To: [redacted]@cwi.nl]
Cc: [redacted]@minvws.nl]; [redacted]@umcutrecht.nl]
From: [redacted]
Sent: Thur 9/24/2020 7:25:22 PM
Subject: Re: 'Meldcode' voor coronamelder notificaties
Received: Thur 9/24/2020 7:25:46 PM

Hoi [redacted]

Reden dat je nog gehoord had: morgen hebben we overleg met [redacted] en iedereen die deze feature 'raakt' om de diverse opties te bespreken. Push werd idd door onze eigen mensen afgeraden.

Een geheime sleutel zou *notarieel* misschien kunnen (de notaris maakt zelf de build niet dus die zou via de build straat geïnjecteerd moeten worden) maar is zwak beveiligd. De apk extracten van een android device en je hebt m al te pakken. Bovendien maakt het een reproducible build door de community onmogelijk. Dus denk niet dat dit veel toevoegt toch van eeen pseudo geheime code (Combi van iets dat van de server komt en de datum van exposure).

Maar ik zal m bij de opties zetten.

Greetings,
[redacted]
On 24 Sep 2020, 18:37 +0200, [redacted] <[redacted]@cwi.nl>, wrote:

> Beste [redacted]
>
> Ik heb niet verder van je teruggehoord. Ik denk dus dat een pushbericht geen goed idee is, vanwege het lekken van informatie naar Google en Apple.
>
> Mijn eigen suggestie van een tijd min of meer onopvallend verstopt in de code, is niet waterdicht. Het is meer een trucje om achteraf het kaf van het koren te scheiden in analyses. Maar als iemand een website gebruikt die codes genereert, tijdens het gesprek, kan ik er niet achter komen. Ik begrijp dus dat je mijn suggestie niet aantrekkelijk vindt.
>
> Een ander idee zou zijn om in de source code een geheime sleutel te zetten, of liever een template-sleutel. In een constante in het programma. Bij de laatste compilatie wordt die template-sleutel vervangen door een echte sleutel, die niet openbaar is. We moeten dit dan notarieel vastleggen. Dwz notarieel vastleggen dat het enige dat verschilt tussen open-source prgoramma-code en de code die uiteindelijk gecreerd wordt is dat de bewuste constante in de geheime code is vervangen. Dat betekent dat de notaris kan beschikken over de uiteindelijke geheime sleutel en daarmee kan vaststellen dat de open source programmacode plus de geheime code inderdaad de openbare binary in de appstores oplevert.
>
> Dit is nog steeds te hacken, maar het is wel moeilijker. Mijn voorstel zou zijn om dit *alleen* te gebruiken (vooralsnog) voor analyses. Dus als iemand een website maakt die codes falsificeert met de template-key, zou ik ze ook goed rekenen. Op die manier komen de valsspelers er niet achter, dat we ze door hebben. Maar in de CoronaMelder analyse weten we dan wel dat we die melding moeten negeren.
>
> mvg,
>
> [redacted]
>
> ----- Original Message -----
> From: "[redacted]" <[redacted]@cwi.nl>
> To: "[redacted]" <[redacted]>
> Cc: [redacted]@minvws.nl>, "[redacted]" <[redacted]@umcutrecht.nl>
> Sent: Thursday, September 17, 2020 10:23:00 PM
> Subject: Re: 'Meldcode' voor coronamelder notificaties
>
> Beste [redacted]

Bedankt voor je reactie. Het is inderdaad jammer dat jullie voorgestelde uitbreiding niet in GAEN zit.

Ondanks het feit dat deze codes te vervalsen zijn, zal het moeten oplezen van een code toch een drempel zijn. Als je in Nederland een corona test wilt, kun je ook liegen over het hebben van symptomen. Je kunt makkelijk zeggen dat je moe bent, hoofdpijn en keelpijn hebt; deze symptomen zijn niet te checken door een arts. Dit liegen over het hebben van symptomen gebeurt al heel veel (meer nog dan het liegen over een alert). Dus mijn verwachting is dat zodra een code nodig zou zijn, de mensen die een test willen en daarvoor bereid zijn te liegen, dan symptomen gaan veinzen in plaats van te claimen een CoronaMelder alert te hebben gehad.

