Statsministeren <stm@stm.dk>
Sundhedsministeren <magnus.heunicke@ft.dk>
Cc:
Sundhedsudvalget https://www.ft.dk/da/udvalg/udvalgene/suu/kontakt
IT-ordførere: ida.auken@ft.dk; karina.dehnhardt@ft.dk; dennis.flydtkjaer@ft.dk;
eva.flyvholm@ft.dk; torsten.gejl@ft.dk; mona.juul@ft.dk; kasper.roug@ft.dk;
christoffer.melson@ft.dk
Sundhedsstyrelsen <sst@sst.dk>
SSI <serum@ssi.dk>

København d. 2020-04-07

App til smitteopsporing med privatlivsbeskyttelse

Vi skal have COVID-19 under kontrol. Hvis vi kan bruge IT til at hjælpe os med det, så bør vi overveje, om der ikke kan laves en fornuftig løsning, der kan hjælpe til med at bremse smitteudbredelsen. Med en fornuftig løsning mener vi en løsning, som respekteter borgernes privatliv og samtidig opfylder behovet for at få spredningen under kontrol.

PROSA vil med denne henvendelse gøre opmærksom på, at en sådan løsning er mulig, og vi vil også skitsere, hvordan den kan se ud.

Flere lande (Kina, Singapore, og Norge) har allerede udviklet apps til at hjælpe med smitteopsporing.

Desværre har de nuværende løsninger ikke indbygget privatlivsbeskyttelse: Borgerne er nødt til at stole på, at myndighederne ikke bruger data på en måde, som borgeren ikke ønsker, eller ikke har givet tilladelse til. Det betyder, at folk, der er kritiske overfor overvågningen, næppe vil installere appen.

Det er ærgerligt, for det kan godt lade sig gøre at lave en app til smitteopsporing, som respekterer borgernes privatliv og samtidig opfylder vores behov for at få smitten under kontrol.

PROSA er yderst kritisk overfor brug af data, som er indsamlet med ét formål, men som bliver brugt til noget andet. Desværre er der god grund til at være kritisk.

I 2014 kom det frem, at myndighederne ulovligt havde indsamlet diagnosekoder fra lægerne. Historien blev kendt som DAMD-skandalen – opkaldt efter databasens navn, DAMD. På trods af, at der var enighed om, at der ikke var noget juridisk grundlag for indsamlingen, prøvede nogle at få gjort indsamligen lovlig med tilbagevirkende kraft. Dette er en af grundene til, at flere borgere har mistet tilliden til, at sundhedsmyndighederne kun vil bruge data på en måde, som borgeren forventer.

Men vi kan faktisk godt lave en app til smitteopsporing, som respekterer borgernes privatliv. Noget af det vigtiste er at sørge for, at data ikke bliver samlet hos en myndighed, men i stedet ligger ude hos borgerne selv. Det kan lyde overraskende, at dette kan lade sig gøre, men designet er beskrevet nedenfor.

Brugseksempel

Amalie er på legepladsen med sin mor (Alice), hvor hun leger med Birgitte. Birgittes far (Bob) er også på legepladsen. Hverken Amalie eller Birgitte har mobiltelefoner, men det har Alice og Bob. Alice og Bob kender ikke hinanden.

På et senere tidspunkt bliver Amalie syg og får konstateret COVID-19. Da Alice jævnligt er i fysisk kontakt med Amalie, så kan Alice også være smittebærer. Derfor klikker hun i appen: ”Jeg er muligvis smittebærer”.

Bob får via appen information om, at han har været i kontakt med en mulig smittebærer. Appen fortæller ham tid og sted. Bob kan se, at det var på legepladsen, og kan huske, at Birgitte var med. Derfor kan Birgitte også være blevet smittet.

Herefter kan Bob fortælle Birgitte og andre, som var med på legepladsen, at de muligvis er blevet smittet, og han kan ringe til sin læge og spørge, hvordan han skal forholde sig.

Mulig udvidelse: For at undgå at alle og enhver blot hævder, at de er smittede, kan Appen udvides, så lægen kan bekræfte, at Alice er mulig smittebærer. Beskeden til Bob kommer så til at indeholde, at dette er bekræftet af en læge.

Mulig udvidelse: Hvis borgerne gerne vil dele information til myndighederne, så kan de bede Appen sende alle data til myndighederne. Dette skal dog være borgerens eget valg.

Simpel teknisk beskrivelse

Alices mobiltelefon søger konstant efter mobiltelefoner i nærheden, som har Appen installeret. Det har Bobs mobiltelefon.

