IDEA anti COVID-19 # 14

Using Bluetooth technology for COVID-19 contact tracing[1]

APRIL 2020

Ole Jann, Pavel Kocourek and Jakub Steiner[2]

Summary

- The coronavirus is transmitted indiscriminately through proximity, which makes tracing infections difficult.
- Bluetooth tracing apps can reliably record transmission possibilities even when the participants do not know each other and do not remember the interaction.
- This can be done with a high degree of privacy. A well-designed app provides a similar level of privacy to not using an app at all.
- Decentralized data storage means that the privacy and security of the system is highly resilient against exploitation by any powerful actor (such as a government).
- A disadvantage of protecting privacy through decentralization is that tracing apps need to be taken up by the population one person at a time. Their use cannot be checked remotely and hence cannot be effectively mandated by governments or health authorities. A very high degree of take-up is necessary to make them an effective weapon against the virus.
- The eRouška app by COVID19cz follows these principles and offers a very high degree of privacy protection. Specifically, it does not collect any data except the phone

[1] This study represents the views of the authors, and not the official position of the Economics Institute of the Czech Academy of Sciences as well as the Charles University, Center for Economic Research and Graduate Education. The authors wish to thank Daniel Munich for useful comments and suggestions on the draft text. Any possible inaccuracies and errors are the responsibility of the authors. The study was also published thanks to the support of the Czech Academy of Sciences within the framework of the AV21 Strategy program and a donation from the Experientia Foundation.

[2] Contact: ole.jann@cerge-ei.cz

numbers of non-infected users, and only collects anonymized meeting data (and no location or other metadata) of infected users – this data is only available to a hygienist after voluntary data transmission by the user.

- No data is transmitted to the server without explicit user agreement.

IDEA anti COVID-19 # 14

Využití technologie Bluetooth pro trasování šíření covid-19[3]

DUBEN 2020

Ole Jann, Pavel Kocourek, Jakub Steiner[4]

Shrnutí

- Koronavirus se přenáší i bezkontaktně vzduchem. Proto k nakažení stačí i pohyb v blízkosti nakaženého. Navíc člověk nákazu přenáší již ve stádiu, kdy sám ještě její příznaky nepociťuje. To komplikuje sledování šíření nákazy – trasování.
- Technologie *Bluetooth* je široce rozšířený standard bezdrátové komunikace umožňující propojení dvou a více elektronických zařízení v blízkém okolí, jako jsou například mobilní telefony či přenosné počítače. Aplikace (program) v takovém zařízení potom díky tomu mohou zaznamenávat fyzicky blízké kontakty osob, při kterých mohlo dojít k přenosu nákazy. K přenosu totiž může docházet i v případech, kdy se lidé navzájem neznají a nevybavují si, že se někdy setkali.
- Potenciálně nakažlivé kontakty lze pomocí trasovací aplikace zaznamenávat s minimálním narušením soukromí uživatelů. Dobře nastavená aplikace poskytuje jejím uživatelům srovnatelnou míru soukromí, jako kdyby ji nepoužívali.
- Data o kontaktech nejsou ukládána centralizovaně, ale pouze na telefonu uživatelů a s jejich souhlasem. I proto je systém z hlediska ochrany soukromí a bezpečnosti odolný vůči případnému zneužití z pozice síly, jako například vládou nebo hackery.
- Negativním důsledkem této snahy o ochranu soukromí je, že aplikace musí být mnoha jednotlivci přijata dobrovolně. Nelze na dálku kontrolovat, zda lidé aplikaci

[3] Tato studie reprezentuje pouze názory autorů a nikoli oficiální stanovisko Národohospodářského ústavu AV ČR, v. v. i. či Centra pro ekonomický výzkum a doktorské studium UK v Praze (CERGE). Poděkování za užitečné připomínky a podněty k pracovní verzi patří Danielu Munichovi. Veškeré případné nepřesnosti a chyby jdou na vrub autorů. Studie byla vydána i díky podpoře AV ČR v rámci programu Strategie AV21 a daru Nadace Experientia.

[4]Autoři působí na CERGE-EI, společném akademickém pracovišti Univerzity Karlovy a Národohospodářského ústavu AV ČR, v. v. i., Jakub Steiner navíc působí i na Curyšské univerzitě. Korespondenční kontakt: ole.jann@cerge-ei.cz

používají, a její používání nelze vymáhat vládou či orgány veřejného zdraví. Aby trasovací aplikace skutečně pomáhala zastavit šíření infekce, musí ji dobrovolně používat velká část populace.

