Own Analysis of SwissCovid

The National Cyber Security Center (NCSC) organized a public security test of the SwissCovid app. The test "aims to provide full transparency".

In response to the public test, we provided a report on June 5 which was subject to Responsible Disclosure with no duration limit. A summary of our conclusions were quickly published by NCSC without our report. However, our report were commented and even criticized in the press on June 10 by SwissCovid representatives (while we were still forbidden to publish the report itself).

On June 16, we received an authorization to publish by ourselves. The NCSC site lists many security evaluation reports which are quite positive about SwissCovid. It does not list ours. Instead, it contains a "detailed analysis" by NCSC about out report. We are in a disagreement with this analysis.

As it appears to be quite clear that communication is not transparent, we put here our observations for the public.

Our Report

The June 5 report was augmented with an addendum. In summary, our observations are as follows.

- Although the source code of the app is available, we cannot compile it, run it, and make it work without signing an agreement with Apple or Google. We do not find it compatible with the notion of *open source*.
- A big part of the contact tracing protocol (which was originally the DP3T protocol) is implemented by Apple-Google in a part of the system called GAEN. This part has no available source code although the law requires disclosure of the source code of all components of the system.
- Some servers are hosted by Amazon, as part of a CDN service.
- The available information to potential users is unclear, incomplete, or incorrect.
- Users may be traced or identified by surveillance systems of third parties while using SwissCovid.
- Diagnosed users who report have a risk to be identified by a third party.
- Third parties could inject false possible contamination alerts on a target phone or on a large group of target phones. This would result in making people go to quarantine without being considered at risk.

To resolve GAEN having no available source code although the law mandates all components to have an available source code, the Federal Council issued an ordinance making an exhaustive list of components which does not include GAEN. To justify such exclusion, SwissCovid promoters argue that GAEN is part of the operating system of the phone, or sometimes part of the Bluetooth communication interface of the phone, and that it is not common to require to disclose the source code of such parts. We deny that GAEN is any such part of the phone, at least on Android phones. GAEN is part of the Google Play Services which are independent of the operating system and of the communication interfaces. We could actually run a pre-standard version of SwissCovid on an Android phone which had no Google Play Services. However, this phone had the Android operating system and could use Bluetooth. Furthermore, most of the former DP3T protocol which was implemented in this pre-standard version disappeared in the current version of the app since an equivalent protocol is now in GAEN. We conclude that **there is no founded technical justification for excluding GAEN from the components of the system**. We strongly believe that the ordinance is a legal trick to bypass the law which is the consequence of a disagreement between SwissCovid and Apple-Google. We urge constitutional experts to make an assessment on the validity of the ordinance.

- Analysis of SwissCovid

The NCSC Analysis

We put here the NCSC analysis on our report together with our own notes. The summary of our remarks are as follows.

- NCSC says that the results of the public test are available on the NCSC web site. However, our report is not there and we wonder if other reports are missing. We think that the public test is not as transparent as it aimed.
- NCSC still insinuates that GAEN is part of the operating system, which is not the case.
- NCSC claims that using GAEN increased the privacy of the users. We strongly disagree with this statement. Outsourcing a big part of contact tracing to an opaque implementation, which is made available by a third party, which was installed on up-to-date phones without the consent of the users, and which was not subject to an independent audit cannot improve the privacy of anyone.
- NCSC claims that GAEN is an interface and not a protocol. We disagree with this statement. GAEN implements a big part of the contact tracing protocol, what used to be the DP3T protocol. We rather take the app as being an interface between GAEN, the servers, and the user.

- NCSC argues that Amazon hosting some servers is harmless because the service is only about distributing non-sensitive data. In other context, such claim has been proven to be wrong. However, we have insufficient information to assess on the security impact of this service.
- NCSC mentioned several possible attacks being known and documented without providing any reference. We are aware those attacks are not new and we cannot imagine NCSC is unaware of those attacks. Our main point is that users should be aware of those attacks and information is not easily available at this time.
- NCSC states that "Users can always turn off tracing if they are in what they consider to be a sensitive environment". We strongly agree with it but we believe that users need to know about possible attacks and to be reminded that they can turn off SwissCovid if they are concerned.
- NCSC argues that having apps scanning Bluetooth although the user turned off Bluetooth is not a risk for the user. This is incorrect. Some apps (or even GAEN) may continue scanning (against the user's consent). They could determine the risk of infection of the user with thresholds different than the ones from FOPH and also identify the contacts of the user. At the moment, turning off Bluetooth scanning is difficult on phones and this is known as a privacy risk.
- NCSC claims that malicious apps are not a problem specific to SwissCovid. Our point is that SwissCovid adds a threat that malicious apps can exploit.

