Anonyme Verfolgung, ein gefährliches Oxymoron

Eine Risikoanalyse für Laien

Ein Artikel von

Xavier Bonnetain , Universität von Waterloo, Kanada; Anne Canteaut , Inria; V´eronique Cortier , CNRS, Loria; Pierrick Gaudry , CNRS, Loria; Lucca Hirschi , Inria; Steve Kremer , Inria; St´ephanie Lacour , Universität Paris-Saclay, CNRS; Matthieu Lequesne , Sorbonne Universit´e et Inria; Gaetan Leurent , Inria; L´eo Perrin , Inria; Andr´e Schrottenloher , Inria; Emmanuel Thom´e , Inria; Serge Vaudenay , EPFL, Suisse; Christophe Vuillot , Inria. Kontakt : contact@risques-tracage.fr

Netz: https://risques-tracage.fr/

Übersetzt aus dem Französischen von Tom Lancaster (tom.lancaster@durham.ac.uk).

Um den Fortschritt der COVID-19-Epidemie aufzuhalten, plant Frankreich die Einrichtung eines Systems zur Verfolgung von Patienten mithilfe einer mobilen App. Die Entwickler dieser Art von App möchten sicherstellen, dass sie die Privatsphäre respektieren. Dieser Begriff bleibt jedoch vage. Wir hoffen daher, einen Beitrag zur öffentlichen Debatte zu leisten, indem wir klären, was eine Tracking-App garantieren kann und was nicht, mit der Absicht, dass sich die Leute eine Meinung darüber bilden können, ob ihre Bereitstellung ratsam ist.

Der Nutzen dieser Anwendung liegt in ihrer Fähigkeit, gefährdete Kontakte zu erkennen und diese Informationen in relevanter Weise zusammen mit anderen Maßnahmen zur Bekämpfung der Epidemie wie Screening oder Quarantäne zu verwenden. Da wir kein Fachwissen in Epidemiologie haben, sind wir uns bewusst, dass wir die Auswirkungen der Tracking-App auf die Ausbreitung der Krankheit nicht beurteilen können. Diese Bewertung erscheint jedoch unabdingbar, um die möglichen Vorteile und Risiken auszugleichen.

Unsere Expertise als Spezialist für Kryptographie-, Sicherheits- oder Technologierecht liegt insbesondere in unserer Fähigkeit, die möglichen Mehrfachmissbräuche und -veruntreuungen sowie andere böswillige Verhaltensweisen zu antizipieren. Gegenwärtig wird eine lebhafte Debatte über die vorgeschlagenen Anträge zwischen Spezialisten auf dem Gebiet der Sicherheit geführt, wobei häufig sogenannte "zentralisierte" Anträge gegen "dezentralisierte" Anträge gestellt werden. Unabhängig von diesen technischen Überlegungen möchten wir die Menschen auf die Gefahren einer Tracking-Anwendung aufmerksam machen. Anhand verschiedener Szenarien wie dem folgenden untersuchen wir den möglichen Missbrauch einer solchen Technologie, unabhängig von den Details ihrer Implementierung.

Szenario. *Das Unternehmen KROOKS beabsichtigt, einen Zeitarbeitnehmer einzustellen. Sie wollen sicherstellen, dass der Kandidat zwischen dem Vorstellungsgespräch und der Vertragsunterzeichnung nicht krank wird. Sie verwenden daher ein spezielles Telefon, das nur während des Interviews eingeschaltet wird und das eine Warnung erhält, wenn der Kandidat später positiv auf die Krankheit testet.*

Zusammenfassung

- - Es gibt keine Datenbank mit Patientennamen.	WAHR
- - Daten sind anonym	⊘ FALSCH
- - Es ist unmöglich herauszufinden, wer wen kontaminiert hat	⊘ FALSCH
- - Es ist unmöglich zu wissen, ob eine bestimmte Person krank ist oder nicht	⊘ FALSCH
- - Es ist unmöglich, einen Fehlalarm auszulösen	⊘ FALSCH
- - Die Verwendung von Bluetooth ist kein Sicherheitsproblem	⊘ FALSCH
- - Das System macht das Schnüffeln in großem Maßstab unmöglich	⊘ FALSCH

Einführung

Die Welt ist mit der COVID-19-Epidemie konfrontiert. Viele Länder, einschließlich Frankreich, planen die Einrichtung eines Systems zur Verfolgung der Patientenkontakte mithilfe einer mobilen App. Das Leitprinzip ist, dass, wenn jemand positiv auf das Virus getestet wurde, es möglich ist, mithilfe der Anwendung alle Personen zu alarmieren, mit denen er kürzlich Kontakt hatte, und sie dabei zu ermutigen, sich selbst unter Quarantäne zu stellen und zu konsultieren ein Arzt oder getestet werden. Seit Beginn der Epidemie haben Forscher im Bereich Computersicherheit Anstrengungen in den Entwurf solcher Systeme investiert. andere wie R. Anderson [1], S. Landau [2], B. Schneier [3] und S. Vaudenay [4], über die Gefahren eines solchen Systems gesprochen oder sich gegen dessen Umsetzung ausgesprochen haben. Angesichts der potenziellen Risiken für die Privatsphäre hat die Verwendung einer solchen Anwendung eine Debatte ausgelöst.

Erstens sind diese Apps nur dann sinnvoll, wenn sie wirklich die Erkennung gefährdeter Kontakte ermöglichen. Dies setzt voraus, dass Tracking-Anwendungen die Entfernung zwischen Personen (möglicherweise mit einer Genauigkeit von einem Meter) unabhängig von der Umgebung oder Position des Telefons genau einschätzen können. In der Praxis wird es notwendig sein, einen Kompromiss einzugehen, aber es wird wahrscheinlich sowohl unerkannte Kontakte (einschließlich Fälle von Übertragung über Oberflächen) als auch Fehlalarme (wie eine Erkennung durch eine Wand) geben. Der Plan setzt auch eine Massenakzeptanz dieser Lösungen durch die Bevölkerung voraus, für die im Allgemeinen ein Smartphone und häufig Bluetooth erforderlich sind.

