Technische kanttekeningen bij een contact-tracing app

Maarten van Steen
Hoogleraar Grootschalige Gedistribueerde Computersystemen
Wetenschappelijk Directeur Digital Society Institute, Universiteit Twente

In dit position paper stel ik dat er meer geprioriteerd moet worden op een aantal hardnekkige en wellicht onoplosbare technische problemen die eerst opgelost moeten worden willen we smartphones inzetten voor nabijheidsmetingen. In het bijzonder stel ik dat nu vooral gekeken moet worden naar de inzet van smartphones voor het detecteren van het feit of een besmet persoon in iemands buurt is geweest. Problemen rondom privacy lijken oplosbaar, maar verdienen nu wellicht meer specifieke aandacht.

Er is in de aanloop naar mogelijke apps die helpen bij het bestrijden van de verspreiding van het COVID-19 virus al veel gezegd en geroepen. Een probleem hierbij is dat de inzet van een dergelijke app veel verschillende kennisgebieden bestrijkt: sociale wetenschappen, recht, psychologie, epidemiologie, beveiliging, informatietechnologie, om maar eens een aantal te noemen. Deze multidisciplinariteit bemoeilijkt doorgaans besluitvorming: er zijn gewoon veel aspecten waar rekening mee gehouden dient te worden.

Het helpt hierbij om te prioriteren op die deelproblemen die niet evident oplosbaar lijken te zijn, maar waarbij die oplossing wel onvoorwaardelijk nodig is voor de effectieve inzet van een app. Daarbij is het essentieel dat het specifieke probleem, hoe ingewikkeld het ook lijkt, klip en klaar uitgelegd wordt, als ook een eventuele oplossing, en wel zo dat ook niet-deskundigen op het specifieke probleemgebied, maar die uiteindelijk wel besluiten moeten nemen, inderdaad goed geïnformeerd zijn.

Informatietechnologische toepassingen, en vooral de apps op smartphones, zijn tegenwoordig dikwijls verbluffend eenvoudig te bedienen en bieden bovendien ook nog eens een enorme krachtige functionaliteit. Zo ook verschillende beoogde COVID-19 apps. Echter, juist voor dergelijke apps waar veel verschillende meningen over zijn is het essentieel te begrijpen wat er zich onder de motorkap bevindt.

Er spelen hierbij minstens drie aspecten:

1. De inzet van een smartphone als meetinstrument.
2. Het technische protocol voor detectie, registratie en disseminatie van informatie over besmettingen.
3. De implementatie van dat protocol in de vorm van een app.

De smartphone als meetinstrument

Voor contact tracing is het belangrijk dat we kunnen vaststellen of iemand gedurende enige tijd in de fysieke nabijheid is geweest van een geïnfecteerde persoon. Doordat veel mensen een smartphone bij zich dragen, is het idee om deze in te zetten als instrument om te bepalen of mensen bij elkaar in de buurt zijn geweest. Om technische, maar ook niet-technische redenen vallen inmiddels technieken af die gebaseerd zijn op locatiebepaling. Er wordt daarom nu door veel ontwikkelaars gekeken naar directe detectie door middel van Bluetooth. De essentie is dat smartphones met Bluetooth met een bepaalde regelmaat signalen uitzenden, maar ook dat die signalen een beperkte reikwijdte hebben van enkele tientallen meters. Het ontvangen van een signaal betekent dat er een smartphone in de buurt is. De sterkte van het ontvangen signaal kan door de ontvanger gemeten worden en zou indicatief kunnen zijn voor de feitelijke afstand.

Het probleem is dat het uiterst lastig is, wellicht zelfs praktisch onmogelijk, om met een gewenste nauwkeurigheid te bepalen hoe dicht een smartphone in de buurt is. Bluetooth signalen zijn, net zoals alle radiosignalen, (dikwijls zeer) gevoelig voor omgevingsinvloeden. Daarom maakt het uit of het bijvoorbeeld regent, of waar een smartphone op het lichaam gedragen wordt. Ook maakt het uit of men op een open plein loopt, zich in een kamer bevindt, op een gang loopt, etc. De kwaliteit van de gebruikte antennes, en die per telefoon kunnen verschillen, zijn ook van invloed op de kwaliteit van het Bluetooth signaal. Signalen correct interpreteren zal nauwkeuriger kunnen plaatsvinden op basis van eerdere calibratiemetingen, metingen die bovendien omgevingsinvloeden zullen moeten meenemen. Vervolgens zal een smartphone ook nog automatisch moeten kunnen detecteren in welke soort omgeving het zich bevindt. Daarbij komt dat het feitelijk onmogelijk is om op basis van een ontvangen signaal vast te stellen of een detectie zelfs relevant is: Bluetooth signalen gaan door muren en andere COVID-19 beschermende barrières.

Kortom, er is voldoende reden om te twijfelen aan de effectieve inzet van een smartphone als instrument om te meten of iemand binnen het gebied van een geïnfecteerde persoon is geweest waar overdracht van het virus zou kunnen plaatsvinden. Wordt een smartphone toch ingezet, dan dient rekening gehouden met enerzijds veel onterechte detecties (omdat de ontvanger buiten het overdrachtsgebied was), maar ook veel gemiste detecties (binnen het overdrachtsgebied, maar het signaal is niet overgekomen). Het is vooralsnog onduidelijk hoe groot deze onnauwkeurigheid is, of die nauwkeurigheid op een gewenst niveau te krijgen is, maar ook in hoeverre die nauwkeurigheid van belang is.

