Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Corona-Warn-Apps haben Defizite bei Sicherheit und Datenschutz

Forschungskonsortium belegt Risiken in Google- und Apple-Spezifikation für Corona-Apps

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. +49 6151 16 - 20018
joerg.feuck@tu-darmstadt.de
www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 12. Juni 2020. Ein Forschungsteam der Technischen Universität Darmstadt, der Universität Marburg und der Universität Würzburg hat jüngst in Publikationen als theoretisch möglich beschriebene Datenschutz- und Sicherheitsrisiken der Spezifikation des von Google und Apple vorgeschlagenen Ansatzes für Corona-Apps unter realistischen Bedingungen praktisch demonstriert und bestätigt. Auf diesem Ansatz basiert unter anderem die von der Deutschen Telekom und SAP im Auftrag der Bundesregierung entwickelte deutsche Corona-Warn-App; aber auch die schweizerischen und italienischen Kontaktnachverfolgungs-Apps nutzen diese Plattform.

Durch Experimente in realen Szenarien zeigte das Forschungsteam, dass bereits theoretisch bekannte Risiken mit gängigen technischen Mitteln ausgenutzt werden können. So kann zum einen ein externer Angreifer detaillierte Bewegungsprofile von mit COVID-19 infizierten Personen erstellen und unter bestimmten Umständen die betroffenen Personen identifizieren. Zum anderen ist ein Angreifer in der Lage, die gesammelten Kontaktinformationen durch sogenannte Relay-Angriffe zu manipulieren, was die Genauigkeit und Zuverlässigkeit des gesamten Kontaktnachverfolgungssystems beeinträchtigen kann.

Kontaktnachverfolgungs-Apps auf mobilen Geräten versprechen die Möglichkeit, den manuellen Aufwand zur Identifizierung von Infektionskreisläufen erheblich zu reduzieren und die Abdeckung der Kontaktnachverfolgung zu erhöhen. Einer der bekanntesten Vorschläge zur Kontaktnachverfolgung stammt aus der Zusammenarbeit der Konzerne Google und Apple. Es ist zu erwarten, dass die beiden US-amerikanischen Firmen diese neue Standardfunktionalität in ihre jeweiligen mobilen Betriebssysteme, Android und iOS, integrieren werden. Einige Länder, darunter auch Deutschland, haben in ihren nationalen Projekten zur digitalen Ermittlung von Kontaktpersonen bereits diesen Ansatz gewählt.

Ausgangspunkt für die Experimente der IT-Sicherheitsexperten und -expertinnen der drei Universitäten waren zuvor veröffentlichte Berichte über mögliche Datenschutz- und Sicherheitsrisiken im Zusammenhang mit den Entwicklungen des sogenannten „Google Apple Protokoll“ (GAP). Das Forschungsteam testete, ob die konzeptionell beschriebenen Angriffe in der Praxis ausgeführt werden können. Die Experimente zeigen, dass GAP einerseits anfällig ist für die Erstellung von Profilen und so möglicherweise die De-Anonymisierung von infizierten Personen erlaubt. Andererseits sind in GAP auch so genannte Relay- oder Wurmloch-Angriffe möglich, wodurch

Angreifer falsche Kontaktinformationen generieren können und somit die Genauigkeit und Korrektheit des Gesamtsystems leidet.
Das Forschungsteam realisierte die Angriffe mithilfe handelsüblicher preiswerter Werkzeuge wie Bluetooth-Sniffer (als App auf Smartphones oder Raspberry Pis), die auch in mobilen Umgebungen eingesetzt werden können. Da die Implementierung des GAP-Ansatzes noch nicht für die breitere Wissenschafts-Community verfügbar ist, hat das Forschungsteam die Angriffe basierend auf bereits publizierten Spezifikationen konstruiert.
Die Ergebnisse zeigen, dass bei Verwendung strategisch platzierter Sensoren auf Smartphones in einem bestimmten Gebiet die Bewegungen infizierter Personen, simuliert durch Testpersonen, detailliert rekonstruiert werden können. Dadurch war es möglich, sensible Aufenthaltsorte der Testpersonen sowie mögliche soziale Beziehungen zwischen ihnen zu identifizieren.
Die Anfälligkeit von GAP für sogenannte Relay- oder Wurmloch-Attacken offenbart ebenfalls Schwächen. Diese Methode versetzt einen Angreifer in die Lage, die sogenannten Bluetooth-Benutzer-IDs, die von einer Kontaktnachverfolgungs-App erzeugt werden, zu sammeln und unbemerkt an weiter entfernte Orte weiterzuleiten. Unter anderem konnten erfolgreich Bluetooth-IDs zwischen zwei 40 Kilometer voneinander entfernten Städten übertragen werden. Dadurch kann ein Angreifer das Kontaktnachverfolgungssystem als Ganzes beeinträchtigen, indem er Informationen über die Anwesenheit von Infizierten an vielen Orten fälschlicherweise dupliziert, was zu einer erheblichen Zunahme von Fehlalarmen über das potenzielle Infektionsrisiko führen könnte.
Insgesamt sieht das Forschungsteam noch deutliches Verbesserungspotenzial für den von Google und Apple vorgeschlagenen Ansatz für Corona-Apps.

Eine detaillierte Beschreibung der Experimente und ihrer Ergebnisse ist im vollständigen Studienbericht zu finden unter
http://arxiv.org/abs/2006.05914

Ansprechpartner für die Medien

Prof. Dr. Ahmad-Reza Sadeghi, TU Darmstadt
Fachbereich Informatik
Email: ahmad.sadeghi@trust.tu-darmstadt.de
Mobil: 0 175 72 0 55 45

Prof. Dr. Bernd Freisleben, Philipps-Universität Marburg
Fachbereich Mathematik und Informatik
Email: freisleben@uni-marburg.de
Mobil: 0171 4722249

Prof. Dr. Alexandra Dmitrienko, Julius-Maximilians-Universität Würzburg
Fachbereich Informatik
Email: alexandra.dmitrienko@uni-wuerzburg.de
Mobil: 0152 217 99 773

Über die TU Darmstadt

Die TU Darmstadt zählt zu den führenden Technischen Universitäten in Deutschland. Sie verbindet vielfältige Wissenschaftskulturen zu einem charakteristischen Profil. Ingenieur- und Naturwissenschaften bilden den Schwerpunkt und kooperieren eng mit prägnanten Geistes- und Sozialwissenschaften. Weltweit stehen wir für herausragende Forschung in unseren hoch relevanten und fokussierten Profilbereichen: Cybersecurity, Internet und Digitalisierung, Kernphysik, Energiesysteme, Strömungsdynamik und Wärme- und Stofftransport, Neue Materialien für Produktinnovationen. Wir entwickeln unser Portfolio in Forschung und Lehre, Innovation und Transfer dynamisch, um der Gesellschaft kontinuierlich wichtige Zukunftschancen zu eröffnen. Daran arbeiten unsere 308 Professorinnen und Professoren, 4.500 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie 25.200 Studierenden. Mit der Goethe-Universität Frankfurt und der Johannes Gutenberg-Universität Mainz bildet die TU Darmstadt die strategische Allianz der Rhein-Main-Universitäten.

www.tu-darmstadt.de

MI-Nr. 31/2020, CYSEC/feu