To: 5.1.2e)[5.1.2e @minvws.nl]
From: 5.1.2e)
Sent: Mon 2/8/2021 8:59:32 AM
Subject: FW: vervolg Security aspecten app3 5.1.2h
Received: Mon 2/8/2021 8:59:33 AM
DepV-TLPAmber Dreigings- en risicoanalyse CoronaTester -werkversie.docx
DepV-TLPAmber Matrix actoren-tbb CoronaTester - werkversie.xlsx

5.1.2e

Formeel advies lijkt mij wenselijk, eens?
Argumentatie:
- de app vraagt testresultaten op bij testaanbieders
- publiek vertrouwen in geding
- bewust saboteren / frustreren van de app kan leiden tot onrust

5.1.2e

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 8 februari 2021 09:38
Aan: 5.1.2e) < 5.1.2e @minvws.nl>
CC: 5.1.2e < 5.1.2e @vka.nl>
Onderwerp: RE: vervolg Security aspecten app3 5.1.2h

Hoi 5.1.2e

Nog even een update, beetje uitgebreid maar leek me handig gezien deze week mijn laatste week is voor ik 5.1.2e

- Ik heb de dreigingen obv meeting vorige week verwerkt in het document, zie bijlage.
- Vrijdag heb ik met 5.1.2e gesproken, hij werkt nog aan de security architecture. Op basis daarvan volgt verdere aanscherping van maatregelen en restrisico's. Ik heb met 5.1.2e afgesproken dat ik de maatregelen niet in detail uitwerk voor zover die ook al in de security architecture staan.
- Er zijn nog wat losse eindjes in de analyse, zoals de beschrijving van de oplossing en een betere analyse van de actoren op basis van de lijst van DW. Pak ik vandaag op!

Ik probeer 5.1.2e vandaag ook even te spreken hierover om te zien hoe ver we zijn, wellicht kan ik obv zijn eerste versie al veel van de maatregelen en restrisico's aanscherpen. Ik stuur sowieso vanmiddag nog een nieuwe versie naar de aanwezigen bij het overleg vorige week om op te schieten.

Dan nog even over het vervolg:

- Het lijkt me goed om advies van 'de diensten' in te winnen op basis van deze analyse. Ik heb dat in januari al bij hen aangekondigd en afgestemd. Het gaat dan om hun expertadvies (BZK/NCSC), dat doen we in een sessie van +/- 2 uur (geen WebEx/videoconf, maar fysiek is dat); zijn ook mensen van VWS bij (bv 5.1.2e).
- Als we willen kunnen we ook een formeel advies krijgen, maar ik heb afgesproken met hen dat alleen te doen als er zwaarwegende redenen zijn. Dat kan bijvoorbeeld verband houden met de gevoeligheid van het traject, grote risico's of een hoge mate van zekerheid die we als VWS willen. Zo'n formeel advies kost de diensten veel tijd dus vandaar dat we de lat in samenspraak hoog hebben gelegd hiervoor. Ter info: Voor CoronaMelder en GGD Contact is wel zo'n advies gegeven.
- Ik kan een sessie voor advies gaan plannen. Probleem is dat ik twee weken vrij ben vanaf maandag 15/2. Ik kan kijken of we donderdag of evt woensdag de sessie kunnen beleggen. Als dat niet lukt moet iemand anders uit het team dit overneemt.

Groeten,
5.1.2e

5.1.2e ; 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: donderdag 4 februari 2021 09:28
Aan: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e < 5.1.2e @vka.nl>
Onderwerp: RE: vervolg Security aspecten app3 5.1.2h

Hi 5.1.2e,

Dank voor snelle eerste en gedegen versie. Mooi om te zien dat we het eerdere werk voor BRBA en CM kunnen hergebruiken.

Wat mij betreft zeker op de goede weg, waarbij de grootste behoefte nu is aan goede gedegen extrapolatie van specifieke dreigingen en risico's die horen bij CoronaTester en de analyse of de maatregelen afdoende zijn (de lijst van DW hieronder). Dus welke maatregelen moeten we nemen / hebben we genomen voor het risico van:
- Onderlinge overdracht / kopiëren / vermenigvuldiging van geldige testbewijzen (op verschillende manieren: screenshot / movie, overdracht telefoon, inloggen met elkaars digid, etc)
- Een commerciële testaanbieder die fake testen verkoopt die in de app omgezet worden tot geldig testbewijs
- gemanipuleerde QR codes die verifier app frustreren
- etc.

Daarbij speelt dat we specifieke privacy eisen hebben geformuleerd én alles open source willen. Precies die combinatie sluit bepaalde maatregelen uit en dat maakt het ontwerpproces uitdagend.

Kan je vanavond om 20:00 aanhaken bij de tech discussie hierover? 5.1.2h

---

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: woensdag 3 februari 2021 22:34
Aan: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e < 5.1.2e @vka.nl>
Onderwerp: RE: vervolg Security aspecten app3 5.1.2h

Hoi,

Ik heb een eerste slag gemaakt met het volgende:

- Opzet voor dreigings- en risicoanalyse (word document)
- Dreigingsmatrix met inschattingen van de waarschijnlijkheid van een bepaalde dreiging
- Aantal van de meest waarschijnlijke scenario's (paragraaf 2.3/pag 7)
- Algemene maatregelen (standaardsetje uit eerdere oplossingen)

De scenario's heb ik nu vooral benoemd, maar nog niet uitgewerkt. Daar ga ik hierna mee verder. Dat gaat vrij snel over het algemeen, de maatregelen en restrisico's duren het langst om volledig in kaart te brengen. Ik probeer de scenario's te omschrijven in (mogelijke) specifieke varianten/variaties die ook direct te gebruiken zijn in een FMEA.