Entgegen der derzeitigen Praxis [1], Diese Technologien alarmieren Personen, die systematisch und differenziert mit einem Patienten in Kontakt gekommen sind, so dass sowohl der Patient als auch die Fachkräfte nicht in der Lage sind, zu bestimmen, wer alarmiert werden muss. Wir könnten zum Beispiel die Notwendigkeit in Frage stellen, allen Kontakten zu empfehlen, zu einem Test zu reisen, da dies für ältere Menschen oder Personen mit bereits bestehenden Krankheiten ein zusätzliches Risiko darstellen würde. Diese Aspekte werden in der öffentlich zugänglichen Dokumentation zu den vorgeschlagenen Anträgen häufig nur sehr wenig angesprochen. Wir werden daher hier nicht auf die Wirksamkeit der Tracking-Anwendungen eingehen, sondern auf deren Sicherheit, auch wenn es uns wichtig erscheint, ihre Wirksamkeit zu bewerten und mit der der bestehenden Verfahren oder der Erkennung von Clustern durch Epidemiologen zu vergleichen.

Die Frage nach den Risiken für die öffentliche Freiheit wurde bereits aufgeworfen, insbesondere von Quadrature du Net [7]. Unser Beitrag wird sich auf die Untersuchung mehrerer Szenarien beschränken, um das Kriechen hervorzuheben, das eine solche Anwendung ermöglichen würde. Selbst wenn einige dieser Sicherheitslücken teilweise durch erhebliche Änderungen an den vorgeschlagenen Protokollen vermieden werden könnten, sind die meisten der von uns geplanten Szenarien den Funktionen dieser Apps inhärent.

Wir beginnen mit der Darstellung der allgemeinen Funktionsweise dieser Art von App. Die Szenarien werden ab Abschnitt erläutert 4 .

1. Das bestehende Verfahren basiert auf Mechanismen zur Meldung von Krankheiten und den Behörden, die eine Untersuchung zur Verfolgung der gefährdeten Kontakte einer infizierten Person. Die Behörden alarmieren diese Kontakte und beraten sie. Indem wir versuchen, diese bestehenden Verfahren mit einer technischen Lösung nachzuahmen, vernachlässigen wir auch die Tatsache, dass die Umsetzung der Rechtsstaatlichkeit immer zu vielen Bestimmungen führt [5 , 6].

1 Gerätebetrieb

Unsere Analyse konzentriert sich auf aktuelle Vorschläge für ein Tracking-System mit Bluetooth. Diese Systeme wurden als zufriedenstellendere Lösung in Bezug auf die Privatsphäre vorgeschlagen als diejenigen, die auf der genauen Geolokalisierung von Mitgliedern der Bevölkerung beruhen, wie sie in China durchgeführt wurde und über die die meisten europäischen Länder sowie die Europäische Kommission [2], haben sich nur ungern in Betracht gezogen. Mehrere alternative Tracking-Systeme [3] wurden in den letzten Wochen von IT-Sicherheitsspezialisten, Forschern und der Industrie vorgeschlagen. Ein besonderer Schwerpunkt unserer Studie liegt auf (und dies ist eine nicht erschöpfende Liste): dem DP3T [4] Protokoll (verschiedene Varianten), dessen Variation von Apple / Google [5] Allianz, die PACTEst [6] Protokoll, das PACT-Ouest [7] Protokoll, das TCN [8], Protokoll, der ROBERT [9] Protokoll. Die Synopsen der meisten dieser Systeme versprechen, „die Privatsphäre der Benutzer zu respektieren“. Es ist jedoch wichtig zu klären, was dieser Slogan bedeutet (und was nicht).

Wir nutzen diese Gelegenheit, um an ein grundlegendes Prinzip der Computersicherheit zu erinnern: Es ist wichtig, dass die Beschreibung und der Code eines Systems veröffentlicht und ausgewertet werden, um Vertrauen in das System zu schaffen.

1.1 Allgemeiner Grundsatz

Verschiedene veröffentlichte Varianten von Tracking-Systemen, die die Privatsphäre respektieren, folgen einem Muster, das dem in dem auf der Seite gezeichneten Streifen relativ nahe kommt [4] . Das Mobiltelefon jedes Benutzers generiert häufig (z. B. alle 5 Minuten) einen Zufallscode (eine Reihe von Buchstaben und Zahlen), den wir als Pseudonym bezeichnen werden. Immer wenn zwei Telefone in der Nähe Kontakt haben, tauschen sie ihre aktuellen Pseudonyme über Bluetooth aus [10], und notieren Sie Datum und Uhrzeit des Austauschs. Diese Informationen werden zwei Wochen lang im Telefon jedes Benutzers gespeichert. Wenn ein Benutzer (nennen wir sie Alice) positiv getestet wird, benachrichtigt die App alle Personen, mit denen sie in den letzten 14 Tagen Pseudonyme ausgetauscht hat, wie z. B. den Benutzer Bob. Bob erhält dann eine Benachrichtigung (mit Empfehlungen basierend auf der Zeit, die er mit dem Patienten verbracht hat). Das Verfahren, mit dem die Anwendung Pseudonyme verwenden kann, um einen Kontakt zu verhindern, hängt von bestimmten Protokollen ab und wird im nächsten Abschnitt beschrieben.

1.2 Wer bescheinigt, dass Alice krank ist?

Wenn Alice krank wird, muss sie die App auslösen, damit Personen benachrichtigt werden, mit denen sie Kontakt hatte. Aber wer bescheinigt, dass Alice krank ist und dass die

---

2. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670 , konsultieren le 18. April 2020.

3. Diese Systeme erlauben es nicht, "Cluster" nicht zu identifizieren, da sie keine Geolokalisierung verwenden Information.

4. DP3T = *Dezentrale, datenschutzbewahrende Annäherungsverfolgung* https://github.com/DP-3T/ documents / konsultiert am 18. April 2020.