- (Annotated) Security Issue Submission [INR-4434]. Detailed analysis.

Compliance

[Note: this section was written before June 24. Please read Episode II for evolution.]
The Law on Epidemics (LEp) was extended with Art.60a on June 20, 2020. This is the legal frame of SwissCovid. This article restricts the use of SwissCovid to the intended purpose, imposes that usage is voluntary, prohibits discrimination based on usage or not (except for a free medical test if notified at-risk by the application), and gives (in alinea 5) five requirements on the design of SwissCovid. The compliance of SwissCovid must be done with respect to those requirements.

- *All possible means must be taken to avoid users to be identified.*
  The fact is that many possible identifications attacks exist. For SwissCovid to be compliant with this criterion, it must be shown that there is no possible mean, beyond what is already in place, to avoid those attacks. We believe that systems which are better than SwissCovid are technically possible but would require more development time than what was done for SwissCovid.

Hence, given the emergency, SwissCovid could be considered as compliant with this criterion.

- *Data are treated in a decentralized manner on the telephones.*
  SwissCovid is compliant with this criterion.
- *Only necessary data are collected and processed. No geolocalization data is collected nor processed.*
  We can wonder if SwissCovid is subject to the same controversy which happened in France - that all data are collected, beyond encounters which last enough in time and which are close enough. It however seems that this is necessary for technical reasons. Currently, SwissCovid does not use geolocalization. Hence, SwissCovid is compliant with this criterion (although we have no mean to check that it is the case on the Apple-Google part of the system).
  However, the forthcoming development with respect to interoperability between regions may require to process geographic information about the location. By doing so, SwissCovid may become not compliant with this requirement.
- *Unnecessary data are erased.*
  SwissCovid is compliant with this criterion (although we have no mean to check that it is the case on the Apple-Google part of the system).
- *The source code and specifications of all components are public. Programs must be verifiably made from the source code.*
  At this time, specifications are still missing. Verifiability is not implemented yet. The point about the source code is discussed below. We believe that SwissCovid is not compliant with this criterion.

In addition to this, regulation on data protection applies (alinea 6). This implies restrictions when using *personal information*. A delicate question, both technically and legally, is whether the *ephemeral identifiers* which are exchanged via Bluetooth, as well as the *diagnosed keys* which are stored on the server and transit via Amazon services, are personal information or not. Since ephemeral identifiers can be computed from diagnosed keys, we believe that either both or none should be considered as personal information.

On the FOPH website we can read *"The phone does not send any personal or location data to a central storage location or server"*. On another page we can read *"The CDN only gives users access to information that cannot be used to obtain personal information (i.e. anonymous keys)"*. This defends that none are personal information, hence not subject to regulation on data protection. One consequence is that it seems perfectly legal that anyone collects ephemeral identifiers which are sent via Bluetooth and run some of the known attacks. We rather believe that those information should be considered as personal information hence subject to regulation. Collecting those information should be subject to legal restriction. This may have legal consequences on how data is treated on the server and transits via the Amazon CDN service.

Most of the former DP3T protocol is now replaced by what Apple and Google implemented in a component of the system called *GAEN*. It implements most of the crucial operations which are required in the SwissCovid system. GAEN is undoubtedly a *component* from a technical viewpoint. However, GAEN has no available source code, as required by law. Promoters argue that GAEN is part of the phone design, either of the operating system or of the Bluetooth communication interface, which justifies this exception. This argument is incorrect, at least on Android systems.

GAEN is part of the *Google Play Services* which are not open source. Telephones in which those services are removed still have the same working Android operating system and can use Bluetooth. We can live with such phones. SwissCovid does not work on them, but the pre-standard version of SwissCovid does, with available source codes. Therefore, **the switch from pre-standard to GAEN-based version made SwissCovid not compliant with the law**.

Compliance (Episode II)

On June 24, 2020, the Federal Council released an *Ordinance on the proximity tracing system for coronavirus* (OSTP). It refines LEp about SwissCovid. Quite predictably, OSTP defines the components of the system by excluding GAEN (Art.2). The system is composed of servers and of the SwissCovid app that users install on their phone. We already qualified this as a trick to exclude GAEN from the source code disclosure requirement.

Quite surprisingly, Art.5 al.2 describes the functions that the SwissCovid app is fulfilling *with the help of an interface of the operating system*. We understand this as a reference to GAEN (although GAEN is not part of the operating system, as already discussed). We observe below that nearly none of the 5 listed functionalities have any corresponding line of code in the available source code, for the simple reason that these are the functionalities which are fulfilled by ("with the help of") GAEN.