Persoonlijk kan het mij niet zo veel schelen dat mensen zonder symptomen een test krijgen door te liegen (sorry). Ik ben namelijk voor het beschikbaar maken van testen aan iedereen die dat wil. Maar dat heeft even niks met de CoronaMelder te maken. Wat mij wel kan schelen is dat er behoorlijk onderzoek naar de effectiviteit van CoronaMelder plaats kan vinden. Dat is nodig om de CoronaMelder te testen, te monitoren & te sturen en evt ook af te schaffen. Daarom is het belangrijk toch een drempel op te werpen, een meldcode dus, gebaseerd op een of ander dagelijks getal dat van de TEK server komt.

Het kan natuurlijk zijn dat er toch mensen een website bouwen om de codes te vervalsen. Een strategie om daarmee om te gaan zou kunnen zijn dit juridisch te verbieden. De CoronaMelder-wet heeft het tegengaan van misbruik in de subtitel. Dit misbruik betreft momenteel slechts het "verplichten tot gebruik van CoronaMelder". Een amendement door toevoeging zou zijn het vervalsen van signalen en codes in CoronaMelder ook strafbaar te stellen. Hiermee zou je ook bluetooth manipulaties en andere ongein strafbaar kunnen stellen. Maar mijn voorkeur heeft deze juridische gang niet.

Om de goede evaluatie en monitoring van de app mogelijk te maken, is het namelijk niet nodig om valse alerts tegen te houden, het is alleen nodig ze "in de smiezen" te hebben. Dan krijgen die mensen nog steeds een test, maar als we weten dat de melding waarschijnlijk vals is, dan kunnen we de melding en testresultaten weglaten uit de evaluatie en monitoring van de effectiviteit van CoronaMelder.

Een mogelijkheid hiertoe is om het 5.1.2e voorstel te volgen, maar in plaats van de dag van besmetting, het huidige timestamp (tijd in uren:minuten) in de code te verwerken. Door een trucje toe te passen, bijvoorbeeld door in de app vanzelf na 1 minuut uit het schermpje met de code terug te gaan, dwing je af dat als mensen de code van de telefoon voorlezen, dat die recent is gegenereerd. De code verandert dus in feit iedere minuut.

Ik stel dus voor om alle codes goed te rekenen als ze cryptografisch goed zijn. Maar mensen die een code oplezen die meer dan 3 minuten "oud" is, spelen dan waarschijnlijk vals en lezen een code voor die van een website komt. Deze gevallen kunnen dan in een onderzoek genegeerd worden. Het websysteem van de GGD moet naast de code natuurlijk het exacte tijdstip waarop de code is doorgegeven correct opslaan. Moet te doen zijn, lijkt me.

Het enige dat ik niet ondervang van jouw kanttekeningen, denk ik, is de laatste: dat de pers aan de haal kan gaan met het idee dat de codes vervalst kunnen worden of worden, en dat de CoronaMelder "gehackt" is. De beste strategie is dan denk ik te downplayen dat dit vaak gebeurt.

met vriendelijke groet,

5.1.2e

PS
Ik neem overigens aan dat het laten zien van de CoronaMelder app, met daarin een alert-status, in de teststraat als confirmatie van recht op de test om goede redenen is afgeschoten als optie om dit te checken -- waarschijnlijk is de status nu onzichtbaar gehouden om corona-paspoort gebruik tegen te gaan. Je zou kunnen zeggen dat dit nu strafbaar is en er een meldpunt voor is dus wellicht is een zichtbaar te maken status toch weer verdedigbaar? Want het tevoorschijn halen van de telefoon, openen van CoronaMelder, en laten zien van de alert status, is ook redelijk bewijs (niet helemaal waterdicht: je kunt natuurlijk met een geroot-te telefoon met een nep CoronaMelder app aankomen, maar veel mensen rooten hun telefoon niet graag en aan zo'n ding komen als die niet van jou is, is wel een gedoe)