5. https://www.apple.com/covid19/contacttracing/ konsultiert am 18. April 2020.

6. PACT = *Private automatisierte Kontaktverfolgung,* https://pact.mit.edu/ konsultiert am 18. April 2020.

7. https://covidsafe.cs.washington.edu/ konsultiert am 20. April 2020.

8. https://tcn-coalition.org/ konsultiert am 20. April 2020.

9. ROBERT = ROBust und datenschutzrechtliche Nähe Tracing, https://github.com/ROBERTproximity-tracing/documents/ konsultiert am 18. April 2020.

10. Beachten Sie, dass Bluetooth nicht zum Testen der physischen Nähe ausgelegt ist und tatsächlich davon ausgeht, dass zwei Personen auf verschiedenen Seiten einer Wand „in Kontakt“ waren. Durch seine Verwendung wird jedoch die Verwendung von Geolokalisierungsmethoden vermieden, die die genaue Position der Bewegungen von Personen anzeigen.

Feige. 1 - *Der Betrieb der App im dezentralen Modell (von D3PT und Apple / Google verwendet). Zentralisierte Protokolle wie ROBERT folgen nicht dem gleichen Verfahren, um Bob zu warnen, wenn Alice krank wird. [Abbildung aus einer Zeichnung von Nicky Case (ncase.me).]*

Informationen sollen übertragen werden? Es gibt zwei Möglichkeiten:

1. Alice diagnostiziert den Bericht selbst und löst ihn aus.
2. Die Krankheit von Alice muss von einem Test oder einem Arzt bestätigt werden, damit die Informationen verbreitet werden können (z. B. indem Alice einen Einwegcode gegeben wird, der die Warnung auslöst).

Wir werden nur die zweite Möglichkeit betrachten, die die Option zu sein scheint, die in den in Europa vorgeschlagenen Protokollen gewählt wurde [11]. In der Tat kann jeder böswillige Benutzer falsche Krankheitserklärungen abgeben, wenn sich Menschen ohne die Bescheinigung einer medizinischen Behörde für krank erklären können, wie im folgenden Szenario. Die Multiplikation solcher falschen Berichte macht das System schnell funktionsunfähig.

Szenario 1 (Falsche Erklärung). *Fußballspieler Gronaldo wird in einem bevorstehenden Champions-League-Spiel spielen. Um ihn am Spielen zu hindern, ist es ausreichend, dass ein Gegner sein Telefon ohne Gronaldos Wissen neben Gronaldos lässt und sich dann für krank erklärt. Gronaldo wird benachrichtigt, weil er angeblich mit einer infizierten Person in Kontakt war und sich 14 Tage lang vom Fußballplatz fernhalten muss.*

2 Es gibt keine Datenbank mit Patientennamen

Wir haben noch nicht erklärt, wie es möglich war, Bob zu warnen, dass er Kontakt mit einer kranken Person hatte. Eine einfache Idee (riskant in Bezug auf die Vertraulichkeit medizinischer Daten) würde darin bestehen, eine Liste von Kranken zu erstellen. Diese Idee wird von Apps, die den Datenschutz respektieren, nicht berücksichtigt. Diese bevorzugen zwei alternative Lösungen, die zwei unterschiedlichen Modellen der Datenverbreitung entsprechen.

1. Das "dezentrale" Modell. Bei der Diagnose sendet Alice jedem die Liste von Pseudonyme, die sie in den letzten Tagen übermittelt hat. Technisch kann dies als Peer-to-Peer-Operation oder über einen Vermittler wie eine Gesundheitsbehörde, beispielhaft dargestellt durch ein Krankenhaus, erfolgen [12] im Comic. Bob kann diese Datenbank abfragen, um herauszufinden, ob sie einen der Aliase enthält, die er kürzlich erhalten hat. Wenn es eine Übereinstimmung gibt, sendet die App Bob eine Warnung. Die Protokolle DP3T, PACT und Apple / Google folgen diesem Muster.

2. Das "zentralisierte" Modell. Bei der Diagnose sendet Alice die zentrale Behörde die Liste der Pseudonyme, die kürzlich registriert wurden. Diese Liste der gefährdeten Kontakte wird nicht veröffentlicht und ist nur der zentralen Behörde bekannt. In diesem Modell kontaktiert Bob wie jeder Benutzer täglich die zentrale Behörde und stellt ihnen die Liste der von ihm übermittelten Pseudonyme zur Verfügung [13] um herauszufinden, ob sich einer von ihnen in der Datenbank der gefährdeten Kontakte befindet. Bei Bedarf erhält er eine Benachrichtigung.

Beide Modelle haben Vor- und Nachteile. Das zentralisierte Modell erfordert das Vertrauen in eine zentrale Behörde. Beispielsweise kann die Behörde die Liste der Kontakte verwenden, die von „neuen“ Patienten erhalten wurden, und diejenigen Personen erkennen, von denen zuvor berichtet wurde, dass sie dem Virus ausgesetzt waren, und dabei feststellen, dass sie zuvor ihre Quarantänerichtlinien missachtet haben. Das dezentrale Modell tut dies nicht *a priori*

11. Damit das System funktioniert, müssen diese Berichte auf zuverlässigen Tests beruhen.

12. Dies ist die Auswahl, die in den Protokollen DP3T, PACT und Apple / Google getroffen wurde.

13. Im besonderen Fall von ROBERT berechnet die Zentralbehörde alle Pseudonyme des Bob, obwohl sie seine Identität nicht a priori kennt.

stellen dieses Problem dar, öffnet aber die Tür für andere Angriffe. Diese beiden Modelle werden später untersucht. Ihre Unterschiede sind erheblich, obwohl die meisten der von uns diskutierten Szenarien unabhängig vom Modell funktionieren.

