Schneller als Corona

Wie Tracing-Apps Covid-19 bremsen sollen

Bei der Lockerung von Kontaktsperren zur Reanimation der Wirtschaft hoffen viele auf die smarte Hilfe von Tracing-Apps. Mithilfe von Bluetooth will man dem Virus zuvorkommen und Infizierte isolieren, bevor sie erkranken. Doch die technische Umsetzung ist fehleranfällig und birgt Missbrauchsgefahren.

Von Hartmut Gieselmann

SARS-CoV-2 konnte deshalb zu einer weltweiten Pandemie werden, weil das Virus schneller ist als die Gesundheitssysteme. Wenn ein Patient erste Symptome spürt und sich zum Test anmeldet, sind laut Robert-Koch-Institut seit der Infektion durchschnittlich fünf bis sechs Tage vergangen. Doch bereits drei Tage vor Ausbruch der Krankheit kann ein Infizierter das Virus auf andere Menschen übertragen. Erst wenn das Testergebnis nach zwei Tagen vorliegt, klären Mitarbeiter in aufwendigen Interviews, wen der Patient eventuell angesteckt haben könnte. Bis diese Kontakte ermittelt und gewarnt sind, hat ein frisch Infizierter das Virus oft schon unwissentlich weiter verteilt.

Das bestätigt auch eine Oxford-Studie, die Luca Ferretti mit Kollegen Ende März veröffentlichte. Demnach geht die größte Infektionsgefahr von Infizierten aus, die noch keine Symptome von Covid-19 zeigen (in der Grafik hellblau dargestellt). Sie machen bis zur Hälfte aller Übertragungen aus. Am zweithäufigsten läuft die Ansteckung über Patienten mit Symptomen (grüne Kurve). Demgegenüber spielen indirekte Infektionen aus der Umgebung (rote Kurve) sowie über Infizierte ohne Symptome (orange Kurve) nur eine geringe Rolle.

Ferretti zufolge ließe sich die exponentielle Ausbreitung allein dadurch stoppen, dass man die Infektionen der hellblauen Gruppe eindämmt. Genau hier setzen Tracing-Apps an, die die Zeit zur Benachrichtigung drastisch verkürzen sollen, sodass neu Infizierte sich isolieren könnten, bevor sie Symptome zeigen. Der hellblaue Anteil der Infektionskurve würde abflachen. Um die Epidemie unter Kontrolle zu bringen, müssten insgesamt etwa zwei von drei Infektionen verhindert werden.

Weil für die Ausbreitung von SARS-CoV-2 hauptsächlich direkte Kontakte zu Infizierten verantwortlich sind, indirekte Schmierinfektionen über Oberflächen aber kaum eine Rolle spielen, sind die besuchten Aufenthaltsorte der Betroffenen irrelevant. Eine App muss lediglich die Annäherung an andere Personen registrieren. Ein Tracking per GPS, wie es einige Länder in Asien und auch Israel praktizieren, ist weder notwendig noch in Städten mit Hochhäusern praktikabel.

Deshalb setzen rund ein Dutzend weltweite Ansätze auf Bluetooth. Smartphone-Apps sollen erkennen, welchen Personen sich ein Infizierter wie lange genähert hat, wobei das Virus womöglich übertragen werden konnte. Dazu müssen beide ihr Smartphone oder eine Smartwatch am Körper tragen. Die darauf installierten Apps übertragen gegenseitig eine temporär gültige ID und den Gerätetyp des Smartphones, die zusammen mit dem gemessenen Pegel des Bluetooth-Signals, Zeit und Dauer der Begegnung verschlüsselt auf dem Smartphone gespeichert werden. Wird ein Nutzer positiv auf Covid-19 getestet, bekommt er eine TAN, mit der die App ihre IDs an einen Server übermittelt, der die Kontakte informiert. Andernfalls löscht die App nach einem festgelegten Zeitraum von zwei bis drei Wochen die veralteten Kontaktdaten. Den Austausch unterstützen alle Smartphones ab Bluetooth 4.0, das beispielsweise Apple erstmals vor neun Jahren im iPhone 4S einsetzte.

Bei der Umsetzung der Apps müssen Hersteller also zwei technische Probleme lösen: Erstens müssen sie die Entfernung der Geräte möglichst genau per Bluetooth messen, damit nur die Kontakte gespeichert werden, die sich tatsächlich lange genug im infektiösen Radius von circa zwei Metern aufhielten. Zweitens müssen sie die Speicherung und den Austausch der IDs so gut absichern, dass diese nur im Ernstfall zur Warnung vor einer Infektion genutzt, aber nicht von Dritten zur Überwachung oder zur Auslösung von Fehlalarmen missbraucht werden.

