Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG

Technische Information

SwissCovid App: Replay-Angriffe und AEM-Manipulationen

Datum: 18. Juni 2020

Die Möglichkeit von Replay-Angriffen («Replay Attacks») von dezentralisierten Protokollen zur Nahbereichsverfolgung ist seit April bekannt und dokumentiert. Der «Sicherheitsbericht Proximity Scanning» des NCSC vom 28. Mai gibt folgende Erklärung ab [1] (übersetzt; die Originalversion in Englisch ist unter dem Link [1] zu finden):

Replay-Angriffe mit dem Ziel, das System zu vergiften

Der Replay-Angriff ist die einzige wirkliche Sabotagemöglichkeit, die wir im Protokoll finden konnten: Ein Angreifer kann mit einem sehr empfindlichen Empfänger, z.B. in der Nähe eines Drive-In-Testzentrums oder eines Krankenhauses allgemein, EphIDs von Personen mit einer hohen Wahrscheinlichkeit künftiger positiver Ergebnisse sammeln, diese über das Internet an einen ganz anderen Ort senden, an dem viele nicht infizierte Personen erwartet werden (wie in Wohngebieten), und sie dort mit einem sehr starken Bluetooth-Signal wiedergeben. Dies würde eine Menge falscher Erkennungen verursachen.

Ein Bericht, der am 5. Juni dem NCSC von Prof. Vaudenay und Dr. Vuagnoux im Rahmen der öffentlichen Sicherheitstests vorgelegt wurde, identifiziert eine Variante des Replay-Angriffs, bei der ein aktiver Angreifer die «Associated Encrypted Metadata» (AEM) von Baken manipulieren würde, bevor er sie als Teil des Replay-Angriffs weiter abspielen würde. Die Folge ist, dass die Empfänger der wiedergegebenen EphIDs eine andere Sendeleistung als in der ursprünglichen Nachricht entschlüsseln würden.

DP-3T-Forscher der EPFL und der ETH Zürich haben diesen Aspekt des Berichts vom 5. Juni bewertet. Die Forscher erkennen an, dass diese neue Variante durch sie zuvor nicht bewertet wurde.

Die DP-3T-Forscher haben die AEM-Verwundbarkeit durch Manipulation per E-Mail und per Telefonkonferenz an Apple und Google mitgeteilt, da diese Angriffsvariante aus der spezifischen Umsetzung des Rahmens für die Expositionsmeldung durch diese beiden Unternehmen resultiert.

Während des öffentlichen Sicherheitstests (Public Security Test) wiesen verschiedene Tester ebenfalls darauf hin, dass eine Gefahr von Replay-Angriffen bestehe, welche ein ernsthaftes Sicherheitsproblem darstellen könnten. Das NCSC hat deshalb am 15. Juni einen zusätzlichen Report erstellt, um ein Licht auf diese Art von Angriffen zu werfen und um die tatsächliche Bedrohung aufzuzeigen, die von dieser Art von Angriffen ausgehen kann.

Erwähnenswert sind in diesem Bericht z.B. folgende Passagen (übersetzt; die Originalversion des in English ist unter dem Link [2] zu finden):

Es ist jedoch wichtig zu beachten, dass das Risiko für die Privatsphäre nur diagnostizierte Personen betrifft, d.h. Personen, die ein positives Testergebnis erhalten und ihre TEKs anschliessend hochgeladen haben, und nicht Risikopersonen (d.h. gewarnte Personen), wie von einem Forscher behauptet. Die Tatsache, dass die Zahl der Infizierten viel geringer ist als die Gesamtzahl der Anwender oder sogar der Risikopersonen, zeigt, dass die Angriffsfläche recht klein und auf Patienten beschränkt ist, die ohnehin von Gesetzes wegen isoliert werden müssen, was eine viel grössere Auswirkung auf ihre Privatsphäre hat als ein theoretisches Risiko durch vorheriges Abhören. Auch ist der Zeitbereich, in dem dieses Risiko für diese Anwender besteht, auf das Ansteckungsfenster beschränkt, in der Regel auf einige Tage.

Zur Privatsphäre:

Wir glauben, dass unter normalen Umständen die Privatsphäre der Nutzer kein inakzeptabel höheres Risiko bei der Verwendung der App erleidet. Wenn eine Benutzerin ein Smartphone mit aktiviertem Bluetooth (z.B. für Kopfhörer) besitzt, nimmt sie gewisse Risiken in Kauf, die mit dieser Technologie verbunden sind.

Dasselbe gilt für die SwissCovid App. Man könnte argumentieren, dass die Gesamtangriffsfläche für die Bevölkerung steigt, weil die Nutzer dazu gedrängt werden, Bluetooth zu aktivieren. Dies ist zwar richtig, aber wir glauben, dass viele Menschen bereits Bluetooth aktiviert haben und dass Bluetooth-basiertes Proximity Tracing immer noch die bessere Option als die Verwendung tatsächlicher Geolokalisierungsinformationen ist. Wir sehen keine anderen besseren Technologien, die innerhalb des vorgegebenen Zeitrahmens zur Verfügung gestellt werden könnten.

Die Autoren machen auch darauf aufmerksam, dass jederzeit die Möglichkeit besteht, die App zu aktivieren oder zu deaktivieren:

Die Öffentlichkeit sollte darüber informiert werden, dass man die App jederzeit ein- und ausschalten und so die Ausstrahlung von EphIDs für bestimmte Zeiträume unterbinden kann. Es ist wichtig, die App immer dann laufen zu lassen, wenn Infektionssituationen mit unbekannten Personen auftreten können, aber es ist besser, sie zu Hause auszuschalten, was das Risiko eines Replay-Angriffs auf der Empfangsseite, an Orten, die später nicht exponiert werden sollten, oder bei der Arbeit verringert, wenn ein Risiko von BLE-Sammlern besteht, die vom Arbeitgeber betrieben werden. Die Verwendung der App ist keine binäre Entscheidung, sondern kann von den Benutzern je nach ihrer aktuellen Umgebung angepasst werden.

Und als Fazit:

Wir glauben, dass es am wichtigsten ist, zu akzeptieren, dass es Restrisiken gibt, und die App als nur eine zusätzliche Datenquelle für den Umgang mit der Pandemie zu betrachten.

.

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