3 Daten sind nicht anonym

Für dezentrale Verfolgungsprotokolle muss kein Register von COVID19-Patienten erstellt werden, wie dies für bestimmte gesetzlich festgelegte meldepflichtige Krankheiten erforderlich ist. Zentralisierte Modelle verfügen über eine Datenbank mit Personen, bei denen das Risiko besteht, dass sie sich mit der Krankheit infizieren, nachdem sie mit einem Krankheitsfall in Kontakt gekommen sind. In beiden Modellen sind diese Dateien pseudonymisiert, was bedeutet, dass die Patienten nicht anhand ihres Namens oder ihrer Sozialversicherungsnummer identifiziert werden, sondern anhand eines Codes oder einer Nummer, die von ihrer tatsächlichen Identität unabhängig ist. In den vorgeschlagenen Systemen ist die Datei von COVID-19-Patienten mit kryptografischen Mechanismen pseudonymisiert [14] wie zum Beispiel für das Register der Erklärungen von HIV-AIDS. Diese Nummer kann jedoch entkoppelt werden, indem sie mit anderen Informationen in der Datenbank (den Identifikatoren von Personen, die Kontakt hatten) oder außerhalb der Datenbank (z. B. mit einer Bluetooth-Antenne erfasst) oder nach IP-Adresse kombiniert wird . Es handelt sich also nicht um eine anonyme Datenbank wie zum Beispiel von der DSGVO definiert.

> „ *Personenbezogene Daten, die einer Pseudonymisierung unterzogen wurden, könnten einer natürlichen Person durch Heranziehung zusätzlicher Informationen zugeordnet werden, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.* „
>
> -- Allgemeine Datenschutzverordnung (DSGVO)

Diese Datenbank enthält daher personenbezogene Daten im Sinne der DSGVO und des französischen Rechts [fünfzehn] . Es enthält auch Daten, die als vertraulich eingestuft sind (dh medizinische Daten), auf die der Zugriff bestimmte Anforderungen stellt, insbesondere indem die Möglichkeit der Verarbeitung eingeschränkt wird [16] .

Anonym und Pseudonym?

-- Herr Bloggs ist krank	⊘ NOMINATIV
-- Das Pseudonym 439Hxs ist krank	⊘ PSEUDONYM
-- Es gibt 50 437 Fälle	ANONYM

4 Wie finden Sie heraus, wer Sie infiziert hat?

Obwohl die Pseudonyme der Patienten ihre Identität nicht preisgeben, können Benutzer leicht auf Informationen über andere Benutzer schließen, sobald sie erfahren, dass eine Person, die sie in den letzten zwei Wochen getroffen haben, krank geworden ist.

14. Beispielsweise verwenden die Protokolle DP3T und Apple / Google HMAC-SHA256, das derzeit als sicher gilt.

15. In dem Sinne, dass diese Daten es auch indirekt ermöglichen, die betroffenen Personen zu identifizieren.

16. Artikel 6 des Gesetzes Nr. 78-17 vom 6. Januar 1978 in Bezug auf Datenverarbeitung, Dateien und Freiheiten, zuletzt geändert im Jahr 2019, und Artikel 9 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 über den Schutz von Einzelpersonen in Bezug auf die Verarbeitung personenbezogener Daten und den freien Datenverkehr sowie die Aufhebung der Richtlinie 95/46 / EG (Allgemeine Datenschutzbestimmungen).

Szenario 2 (Der einzige Verdächtige). *Mr. Smith, der, um eine Kontamination zu vermeiden, sein Zuhause nie verlässt, außer um im Lebensmittelgeschäft der Nachbarschaft einzukaufen, erhält eine Benachrichtigung von seinem Telefon. Es folgt* [17] *dass nur der Lebensmittelhändler verantwortlich sein kann.*

Szenario 3 (Informationskreuzung). *Frau Jones, die tagsüber auf viele Menschen trifft, erhält eine Benachrichtigung. Sie muss sich nur ein paar Momente mit ihrem Nachbarn und einem Bürokollegen unterhalten, um herauszufinden, dass der Patient kein professioneller Kollege ist, sondern im Gebäude lebt. Dank dieser Hinweise vermutet sie stark (vielleicht zu Unrecht), dass Herr Attrisk im 3. Stock, der Sanitäter ist, alle seine Nachbarn kontaminiert hat. Sie beeilt sich, den Rest der Bewohner des Gebäudes über soziale Netzwerke zu warnen.*

Diese glaubwürdigen Szenarien sind völlig unabhängig von den Details der App. Sie erfordern keine besonderen Computerkenntnisse. Sie veranschaulichen die Einschränkungen, die diesem Systemtyp inhärent sind. Auch wenn es nicht so ist *a priori* Wenn die zentrale Behörde die Pseudonymisierung der Benutzer umgehen kann, ist es für einen Benutzer nicht schwierig, dies zu tun.

Diese Tracking-Technologien haben die Funktion, alle Personen, denen ein Patient begegnet, systematisch und wahllos zu warnen. Sie können stattdessen keine freiwillige und überlegte Benachrichtigung über enge Kontakte der kranken Person sein. In dezentralen Modellen erhält die gesamte Bevölkerung die vom System gesammelten Gesundheitsdaten, die sich grundlegend von allen vorhandenen Systemen unterscheiden.

In dem Maße, in dem Tracking in großem Umfang als Whistleblowing-System fungieren würde, würden die darin enthaltenen Informationen Verdacht erregen und mögliche Kontaminationen in moralische Fehler umwandeln [18] und die Stigmatisierung gefährdeter Personen in einem bereits sensiblen Kontext zu verschärfen. Solche Effekte wurden beispielsweise bereits in Korea gemeldet [19] , Hexenjagden verursachen. Dieses Risiko der Stigmatisierung wurde seit der Erstellung des Registers der mit HIV lebenden Menschen vor zwanzig Jahren als besorgniserregend angesehen, und diese Sorge scheint im Zeitalter der sozialen Netzwerke noch legitimer zu sein.

