Analyse av muligheter til ytterligere styrking av personvernet i ny Smittestopp

Vi har med interesse fulgt prosessen rundt ny versjon av Smittestopp. Den valgte løsningen er grunnleggende sett solid fra et kryptografi-perspektiv, og gjør det vanskelig å bruke systemet til noe annet enn hovedformålet sitt. Skjønt, ingen systemer er likevel perfekte, og vi sender med dette en delvis analyse av enkelte sider ved Smittestopp 2, og hvordan noen utfordringer kan løses på en måte som kan gi en ekstra beskyttelse av personvernet.

Disse punktene er ikke et resultat av en helhetlig analyse av det som er kjent om systemet. Det kan finnes angrepsvektorer vi ikke diskuterer her. Vi har heller ikke vurdert hvilke ressurser en eventuell angriper vil trenge for å utføre det vi skisserer under, og hvilken verdi det er på informasjonen han eller hun eventuelt greier å samle.

Det kan finnes mange veier for å oppnå de angrepsmålene vi skisserer under, og dette er ikke nødvendigvis de enkleste måtene. Det betyr ikke at de ikke er verdt oppmerksomhet, men det kan også finnes andre tiltak, for eksempel organisatoriske, som det er viktigere å se på først. Vi understreker at de scenariene vi tegner opp under ikke nødvendigvis må regnes som reelle sårbarheter. Analysen vår er basert på en metodikk der vi antar at flere parter kan samarbeide for å avdekke opplysninger om én eller flere utvalgte mål, men uten å vurdere hvorvidt slikt samarbeid er realistisk i virkeligheten.

Vi ønsker også å understreke at det vi beskriver under er spesielle tilfeller med begrensede konsekvenser, og at ingenting av det vi påpeker kan sammenlignes med den mer overordnede personverndebatten rundt første versjon av Smittestopp.

For referanse og etablering av felles begreper og forståelse gir vi et kort overblikk over hvordan vi har forstått at FHI vil bruke Smittestopp 2:

1. Brukere laster ned appen, og aktiverer Exposure Notification System (ENS) på telefonen sin. Telefonen sender ut og mottar roterende smittenøkler. Vi legger til grunn at de smittenøklene telefonen mottar blir håndtert sikkert av operativsystemet og er utilgjengelige for alle andre.

2. Dersom en bruker blir bekreftet smittet, skjer det følgende:
    a. Brukeren forteller appen at den ønsker å laste opp sine smittenøkler til Smittestopp-backend. (I realiteten lastes det opp nøkler som gjør det mulig å generere disse verdiene, men denne forenklingen påvirker ikke den videre teksten.)
    b. Appen viser en innloggingsdialog for helsenorge.no. Hvis brukeren lykkes med å autentisere seg gjøres det et oppslag i MSIS, som svarer tilbake med bekreftelse og smittsom periode.
    c. Helsenorge.no genererer et *token* som sendes tilbake til appen.

    d. Appen sender en datapakke til Smittestopp-backend som består av smittenøkler og det mottatte token.
    e. Smittestopp-backend verifiserer tokenet, og publiserer smittenøklene.

3. Appene til andre brukere synkroniserer sitt register av smittenøkler med den sentrale oppslagstavla, og varsler sine brukere dersom de oppfyller gitte kriterier.

Videre konsentrerer vi oss om tre scenarier der det er mulig å avlede data om brukerne fra forskjellige innfallsvinkler.

1. Utbytte fra trafikkanalyse

Som kjent er Exposure Notification System i stor grad bygd på initiativet *Distributed Privacy-Preserving Proximity Tracing* (DP3T). Den opprinnelige protokollen inneholdt også en funksjonalitet der en app regelmessig ville gjøre en simulert opplasting til den sentrale tjenesten. Målet med en slik opplasting er at den skjuler reelle opplastinger av smittenøkler, og derfor gjør at noen som utfører nettverksanalyse ikke kan oppdage hvem som er reelt smittet. Slik trafikk er enkel å utføre, ettersom vi antar at den uansett vil gå i en kryptert TLS-tunnel. Det holder da å generere tilfeldig data som er like stor som en ekte opplasting, og legge ved en ugyldig token.

Slik vi leser den offentlig tilgjengelige informasjonen om Smittestopp skal det umiddelbart før en opplasting av reelle data foregå kommunikasjon med ID-porten og helsenorge.no. Dersom man ønsker å gjennomføre en slik beskyttelse mot nysgjerrige parter som holder kontroll på nettverkstrafikken vil det også være nødvendig å lage simulert trafikk mot ID-porten.

