Pranab Chakraborty
Subhamoy Maitra
Mridul Nandi
Suprita Talnikar

Kontaktverfolgung in der Post-Covid-Welt

Ein kryptologischer Ansatz

Springer Vieweg

Kontaktverfolgung in der Post-Covid-Welt

Pranab Chakraborty · Subhamoy Maitra ·
Mridul Nandi · Suprita Talnikar

Kontaktverfolgung in der Post-Covid-Welt

Ein kryptologischer Ansatz

Springer Vieweg

Pranab Chakraborty
Learning and Development
Wipro Limited
Bengaluru, Karnataka, Indien

Subhamoy Maitra
Applied Statistics Unit
Indian Statistical Institute
Kolkata, Westbengalen, Indien

Mridul Nandi
Applied Statistics Unit
Indian Statistical Institute
Kolkata, Westbengalen, Indien

Suprita Talnikar
Applied Statistics Unit
Indian Statistical Institute
Kolkata, Westbengalen, Indien

ISBN 978-981-97-2647-9 ISBN 978-981-97-2648-6 (eBook)
https://doi.org/10.1007/978-981-97-2648-6

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Dieses Buch ist eine Übersetzung des Originals in Englisch „Contact Tracing in Post-Covid World“ von Pranab Chakraborty, publiziert durch Springer Nature Singapore Pte Ltd. im Jahr 2020. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

Planung/Lektorat: Shamim Ahmad
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Nature Singapore Pte Ltd. und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

An unsere Kollegen im Gesundheitssektor,
die ihr Leben widmen, um uns alle zu retten.

Vorwort

Wir leben in einer Zeit, in der exponentielle Möglichkeiten und ständig wechselnde Unsicherheiten das „neue Normal“ ständig neu definieren. Dieses Mal ist es COVID-19, das das Spielfeld kontrolliert. Optimisten werden auf eine Post-Covid-Welt hoffen, während der Rest sich vielleicht damit abfindet, für lange Zeit, wenn nicht für immer, damit zu leben.

Angesichts der pandemischen Natur der Infektion und der hohen Sterblichkeitsrate, die damit verbunden ist, steht die Welt vor einer beispiellosen Herausforderung, die Krankheit im großen Maßstab zu bekämpfen. Einerseits müssen die Menschen, die an COVID-19 leiden, die bestmögliche medizinische Versorgung und Behandlung erhalten, andererseits ist es von größter Bedeutung sicherzustellen, dass die wenigsten der nicht infizierten Menschen in engen Kontakt mit den Infizierten kommen sollten. Darüber hinaus weiß eine asymptomatische Person möglicherweise nie, dass sie infiziert ist (und möglicherweise ansteckend), es sei denn, sie wird getestet. Gleichzeitig sollte, wenn bekannt ist, dass eine Person infiziert ist, nicht infizierte Personen (abgesehen von den unmittelbaren Familienmitgliedern und medizinischen Fachleuten) von der infizierten Person ferngehalten werden. Dies sollte durch das Mobilfunknetz, Software-Systeme und -Tools und geeignete Richtlinien, Prozesse und Annahmen realisierbar sein. Die Kommunikation zwischen den benachbarten Mobiltelefonen kann über das Bluetooth-Protokoll erreicht werden, während der Standort und andere relevante Informationen an eine zentralisierte Behörde über das Mobilfunknetz übermittelt werden können.

Hier gehen wir davon aus, dass eine Person in der Mehrheit der Umstände wählen würde zu informieren, falls sie infiziert ist oder falls sie das Gefühl hat, dass sie die Infektion möglicherweise an jemand anderen weitergegeben hat. Die andere Annahme ist das Vertrauen der Gemeinschaft in die Regierung und/oder zentrale Verwaltungsbehörden, sodass die persönlich identifizierbaren Informationen einer Person (ob infiziert oder nicht) nicht kompromittiert oder verletzt werden. Es ist bekannt, dass das Thema individueller Datenschutz in bestimmten Ländern mehr Aufmerksamkeit erhält als in anderen. Daher können

politische und soziale Fragen eine dominierende Rolle bei der Entscheidung spielen, wie eine Anwendung im Zusammenhang mit „Kontaktverfolgung“ gestaltet werden sollte. Aus praktischer Sicht könnte die manuelle Kontaktverfolgung immer noch eine der effektivsten Optionen bleiben, um die Ausbreitung der Infektion zu begrenzen. Mit der bemerkenswerten Entwicklung in Berechnung und Kommunikation ist es jedoch nur natürlich, dass die Welt schließlich zu digitalen Systemen übergehen wird, um eine solche globale Pandemie zu bewältigen.