Szenario 4 (Sind meine Nachbarn krank?). *Herr Hipokondriac möchte wissen, ob seine Nachbarn krank sind. Er findet sein altes Telefon in einem Schrank, installiert die TraceVIRUS-App und lässt sie in seinem Briefkasten unten in seinem Gebäude. Alle Nachbarn kommen jedes Mal vorbei, wenn sie nach Hause zurückkehren, und das Telefon erhält eine Benachrichtigung, wenn einer von ihnen krank ist.*

17. Wir stellen fest, dass Mr. Smith möglicherweise falsch liegt: Seine Benachrichtigung könnte auf einen anderen Nachbarn zurückzuführen sein, der krank ist und dessen Smartphone von Mr. Smith durch die Wand erkannt wurde.

18. Tracing ist eine individualisierende Managementlösung für das komplexe Problem der Eindämmung. Diese Interpretation kann beispielsweise auf der Arbeit sozialwissenschaftlicher Forscher beruhen [8], die zeigen, dass die Entwicklung unseres Gesundheitssystems in den letzten Jahrzehnten zu einer Verbesserung der Zahl der rationalen und informierten Personen geführt hat, die auf der Grundlage staatlicher Informationen und wirtschaftlicher Anreize verantwortlich und in der Lage sind, fundierte Entscheidungen zu treffen. Die durch die Verwendung dieser Art von App vorgesehene Reaktion geht in die gleiche Richtung

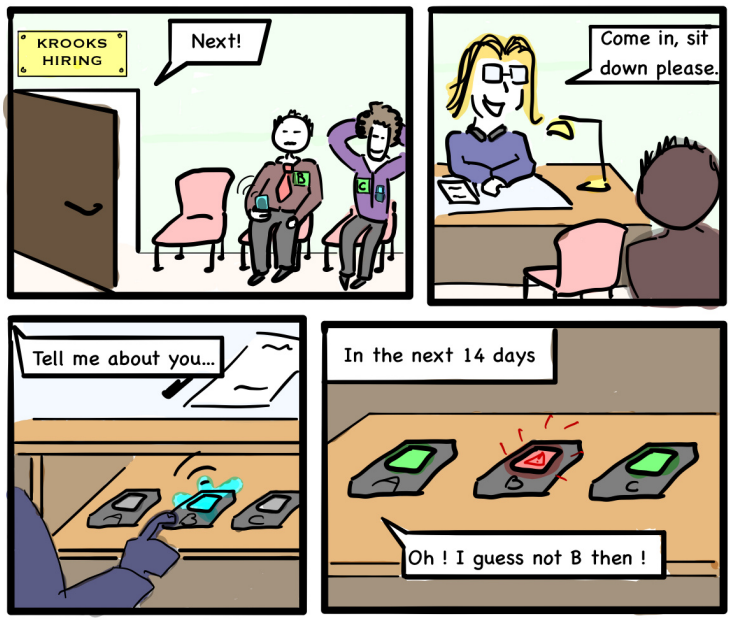
19. In Südkorea können Einwohner benachrichtigt werden, dass jemand, der in derselben Nachbarschaft lebt, positiv auf das Virus getestet wurde. Diese Warnungen geben Geschlecht, Alter und die Liste der letzten Reisen an. Obwohl *a priori* anonym könnten diese Informationen zu Identifizierungen durch die Öffentlichkeit führen, gefolgt von Online-Auswanderungskampagnen (man wird beschuldigt, das Virus möglicherweise verbreitet zu haben). https://www.bbc.com/news/worldasia-51733145

5 Woher wissen Sie, ob eine bestimmte Person krank ist? Spionage in jedermanns Reichweite

Im Wesentlichen können alle Verfolgungssysteme, die Patientenkontakte benachrichtigen, verwendet werden, um herauszufinden, ob eine bestimmte Person krank wird. Um zuverlässige Informationen über eine bestimmte Person zu erhalten, verwenden wir einfach ein **spezielles Telefon, auf dem wir die App installieren** [20] **, und setzen Sie das Telefon nur mit dieser Person in Kontakt. Die beiden Telefone** zeichnen den Kontakt auf, und wenn das Ziel positiv getestet wurde, erhält unser Telefon eine Warnung.

Szenario 5 (Das Vorstellungsgespräch). ***Das Unternehmen KROOKS beabsichtigt, einen Zeitarbeitnehmer einzustellen. Sie*** *wollen sicherstellen, dass der Kandidat zwischen dem Vorstellungsgespräch und der Vertragsunterzeichnung nicht krank wird. Sie verwenden daher ein spezielles Telefon, das nur während des Interviews eingeschaltet wird und das eine* ***Warnung erhält, wenn der Kandidat später positiv auf die Krankheit testet. (Siehe Abb. 2 .)***

Viele ähnliche Szenarien sind möglich (z. B. ein Banker, der nur ungern einen Kredit an einen Kunden vergibt). Alle diese Szenarien sind sehr einfach einzurichten.



Feige. 2 - ***Mögliche Entführung der App während eines Vorstellungsgesprächs.***

Szenario 6 (Die Paparazzi). ***Herr Paparazzo sucht private Informationen bei Frau Star. Er besticht Frau Rimelle, die*** *Maskenbildnerin, die am Set von Stars neuestem Film arbeitet, damit Rimelle ein spezielles Telefon einschaltet und es in der Nähe von Mrs. Stars platziert. Herr Paparazzo nimmt dann den Hörer ab. Er erhält eine Benachrichtigung, wenn Frau Star mit dem Virus infiziert ist.*

Abhängig von den technischen Details des Protokolls kann es möglich sein, in der App falsche Identitäten zu erstellen, um eine große Anzahl von Personen zu verfolgen, ohne eine kaufen zu müssen

20. Durch einfache Techniken kann dieselbe Anwendung auch mehrmals auf demselben Telefon installiert werden, was einen solchen Ansatz weiter erleichtert.

