The stony road to privacy-preserving and secure contact tracing schemes: Summary of a comparative analysis

Prof. Dr.-Ing. Ahmad-Reza Sadeghi, ahmad.sadeghi@trust.tu-darmstadt.de

Dr.-Ing. Markus Miettinen, markus.miettinen@trust.tu-darmstadt.de

M.Sc. Thien Duc Nguyen, ducthien.nguyen@trust.tu-darmstadt.de

Cybersecurity Research Centre CYSEC, TU Darmstadt

April 24th, 2020, v. 1.1

Executive Summary

Huge efforts are being invested in enabling effective contact tracing of infected persons in order to encounter the COVID-19 pandemic. Many contact tracing apps have been proposed and deployed in the last months in China, South Korea, Singapore, Taiwan and several active development efforts are underway in Europe and in the US. While the privacy aspects in some countries were not of high priority, there has been a lively debate around privacy compliance in EU and US.

Some approaches like the one proposed by the MIT are based on tracking the GPS location of participating users. However, use of GPS for this purpose faces challenges, as it relatively inaccurate especially in indoor areas that are particularly important to capture accurately due to the higher contagion risk in enclosed spaces. Privacy of users is addressed in these approaches by allowing users to redact locations that they deem sensitive. However, this approach has its problems. For one, a lot of potential contacts are lost when places like homes and workplaces are redacted from released location traces, thus diminishing the utility of the system. On the other hand, even aggressive redaction of specific locations may not be sufficient for ensuring user privacy, as users may still be identifiable given additional information that, e.g., big social media companies or players like Google have on their users.

Therefore, we focus in this analysis on approaches utilising Bluetooth for sensing proximity between users. A number of proposals using this technology have been made each of them providing different levels of security and privacy to its users.

We present a summary of our detailed analysis of 4 currently debated contract tracing schemes relying on Bluetooth tracking, and compare them according to various criteria. These include PEPP-PT , DP-3T and TraceCORONA as well as a scheme recently proposed by Google and Apple.

Our analysis shows that, as also pointed out by a joint statement of numerous security researchers recently, that the approach proposed by the initiative PEPP-PT has serious problems with regard to the level of privacy it provides to the users of the system, especially with regard to potential misuse by the organisation responsible of operating the system.

The approaches DP-3T and TraceCORONA provide much stronger privacy guarantees by decentralising the contact tracing to individual users of the system and thereby limiting the ability of a misbehaving central authority to inappropriately track the participating users.

In particular, TraceCORONA provides additional advantages with regard to the verifiability of epidemiological data that users may voluntarily share with health care research institutions, making these more resilient to malicious users seeking to negatively impact the accuracy and correctness of the epidemiological models used as basis for political decision making in the crisis situation.

Finally, we also emphasize that a contact tracing app is only a small piece of the solution to the pandemic puzzle we are currently facing. We believe that in a democratic society we need a secure and privacy-preserving ecosystem to which tracing apps can dock and allow users to use services like secure messaging, secure document exchange to communicate securely with relevant stakeholders such as physicians, hospitals and other health organizations. The goal of TraceCORONA is to provide such a platform to which several stakeholders can connect to by providing their dedicated apps that can coexist on the platform. A central feature of the platform is also that users themselves can freely decide, if and which apps they want to use.

Table 1: Comparison of PEPP-PT, DP-3T (design 2) and TraceCORONA

	PEPP-PT	**DP-3T (design 2)**	**TraceCORONA**
App registration	No registration by user	No registration necessary by user	No registration necessary by user
App identifier	Persistent Unique Identifier (PUID) assigned by server to each App	None	None
App user identity	PUID as persistent pseudonym of user	Random and temporary seed, generated by the device, used to generate ephemeral ID (very short lived pseudonym)	No pseudonym at all
Contact tracing identifier (a string that allows the app to identify a contact)	Ephemeral ID (EBID) generated by server from PUID, broadcast over Bluetooth (BT)	Ephemeral ID generated by device (pseudorandom)	Encounter Token: a session key established by pair of devices (random string)
Infected person identity	Pseudonym of users (PUIDs) and EBIDs known to server (can be linked)	Ephemeral IDs of persons	Hashes of Encounter Tokens
Server			

Social contacts of infected person (can server tell which persons had contact to an infected person)	PUIDs of all contact persons known to server	None	None
Linkability of persons who had contact with infected persons (can server tell that that contact tracing identifiers come from the same person)	Full linkability by server	Yes (transmits all ephemeral IDs of infected person during one transaction)	Yes† (transmits all encouter tokens of the infected person during one transaction). However, one can obfuscate this using TOR.
Social graph information (which persons have been co-located at a given time)	Server can derive information about the fact that uninfected persons where at the same place	No	No
User de-anonymisation (Is it possible for the server to recover the real identity of the user)	Server can de-anonymise users through social graph information	No	No
Server colluding with Health Authorities			
Identifying infected users	Yes	Yes	Yes†
External attacker colluding with server			