- Aplikace eRouška, kterou vyvinula skupina Covid19CZ, uvedené principy splňuje a zajišťuje vysokou míru ochrany soukromí uživatelů. Shromažďuje pouze anonymizovaná data o setkáních infikovaných uživatelů a telefonní čísla uživatelů. Ta navíc dokáže s anonymními daty spojit až hygienik, a to až po dobrovolném poskytnutí dat uživatelem.
- Aplikace neshromažďuje informace o místech, kde se uživatelé potkali, ani jiná metadata. Žádná data neodesílá na server bez vědomého souhlasu uživatele.

The role of distance in contact tracing

The current shutdowns in the Czech Republic and worldwide will not make the novel coronavirus disappear, but will only reduce the number of infected persons to a level at which the virus can hopefully be kept under control. Maintaining control will require sophisticated, targeted measures when public life gradually normalizes. In addition to the ability to test widely and to test anyone with symptoms, tracing the contacts of those found to be infected will play a central role. Contact tracing can only be effective if it is done very reliably and quickly [1]. Similar tracing has been carried out for different types of infectious diseases all over the world for a long time, but the coronavirus poses several particular challenges:

- It can be transmitted through proximity of up to a distance of several meters. That means it can be transmitted through intensive personal contact as well as through fleeting contact, and even among people who have no personal contact at all and do not know each other -- such as people who ride public transport together or sit close to each other in restaurants or waiting rooms.
- It can be transmitted at a stage where the carrier is not (yet) symptomatic, meaning that neither person is alert to the fact that a transmission could be taking place.

How phone sensors allow for contact tracing

Effective tracing can thus be hindered by the fact that carriers and receivers do not know each other and/or have no recollection of being in each other's proximity. These problems can be overcome with the help of the bluetooth technology that is ubiquitous in modern smartphones. Phones can be programmed so that if two phones come close to each other with their bluetooth sensors switched on, both make a note of this contact, how close they came and for how long. [5]

[5] Different phones will give different signal readings for the same distance, so such measurements need to be calibrated for each phone type and for different ways people might carry their phone, but experts consider these technical issues surmountable.

Smartphones can thus build a complete record of everyone a person has been close enough to infect in a time period. If a person then tests positive for the virus, this record can be used to contact these people (either through the app or via a phone call, if their contact details are known), to tell them to self-isolate to protect others and to get tested as soon as possible. (Or, depending on the technical setup, the record can be revealed to a hygienist who directly enacts the chain of isolation and testing.)

Decentralization as advantage and disadvantage

Bluetooth contact tracing can in principle be carried out with an extremely high degree of privacy and voluntariness. Every citizen can decide for themselves whether they want to install the app on their phone (if they have one), and they can decide from moment to moment whether to switch bluetooth (and hence the app functionality) on or off. Whether any citizen uses the app is virtually impossible to check unless the observer is in close physical proximity to them. All information about contacts can be saved on the individual phones; no central records of encounters need to be kept and, especially, there is no need to collect location data or other metadata. If a person never tests positive, no data need ever be revealed to anyone. An uninfected person using a well-designed app thus reveals no more information about herself than anyone who goes about their daily life with bluetooth or WiFi activated on their smartphone.

This decentralization of data storage minimizes the privacy risk for any individual person, but it also limits the risk of a central and powerful actor (such as a government or capable cybercriminals) using bluetooth tracing apps to collect any information about citizens. If there is no central record, it cannot be broken into or brought under the control of the government. While it is hard to imagine a scenario in which a government could use the fact that people use a bluetooth tracing app to collect data about them (such as by stationing bluetooth sensors in public places), the citizenry could in that case simply decide to uninstall the app on their phones to thwart such attempts.

This decentralized functioning, however, could also limit the effectiveness of any bluetooth tracing solution. To register any contact between two people, *both* need to have the same tracing app (or at least mutually compatible apps) installed on their phones, need to have their phones charged and on their person, and need to have bluetooth activated.

This means that the number of potential contacts that the app can pick up on average depends on the square of the fraction of the local population who uses the app correctly. If 10% do so, then 10% of the infected will have it, and it will pick up 10% of their contacts, so that overall it will pick up only 1% of contacts between carriers and receivers. In Singapore, which has developed and rolled out an app for bluetooth contact tracing and where the population usually closely follows government recommendations, about 15% of the population is estimated to have installed the app. However, it is to be expected that app usage would be distributed very unevenly, and be more common in densely populated areas and among the younger population, which are more likely to be areas and groups subject to faster spread of the virus. An app's usefulness can hence be much higher than this simple calculation suggests. The percentage of smartphone users among the Czech population is estimated to be around 70%; uptake of a tracing app by a sizable portion of that group could make a substantial contribution to limiting the spread of the disease.

