Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI
Ufficio federale della sanità pubblica UFSP

Informazione tecnica

L'app SwissCovid: Attacchi replay e manipolazioni AEM

Data: 18 giugno2020

La possibilità di attacchi replay («Replay Attacks») di protocolli decentralizzati per il tracciamento a distanza ravvicinata è nota e documentata da aprile. Il «Proximity Scanning Security Report» del NCSC del 28 maggio rilascia la seguente dichiarazione [1] (tradotto; la versione originale in inglese si trova sotto il link [1]):

Ripetere gli attacchi con lo scopo di avvelenare il sistema

L'attacco replay è l'unica possibilità reale di sabotaggio che abbiamo potuto trovare nel registro: Un aggressore può utilizzare un ricevitore molto sensibile, ad esempio vicino a un centro di test drive-in o a un ospedale in generale, per raccogliere gli EphID di persone con un'alta probabilità di risultati positivi futuri, inviarli via Internet in un luogo completamente diverso dove sono attese molte persone non infette (come nelle zone residenziali) e riprodurli lì con un segnale Bluetooth molto forte. Questo causerebbe un sacco di falsi positivi.

Un rapporto presentato al NCSC il 5 giugno dal Prof. Vaudenay e dal Dr. Vuagnoux nell'ambito dei test di pubblica sicurezza identifica una variante dell'attacco di replay in cui un aggressore attivo manipolerebbe i metadati crittografati associati (AEM) dei radiofari prima di continuare a riprodurli come parte dell'attacco di replay. Di conseguenza, i destinatari degli EphID riprodotti decifrerebbero una potenza di trasmissione diversa da quella del messaggio originale.

I ricercatori del DP-3T dell'EPFL e del Politecnico di Zurigo hanno valutato questo aspetto del rapporto del 5 giugno. I ricercatori riconoscono che questa nuova variante non è stata valutata da loro in precedenza.

I ricercatori del DP-3T hanno comunicato la vulnerabilità AEM mediante manipolazione via e-mail e teleconferenza ad Apple e Google, in quanto questa variante di attacco deriva dall'implementazione specifica del framework di reporting dell'esposizione da parte di queste due aziende.

Durante il test di sicurezza pubblica, diversi tester hanno inoltre sottolineato il rischio di attacchi di replay, che potrebbero rappresentare un grave problema di sicurezza. Il 15 giugno il NCSC ha pertanto pubblicato un rapporto supplementare per far luce su questo tipo di attacco e per mostrare la reale minaccia che questo tipo di attacco può rappresentare.

Degni di nota in questo rapporto sono i seguenti passaggi (tradotti; la versione originale in Inglese del rapporto si trova sotto il link [2]):

È importante notare però che il rischio per la privacy riguarda solo le persone diagnosticate, cioè quelle che hanno ricevuto un risultato positivo del test e che hanno successivamente caricato le loro TEK, e non le persone a rischio (cioè avvertite), come sostenuto da un ricercatore. Il fatto che il numero di persone infette sia molto inferiore al numero complessivo di utenti o anche di utenti a rischio dimostra che la superficie di attacco è piuttosto piccola e limitata ai pazienti che dovranno comunque andare in isolamento per legge, il che comporta un impatto molto maggiore sulla loro privacy rispetto a un rischio teorico dovuto a precedenti intercettazioni. Inoltre, l'intervallo di tempo in cui esiste questo rischio per questi utenti è limitato alla finestra contagiosa, di solito qualche giorno.

Alla sfera privata:

Riteniamo che, in circostanze normali, la privacy degli utenti non costituisca un rischio maggiore inaccettabile quando si utilizza l'app. Se un utente dispone di uno smartphone con Bluetooth abilitato (ad es. per le cuffie), accetta determinati rischi associati a questa tecnologia.

Lo stesso vale per l'app SwissCovid. Si potrebbe sostenere che la superficie di attacco complessiva per la popolazione aumenta perché gli utenti sono spinti ad attivare il Bluetooth. Anche se questo è vero, riteniamo che molte persone abbiano già attivato il Bluetooth e che il tracciamento di prossimità basato sul Bluetooth sia ancora la soluzione migliore rispetto all'utilizzo di informazioni reali sulla geolocalizzazione. Non vediamo altre tecnologie migliori che potrebbero essere pronte entro i tempi previsti.

Gli autori sottolineano inoltre che c'è sempre la possibilità di attivare o disattivare l'app:

Il pubblico dovrebbe essere informato che le persone possono accendere e spegnere l'applicazione in qualsiasi momento e quindi smettere di trasmettere EphID per periodi di tempo definiti. È importante mantenere l'app in funzione ogni volta che possono verificarsi situazioni di infezione con persone sconosciute, ma è meglio spegnerla a casa, il che riduce il rischio di attacchi di replay sul lato ricevente, quando si trova in luoghi che in seguito non dovrebbero essere esposti, o quando si lavora se esiste un rischio di collettori BLE gestiti dal datore di lavoro. L'utilizzo dell'app non è una decisione binaria, ma può essere adattata dagli utenti a seconda del loro ambiente attuale.

E in conclusione:

Riteniamo che la cosa più importante da fare sia accettare che ci sono dei rischi residui e percepire l'app come una sola fonte di dati aggiuntiva per la gestione della pandemia.

[1] Security Report Proximity Scanning; 28 mai 2020 (PDF: «Risk-Estimation-Proximity-Tracing_Signed»): https://www.melani.admin.ch/melani/it/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/it/home/public-security-test/current_findings.html