Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la santé publique OFSP

Information technique

L'application SwissCovid: Attaques par rediffusion et manipulations AEM

Date: 18 juin 2020

La possibilité d'attaques par rediffusion («replay attacks») des protocoles de traçage de proximité décentralisés est bien connue et documentée depuis le mois d'avril. Le rapport «Security Report Proximity Scanning» du NCSC du 28 mai fait la déclaration suivante [1] (traduit ; la version originale en anglais peut être trouvée sous le lien [1]):

Reproduire les attaques dans le but d'empoisonner le système

L'attaque par rediffusion est la seule possibilité réelle de sabotage que nous ayons pu trouver dans le journal : Un agresseur peut utiliser un récepteur très sensible, par exemple près d'un centre d'essai au volant ou d'un hôpital en général, pour collecter les EphID de personnes ayant une forte probabilité de résultats positifs futurs, les envoyer par Internet à un endroit complètement différent où de nombreuses personnes non infectées sont attendues (comme dans les zones résidentielles), et les y rejouer avec un signal Bluetooth très puissant. Cela provoquerait beaucoup de faux positifs.

Un rapport soumis le 5 juin au NCSC par Prof. Vaudenay et le Dr. Vuagnoux dans le cadre des tests publics de sécurités identifie une variante de l'attaque par rediffusion dans laquelle un attaquant actif manipulerait les «métadonnées cryptées associées» («Associated Encrypted Metadata» ou AEM) des balises avant de les rejouer dans le cadre de l'attaque par rediffusion. La conséquence est que les récepteurs des EphIDs rejoués décrypteraient un niveau de puissance de transmission différent de celui du message original.

Les chercheurs du projet DP-3T de l'EPFL et à de l'ETH Zürich ont évalué cet aspect du rapport du 5 juin. Les chercheurs reconnaissent que cette nouvelle variante n'a pas été évaluée auparavant d'eux.

Les chercheurs du projet DP-3T ont communiqué à Apple et à Google, par courrier électronique et par téléconférence, la vulnérabilité liés à l'altération des AEM, puisque cette variante d'attaque résulte de la mise en œuvre spécifique de l' «exposure notification framework» développée par ces deux entreprises.

Lors du test de sécurité publique, plusieurs testeurs ont également souligné qu'il y avait un risque d'attaques à répétition, ce qui pourrait poser un sérieux problème de sécurité. Le 15 juin, le NCSC a donc publié un rapport supplémentaire pour faire la lumière sur ce type d'attentat et montrer la menace réelle que ce type d'attaque peut représenter.

Les passages suivants méritent d'être mentionnés dans ce rapport (traduit; la version originale en Anglais du rapport se trouve sous le lien [2])

Il est toutefois important de noter que le risque pour la vie privée ne concerne que les personnes diagnostiquées, c'est-à-dire celles qui ont reçu un résultat de test positif et ont

téléchargé leurs CET par la suite, et non les personnes à risque (c'est-à-dire averties), comme le prétend un chercheur. Le fait que le nombre de personnes infectées soit beaucoup plus faible que le nombre total d'utilisateurs ou même d'utilisateurs à risque montre que la surface d'attaque est assez réduite et limitée aux patients qui devront de toute façon être isolés par la loi, ce qui représente un impact beaucoup plus important sur leur vie privée qu'un risque théorique dû à une écoute préalable. En outre, la période pendant laquelle ce risque existe pour ces utilisateurs est limitée à la fenêtre de contagion, généralement quelques jours.

Pour la sphère privée :

Nous pensons que dans des circonstances normales, la vie privée des utilisateurs ne constitue pas un risque inacceptable plus élevé lors de l'utilisation de l'application. Si un utilisateur possède un smartphone avec Bluetooth activé (par exemple pour les écouteurs), il accepte certains risques liés à cette technologie.

Il en va de même pour l'application SwissCovid. On pourrait avancer que la surface d'attaque globale de la population augmente parce que les utilisateurs sont poussés à activer le Bluetooth. Bien que cela soit vrai, nous pensons que de nombreuses personnes ont déjà activé le Bluetooth et que le traçage de proximité basé sur le Bluetooth reste la meilleure option par rapport à l'utilisation d'informations de géolocalisation réelles. Nous ne voyons pas d'autres technologies plus performantes qui pourraient être mises en place dans les délais impartis.

Les auteurs soulignent également qu'il est toujours possible d'activer ou de désactiver l'application :

Le public doit être informé que les gens peuvent allumer et éteindre l'application à tout moment et donc cesser de diffuser les EphID pendant des périodes de temps définies. Il est important de maintenir l'application en marche chaque fois que des situations d'infection avec des personnes inconnues peuvent se produire, mais il est préférable de l'éteindre à la maison, ce qui réduit le risque d'attaque de rediffusion du côté de la réception, dans des endroits qui ne devraient pas être exposés par la suite, ou sur le lieu de travail s'il existe un risque de présence de collecteurs BLE exploités par l'employeur. L'utilisation de l'application n'est pas une décision binaire, mais peut être adaptée par les utilisateurs en fonction de leur environnement actuel.

Et en conclusion :

Nous pensons que la chose la plus importante à faire est d'accepter qu'il existe des risques résiduels et de percevoir l'application comme une source de données supplémentaire pour la gestion de la pandémie

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