Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Home Affairs
Federal Office of Public Health FOPH

Technical Information

SwissCovid app: Replay attacks and AEM-tampering

Date: 18 June 2020

The possibility of Replay attacks of decentralized proximity tracing protocols is well-known and documented since April. «The Security Report Proximity Scanning» from NCSC of May 28th makes the following statement [1] (English original version):

«*Replay attacks in order to poison the system*

Replay attack is the only real sabotage possibility we could find in the protocol: An attacker can collect EphIDs of people with a high probability of future positives with a very sensitive receiver, e.g., near a drive-in test center or a hospital in general, send these via internet to a very different location where a lot of non-infected people are expected (like in residential areas), and replay them there using a very strong Bluetooth signal. This would cause a lot of false detections.»

A report submitted on June 5th to the NCSC by Prof. Vaudenay and Dr. Vuagnoux as part of the public security tests identifies a variant of the replay attack in which an active attacker would tamper the «Associated Encrypted Metadata» (AEM) of beacons before replaying them further as part of the Replay attack. The consequence is that the receivers of the Replayed EphIDs would decrypt a different transmission power level than in the original message.

DP-3T researchers at EPFL and ETH Zürich have evaluated this aspect of the June 5th report. The researchers acknowledge this new variant was not previously evaluated by them.

DP-3T researchers have communicated the AEM tampering vulnerability to Apple and Google, via email and via teleconference, since this attack variant results from the specific implementation of the exposure notification framework by these two companies.

During the Public Security Test, several testers also pointed out that there was a risk of replay attacks, which could pose a serious security problem. The NCSC therefore issued an additional report on 15 June to shed light on this type of attack and to show the real threat that this type of attack can pose.

In this report, the following passages are worth mentioning in this context (full version can be found under link [2]):

«It is important to notice though that the privacy risk only affects diagnosed people, i.e. those that received a positive test result and uploaded their TEKs subsequently, and not at-risk (i.e. warned) people, as claimed in by one researcher. The fact the number of infected people is much lower than the overall number of users or even of at-risk users shows that the attack surface is quite small and restricted to patients who will need to go into isolation by law

anyway, which poses a much larger impact to their privacy than a theoretical risk due to preceding eavesdropping. Also, the time range where this risk exists for these users is restricted to the contagious window, usually a few days.»

With regard to privacy:

«We believe that under normal circumstances, the privacy of the users does not constitute an unacceptable higher risk when using the app. If a user has a smartphone with Bluetooth enabled (e.g. for headphones), she accepts certain risks associated with this technology.

The same is true for the Swisscoovid App [sic]*. One might argue that the overall attack surface for the population rises because users are pushed into activating Bluetooth. While this is true, we believe that many people already have Bluetooth enabled and that Bluetooth based proximity tracing is still the better option than using actual geolocation information. We do not see any other better technologies that could be made ready within the given timeframes.»*

The authors also point out that it is always possible to activate or deactivate the app:

«The public should be informed that people can turn on and off the app at any time and so stop broadcasting EphIDs for defined periods of time. It is important to keep the app running whenever infection situations with unknown people can occur, but it is better to turn it off at home, which reduces the replay attack risk on the receiving side, when in places that should later not be exposed, or when at work if a risk of BLE collectors operated by the employer exists. Using the app is not a binary decision, but can be adapted by users depending of their current environment.»

And in conclusion:

«We believe that the most important thing to do is to accept that there are residual risks and to perceive the app as just one additional data source for the handling of the pandemic.»

[1] Security Report Proximity Scanning; version of May 28 (PDF: «Risk-Estimation-Proximity-Tracing_Signed»): https://www.melani.admin.ch/melani/en/home/public-security-test/current_findings.html

[2] Replay Attacks; 15. Mai 2020 (PDF: «Replay-Attacke-Risk-Estimation_Public_Signed»): https://www.melani.admin.ch/melani/en/home/public-security-test/current_findings.html