Aus unserer Sicht wird die Kryptologie weiterhin als grundlegende Wissenschaft hinter der Kontaktverfolgungssoftware (Anwendungen/Apps) verwendet, angesichts der Sicherheits- und Datenschutzprobleme. In diesem Buch konzentrieren wir uns hauptsächlich auf verschiedene Kontaktverfolgungsprotokolle aus kryptologischer (d. h. kryptographischer und kryptanalytischer) Sicht. Solche Anwendungen werden in vielen Ländern entwickelt. Die Designer und Entwickler kommen aus Regierungsorganisationen, Industrien, Akademien und Forschungseinrichtungen. Angesichts der Art des Ausbruchs von Covid-19 beobachten wir reflexartige Reaktionen in den meisten Entscheidungsprozessen. Das Gleiche gilt für das Design von Kontaktverfolgungsprotokollen und deren Implementierungen. In einem sehr kurzen Zeitraum, der nur ein paar Monate umfasst, gibt es mehr als zwei Dutzend Vorschläge. Gleichzeitig lesen wir verschiedene kritische Berichte in den Medien über Datenschutzprobleme. Es gibt auch bedeutende technische Analysen in Form von Forschungsmanuskripten. Vor diesem Hintergrund treten wir ein, um das erste kurze und umfassende Buch in diesem Bereich zu schreiben, in dem wir versuchen, die bestehenden Protokolle zu studieren, sie zu analysieren und schließlich einen technischen Vorschlag für ein weiteres logisches Design zu machen.

Wir beginnen mit einem einleitenden Kapitel, in dem wir von den informellen Diskussionen über Kontaktverfolgungsvorschläge zu einer technischeren Analyse übergehen. Wir berühren die meisten der bestehenden digitalen Kontaktverfolgungsprotokolle und Software, die weltweit verwendet und/oder entwickelt werden. Der Übertragungsmechanismus der Virusinfektion wird diskutiert, damit verstanden werden kann, wie die Kontaktverfolgungsanwendungen gestaltet werden sollten. Dann gehen wir zum technischen Rahmenwerk über. Die grundlegenden kryptologischen Primitive werden kurz erklärt. Dies ist notwendig, um die Sicherheits- und Datenschutzprobleme bei der digitalen Kontaktverfolgung zu verstehen. Damit zählen wir einige bekannte Vorschläge auf und versuchen, sie in zwei Kategorien zu unterteilen: zentralisiert und dezentralisiert. Aus kryptologischer Sicht tragen das Design und die Analyse von dezentralisierten Kontaktverfolgungsprotokollen mehr vielfältige und innovative Ideen mit besserer Handhabung von Datenschutzüberlegungen.

Wir diskutieren einige der zentralisierten Anwendungen im zweiten Kapitel, einschließlich Arogya Setu, TraceTogether, BlueTrace, OpenTrace, COVIDSafe usw., die derzeit in Ländern wie Indien, Singapur oder Australien verwendet werden. Wir untersuchen die Elemente und Eigenschaften dieser Vorschläge aus

kryptologischer Sicht. Anschließend diskutieren wir das ROBERT-Protokoll, das sowohl zentralisierte als auch dezentralisierte Eigenschaften aufweist, bevor wir das Kapitel abschließen.