(an attacker observing users at arbitrary places colludes with the server)			
Identification of specific users	Possible	No	No
Identification of groups of users	Possible	No	No
Powerful Attacker*			
Movement tracking of uninfected users	No	No	No
Movement tracking of infected users	No	No	No
User de-anonymisation	No	No	No
Passive Powerful Attacker colluding with server			
Movement tracking of uninfected users	Yes	No	No
Movement tracking of infected users	Yes	Yes	No
Infected user de-anonymisation	Possible via movement traces	Possible via movement traces	No
Active Powerful Attacker colluding with server			

Movement tracking of uninfected users	Yes	No	No
Movement tracking of infected users	Yes	Yes	Yes†
Infected user de-anonymisation	Possible via movement traces	Possible via movement traces	Possible via movement traces†
Epidemiological data			
Sharing of contacts with infected persons	Always known to server without user consent	Upon user consent	Upon user consent
Sabotage of epidemiological data	No	Malicious users can fabricate information about contacts	Contacts with infected persons can be anonymously verified
Manipulation attacks			
Injection of fake encounters into the system	Yes, via relaying/duplication of EBIDs	Yes, via relaying/duplication of EphIDs	Possible only via two-way-relaying
Protections against manipulation of encounter information into the app	Collected information encrypted locally	Ephemeral IDs not accessible through AppUI	Encounter Tokens not accessible through App UI
Removing encounter information in the app	Not possible (encrypted), only all-or-nothing delete	Users are by design entitled to redact encounter information for protecting privacy	Users are by design entitled to redact encounter information for protecting privacy

* A Powerful Attacker is an entity having multiple Bluetooth sensing nodes in an area where users move. Using information sensed by these nodes it tries to track movements of users between the locations of the sensing nodes. The Powerful Attacker can be either passive or active: passive Attacker only senses Bluetooth information in its vicinity. An active Attacker also emits information into its proximity via Bluetooth.

†Concept for stopping tracking/linkability exists but needs to be verified.

Table 2: Analysed properties for the Apple/Google approach

	Apple/Google
App registration	Random tracing key generated by device
App identifier	Daily tracing key derived from tracing key, Pseudorandom Ephemeral IDs derived from daily tracing key all generated locally by device
App user identity	Ephemeral IDs
Contact tracing identifier (a string that allows the app to identify a contact)	No
Infected person identity	Full linkability by server
Server	
Social contacts of infected person (can server tell which persons had contact to an infected persons)	None

Linkability of persons who had contact with infected persons (can server tell that that contact tracing identifiers comes from the same person)	Yes (transmits all daily tracing keys of infected person during one transaction)
Social graph information (which persons have been co-located at a give time)	No
User de-anonymisation (Is it possible for the server to recover the real identity of the user)	No
Server colluding with Health Authorities	
Identifying infected users	Yes
External attacker colluding with server (an attacker observing users at arbitrary places colludes with the server)	
Identification of specific users	No
Identification of groups of users	No
Powerful Attacker*	
Movement tracking of uninfected users	No

Movement tracking of infected users	Yes
User de-anonymisation	No
Passive Powerful Attacker colluding with server	
Movement tracking of uninfected users	No
Movement tracking of infected users	Yes
Infected user de-anonymisation	Possible via movement traces
Active Powerful Attacker colluding with server	
Movement tracking of uninfected users	No
Movement tracking of infected users	Yes
Infected user de-anonymisation	Possible via movement traces
Epidemiological data	
Sharing of contacts with infected persons	No
Sabotage of epidemiological data	Malicious users can fabricate information about contacts
Manipulation attacks	
Injection of fake encounters into the system	Yes, via relaying/duplication of EphIDs

Protections against manipulation of encounter information into the app	Ephemeral IDs not accessible through AppUI
Removing encounter information in the app	Users need to share daily tracing keys revealing all encounter information for shared days in an all-or-nothing fashion

Acknowledgement: We are grateful for the in-depth discussions with following colleagues:

Dr. Jean-Paul Degabriele, TU Darmstadt

Prof. Dr. Farinaz Koushanfar, UC San Diego

Prof. Dr.-Ing. Mira Mezini, TU Darmstadt

Anand Rajan, Intel Labs

Prof. Dr.-Ing. Thomas Schneider, TU Darmstadt

Dr. Matthias Schunter, Intel Labs

Jan Wunderlich, Kobil Systems GmbH