To: 5.1.2e [5.1.2e@egeniq.com]
Cc: 5.1.2e [5.1.2e@vka.nl]; 5.1.2e)[5.1.2e@minvws.nl]; 5.1.2e. 5.1.2e [5.1.2e@minvws.nl]; 5.1.2e [5.1.2e@cmptr.nl]; 5.1.2e@windmeeadvies.nl[5.1.2e@windmeeadvies.nl]; 5.1.2e 5.1.2e [5.1.2e@igh.com]; 5.1.2e)[5.1.2e@minvws.nl]; 5.1.2e 5.1.2e 1.2e]; 5.1.2e [5.1.2e@5.1.2enl]; 5.1.2e [5.1.2e@gmail.com]
From: 5.1.2e
Sent: Sat 2/6/2021 3:37:41 PM
Subject: Re: Nav suggestie privacy / fraude in community te bespreken
Received: Sat 2/6/2021 3:42:26 PM

Verzoek SMS toevoegen -- Nobel verzoek - en ik zie wel een set van gevallen waarin dit de zaak wezenlijk beter maakt. De analyse of dit ook proportioneel is (en de noodzaak tot extra opslag PII en te de extra observatie van medische data van een hele trits (niet USA) partijen) is goed meegewogen en uitgezocht ? En is die al opgeschreven ?

En omdat we met SMS dan het relatief open & onveilige SS7 land zijn - zou ik ook uit beleefdheid dit ***vooraf*** doornamen met de diverse diensten - zodat zij later geen te snelle afkeurende reactie hebben. En dat je dan moet praten als brugmans.

Want ander zou ik daar even heel erg voorzichtig mee zijn / dit beslist nog niet doen.

5.1.2e

> On 6 Feb 2021, at 12:26, 5.1.2e <5.1.2e@egeniq.com> wrote:
>
> Hoi,
> Voor die anti-fraude is ook relevant: op verzoek van 5.1.2e hebben we sms verificatie toegevoegd aan het protocol. De testaanbieder kan (*), op het moment dat je in de app het testbewijs inlaadt, een 4 cijferige code per sms (of email) naar de persoon sturen, en de app zal daar dan om vragen voordat het bewijs wordt opgehaald. Als in een eerdere fase een test resultaat is doorgegeven aan een ander, zorg je zo dat je nog steeds een code hebt die op het laatst mogelijke moment naar de telefoon van de geteste persoon is gestuurd. (ook niet 100% waterdicht maar een 'doorgever' moet veel bewuster fraude plegen)
>
> In het community document zou ik willen suggereren dat het duidelijk aangeeft dat het om *balans en proportionaliteit* gaat. Wil je misbruik dusdanig graag voorkomen dat je bereid bent een 'identificatieplicht' in te voeren? Of accepteer je dat je omwille van de privacy 99% waterdicht bent. Ook epidemiologisch belangrijk: wat betekent het voor de verspreiding van het virus als 1 op de x bezoekers toch besmet zou kunnen zijn? (en moet je dat wel technisch willen afdichten, als ook een testresultaat er al naast kan zitten?)
>
> Overigens ligt het 'testaanbieder aansluit protocol' ter review bij 5.1.2e en 5.1.2e als die goed is gekeurd wil ik die ook op github zetten en aan de community vragen of ze referentie implementaties willen maken die aanbieders kunnen helpen sneller aan te sluiten.
>
> Mvg,
> 5.1.2e
>
> *) omdat dit wel meer moeite is voor de testaanbieder is het vooralsnog optioneel en niet verplicht, als ze op andere manier ervoor zorgen dat het 'token' niet zomaar door jan en alleman kan worden ingelezen.
>
> Op za 6 feb. 2021 om 12:11 schreef 5.1.2e <5.1.2e@5.1.2e>:
>
> > Uitstekend / goed idee om dit met de gemeenschap te bespreken.
> > Dit soort gesprekken hebben diverse doelen; en hebben ***ook*** een groot element van stakeholder management in zich. Dus uitleggen, verklaren, betrekken, etc. Naast de in dit document goed beschreven aspecten.
> > Daarvoor is het van belang dat de partijen op de juiste manier betrokken en van informatie voorzien worden.
> >
> > Tevens is er een kennis gap - en moet je de mensen uit het veld die meteen met hun (foute) aannames komen - helpen die aannames goed te krijgen. Zodat zij inhoudelijk je gaan helpen - en men niet (meeteen (en terecht)) het gevoel heeft dat je iets achterhoud - dus dat zij zich open moeten op stellen - terwijl jij met

duveltje-uit-doosje replieken komt.

Om deze reden lijkt het mij uiterst verstandig om **éérst** de crypto tell & reveal te doen (die dus afgelopen vrijdag hand moeten zijn - maar verschoven is).