Das dritte Kapitel analysiert die bekannten dezentralisierten Anwendungen wie DP3T und PACT. Solche Designs sind im öffentlichen Bereich für eine vollständige Analyse verfügbar. Auch Technologiegiganten wie Apple und Google sind an ähnlichen Bemühungen beteiligt. Verschiedene kryptologische Primitive und kryptoanalytische Probleme müssen in dieser Perspektive diskutiert werden. Wir gehen durch das Design sowie die Designmethoden dieser Algorithmen und beachten auch die kryptoanalytischen Ergebnisse zur Bewertung der Protokolle. Ein detaillierter Vergleich solcher Protokolle wird ebenfalls diskutiert, um die Vor- und Nachteile hervorzuheben.

Im vierten und letzten Kapitel konzentrieren wir uns darauf, wie ein digitales Kontaktverfolgungssystem gestaltet sein sollte, um die Privatsphäre der Benutzer zu wahren. Wir erklären alle Annahmen und kryptologischen Fragen in diesem Zusammenhang und präsentieren die genaue Problemstellung nach bestem Wissen und Gewissen. Wir diskutieren speziell über höhergradige Kontaktverfolgung in Bezug auf die Nachbarschaft einer Nachbarschaft. Dies geht in die Richtung, dass die Menschen in der ersten Nachbarschaft sofort getestet werden sollten, während die zweite Schicht unter Quarantäne gestellt werden sollte. Wir präsentieren eine detaillierte Analyse unseres allgemeinen Vorschlags und schließen dann ab. Das Buch enthält am Ende jedes Kapitels eine detaillierte Liste von Referenzen.

Die Leser dieses Dokuments sollten ein grundlegendes Verständnis für Kryptologie und Sicherheit haben. Gleichzeitig bietet das erste Kapitel des Buches einen kurzen Hintergrund, sodass die Materialien weitgehend verfolgt werden können. Einige grundlegende Vorstellungen von der Computer- und Kommunikationswissenschaften könnten ebenfalls nützlich sein. Dieses Buch richtet sich an Studenten und Forscher jeder naturwissenschaftlichen und technischen Disziplin sowie an Ingenieure und Fachleute, die im breiten Feld der Berechnung und Kommunikation arbeiten.

Gleichzeitig eröffnet dieses Material einige tiefe Forschungsprobleme für Experten, die eine formale Ausbildung in Kryptologie haben. Die Protokolle, die hier analysiert und beschrieben werden, müssen sorgfältig untersucht werden und die Kryptoanalyse bestimmter Aspekte könnte interessante Forschungsprobleme darstellen.

Bevor wir weiter vorgehen, lassen Sie uns auflisten, was von diesen Bemühungen erwartet wird.

- Dies ist das erste umfassende Buch über den Entwurf und die Analyse von Anwendungen zur Ermittlung von Kontaktpersonen aus einer kryptographischen Perspektive.
- Dieses Buch vermittelt ein klares Verständnis für das Design von Anwendungen zur Ermittlung von Kontaktpersonen, die in verschiedenen Ländern und Kontinenten entwickelt wurden.

- Dieses kurze Dokument stellt eine Verbindung zwischen sehr aktuellen Bemühungen im Zusammenhang mit digitaler Kontaktverfolgung im COVID-19-Szenario und einer kurzen kontextuellen Literaturübersicht in diesem Bereich her.
- Dieser Entwurf gibt einen Einblick in die Entwicklung solcher Anwendungen in einer mobilen, verteilten Umgebung und berücksichtigt dabei die Fragen der Sicherheit und des Datenschutzes, die eine große Herausforderung im Bereich der Computer- und Kommunikationswissenschaften darstellen.
- Dieses Buch bietet eine kurze Darstellung der Kernkonzepte bei der Entwicklung und Analyse von Anwendungen zur Kontaktverfolgung.
- Für Experten in der Kryptologie weist dieses Buch auf mögliche Forschungsrichtungen hin, die auf die Sicherheitsbewertung bestehender Kontaktverfolgungsanwendungen abzielen.

