Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Populäre Messenger-Dienste sind extrem unsicher

WhatsApp, Signal & Co: Angriffe auf die Privatsphäre von über einer Milliarde Menschen

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:
Jörg Feuck
Tel. 06151 16 - 20018
Fax 06151 16 - 23750
feuck@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 15. September 2020. Forschungs-Teams der Technischen Universität Darmstadt und der Universität Würzburg zeigen, dass populäre mobile Messenger persönliche Daten über Kontaktermittlungsdienste preisgeben. Diese ermöglichen, Kontakte anhand von Telefonnummern aus dem persönlichen Adressbuch zu finden.

Nach der Installation eines mobilen Messengers wie WhatsApp können Nutzerinnen und Nutzer direkt mit ihren Kontakten interagieren, deren Telefonnummern in ihrem Adressbuch gespeichert sind. Dafür müssen die Nutzenden der App die Erlaubnis erteilen, auf ihr Adressbuch zuzugreifen und dieses regelmäßig zum Kontaktabgleich an die Server des Dienstanbieters hochzuladen. Eine aktuelle Studie eines Teams von Forscherinnen und Forschern der Secure Software Systems Group an der Universität Würzburg und der Cryptography and Privacy Engineering Group an der TU Darmstadt zeigt, dass derzeit verwendete Methoden zur Kontaktermittlung die Privatsphäre von weit mehr als einer Milliarde Nutzenden massiv bedrohen. Unter Verwendung sehr weniger Ressourcen war das Team in der Lage, praktikable Crawling-Angriffe auf die populären Messenger WhatsApp, Signal und Telegram durchzuführen. Die Experimente zeigen, dass bösartige Nutzende oder Hacker in großem Stil und ohne nennenswerte Einschränkungen sensible Daten sammeln können, indem sie bei Diensten zur Kontaktermittlung zufällige Telefonnummern abfragen.

Angreifer können genaue Verhaltensmodelle erstellen

Für die umfangreiche Studie haben die Forscherinnen und Forscher 10% aller Mobilfunknummern in den USA für WhatsApp und 100% für Signal abgefragt. Dadurch waren sie in der Lage, persönliche (Meta-) Daten zu sammeln, wie sie üblicherweise in den Nutzerprofilen der Messenger gespeichert sind, inklusive Profilbilder, Nutzernamen, Statustexte und die „zuletzt online“ verbrachte Zeit. Die analysierten Daten offenbaren auch interessante Statistiken über das Nutzerverhalten. Beispielsweise ändern sehr wenige Nutzende die standardmäßigen Privatsphäre-Einstellungen, die für die meisten Messenger ganz und gar nicht Privatsphäre-freundlich sind.

Das Team fand heraus, dass ungefähr 50% aller WhatsApp-Nutzerinnen und -Nutzer in den USA ein öffentliches Profilbild haben und 90% einen öffentlichen Infotext. Interessanterweise verwenden 40% aller bei Signal Registrierten (von denen man allgemein vermuten würde, dass sie mehr um ihre Privatsphäre besorgt sind) auch WhatsApp, und die Hälfte von diesen hat ein öffentliches Profilbild bei WhatsApp. Solche Daten über die Zeit zu verfolgen verhilft Angreifenden dazu, genaue Verhaltensmodelle zu erstellen. Wenn die Daten mit sozialen Netzen und anderen öffentlichen Datenquellen abgeglichen werden, können Dritte auch detaillierte Profile erstellen und beispielsweise für Betrugsmaschen nutzen. Bezüglich Telegram fanden die Forscherinnen und Forscher heraus, dass der Dienst zur Kontaktermittlung auch sensible Informationen selbst über die Besitzerinnen und Besitzer von Telefonnummern preisgibt, die nicht bei dem Dienst registriert sind.