Ik acht momenteel dit probleem een serieus obstakel voor de effectieve inzet van een COVID-19 app voor nabijheidsmetingen. Het probleem zal eerst op bevredigende wijze opgelost moeten worden.

Het technische protocol

Er is al veel gezegd over de eisen waaraan een technisch protocol voor detectie, registratie en disseminatie van besmettingen moet voldoen.[1] Privacy en beveiliging staan hierbij voorop. Er lijkt hiervoor een oplossing te zijn. De kern ervan kan als volgt samengevat worden:

- Een COVID-19 app genereert een nieuwe en voor de smartphone wereldwijde unieke ID waaruit op geen enkele wijze persoonsgevoelige informatie valt te destilleren.
- De COVID-19 app zendt via Bluetooth een ID uit, en ontvangt de IDs van andere apparaten. Het slaat lokaal, op de telefoon, de ontvangen IDs op.
- Wanneer iemand besmet is, meldt hij/zij dit via de app, en de app geeft de ID door aan de centrale server. De melding gaat samen met een autorisatiecode (zoals de wellicht nog bekende TAN codes bij bankverkeer) van een BIG-geregistreerde zorgverlener voor validatie dat de persoon inderdaad positief getest is.
- De app gaat ook regelmatig (zeg 1 of 2 keer per dag) naar de server en haalt alle IDs op waarvan men weet dat die horen bij geïnfecteerde personen, om vervolgens lokaal deze lijst te vergelijken met ontvangen IDs om vast te stellen of er een besmetting plaatsgevonden zou kunnen hebben.

Dit is een korte samenvatting van het zogeheten Decentralized Privacy-Preserving Proximty Tracing protocol (DP3T).[2] Ik laat belangrijke details weg die nodig zijn om de privacy en beveiliging beter te borgen dan hierboven geschetst. Echter, het belangrijke is dat het protocol uit te leggen is aan niet deskundigen (de ontwerpers hebben zelfs een waarheidsgetrouwe strip opgetekend), maar ook dat aannames expliciet gemaakt zijn, zoveel mogelijk ontwerpkeuzes toegelicht zijn, en ook zoveel mogelijk bekeken is waar eventuele zwakheden zitten die extra bescherming vereisen. Kortom: het protocol is openbaar en vooral transparant. Het kan dus door partijen met verschillende achtergronden op voorhand geïnspecteerd worden.

Vanuit mijn eigen expertise (met een focus op grootschalige gedistribueerde en dikwijls draadloze computersystemen) stel ik vast dat we hier met een schaalbaar ontwerp te maken hebben waarin minimale informatie op centrale plekken ligt. Vanuit diezelfde expertise heb ik het sterke vermoeden dat het protocol privacy volledig bewaakt en bovendien veilig is, maar weet dat er andere experts zijn (met een focus op technische privacy en beveiliging) met jarenlange training en onderzoek die hier een scherper oog voor hebben dan ikzelf.

Daarmee concludeer ik (voorlopig) dat een technisch protocol voor detectie, registratie en disseminatie van informatie over besmettingen niet in de weg staat voor de effectieve inzet van een COVID-19 app voor nabijheidsmetingen. Echter, het is essentieel dat juist technische privacy- en beveiligingsexperts het protocol inspecteren.

De feitelijke implementatie

Een protocol is een specificatie, uiteindelijk komt het aan op de realisatie daarvan in de vorm van een app. Laten we uitgaan van het feit dat het DP3T protocol aan de gewenste eisen voldoet. Wie garandeert mij dat een app ook daadwerkelijk het DP3T protocol geïmplementeerd heeft? Of dat die implementatie correct is, dat er geen extra "features" bedoeld of onbedoeld in de implementatie beland zijn, en vooral, dat de implementatie ook beveiligd is? Welke app we ook zullen inzetten, de broncode zal geïnspecteerd moeten kunnen worden door onafhankelijke specialisten. Zonder de transparantie zoals bij DP3T zullen gebruikers moeten vertrouwen op de ontwikkelaars. Voor COVID-19 apps acht ik dit laatste volstrekt onwenselijk.

De keuze om de broncode van een app openbaar te maken is terecht en essentieel. Van die keuze mag niet afgeweken worden. Wel is het van belang dat ook hier experts daadwerkelijk aan het werk gezet worden om die broncode te inspecteren en te valideren.

Credits

Dit paper was niet tot stand gekomen zonder de inzet van veel collega's, maar in het bijzonder die van Prof.dr.ir. Bart Nieuwenhuis, hoogleraar Telematica Services, die de drijvende kracht is bij de Universiteit Twente als het gaat om corona contact tracing. Prof.dr.ing. Paul Havinga, expert o.a. op het gebied van draadloze communicatie en sensornetwerken, heeft bijgedragen aan de articulatie van een aantal belangrijke technische aspecten, vooral met betrekking tot de inzet van smartphones als meetinstrument.

---

[1] Zie bijvoorbeeld het EU rapport "Mobile applications to support contact tracing in the EU's fight against COVID-19", dd. 15 april 2020.

[2] Zie https://github.com/DP-3T/.