- Generation of a new key of the day.
  This is done by GAEN. The app has no access to it unless the user is diagnosed and receives a code to unlock it.
- Exchange of ephemeral identifiers via Bluetooth.
  This is done by GAEN. The app never sees it.
- Storage of received ephemeral identifiers.
  This is done by GAEN. The app never sees it.
- Download of diagnosed keys and comparison.
  The app downloads but comparison is made by GAEN. The app only sees the matching results.

- Notification in case of matching.
  This is done by the app based on the input from GAEN.

This is actually the list of the tasks of GAEN. What the app is really doing is not listed here.

OSTP also strengthens the exclusion of GAEN to the source code disclosure requirement of LEp by adding **an explicit exception to the law** for the *functions of the operating system which are used via the interface*, hence GAEN (Art.5 al.3). Adding an exception to a law for a part which is not recognized as a component is quite awkward. What is clear it that the job of the app (which is subject to LEp) is nealry totally outsourced to GAEN (which is exempted from LEp by OSTP). Obviously, this is not compliant with the spirit of LEp.

In a nutshell, the 19.6.2020 LEp law says all *components* of the SwissCovid system must have a publicly available source code and lets the Federal Council the responsibility to address the deployment details. The 24.6.2020 ordinance from the Federal Council defines the components by excluding what is provided by Google-Apple and is implementing the DP3T functionalities. Consequently, **the implementation of DP3T has bypassed the law**. We believe that the ordinance was already in preparation while the Council of States and the National Council were discussing on the necessity to have a publicly available source code and our analysis was censored. Citizens and the parliament have been deceived. May it be for good reasons (e.g. to hit the second wave), it is a blatant cheat. In our opinion, **the law, which was made to protect people for having to use an opaque system, has proven itself to be insufficient 5 days after adoption.**

References

Caution: as far as we know, no scientific reference (ours included) went through any peer review process.

Our references:

- 8.4.2020 Serge Vaudenay. Analysis of DP3T - Between Scylla and Charybdis. IACR-EPRINT 2020.
- 21.4.2020 Xavier Bonnetain, Anne Canteaut, Véronique Cortier, Pierrick Gaudry, Lucca Hirschi, Steve Kremer, Stéphanie Lacour, Matthieu Lequesne, Gaëtan Leurent, Léo Perrin, André Schrottenloher, Emmanuel Thomé, Serge Vaudenay, Christophe Vuillot. Le traçage anonyme, dangereux oxymore. (English version available.)
- 6.5.2020 Serge Vaudenay. Centralized or Decentralized? The Contact Tracing Dilemma. IACR-EPRINT 2020.
- 5.6.2020 Serge Vaudenay, Martin Vuagnoux. Analysis of SwissCovid
- 17.6.2020 Serge Vaudenay, Martin Vuagnoux. (Annotated) Security Issue Submission [INR-4434]. Detailed analysis.

Legal references (some references in French):

- 818.101 LEp Art.60a. Loi fédérale sur la lutte contre les maladies transmissibles de l'homme (LEp). Current state.
- 235.1. Federal Act on Data Protection (FADP). Current state.
- 20.5.2020 20.040 message from the Federal Council. Message concernant la modification urgente de la loi sur les épidémies en lien avec le coronavirus (Système de traçage de proximité).
- 13.5.2020 Ordinance for public pilot test. Coronavirus : le Conseil fédéral adopte l'ordonnance sur l'application de traçage de proximité et prolonge le soutien à la culture.
- 24.6.2020 Ordinance on the proximity tracing system for coronavirus (OSTP). Coronavirus : la Confédération prend en charge les tests de dépistage, l'application SwissCovid démarre le 25 juin.

Other references:

- 10.6.2020 Lars Baumgärtner, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini, Markus Miettinen, Anel Muhamedagic, Thien Duc Nguyen, Alvar Penning, Dermot Frederik Pustelnik, Filipp Roos, Ahmad-Reza Sadeghi, Michael Schwarz, Christian Uhl. Mind the GAP: Security & Privacy Risks of Contact Tracing Apps. Preprint arXiv:2006.05914 [cs.CR], 2020.
- 16.6.2020 Douglas J. Leith, Stephen Farrell. GAEN Due Diligence: Verifying The Google/Apple Covid Exposure Notification API.
- 18.6.2020 Paul-Olivier Dehaye, Joel Reardon. SwissCovid: a Critical Analysis of Risk Assessment by Swiss Authorities. Preprint arXiv:2006.10719 [cs.CR], 2020.
- 26.6.2020 Stephen Farrell, Douglas J. Leith. Transparency in the Deployment of Coronavirus Contact Tracing Apps.

Last update: June 28, 2020.