Når Alices telefon opdager det, så giver den Bob anonyme kontaktoplysninger (lidt svarende til en emailadresse) samt et tilfældigt tal. Bobs telefon registrerer kontaktoplysningerne og det tilfældige tal.

Herefter registrerer Alices telefon:

- Det tilfældige tal, som er givet til Bobs telefon
- Tidspunkt
- Sted
- Afstanden til Bobs telefon
- Hvor lang tid telefonen er i nærheden af Bobs telefon

Bobs telefon gør det tilsvarende over for Alices telefon.

Hvis Alice senere klikker ”Jeg er mulig smittebærer”, så løber telefonen alle de registrerede kontakter i gennem og sender dem en besked. Beskeden indeholder det tilfældige tal, som kom fra

kontakten. Da Bobs telefon har registereret tid og sted sammen med det tilfældige tal, så kan Bobs telefon også fortælle Bob præcis, hvor og hvornår kontakten fandt sted.

Mulig udvidelse: For at undgå at alle og enhver blot hævder, at de er smittede, kan Appen udvides, så lægen kan bekræfte, at Alice er mulig smittebærer. Det sker ved at lægen digitalt underskriver et brev. Brevet indeholder Alices anonyme kontaktoplysninger, og Alices app sender herefter beskeden til Bobs telefon. Lægen får altså ikke kendskab til Bob. Beskeden til Bob kommer så til at indeholde, at dette er bekræftet af en læge.

Mulig udvidelse: Myndighederne kan opdatere information om, hvor lang tid og hvor tæt Alice skal have været på Bob, før det skal betragtes som en mulig smitterisiko. Måske er det vigtigere, at man har været tættere end at man har været samme sted i flere timer. Alice kan så vælge, om Appen skal følge disse anbefalinger (default) eller lade være. Anbefalingerne kan ændres af myndighederne dagligt. Alices telefon henter de nyeste anbefalinger dagligt.

Teknisk beskrivelse

I det følgende er A = Alices telefon og B = Bobs telefon.

Appen tænder Bluetooth på A og scanner efter andre Bluetooth enheder i nærheden. Når den finder B, så kontakter den B og spørger, om Appen er installeret.

Hvis Appen er installeret, så sættes en Tor-hidden service op på A. URLen for denne hidden service er den anonyme kontaktoplysning. Man kan altså forbinde sig til den URL uden at vide, hvem der står bag. Ved at bruge Tor-hidden services er der ikke en central myndighed, der ”ved alt”. Viden er i stedet distribueret ud hos de enkelte telefoner.

Den anonyme kontaktoplysning sender A sammen med et 256-bit tilfældigt tal (et token) til B, som registerer dette.

Afstanden mellem A og B estimeres med signalstyrken af B’s Bluetooth signal. Det er ikke helt præcist, men kan dog give en indikation af afstanden.

Herefter logges tid, sted og styrken af B’s Bluetooth signal hvert minut kædet op på det token, som A har givet B.

Hvis Alice klikker, at hun er mulig smittebærer, så finder A alle kontakter, og via B’s anonyme Tor hidden service, kontakter A B, og oplyser det token, som A tidligere har givet til B.

Da ingen andre end A kan have givet det token til B, så ved B, at det kun kan komme fra A. B kan desuden finde de registreringer, som B har lavet, der er kædet til A’s token. Dermed kan B oplyse Bob om tid og sted.

Mulig udvidelse: Myndighederne kan opdatere information om, hvor lang tid og hvor tæt A skal have været på B, før det skal betragtes som en mulig smitte risiko. A henter de nyeste informationer dagligt. Dette kan ske via Tor, og dermed ved er A anonym over for myndighederne.

Mulig udvidelse: Hvis borgerne gerne vil dele information til myndighederne, så kan de bede Appen sende alle data til myndighederne. Dette kan se via Tor, så Alice ikke umiddelbart kan identificeres. Dog kan man ud fra tid og sted muligvis identificere Alice, og derfor skal Alice oplyses om, at hun ikke længere er anonym.

Mulig teknisk begrænsing: Antallet af Tor hidden services bliver i størrelsesorden antallet af personmøder. Hvis Tor hidden services ikke kan skalere til det, så kan vi gå lidt på kompromis ved at hver telefon kun opsætter én hidden service. Det gør anonymiteten en smule ringere, idet hvis A først har mødt B og derefter C, så kan B og C se, at de begge har mødt A.

Jeg håber derfor, at I vil være med til at arbejde for, at en udviklingen af en app til smittesporing, vil tage udgangspunkt i, at borgernes privatliv repspekteres.

Venlig hilsen

Niels Bertelsen
Formand for PROSA
Telefon: 40 11 41 23