Es gibt vier aufgeführte Autoren dieses Buches (in alphabetischer Reihenfolge der Nachnamen), aber diese Anstrengung ist ein Ergebnis der Forschungsbemühungen auf der ganzen Welt. Wir danken allen Forschern, die im Bereich der Kontaktverfolgung arbeiten. Gleichzeitig müssen wir unsere Familienmitglieder und Freunde anführen, die uns in dieser schwierigen Zeit ständig ermutigt haben. Ihre Freundlichkeit, Liebe und Inspiration waren die Hauptmotivation hinter jedem Wort dieses gedruckten Materials. Wir danken auch der Unterstützung von Herrn Rishabh Kothary, einem B.S. Mathematik- und Wissenschaftliches-Rechnen-Studenten vom Indian Institute of Technology Kanpur, der während dieser Anstrengung als Praktikant gearbeitet hat und einige interessante Hinweise gegeben hat. Dr. Dibyendu Roy, Dr. Pinakpani Pal und Herr Manmatha Roy vom Indian Statistical Institute, Kolkata, haben ebenfalls zusätzliche Beiträge in dieser Hinsicht geleistet. Wir möchten Herrn Shamim Ahmad, dem leitenden Redakteur von Springer Nature India Private Limited, für seine Fähigkeit zur Führung danken. Nicht zuletzt danken alle Autoren ihren jeweiligen Familienmitgliedern für die große Unterstützung während dieser Pandemie. Ohne all diese Ermutigungen und Beiträge hätte dieses Buch nicht in kurzer Zeit geschrieben werden können.

Jeder Autor möchte darauf hinweisen, dass alle in diesem Buch (zusammen mit anderen Co-Autoren) geäußerten Ansichten und Empfehlungen ausschließlich persönlicher Natur sind und in keiner Weise mit der jeweiligen aktuellen Organisation in Verbindung stehen. Darüber hinaus basiert diese Arbeit rein auf einem persönlichen Forschungsinteresse und steht nicht in Zusammenhang mit ihrer beruflichen Arbeit.

Das Gebiet der digitalen Kontaktverfolgung ist ein aufkommendes Feld. Wir alle wünschen jedoch, dass die gegenwärtige Pandemie so schnell wie möglich vorbei sein wird. Wir würden uns mehr als je zuvor freuen, unsere Welt ohne

jegliche Notwendigkeit der Kontaktverfolgung zu haben, wo dieses Buch nutzlos werden würde. Blättern Sie etwa immer noch die Seiten um?

Bangalore, Indien — Pranab Chakraborty
Kolkata, Indien — Subhamoy Maitra
Kolkata, Indien — Mridul Nandi
Juli 2020 — Suprita Talnikar

Inhaltsverzeichnis

Über die Autoren

Pranab Chakraborty ist Senior Manager im Learning and Development Team von Wipro Limited, Bengaluru, Indien. Er erwarb seinen Hochschulabschluss in Informatik am Indian Statistical Institute, Kolkata, Indien, und seinen Bachelor-Abschluss in Elektronik und Telekommunikationstechnik an der Jadavpur University, Kolkata, Indien. Er hat verschiedene Netzwerkprotokollstapel implementiert, einschließlich TCP/IP, und verschiedene organisatorische Rollen gespielt, einschließlich der eines technischen Architekten und technischen Liefermanagers, abgesehen von seiner aktuellen Beteiligung im Bereich der Verhaltens- und Führungskräfteentwicklung. Er hat ein besonderes Interesse an den Forschungsbereichen der Kryptologie.

Subhamoy Maitra ist Senior Professor an der Abteilung für Angewandte Statistik des Indian Statistical Institute in Kolkata, Indien. Er erwarb seinen Doktortitel und seinen Hochschulabschluss in Informatik am Indian Statistical Institute in Kolkata, Indien, und seinen Bachelor-Abschluss in Elektronik und Telekommunikationstechnik an der Jadavpur University in Kolkata, Indien. Nach einigen Jahren in der Hardware- und Softwaretechnik trat Prof. Maitra 1997 als Dozent am Indian Statistical Institute in Kolkata ein. Mit rund 6000 Zitaten hat Prof. Maitra mehrere Bücher und etwa 200 Forschungsarbeiten auf dem Gebiet der Kryptologie und Quanteninformation verfasst.