Schwierige Messungen

Als eines der ersten Länder setzt Singapur eine solche Bluetooth-App zur Kontaktüberwachung ein. Die App TraceTogether erschien am 20. März für Android und iOS. Mitte April gab Singapur den Code des zugrunde liegenden Systems BlueTrace auf GitHub frei, inklusive Informationen zur Kalibrierung der Bluetooth-Sender und -Empfänger in Smartphones.

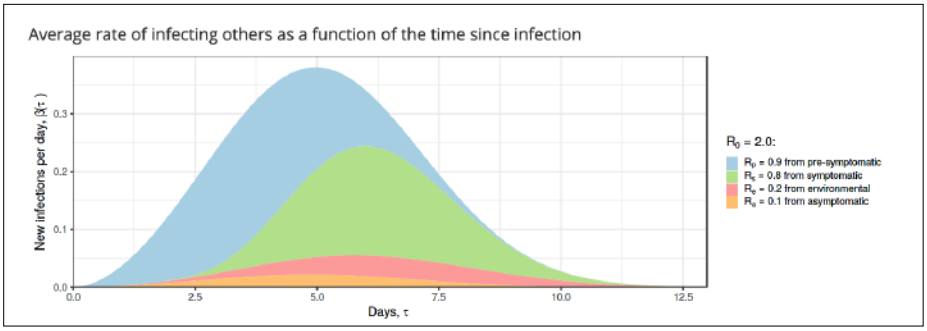

Bild: Michelle Kendall

Tracing-Apps sollen frisch Infizierte warnen, bevor sie Symptome verspüren und somit den blauen Anteil der Infektionskurve abschwächen (hier beispielhaft bei einer Verdopplungszeit von 5 Tagen).

Um die Distanz per Bluetooth zu bestimmen, muss der Empfänger den Signalpegel des Senders messen. Im Unterschied zu fest installierten Beacons in Museen und Einkaufszentren senden Smartphones jedoch nicht mit einer kalibrierten Leistung. Entwickler aus Singapur ermittelten bei verschiedenen Modellen Unterschiede von 30 Dezibel (Faktor 1000). Selbst bei ein und demselben Smartphone schwankte der Pegel so erheblich, dass eine Abschätzung der Entfernung nur über eine Gewichtung vieler Messungen über einen längeren Zeitraum möglich war. TraceTogether speichert denn auch nur Kontakte, die mindestens eine halbe Stunde dauern. Andere Konzepte setzen eine Kontaktdauer von 15 Minuten voraus.

Darüber hinaus machten den Entwicklern die Stromsparmodi von iOS zu schaffen. Sie verhindern, dass Apps auch im Hintergrund regelmäßig nach Bluetooth-Geräten scannen und ihre eigene Kennung senden. Auf einem iPhone muss die Tracing-App deshalb ständig im Vordergrund laufen – nicht sehr praktikabel, wenn man in einer vollbesetzten Bahn oder im Wartezimmer ein wenig surfen will. Android lässt das Tracing hingegen auch im Hintergrund zu.

Um die grundsätzlichen Probleme mit der schwankenden Sendeleistung und den Stromsparmodi zu lösen, sind Apple und Google gefragt. Zu Ostern kündigten beide Konzerne an, gemeinsame Lösungen zum Kontakt-Tracing per Bluetooth anzubieten. Apple will dazu Mitte Mai ein Update für iOS veröffentlichen. Da es bei Android deutlich schwieriger ist, entsprechende System-Updates für sämtliche Smartphone-Hersteller auszuspielen, setzt Google auf eine eigene Tracing-App im Play Store.

Zentrale und dezentrale IDs

Bei ihrem bislang nur rudimentär skizzierten Konzept folgen Apple und Google weitgehend dem europäischen Ansatz von PEPP-PT. Zu der in der Schweiz ansässigen Non-Profit-Organisation Pan-European Privacy-Preserving Proximity Tracing gehören inzwischen 130 Mitglieder aus ganz Europa, darunter mehrere Universitäten und Fraunhofer-Institute. Am weitesten vorangeschritten ist dabei das offene Protokoll DP-3T. Deren Entwickler haben auf GitHub eine ausführliche Analyse veröffentlicht, die mögliche Angriffsszenarien auf eine Tracing-App untersucht.

Zentraler Punkt ist dabei die Ausgabe der Erkennungs-IDs, unter denen die Kontakte gespeichert und im Fall einer Infektion benachrichtigt werden. Die IDs wechseln alle paar Minuten, um ein Tracking der Personen zu erschweren. Zusätzliche Zeitstempel erschweren Replay-Attacken, bei denen ein Angreifer ein Bluetooth-Signal aufzeichnet und später an anderer Stelle wieder ausspielt. Damit könnte er Kontakte vortäuschen, die gar nicht stattgefunden haben und gezielt Leute in Quarantäne schicken, obwohl sie nicht gefährdet sind.