Welche Informationen während der Kontaktermittlung preisgegeben und über Crawling-Angriffe gesammelt werden können, hängt vom Dienstanbieter und den gewählten Privatsphäre-Einstellungen ab. Beispielsweise übertragen WhatsApp und Telegram das komplette Adressbuch der Nutzenden an entsprechende Server. Privatsphäre-schützende Messenger wie Signal übertragen nur kurze kryptographische Hashwerte von Telefonnummern oder verlassen sich auf vertrauenswürdige Hardware. Die Forschungs-Teams zeigen jedoch, dass es mit Hilfe neuer und optimierter Angriffsstrategien dennoch möglich ist, innerhalb von Millisekunden von den Hashwerten auf die zugehörigen Telefonnummern zurückzuschließen. Noch gravierender, da es keine nennenswerten Hürden für die Registrierung bei solchen Messengern gibt, ist dies: Dritte können eine große Anzahl an Accounts erstellen und die Nutzerdatenbanken eines Messengers nach Informationen durchforsten, indem Daten für zufällige Telefonnummern abgefragt werden. „Wir empfehlen bei der Verwendung von mobilen Messengern dringend, sämtliche Privatsphäre-Einstellungen zu überprüfen. Dies ist derzeit der effektivste Schutz gegen unsere untersuchten Crawling-Angriffe“ sind sich Prof. Alexandra Dmitrienko (Universität Würzburg) und Prof. Thomas Schneider (TU Darmstadt) einig.

Auswirkungen der Forschungsergebnisse:
Dienstanbieter verbessern ihre Schutzmaßnahmen

Die Forschenden haben ihre Erkenntnisse mit den jeweiligen Dienstanbietern geteilt. WhatsApp hat seine Schutzmaßnahmen daraufhin derart verbessert, dass großangelegte Angriffe nun erkannt werden und

Signal hat die Anzahl möglicher Abfragen reduziert, um Crawling zu erschweren. Die Forscherinnen und Forscher schlagen auch verschiedene andere Techniken zum Schutz vor, inklusive eines neuen Verfahrens zur Kontaktermittlung, das die Effizienz von Angriffen reduzieren würde, ohne die Nutzbarkeit negativ zu beeinflussen.

Sämtliche Ergebnisse sind in dem Paper “All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers” beschrieben, welches im Februar 2021 auf dem 28. Annual Network and Distributed System Security Symposium (NDSS) präsentiert wird, einer Topkonferenz für IT-Sicherheit.

Kontakt

Prof. Dr.-Ing. Alexandra Dmitrienko
Secure Software Systems Group
Universität Würzburg
E-Mail: alexandra.dmitrienko@uni-wuerzburg.de
Tel.: 0931/31-81667
https://go.uniwue.de/dmitrienko

Prof. Dr.-Ing. Thomas Schneider
Cryptography and Privacy Engineering Group (ENCRYPTO)
TU Darmstadt
E-Mail: schneider@encrypto.cs.tu-darmstadt.de
Tel.: 06151/16-27300
https://encrypto.de/schneider

Publikation

All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers von Christoph Hagen (Universität Würzburg), Christian Weinert (TU Darmstadt), Christoph Sendner (Universität Würzburg), Alexandra Dmitrienko (Universität Würzburg) und Thomas Schneider (TU Darmstadt) in 28. Annual Network and Distributed System Security Symposium (NDSS’21). Pre-print: https://encrypto.de/papers/HWSDS21.pdf

Mehr zum Thema

Mehr Details: https://contact-discovery.github.io

Video zur Bedrohung der Privatsphäre durch Dienste zur Kontaktermittlung und mögliche Gegenmaßnahmen: https://youtu.be/P_K166jvG7U

Beteiligte Forschungsgruppen:

- Secure Software Systems Group an der Universität Würzburg: https://go.uniwue.de/sss
- Cryptography and Privacy Engineering Group (ENCRYPTO) an der TU Darmstadt: https://encrypto.de

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 312 Professorinnen und Professoren, rund 4.500 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie rund 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. 51/2020 Christian Weinert/Daniela Fleckenstein