Mridul Nandi ist Professor an der Abteilung für Angewandte Statistik des Indian Statistical Institute in Kolkata, Indien. Zuvor arbeitete er für das National Institute of Standards and Technology (NIST), USA, als eines der technischen Mitglieder im Auswahlprozess der SHA3-Hash-Funktion. Seine Forschungsbereiche konzentrieren sich auf verschiedene Aspekte der Kryptographie, einschließlich Hash-Funktionen, MAC, authentifizierte Verschlüsselung, Identitäts- (oder Attribut-) basierte Verschlüsselung, IoT, Hardware-Implementierung und leichte Kryptographie. Er ist der Mitgestalter von COLM (authentifizierte Verschlüsselung), das als Gewinner in der Sicherheitskategorie des CAESAR-Portfolios ausgewählt wurde. Algorithmen seiner entworfenen 10 leichten Chiffren wurden für die zweite Runde des NIST-Leichtgewichtsstandardprozesses

ausgewählt. Er veröffentlicht aktiv Beiträge in erstklassigen Konferenzen wie Eurocrypt, Crypto, Asiacrypt, FSE und renommierten Zeitschriften.

Suprita Talnikar ist Senior Research Fellow an der Abteilung für Angewandte Statistik des Indian Statistical Institute in Kolkata, Indien. Sie promoviert in Informatik unter der Aufsicht von Prof. Mridul Nandi. Sie hat ihren M.Sc. in Mathematik vom Visvesvaraya National Institute of Technology, Nagpur, Indien, mit einer Goldmedaille abgeschlossen und ihren B.Sc. in Physik, Informatik und Mathematik von der Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Indien, erworben. Ihre Forschung konzentriert sich auf verschiedene Bereiche der Kryptographie, mit besonderem Interesse an nachweisbarer Sicherheit und Kryptoanalyse in der symmetrischen Schlüsselkryptographie.

Kapitel 1
Einführung und Vorüberlegungen

Zusammenfassung In diesem Kapitel werden wir das grundlegende Verständnis von Kontaktverfolgungssoftware und den damit verbundenen kryptographischen Techniken diskutieren. Die zugrunde liegenden Modelle der Berechnung und Kommunikation werden erklärt. Ein Standard-Smartphone kann als das grundlegende Gerät betrachtet werden und es wird eine Kommunikation zwischen diesen Geräten mit Bluetooth-Technologie geben. Die Datenübertragung zwischen dem mobilen Gerät und dem Backend-Server (könnte von staatlichen Behörden kontrolliert werden) wird durch den standardmäßigen Datenkommunikationskanal, der vom Dienstanbieter bereitgestellt wird, sichergestellt. Soziale Fragen im Zusammenhang mit der Privatsphäre werden auch in diesem einleitenden Kapitel angesprochen.

1.1 Einführung

Betrachten Sie das Design einer Anwendung, sodass, wenn Sie sich räumlich nahe bei einem Ihrer Freunde befinden, Ihr Mobiltelefon Ihnen ein Signal gibt. Es könnte zwei verschiedene Ansätze zur Implementierung geben. In einem Ansatz könnten die Standorte der Telefone kontinuierlich von einem Ortungssystem analysiert werden. Immer wenn das System zwei Telefone in unmittelbarer Nähe zueinander findet, würde es überprüfen, ob eine Telefonnummer in der Kontaktliste der anderen ist. Wenn gefunden, dann werden beide Telefone mit einem charakteristischen Ton, einer Vibration oder einer Nachricht benachrichtigt. Was sind die Probleme bei diesem Ansatz?

1. Zunächst einmal gibt es an einem Ort eine große Anzahl von Mobiltelefonen und daher könnte ein solcher Abgleichsalgorithmus möglicherweise enorme Kosten für Berechnung und Kommunikation verursachen.
2. Die Komplexität des Algorithmus würde sich aufgrund der dynamischen und Echtzeit-Natur des Prozesses vervielfachen.

P. Chakraborty et al., *Kontaktverfolgung in der Post-Covid-Welt*,
https://doi.org/10.1007/978-981-97-2648-6_1