Telefon für jedes Ziel. Man kann Bluetooth-Nachrichten auch über eine große Entfernung (mehr als einen Kilometer) empfangen [9]) mit einer speziellen Antenne. Im dezentralen Modell erfassen wir daher das Pseudonym des Ziels und können innerhalb von zwei Wochen prüfen, ob es zu den als krank identifizierten Personen gehört. Die vorherigen Angriffsszenarien sind für alle vorgesehenen Verfolgungsprotokolle möglich, im dezentralen Modell jedoch einfacher zu implementieren.

6 So lösen Sie einen Fehlalarm aus und lassen ihn so aussehen: meone ist krank

Szenario 7 (Der Anti-System-Aktivist). *Herr Spart, der Symptome von COVID-19 hat, ist ein Anti-System-Aktivist. Aus Protest gegen die Implementierung der TraceVIRUS-App bindet er sein Handy an seinen Hund und lässt ihn den ganzen Tag im Park herumlaufen. Am nächsten Tag geht er zum Arzt und wird positiv getestet und alle Hundewanderer erhalten eine Benachrichtigung.*

Szenario 8 (Ausländische Einmischung). *Das schreckliche U-Boot muss in ein paar Tagen segeln, aber John Bond ist ein ausländischer Agent, der seine Abfahrt verhindern will. Er rekrutiert Sni Gal es Galore, der Symptome zeigt, und bittet sie, um Bars am Wasser herumzugehen. Sni ffl es Galore wird dann getestet und fünf Segler erhalten eine App-Benachrichtigung. Der Schreckliche wird dann gezwungen, im Dock zu bleiben.*

Das gleiche Szenario kann verwendet werden, um bestimmte Personen (einen Gegner in einem Sportwettbewerb, einen Konkurrenten für ein Vorstellungsgespräch, eine Schlüsselperson während einer Verhandlung usw.) oder gemeinsam in großem Maßstab anzusprechen, um ein ganzes System funktionsunfähig zu machen. Die Möglichkeit, Fehlalarme auszulösen, könnte auch in Szenarien ausgenutzt werden, in denen ein Benutzer vorgibt, einen Patienten getroffen zu haben, um zuerst getestet zu werden, vom Krankenstand zu profitieren oder einer von ihm gefürchteten Gelegenheit zu entkommen, wie im folgenden Szenario.

Szenario 9 (Der Schüler Bart Symptomson). *Der Schüler Bart Symptomson hat nächste Woche einen Test, den er jedoch nicht überarbeitet hat. Dank einer klassifizierten Anzeige findet er Mr. Sneeze, der Symptome hat und sich bereit erklärt, Bart sein Handy zu leihen. Bart reicht Mr. Sneezes Telefon während des Unterrichts und hängt dann im Arbeitszimmer herum. Bart gibt es dann an Mr. Sneeze zurück, der zum Arzt geht. Der Arzt stellt fest, dass Herr Sneeze an COVID erkrankt ist und meldet ihn über die App. Dies löst eine Warnung für die gesamte Klasse und für alle Lehrer aus, wodurch die Schule geschlossen wird!*

7 Das Einschalten von Bluetooth wirft Sicherheitsbedenken auf

Das einfache Aktivieren von Bluetooth auf Ihrem Telefon wirft Sicherheits- und Datenschutzprobleme auf. Aus diesem Grund wird generell empfohlen, Bluetooth so oft wie möglich zu deaktivieren.

Durch seine Verwendung können Sicherheitslücken geöffnet werden, durch die Fehler im Bluetooth-System des Telefons ausgenutzt werden. Insbesondere der Blueborne-Angriff [10], das 2017 veröffentlicht wurde, ermöglicht es, die Kontrolle über viele elektronische Elemente (Computer, Telefone usw.) zu übernehmen, indem diese Art von Fehler ausgenutzt wird. Wenn einige Telefone seit 2017 nicht aktualisiert wurden, kann die Aktivierung von Bluetooth sehr gefährlich sein!

Das Bluetooth-Signal kann auch zum Verfolgen von Benutzern verwendet werden. Wir haben alle gesehen, wie einfach es ist, die Bluetooth-Geräte der Nachbarn oder die von Reisenden in einem Zug zu identifizieren. Die Verallgemeinerung seiner Verwendung eröffnet viele Möglichkeiten.

Szenario 10 (Einbruch). *Frau Beagle will Onkel Ducks Haus ausrauben. Vor dem Betreten erkennt sie mit einer Antenne Bluetooth-Signale. Sie weiß, dass Onkel Duck TraceVIRUS benutzt, und wenn es kein Signal gibt, ist das Haus leer.*

Szenario 11 (Einkaufszentrum). *Das Einkaufszentrum Snitch Avenue möchte seine Kunden schützen und diejenigen ablehnen, die die TraceVIRUS-App nicht verwenden. Da die App regelmäßig Nachrichten sendet, muss der Sicherheitsbeamte am Eingang nur eine Bluetooth-Antenne verwenden, um zu erkennen, welche Kunden die Anwendung verwenden und welche nicht.*

Mehrere Kaufhausketten verwenden bereits Bluetooth-Tracking, um ihren Kunden im Geschäft zu folgen und Werbung besser auszurichten [11]. Wenn die Verwendung von Bluetooth verallgemeinert ist, kann man sich viele Möglichkeiten vorstellen, es für viele andere Arten der Verfolgung zu verwenden.

8 Auf dem Weg zum groß angelegten Schnüffeln?

Selbst wenn die geplante App die Kranken nicht selbst verfolgt, ist es möglich, die von der App ausgetauschten Signale zu verwenden, um ein umfangreiches Krankenregister zu erstellen. Die Schwierigkeit, eine solche Datenbank zu erstellen, hängt von den technischen Details des verwendeten Protokolls ab. Mit einem dezentralen System ist dies besonders einfach, da die Liste der Pseudonyme von Patienten öffentlich ist und es ausreicht, sie neu zu identifizieren. Bei einem zentralisierten System müssen Sie in der Lage sein, eine falsche Identität zu erstellen oder ein neues Telefon zu verwenden, und dann Kontakt mit der Person aufnehmen, die Sie verfolgen möchten. In jedem Fall wird es schwierig sein, ein Protokoll zu definieren, das diese Art von Angriff vollständig vermeidet.