Det er verdt å merke seg at dette er et avansert angrep med relativt lite utbytte. For å kunne kjøre angrepet effektivt mot mange brukere vil det være nødvendig å ha stort innsyn hos for eksempel en teleleverandør. Dersom man målretter det mer mot enkeltpersoner kan man oppnå det ved å installere spionprogramvare på personens telefon, og som kan overvåke nettverkstrafikken. Da finnes det antageligvis likevel enklere måter å skaffe samme informasjon på. Vi tror likevel det er greit å vite om at en ukritisk implementering av simulerte opplastinger kun til Smittestopp-backend neppe vil gi ekstra sikkerhet i det norske systemet.

2. Kobling av nærkontakter

Vi legger til grunn at Smittestopp ikke skal kunne gi myndighetene innsikt i enkeltpersoners kontaktnett. Det oppnås blant annet ved at Smittestopp-backend bare skal motta et token sammen med smittenøklene, men ikke identiteten til den som laster opp dataene. Et slikt token skal utstedes fra helsenorge.no, som skal hente data fra MSIS om hvorvidt en person er smittet, og hva som er smittefarlig periode. Dersom Smittestopp og helsenorge.no går sammen vil det være mulig å koble de opplastede smittenøklene mot identiteter.

Dersom noen på et senere tidspunkt får kontroll på en telefon med Smittestopp, og ønsker å bevise at eieren har vært i kontakt med en navngitt person som er registrert smittet, vil det være mulig å utsette denne telefonen for kun disse nøklene, og se om den varsler om mulig

smitte. Dette er utenfor formålet til appen, og denne muligheten burde dermed hindres. Det kan også finnes andre angrep som kommer fra muligheten til å koble smitte og identiteter, men vi har ikke sett nærmere på dette.

Vi foreslår løsninger for å eliminere muligheten. Da er det to muligheter, enten ved design, eller gjennom regelverk og begrenset loggføring.

- For det første valget foreslår vi å bruke *Privacy Pass*. Ideen er at brukerens app vil sende en spesielt utformet melding til helsenorge.no. Meldingen består av en hash av en unik tekst, og er i tillegg tilført et ekstra lag med tilfeldighet. MSIS melder tilbake med bekreftelse og tidligste dato for smittsomhet. Basert på den valgte datoen velger helsenorge.no en signeringsnøkkel, og signerer den skjulte meldingen med riktig nøkkel. Når brukerens app får meldingen tilbake kan appen fjerne det ekstra laget med tilfeldighet uten å ødelegge signaturen, og sender så den nye signaturen sammen med den opprinnelige, unike teksten til Smittestopp-backend. Smittestopp-backend verifiserer at alt stemmer, og får derfor garanti for at det er et reelt smittetilfelle. Den får også verifisert hva som var første smittsomme dag, og kan sammenligne det med datostempling på smittenøklene. Ved å loggføre den unike meldingen er man sikret at samme token ikke kan brukes flere ganger.

  Løsningen garanterer at det ikke er mulig å koble en innlogging hos helsenorge.no og en opplasting til Smittestopp utelukkende ved hjelp av et token. Det finnes en rest-risiko ved å sammenligne logger over IP-adresser eller kontakt-tidspunkt. Det kan derfor være formålstjenlig å lage regler som begrenser slik logging.

  De tekniske detaljene, sammen med referanser til den opprinnelige publikasjonen av *Privacy Pass* fra 2018 og foreslåtte parametre, er vedlagt.

- Dersom vår foreslåtte løsning ikke er mulig å implementere på så kort tid, kan mye av det samme oppnås ved at det vedtas regelverk som kraftig begrenser hva som skal logges fra ID-porten, helsenorge.no, MSIS og Smittestopp-backend. Spesifikt vil slik sporing vi har skissert her være umulig dersom det aldri loggføres hvilken identitet som hører til hvilket token. Et slikt regelverk kan også inneholde bestemmelser som gjør det ulovlig å gjøre koblinger mellom dataene til helsenorge.no og Smittestopp.

3. Identifisering av smittede

En særlig kyndig bruker vil kanskje kunne lage sin egen variant av Smittestopp, der han eller hun kan se smittenøklene etter hvert som de blir samlet inn, for eksempel ved å bruke en mikrokontroller med Bluetooth Low Energy som ikke bruker ENS direkte. De kan da samtidig merkes med hvem man er i nærheten av. La oss si at en av disse senere blir bekreftet smittet, og laster opp nøklene sine. Fordi vår kyndige bruker har merket disse, kan han eller hun vite hvem som har blitt smittet.

Dette kan unngås ved å ikke publisere smittenøklene direkte, men i stedet bruke DP3Ts løsning med et Cuckoo-filter. Det gjør det mulig å verifisere at det eksisterer et tilstrekkelig overlapp uten å se direkte på dataene.

I likhet med det første angrepet har dette også begrenset effekt i forhold til innsats.

Vi ønsker lykke til med utviklingen, og står gjerne til rådighet om dere måtte ha spørsmål.

Tjerand Silde,
stipendiat NTNU
tjerand.silde@ntnu.no

Martin Strand,
forsker
martin.strand@ffi.no