Het lijstje van 5.1.2e in de lijst hieronder passen binnen deze scenario's (maar moet ik daar nog als varianten onder benoemen – komt nog vrijdag of dit weekend).

Lijst met scenario's is natuurlijk ook uit te breiden.

Tot zover, ik hoor graag of dit een beetje op de goede weg is en wat jullie voor ogen hadden!

Groeten,
5.1.2e

5.1.2e: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: woensdag 3 februari 2021 15:25
Aan: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e < 5.1.2e @vka.nl>
Onderwerp: RE: vervolg Security aspecten app3 5.1.2h

Super!

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: woensdag 3 februari 2021 15:07
Aan: 5.1.2e < 5.1.2e @vka.nl>; 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: vervolg Security aspecten app3 5.1.2h

Dank 5.1.2e ☺
Ik zet er vaart achter 5.1.2e Ik heb al wat materiaal liggen en ga er vanavond meer verder.

Groeten,
5.1.2e

5.1.2e : 5.1.2e < 5.1.2e @vka.nl>
Verzonden: woensdag 3 februari 2021 14:38
Aan: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: vervolg Security aspecten app3 5.1.2h

Ik kom een beetje voor 5.1.2e op (kan ie zelf ook, maar dit hadden we al afgesproken): hij levert vrijdag versie 1 op. Daarna kan het iteratief.

5.1.2e
5.1.2e
VERDONCK KLOOSTER & ASSOCIATES
M: +31 6 5.1.2e
T: +31 79 5.1.2e
www.vka.nl

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: woensdag 3 februari 2021 13:17
Aan: 5.1.2e < 5.1.2e @vka.nl>; 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: vervolg Security aspecten app3 5.1.2h

Mooi!

Fijn 5.1.2e, er zit flinke urgentie op, kunnen we iteratief opleverproces afspreken? (elke dag een versie)?

Van: 5.1.2e < 5.1.2e @vka.nl>
Verzonden: woensdag 3 februari 2021 12:55
Aan: 5.1.2e < 5.1.2e >; 5.1.2e @cmptr.nl; 5.1.2e < 5.1.2e @mobach.nl>; 5.1.2e < 5.1.2e @dewinter.com>; 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e < 5.1.2e @egeniq.com>
CC: 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: FW: vervolg Security aspecten app3 5.1.2h

Dag allemaal,

5.1.2e gaat ons helpen om structuur te houden in de risicoanalyses's en de afwegingen die we maken.

5.1.2e

5.1.2e
5.1.2e
VERDONCK KLOOSTER & ASSOCIATES
M: +31 6 5.1.2e
T: +31 79 5.1.2e
www.vka.nl

Van: 5.1.2e <5.1.2e>
Verzonden: dinsdag 2 februari 2021 21:47
Aan: 5.1.2e <5.1.2e @minvws.nl>
CC: 5.1.2e <5.1.2e @dewinter.com>; 5.1.2e <5.1.2e @mobach.nl>; 5.1.2e @cmptr.nl; 5.1.2e <5.1.2e @vka.nl>; 5.1.2e <5.1.2e @egeniq.com>
Onderwerp: Re: vervolg Security aspecten app3 5.1.2h

Hieronder denk ik de nog relevante dingen van de security lijst - met toevoeging in E.

5.1.2e

A. Faking/cloning results

general
- local down to time (and/or place)
- Show the 'frog' and other memnonics
- repeat detection (small/local scale - or with care - at larger scales)
- normal appstore/apple/google ecosystem protection

screenshots
- Animations
- Moire patterns that break jpeg

Movies
- Rythm, timing that the eye is sensitive for
- Moire patterns that break jpeg
- Color gamut

Photos/recordings
- Moire for bayer-patterns and lenzes

interactive counterfeit measures

Live screensharing
Moire patterns that break jpeg
interactive counterfeit measures

B. Cloning Apps / building good looking copies

Small scale - no business case
faking it web/low code base
sophistication of animations/counterfeit measures
most of section A.

C. Cloning Apps / (using open source version of verifier)

Small scale - no business case
(developer; using dev-cert to roll out to 10's of friends)
relatively little really
SIM card / attestation specials.

Medium scale - business case
general ecosystem management/monitoring
make it too expensive (A) for the business case
churn

Large scale / well funded (using open source version of verifier)
all of above
ecosystem management & monitoring; relying on walled garden.

D. Passing on the phone
local down to time (and/or place)
repeat detection (small/local scale - or with care - at larger scales)

G. Moving key material from one phone to another (usually jailbroken).
normal ecosystem protection.
relatively little really
SIM card / attestation specials.

F. Using someone else their phone (in isolation)
show first initials
show photo (locked to either the app/phone -OR- locked to the issued certificate)
lock phone temporarily to something circumstantial (e.g. colour of coat, sweater, etc, or to a photo just made that is locked for the next hour once Qr is shown).

J. Repeat activation with one test:
tie in with DigiD
use something unique in test & keep 'used up' list for 48 hours