Von Benutzern. Die Rückverfolgung kann von den Benutzern selbst durchgeführt werden, um einen besseren Schutz zu gewährleisten. Die zur Verfolgung ausgetauschten Informationen sind auf lokaler Ebene. Wenn sich Benutzer zusammenschließen, können sie globale Informationen wie in Straßenradarerkennungs-Apps neu erstellen. Zum Beispiel können wir das Erscheinen einer „verbesserten“ App (nennen wir sie GeoTraceVIRUS) nicht verhindern, die zusätzlich zu den direkten Kontakten mit Patienten die Orte aufzeichnet, an denen sich Patienten befinden.

In einem dezentralen System reicht es für GeoTraceVIRUS aus, die GPS-Koordinaten gleichzeitig mit den empfangenen Bluetooth-Nachrichten aufzuzeichnen. Wenn ein Pseudonym für krank erklärt wird, kann GeoTraceVIRUS genau wissen, wo sich der Patient befand, als er den Kontakt erhielt, und diese Informationen an andere Benutzer weitergeben. In einem zentralisierten System kann GeoTraceVIRUS die Bewegungen von Benutzern aufzeichnen und eine Gegenprüfung durchführen, wenn bestimmte Benutzer eine TraceVIRUS-Benachrichtigung erhalten. Mit genügend GeoTraceVIRUS-Benutzern ist es zumindest möglich, den Bezirk zu lokalisieren, in dem die Patienten leben.

Szenario 12 (Die GeoTraceVIRUS-Anwendung). *Kurz nach der Installation der App TraceVIRUS erfährt Frau Jones von der GeoTraceVIRUS-App, die TraceVIRUS-Informationen zum Auffinden von Patienten verwendet. Frau Jones erfährt somit, dass ein Patient letzten Samstag in den LowPrice-Supermarkt gegangen ist. Aus (vielleicht unbegründeter) Angst, sich mit dem Virus zu infizieren, wird sie diese Woche nicht bei LowPrice einkaufen gehen.*

Eine andere „verbesserte“ Anwendung, die Benutzer möglicherweise installieren möchten, bietet die Möglichkeit, das Bluetooth-Signal zu verstärken, sodass bei weniger engem Kontakt mit Patienten gewarnt werden kann. Einige dieser alternativen Anwendungen können böswillig sein und die privaten Daten der Benutzer erfassen. Unabhängig von der Qualität der offiziellen Anwendung können die Bluetooth-Signale, auf denen sie basiert, von anderen Apps in einer Verbreitung wiederverwendet werden, die schwierig zu verwalten scheint.

Von Datenanalyseunternehmen. Nach dem Skandal von Cambridge Analytica [12] wissen wir, dass einige Unternehmen nicht zögern, Daten auf illegale Weise zu finanziellen Zwecken zu sammeln. Versicherungsunternehmen oder skrupellose Arbeitgeber könnten an einer Liste von COVID-19-Patienten interessiert sein, wenn beispielsweise die Ansteckung mit der Krankheit das Risiko einer späteren Erkrankung erhöht. Selbst wenn der Staat keine solche Liste hat, ermöglicht die Verwendung einer Verfolgungsanwendung die Erstellung einer solchen Datenbank durch private Agenturen.

Szenario 13 (Versicherung). *Die Supermarktkette ScrupuleFree verwendet Bluetooth-Tracer, um Kunden in ihren Filialen zu verfolgen [11]. Sie verknüpfen den Bluetooth-Identifikator mit dem echten Identifikator, der von der MyScrupuleFree-App oder von Bankkarten abgeleitet wurde, die beim Auschecken verwendet wurden. Während Mr. Smith einkauft, kann das Unternehmen den Kontakt mit seinem Telefon simulieren, sodass sie benachrichtigt werden, wenn Mr. Smith krank ist. Diese Informationen werden an die Versicherungsabteilung gesendet.*

Von Cyberkriminellen. Die Verbreitung organisierter Computerangriffe in den letzten Jahren hat uns davon überzeugt, dass organisierte Cyberkriminelle auch versuchen könnten, diese Informationen abzurufen.

Szenario 14 (Malware). *Mrs. Jones hat die CuteKittens-App auf ihrem Telefon installiert, ohne zu wissen, dass Spyware (dh Malware) sie ausspioniert. Nachdem sie in TraceVIRUS erklärt hat, dass sie krank ist, erhält sie eine Nachricht, um sie zu erpressen, und droht, ihre Krankheit ihrer Versicherungsgesellschaft und ihrem Arbeitgeber zu offenbaren, die ihr Arbeitsverhältnis während der Probezeit kündigen könnten.*

Eine weitere lukrative Aktivität im Bereich der organisierten Kriminalität, die in einigen der vorgeschlagenen Verfolgungssysteme sehr einfach umzusetzen ist, besteht darin, gegen eine Gebühr die obligatorische Quarantäne von zwei Wochen für Zielpersonen auszulösen.

Szenario 15 (Verkauf von positiven Warnungen). *Don Covideone verkauft eine InfectYourNeighbour-App im Internet. Nach dem Herunterladen der App müssen Sie sich nur an das Telefon einer Person wenden, um eine Benachrichtigung zu erhalten, dass sie gefährdet ist. Angriffe sind jetzt ohne technische Fähigkeiten möglich. Daher beabsichtigt Herr Bouque-Maeker, während des nächsten Champions-League-Spiels zu wetten. Zum Glück wird er an der Pressekonferenz von Gronaldo teilnehmen. Er setzt dann trotz der 10: 1-Gewinnchancen stark auf die gegnerische Mannschaft. Er lädt die InfectYourNeighbour-Anwendung herunter und stellt sicher, dass sich sein Telefon während des Interviews in der Nähe von Gronaldo befindet. Gronaldo erhält eine Warnung, er kann das Spiel nicht spielen. Sein Team verliert und Herr Bouque-Maeker gewinnt!*

Eine böswillige Anwendung dieser Art würde dank Sendern oder Empfängern in der Nähe von Personen funktionieren, die möglicherweise infiziert sind (z. B. in der Nähe eines medizinischen Labors). Anschließend werden nur die Nachrichten zwischen potenziell infizierten Personen und der Person weitergeleitet, die Sie als gefährdet melden möchten. Dies kann in mehreren der vorgeschlagenen Tracking-Systeme implementiert werden (zum Beispiel: sehr einfach für DP3T und mit etwas mehr Technologie für ROBERT).