Daarnaast is het van belang het speelveld juist te definieren.

Security engineering is, in de eerste plaats, engineering. Het maken van de juiste *compromissen*. Want 'alles wat een mens maakt, kan door een mens kapot gemaakt worden'. Geen enkel systeem is ooit volledig veilig. En mensen (en zeker stakeholders wier message je niet controleerd) tegen elkaar laten opbieden in slimmigheid hoe iets stuk kan - levert je zelf niet meer dan dat op `hoe het stuk kan'. Want het is triviaal te vertellen hoe je iets kan kraken. De kunst is om te zorgen dat het systeem als geheel niet 'te' kraakbaar is in het licht van de actoren en hun motiviaties*.

Maar het levert de gemeenschap allereij emoties, ingraven, teleurstelling, aggressie, gevoel van `de overheid kan ook niets', etc op (en ik pick hier niet specifiek de Overheid - binnen de open source Apache Software Foundatation doen we zo'n 100 vulnerability rapporten (CVE)'s per jaar - en daar is de situatie exact zo). En dat wil je niet - dan ben je weken verder voordat je een normale dialoog hebt.

En die gaat in eerste instantie over **wat je kraken** vindt. Want of "ik mijn telefoon aan mijn neef uitleen (zelfde voorletters en we lijken echt op elkaar)" of dat "ik een justitie/bomb-proof website in rusland heb waar je voor 5 euro een schone app kan downloaden" - is niet altijd allebij even erg.

Om deze reden lijkt het me verstanding dat je begint met (een dialoog over) het model van de dreigingen, de actoren en hun motivatie en (beperkingen van) methodes - alsmede het doel van je beveiliging - en waarom dat op dat niveau is (je huis heeft immers ook geen kluisdeur; een test certificaat is 48h geldig, etc).

Dat heeft boven dien als benefit dat dat type feedback van de gemeenschap je vaak wel tal van dingen verteld die je zelf niet wist - of dat men je helpt inschattingen te veranderen.

De dialoog aangaan zonder dit voorwerk lijkt me onverstandig - en zal in mijn ervaring leiden tot een negatieve spiraal waarbij mensen aantonen dat het 'toch nooit kan' (of dat de boodschapper c.q. de overheid 'het weer niet snapt'). En waarna je de gemeenschap zo besmet hebt dat je niet meer het soort hulp van ze krijgt dat waardevol is.

Met vriendelijke groet,

5.1.2e

* Voorbeeld uit de coronamelder: Google en Apple hadden de nodige gaten in hun copie van DP3T. Een deel daarvan is publiek in de gemeenschap gefixed. Maar een ander deel was lastiger. Echter - uit het model van de actoren en hun motieven kwam vrij duidelijk naar voren dat de relevante dreingingen van actors een locale/technisch-nieuwschierige motivatie zouden hebben; not direct een zwaar activistische, publieke of financiele. Om die reden is er toen gekozen voor het heel stil inlichten van Apple en Google, ze op de hoogte te houden van de vorderingen bij de CCC en te zorgen dat de uiteindelijke publieke responsible disclosure maanden later netjes via die gemeenschap kwam. Het net resultaat was een gemeenschap die zich erkend voelde, gedurende de hele periode ging meedenken over de engineering overall en daarna nog een heel stel andere waardevolle bijdrages deed.

On 6 Feb 2021, at 10:48, 5.1.2e <5.1.2e @vka.nl> wrote:

Dag allemaal,

Vrijdag kwamen 5.1.2e en ik nav wat vragen over het totale security concept tot de

suggestie om de community te betrekken bij de vraag hoe we 'privacy vriendelijk' en 'fraude bestendigheid' kunnen verenigen. Tot nu toe hebben we met name gekeken vanuit technisch/security/privacy perspectief, maar 5.1.2e heeft daar vrijdag ook nog een beleidsmatig perspectief aan toegevoegd.

Komende woensdag om 16.00 vindt deze afstemming in de community plaats, ik heb vooralsnog een save-the-date hiertoe in de agenda's geplaatst van 5.1.2e

Bijgaand heb ik proberen samen te vatten waar we het woensdag over willen hebben. @ 5.1.2e 5.1.2e, @ 5.1.2e en @ 5.1.2e – uitdaging is natuurlijk de juiste context te schetsen, de juiste vraag te stellen én voldoende Jip-en-janneke te blijven. Is dit goed gelukt? Want dan kunnen we deze gebruiken als inhoudelijke basis voor het gesprek.

Voor de anderen – ter info.

Fijn weekend,
5.1.2e

<image252439.png>

<image161376.png>

<image086242.png>

<image019603.png>
<Community - testbewijs - fraude.docx>

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