In Singapur erzeugt das Gesundheitsministerium die temporären IDs auf einem zentralen Server, verteilt sie von dort an die Apps und speichert die zugehörigen Telefonnummern. Wird ein Infizierter positiv getestet, schickt seine App die auf seinem Smartphone verschlüsselt gespeicherten Kontakt-IDs an den Zentralserver. Dieser prüft die Integrität der IDs, ermittelt die Dauer und Nähe der Kontakte und verschickt Warnungen an die Betroffenen.

Bei diesem zentralen Ansatz erfährt also das Gesundheitsministerium in Singapur, mit wem ein positiv Getesteter in den vergangenen drei Wochen Kontakt hatte und könnte mit diesen Informationen detaillierte Profile erstellen.

Der Ansatz von PEPP-PT, den auch Google und Apple verfolgen, favorisiert hingegen eine dezentrale Lösung. Dabei erzeugen die Smartphones die temporären IDs selbst und tauschen sie untereinander aus. Wird ein Infizierter positiv getestet, muss er seine Kontakte selbst an einen Server schicken. Der Server versendet vereinfacht gesagt täglich alle eingegangenen IDs möglicher Infizierter an alle Smartphones. Diese vergleichen sie mit den eigenen IDs aus der Historie und warnen den Nutzer bei einer Übereinstimmung. So lassen sich Kontaktpersonen benachrichtigen, ohne dass der Server oder der Infizierte ihre Identität kennt.

Doch auch dieses dezentrale System ist laut der DP-3T-Macher angreifbar, wenn auch mit größerem Aufwand. Würde jemand mehrere Bluetooth-Empfänger in einer Stadt verteilen, könnte er womöglich Bewegungsprofile von Infizierten erstellen. Um dies zu erschweren, schlagen die DP-3T-Entwickler mehrere Maßnahmen vor, bei denen die IDs in Schnipsel unterteilt und kodiert werden, sodass jeweils nur die Smartphones der Besitzer berechnen können, ob sie betroffen sind. Dadurch würde sich allerdings das Volumen der täglichen Datenübertragungen erhöhen.

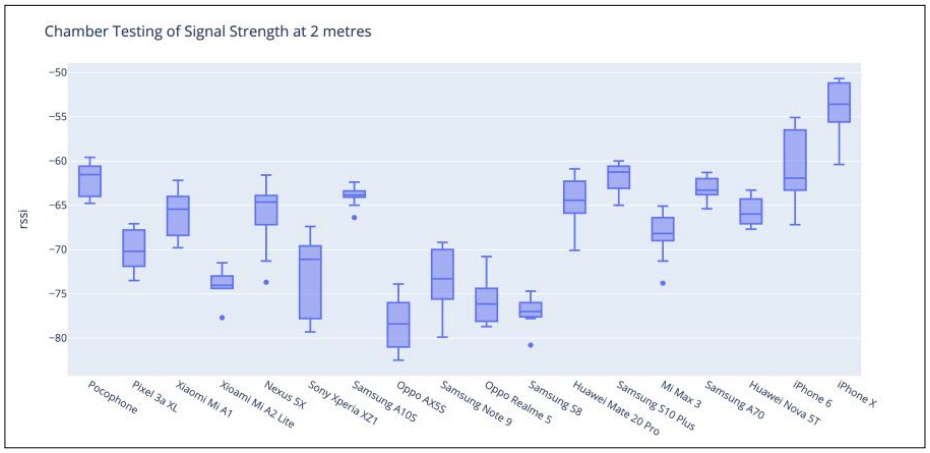

Bild: BlueTrace

Pegel von Bluetooth-Signalen schwanken selbst bei konstantem Abstand zwischen verschiedenen Smartphones erheblich und erschweren eine Distanzmessung.

Unabhängige Prüfungen

Ob solche Tracing-Apps, wenn sie auf den Markt kommen, denn auch sicher sind, müsste extern und unabhängig geprüft werden. Derartige Prüfungen für Corona-Apps biete etwa die TÜV Informationstechnik GmbH kostenlos an, sagte Geschäftsführer Dirk Kretschmar gegenüber c't. Geprüft würden die Absicherung gegenüber Hacker-Angriffen, die Einhaltung der DSGVO sowie anderer Datenschutzbestimmungen. Eine erste Beurteilung auf Level 1 würde mindestens fünf Werktage dauern, eine komplette Überprüfung auf Level 3 bis zu zwei Monate. Um eine solche App möglichst früh nutzen zu können, wird man in der ersten Zeit vermutlich Kompromisse eingehen und den Nutzen bei der Eindämmung der Pandemie gegenüber Datenschutzproblemen möglicherweise höher gewichten. *(hag@ct.de)* c't

Studien und White-Paper: ***ct.de/y6gc***