Fazit

Das Verfolgen von Kontakten wirft viele Sicherheitsprobleme und Probleme im Zusammenhang mit dem Datenschutz auf. Die wenigen Szenarien, die wir vorgestellt haben, veranschaulichen eine kleine Anzahl möglicher Probleme.

In dieser Hinsicht kann die Kryptographie nur eine begrenzte Anzahl dieser Probleme behandeln. Einige der von uns vorgestellten Situationen nutzen die Funktionen dieses Systemtyps und nicht deren Implementierung. Urteile im Zusammenhang mit diesen Risiken können daher nicht durch Technologie geklärt werden, sondern erfordern politische Entscheidungen, die vorhersehbare Rechtsverletzungen und Grundfreiheiten sowie die potenziellen Vorteile, die im Kampf gegen die Epidemie zu erwarten sind, in Einklang bringen. Nach unserem Kenntnisstand sind die Vorteile der digitalen Rückverfolgung bis heute sehr ungewiss, während die Szenarien, die wir hier entwickelt haben, bekannt und plausibel sind. Ein wesentliches Prinzip der Computersicherheit ist, dass die Sicherheit eines Systems in keinem Fall von der angenommenen Ehrlichkeit derjenigen abhängen sollte, die an seiner Erstellung, Verwendung oder Verwaltung beteiligt sind. Das gleiche Prinzip zeigt sich in der Entwicklung unseres Rechts in Bezug auf den Schutz personenbezogener Daten. Wenn mit dem Gesetz über Computer und Freiheiten von 1978 Missbräuche von Behörden (insbesondere vom Staat) befürchtet wurden, gefolgt vom privaten Sektor und anschließend von der DSGVO, wurden alle Mitglieder der Gesellschaft mit diesen Bedenken in Verbindung gebracht. Die Angriffe, die ein Verfolgungssystem auf die Rechte und Freiheiten eines jeden von uns ausüben kann, können nicht nur von den Behörden ausgehen, die seine Entwicklung und Umsetzung empfehlen, sondern auch von anderen Personen, kollektiven oder individuellen Personen, die lernen, wie man es macht Nutzen Sie die vielfältigen Eigenschaften dieser Systeme. Der erste Absatz von Abschnitt 1 des Gesetzes von 1978 hat alle seine Überarbeitungen und Entwicklungen überstanden. *Die Informationstechnologie muss jedem Bürger zur Verfügung stehen. [. . .] Es sollte weder die menschliche Identität noch die Menschenrechte, die Privatsphäre oder die individuellen oder öffentlichen Freiheiten verletzen.*

Verweise

[1] Ross Anderson. Kontaktverfolgung in der realen Welt. https: //www.lightbluetouchpaper. org / 2020/04/12 / Kontaktverfolgung in der realen Welt /. (Veröffentlicht und konsultiert 12/04/20)

[2] Susan Landau. Blick über die Kontaktverfolgung hinaus, um die Ausbreitung zu stoppen. https: // www. lawfareblog.com/lookingbeyond-contact-tracing-stop-spread. (Veröffentlicht am 20.04.20, konsultiert am 14.04.20)

[3] Bruce Schneier. Kontaktverfolgung von COVID-19-Infektionen über Smartphone-Apps. https: //www.schneier.com/blog/archives/2020/04/contact_tracing.html. (Veröffentlicht und konsultiert 13/04/20)

[4] Serge Vaudenay. Analyse von DP3T. Cryptology ePrint Archive, Bericht 2020/399, 2020. https://eprint.iacr.org/2020/399 .

[5] Pascale Fombeur. Un decret d'application ne peut renvoyer a un arrete ulterieur la mise en œuvre des principes de la loi. AJDA, Seite 831, 2000. [6] Alan Hunt. Erkundungen in Recht und Gesellschaft. Auf dem Weg zu einer konstitutiven Theorie von Recht. New York, Routledge, 1993.

[7] La Quadrature du Net. Nos Argumente für Rejeter StopCOVID. https: // www. laquadrature.net/2020/04/14/nosarguments-pour-rejeter-stopcovid . (Veröffentlicht und konsultiert 14/04/20)

[8] Frederic Pierru. Les recompositions paradoxales de l'Etat sanitaire fran¸cais. Trans- Verstaatlichung, Etatisierung und Individualisierung des politiques de sante. Education et Societes, 2012/2 (30): 107–129, 2012.

[9] John Hering, James Burgess, Kevin Maha Ey, Mike Outmesguine und Martin Herweiter. Long Distance Snarf, August 2004. https://trifinite.org/trifinite_ stuff_lds.html (18/04/20)

[10] Ben Seri und Gregory Vishnepolsky. Die Gefahren von Bluetooth-Implementierungen: Aufdeckung von Zero-Day-Schwachstellen und Sicherheitslücken in modernen Bluetooth-Stacks. [11] Michael Kwet. In Geschäften verfolgt die geheime Überwachung jede Bewegung im Juni 2019. https://www.nytimes.com/interactive/2019/06/14/opinion/bluetoothwirelesstracking-privacy.html . (Konsultiert am 18.04.20) [12] Wikipedia. Skandale Facebook-Cambridge Analytica, 2020. http: //fr.wikipedia.

org / w / index.php? title = Scandale_Facebook-Cambridge_Analytica, (Konsultiert am 18.04.20)