Other proprietary solutions are spreading as well.

3.3 Gps Alternatives

An alternative solution could be GPS location tracking technology. Teams at MIT are exploring this solution (Safe Paths) on top of their bluetooth offering. There is emerging evidence that coronavirus can be transferred via surfaces even after a period of time suggesting it may be better to monitor where someone went rather than with whom they crossed paths.

But GPS location data is harder to anonymise and researchers are still looking for ways to better encrypt data.

3.4 Related problems

The main concerns are related to privacy and the possibility of data leakage by the involved actors in the logic.

Related information:

- Beijing appeared to share citizen's data with the police.
- South Korea has broadcast the personal information of infected people when alerting others who may have been exposed to them.
- In Israel, security services are controversially tapping data collected by the country's mobile phone operators.

3.5 Indentified proprietary solutions

- *Pan-European Privacy-Preserving Proximity Tracing*[4] claims to interrupt new chains of SARS-CoV-2 transmission rapidly and effectively by informing potentially exposed people. They enable tracing of infection chains across national borders.

- *Covid19 Contact Alert* Combining NFC and Blockchain technology to monitor contact moments and alert people. German technology company MYNXG[5] introduces a blockchain technology to enable privacy compliant pandemic tracking on regular smartphones. People can download a special app on their smartphone and use any existing NFC to connect their smartphone to the MYNXG blockchain. This technology provides privacy when monitoring individual movements or alerting people if there is an infection in their contact chain.

4 Our approach

4.1 Time contrained decisions

4.2 Possibility to include bluetooth

4.3 Solved problems

4.4 Related problems

5 Architecture

5.0.1 Mobile applications

5.0.2 RiskAssesor

5.0.3 Distributed Digital Ledger

6 The race to new methods

7 Data protection

8 Scalability

9 Epidemiological Research

References

[1] Hack the Crisis NL online Hackathon, *"https://www.hackthecrisis.nl/en"*.

[2] European Centre for Disease Prevention and Control , *"https://www.ecdc.europa.eu/en/publications-data/public-health-management-persons-including-health-care-workers-having-had-contact"*.

[3] Zo werkt contactonderzoek bij het coronavirus, *"https://www.nu.nl/coronavirus/6035667/zo-werkt-contactonderzoek-bij-het-coronavirus.html"*.

[4] Pan-European Privacy-Preserving Proximity Tracing, *"https://www.pepp-pt.org/"*.

[5] Covid19 Contact Alert service, *"https://www.mynxg.com/"*.