----- Original Message -----
From: " 5.1.2e " < 5.1.2e >
To: " 5.1.2e " < 5.1.2e @cwi.nl>
Cc 5.1.2e < 5.1.2e @minvws.nl> 5.1.2e " 5.1.2e @umcutrecht.nl>
Sent: Thursday, September 17, 2020 1:37:14 PM
Subject: 'Meldcode' voor coronamelder notificaties

Ho 5.1.2e

5.1.2e heeft me gevraagd om even contact met je te zoeken m.b.t. de 'meldcode' om na een notificatie een test aan te vragen met iets meer zekerheid dat de aanvrager een melding heeft gehad, zoals je ook aan 5.1.2e gestuurd had.

5.1.2e

5.1.2e Een belangrijke kanttekening is echter dat het, 5.1.2e aangeeft, geen waterdichte code is. Omdat onze ap 5.1.2e is en er geen 'secrets' in zitten is het lastig dit op zo'n manier te doen dat het niet heel makkelijk na te maken is. Iemand zou een site kunnen maken die geldige meldcodes produceert.

We hebben in mei overigens een voorstel naar Apple en Google gestuurd om het protocol uit te breiden met 'validated feedback', een cryptografisch wél waterdichte manier om te valideren dat je een notificatie hebt gehad, zonder de privacy aan te tasten. Dit voorstel heb ik in de bijlage bijgevoegd. Helaas is het nooit door Apple en Google geadopteerd.

Laten we voor nu even uitgaan van een meldcode zoals bij DP-3T. Waar we dan rekening mee moeten houden zijn een aantal dingen:

1) Het proces van aanmelden voor een test moet aangepast worden, die medewerkers moeten een site krijgen waar ze meldcodes kunnen valideren/opzoeken die ze te horen krijgen, en het moet ergens geregistreerd worden (anders heb je er voor de statistiek niets aan).

2) Onze product owners vermoeden dat een meldcode een erg lage drempel is, omdat als je een notificatie wil veinzen maar geen meldcode hebt, je ook gewoon kunt zeggen dat je klachten hebt, dus zij twijfelen of je er daadwerkelijk een drempel mee creeeert.

3) Omdat de methode niet waterdicht is moet iemand gaan monitoren dat er geen sites gemaakt worden waar meldcodes worden uitgedeeld. En daar zou dan aktie op moeten worden genomen (op welke juridische basis?) - dit is ook wat DP-3T in hun voorstel suggereert.

4) Een bijkomend risico bij 3 is dat als de pers ook kan zien dat het systeem niet waterdicht is, je wellicht negatieve pers krijgt rond het feit dat 'de coronamelder gehackt is' - dit is wel een vervelende om te tacklen vermoed ik.

Als we denken dat, ondanks deze kanttekeningen, dit een nuttige route is, dan kan ik hem bij het development team neerleggen en vragen of ze dit gaan inbouwen (op de DP-3T manier).

Hoe denken jullie over bovenstaande kanttekeningen?

(Overigens stelt DP-3T voor om de datum van notificatie mee te nemen in de berekening van de meldcode, ik zie daar niet zoveel meerwaarde in, qua security, want een fake meldcode generator kan dezelfde teks van het cdn downloaden en elke datum in de afgelopen 14 dagen gebruiken om een geldige meldcode te genereren - wellicht is het dan drempelverlagend als de user die datum niet ook hoeft op te geven).

Mvg,
5.1.2e

--
5.1.2e
Egeniq
5.1.2e
5.1.2e
www.egeniq.com
+316 5.1.2e