To: [redacted])[[redacted]@minvws.nl]
From: [redacted].
Sent: Tue 9/1/2020 9:14:24 AM
Subject: Fwd: Advies 10 Testcapaciteit Opschalen 27 aug herziene versie evds kgmm dme PB
Received: Tue 9/1/2020 9:14:28 AM
DP3T - Best Practices for Operation Security in Proximity Tracing.pdf
ATT00001[redacted]

Begin doorgestuurd bericht:

Van: [redacted] <[redacted]@cwi.nl>
Datum: 1 september 2020 om 00:39:29 CEST
Aan: [redacted] <[redacted]@VNG.NL>
Kopie: "[redacted]@minvws.nl" <[redacted]@minvws.nl>, "[redacted]" <[redacted]@umcutrecht.nl>, [redacted] <[redacted]@egeniq.com>, "[redacted]." <[redacted]@umcutrecht.nl>
Onderwerp: Doorst: Advies 10 Testcapaciteit Opschalen 27 aug herziene versie evds kgmm dme PB

?Beste [redacted]

Vanuit de begeleidingscommissie wilden we nog twee dingen kortsluiten.

1. het is duidelijk dat in de proef in Twente/Drenthe veel mensen zijn die valselijk claimen een alert gehad te hebben. In ons laatste advies hebben we aanbevolen om een confirmatie-code in de app beschikbaar te maken die mensen die de GGD bellen vanwege een alert kunnen (of moeten..) voorlezen. Die confirmatiecode kan geverifieerd worden, en zal misbruik tegengaan.

Het zal in ieder geval toestaan om in de evaluatie vast te stellen dat de beller daadwerkelijk een melding had gekregen.

Sterker nog, je zou de confirmatiecode mogelijk ook kunnen gebruiken eventueel om wat statistiek mee te geven over attenuation en duration onderliggend aan de melding. Die moeten jullie dan wel op een ov andere manier uit GAEN peuteren (dat binary search idee?). Het idee is om een cijfer te encoderen zodat je een code krijgt, en alleen de GGD kan die code dan decoderen en het cijfer terugkrijgen.

Een soortgelijk mechanisme (zonder statistieken erin te stoppen, natuurlijk) is na te lezen als aanbeveling van DP-3T in het attached document.

De vraag is dus: kunnen jullie zo'n confirmatiecode realiseren? Hoeveel tijd zou het kosten? Zonder deze code kunnen we volgens ons niets betrouwbaar meten, over de app; vanwege de valse claims, met name. Dit is zelfs bedreigend voor CoronaMelder omdat het nu lijkt alsof de voorspellende waarde van een alert zeer laag is. Ik kan ook wel wat concrete ideeen van de hand doen over zo'n code.

2. er wordt nog steeds gesteggeld, begrijpen wij, over het handelingsadvies. Onze commissie is *voor* het pre-sympotomatisch testen (op dag 7.. vinden we eigenlijk al een beetje laat). Dit baseren we op ons idee dat mensen vaak niet de waarheid vertellen over hun quarantainegedrag, en zonder positieve testuitslag en zonder symptomen niet al te voorzichtig zijn. Pre-symptomatisch testen gaat de test vervroegen, en zo het voorzichtige gedrag vervroegen, denken wij. En daarmee veel vroege besmettingen (en dat zijn er veel) kunnen voorkomen.

Maar, stel dat de slag over het handelingsadvies verloren gaat, is er nog wel een praktisch probleem omdat het huidige handelingsadvies in de app zegt dat je je moet laten testen en de GGD moet bellen. Onze vraag is eigenlijk of het handelingsadvies een configurabele tekst is, of dat er een upgrade van de app nodig zou zijn om het advies te kunnen veranderen? In het laatste geval lijkt het ons goed om het configurabel te maken.

alvast dank voor je reaktie,

5.1.2e

PS
Zouden we niet een vervolgafspraak inplannen voor een call?

===== begint op pagina 19 van attached document

A simple validation mechanism

We present a simple remote validation mechanism. This mechanism can be used during a phone conversation with a hotline operator. The mechanism has been designed to be easy to use by both users and hotline operators.

We make the following assumptions:

a. When the user is notified by the app that their exposure is above the threshold, the app informs the user of the date on which the exposure exceeded the threshold.

b. Users inform hotline operators of this date. This assumption is compatible with our requirements. One, the Google/Apple Exposure Notification API returns this date. Two, communicating this date to the hotline is essential for medical reasons. The exposure date is used to determine how long the user should self-quarantine.

We propose the following mechanism:

1. Before the user calls the hotline, the app prominently displays to the user the exposure date T e and a 6-digit confirmation code, which the device computes as:

code = TRUNCATE(HKDF(tweak, T e || T now))

where HKDF uses SHA256 , TRUNCATE reduces the 256 bits output to a 6-digit response code, the tweak tweak is a value that is only known to the app and operators. The value Te is the exposure date encoded as the start of the corresponding UNIX Epoch day in milliseconds since UNIX epoch and T now is the current timestamp when generating the verification code encoded as milliseconds since UNIX epoch and rounded down to a 5-minute multiple.

The app should recommend that the user writes these values down before calling the hotline.

2. When calling the hotline, the user informs the operator of their exposure date Te and the confirmation code code. The operator enters Te and code into the system.

3. The operator's system computes the confirmation codes for the last half hour and compares them against the supplied code. The system signals the operator if the code is not correct. (Comparing against the last few codes lets the system validate
older codes.)

This mechanism satisfies our requirements. It does not require modification to the EN protocols or APIs, does not require extra permissions, works during a single phone call, and does not reduce the privacy of users.
The tweak tweak can either be encoded into the app, or retrieved from the backend server after successful attestation and then stored in secure storage. However, we recommend making the value of tweak public to ensure verifiability, i.e., that the system uses the same value for all users.

Analysis of the mechanism

As long as the tweak value is secret, users only have a small probability of producing the correct validation code code. For example, when using 6 digit responses and a half-hour window, this probability is 6 in a million.
It is difficult to unconditionally protect the value tweak from tech-savvy users that might decompile the application or circumvent the attestation check. Only providing the (recent) value tweak to apps after successful attestation, does make it harder for tech-savvy users to obtain it.9 Considering the challenges with attestation described above, we do not, at this time, recommend its use.
After obtaining the value tweak, tech-savvy users can compute correct responses despite not having been notified.

We deliberately do not advocate for performing an attestation during the verification process with the hotline. While a "live" attestation further raises the bar, the attestations are too large to transmit via the phone, and therefore induce yet another network side-channel that must be protected against network adversaries. By themselves, we expect that ordinary users are not able to compute the correct response, even if they would know the correct value of tweak . However, tech-savvy users could set up a validation-service in the form of a website or an app that performs the necessary computation on behalf of the ordinary user.

An offline version

Alternatively, it is possible to use an offline version of the above protocol where the validation codes are not verified during the conversation. This has the advantage that the hotline system does not need to know the value tweak and does not need to have a system in place to compute verification codes. Instead, the hotline stores the exposure date T e , the time of the call T now , and the validation code code so that they can be verified at a later time.

Recommendations

The verification mechanism raises the bar somewhat against ordinary users making false claims. However, it is only a small part in a more complex system needed to validate notifications. In particular, we recommend to only deploy it in combination with additional mechanisms to reduce abuse:
1. Use legal measures to penalize fake notification reports.
2. Monitor the availability of services and apps that generate codes.
3. Monitor the number of notifications and compare against predictions based on the
number of positive diagnoses.