Of course, any traced contact helps, but studies suggest that to limit exponential spread of the disease, the number of infections per carrier needs to be reduced by at least 50%, possibly more [1]. Widespread adaption of bluetooth tracing apps would thus be indispensable. Since adoption of the app will be up to every single citizen, it would probably need to be encouraged by governments as well as by influential members of civil society, celebrities and others in advertising and social media campaigns. People who have installed the app could be (subtly) motivated to advertise to friends and family members that they are doing their part to protect the population, and thereby encourage them to do the same.

Using a bluetooth tracing app imposes a small (or no) cost on the user and protects not only the user herself, but also other members of society. It could therefore be argued that since this makes the app similar to driving lessons, accident insurance or, indeed, face masks, their use should be mandated. Once daily life gradually resumes, shops or cafes might require that customers use such an app, or governments may consider requiring app use in certain groups or in certain areas. This would be unwise. Unlike the wearing of face masks, it is not practically feasible to comprehensively check whether the app is in fact active and correctly configured. Making app usage mandatory would hence likely not increase its actual usage (because those who don't want to use it will easily sabotage it), and would probably cause a popular backlash which would in fact decrease usage.

It therefore appears imperative that app use is encouraged and advertised, but remains completely voluntary.

Information collected by smartphone apps can be a privacy concern even if in principle it is only available to the user herself: The user could be forced to give others access to this data, or it might be stolen. A similar worry might apply to bluetooth tracking apps that allows users to see their own contact history, since this data could reveal at which time the user was near (or not near) other people (and how many of them). But it would not reveal any information about other people (since contacts are saved under unidentifiable pseudonyms) or any identity or location data, and so would be far less problematic than most other user data that is stored on smartphones such as location history, banking data, messages and other personal information.

The eRouška app developed by COVID19cz[6]

A Czech solution for bluetooth contact tracing has been developed by the group COVID19cz under the name eRouška and will soon be available for Android and iPhone. It is integrated into the “chytrá karanténa"(Smart Quarantine) structure and will function according to the principles described above.

Users who install the app will register using their phone number, which a hygienist can later use to get in touch should a contact test positive. The app will then run in the background, detecting other nearby phones using the same app, and creating a record of such encounters. The phone will only broadcast a randomly chosen and uninformative pseudonym to nearby phones, which does not give any information about *who* was nearby, but which would later allow the system to track down contacts. (In fact, the broadcast pseudonym changes periodically, thus making it hard to recognize, let alone identify, a phone by its broadcast signal.) If a user tests positive, they will be asked by a hygienist whether they agree that their data can be used for tracing purposes. If they agree and upload the phone's records, the data can then be used to locate the contacts from the past

[6] The authors were able to view internal technical documentation of the eRouška project and speak to developers in the process of conducting this study. The eRouška project was able to review the study before publication to comment on the correctness of technical points, but there were no restrictions imposed on the content or conclusions of the study The authors have no interests, material or otherwise, in the eRouška project or related projects.

few days, who can be identified by their phone numbers (which are the only piece of information known about them in the system). The hygienist can thus not perfectly identify the contacts of infected citizens or impose quarantines on them, but can make recommendations and work with them to protect others.

The only data that will be collected are contacts in pseudonymized form, and old contacts are automatically deleted once they are no longer medically relevant. While we are not in a position to examine the exact functioning of eRouška, the apps for Android and iPhone are open source and can be audited by anyone interested. During its lifetime and if used correctly, the app communicates with the central server at most twice: Upon installation/setup, and if the user tests positive and agrees to make their data available for contact tracing. eRouška is hence an informationally parsimonious, privacy-protecting solution for contact tracing.

Projects in other countries

A bluetooth tracing app called "TraceTogether" has been developed and deployed in Singapore, where it is part of the country's relatively successful effort to control the spread of the disease. Other European countries are developing a common standard for bluetooth proximity tracing under the name PEPP-PT ("Pan-European Privacy-Preserving Proximity Tracing"). Apps based on this standard may be available from mid-April in Germany, Switzerland and other countries. PEPP-PT allows for a privacy standard that is similar to eRouška -- albeit slightly higher in some ways, since accounts are not connected to a phone number and thus not identifiable by anyone. The standard will supposedly allow contact tracing across countries, such as when a citizen of one country enters another member country. At this moment, eRouška is not compatible with PEPP-PT, but given the similar functionality it could be possible to make them compatible with each other when both systems are up and running. A tracing protocol similar to eRouška was also announced by Google and Apple just before this study was completed.

References:

[1] Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D., and Fraser, C. (2020). "Quantifying SARS-CoV-2 transmission suggests epidemic controlwith digital contact tracing." Science.