idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Technische Universität Darmstadt
Bettina Bastian

22.04.2021
http://idw-online.de/de/news767318

Forschungsergebnisse
Informationstechnik
überregional

Apple AirDrop teilt nicht nur Dateien: Forschende der TU entdecken Datenschutzlücke bei Apple-Filesharing-Funktion

Mittels AirDrop können Apple-User Dateien miteinander teilen. Doch Untersuchungen von TU-Forschenden am Fachbereich Informatik zeigen, dass auch ungebetene Personen Daten abgreifen können. Das Forschungsteam entwickelte eine Lösung, die das unsichere AirDrop ersetzen könnte. Apple hat die entdeckte Datenschutzlücke bisher noch nicht geschlossen.

Schnappschüsse, Präsentationen, Videos – solche Dateien können Nutzerinnen und Nutzer von iPhones und MacBooks bequem miteinander teilen. Möglich macht es die Funktion AirDrop, mit der Dateien direkt von einem Apple-Gerät zum anderen gesendet werden können. Da vertrauliche Dateien im Regelfall nur an bekannte Personen weitergegeben werden sollen, zeigt AirDrop standardmäßig nur Empfängergeräte von Adressbuchkontakten an. Um festzustellen, ob die andere Partei ein Kontakt ist, verwendet AirDrop ein Authentifizierungsverfahren, das die eigenen Kontaktdaten mit den Einträgen im Adressbuch des anderen Geräts abgleicht.

Forscher des Secure Mobile Networking Lab (SEEMOO) und der Cryptography and Privacy Engineering Group (ENCRYPTO) der TU Darmstadt haben dieses Verfahren genauer untersucht und ein gravierendes Datenschutzproblem gefunden.

Angreifer können Telefonnummern und E-Mail-Adressen von Apple-Nutzenden abgreifen – ohne jegliches Vorwissen über ihre Opfer. Der Angriff benötigt lediglich ein Wi-Fi-fähiges Gerät und die physische Nähe zu Personen mit Apple-Geräten. Sobald eine Person das ‚Teilen'-Menü öffnet, wird der Erkennungsprozess auf dem Apple-Gerät initiiert und der Angreifer kann sich „einklinken".

Die entdeckte Datenschutzlücke ist auf die Verwendung von sogenannten Hash-Funktionen zurückzuführen, die Apple nutzt, um Kontaktdaten während der Authentifizierung zu „verschleiern". Allerdings haben Forschende der TU Darmstadt bereits nachgewiesen, dass das Austauschen von gehashten Telefonnummern unsicher ist, da sie mithilfe von beispielsweise Brute-Force-Angriffen schnell zurückgerechnet werden können.

Neues kryptographisches Protokoll kann Datenschutz garantieren

Das Forschungsteam entwickelte außerdem eine praktikable Lösung, die das unsichere AirDrop ersetzen könnte. PrivateDrop basiert auf kryptographischen Protokollen für ‚Private Set Intersection', also zur sicheren Berechnung einer Schnittmenge aus vertraulichen Datensätzen. Mit dieser Methode kann die gegenseitige Authentifizierung durchgeführt werden, ohne angreifbare Hash-Werte austauschen zu müssen. PrivateDrop wurde von den Forschern zu Testzwecken auf Apple-Geräten implementiert. Messungen zeigen, dass die Performance mit der des unsicheren AirDrop konkurrieren kann: Die benötigte Zeit für die Authentifizierung liegt weit unter einer Sekunde.

Bereits im Mai 2019 informierten die Forscher den Apple-Konzern über die gefundene Datenschutzlücke. Bisher hat Apple die Datenschutzlücke weder bestätigt noch angekündigt, an einer Lösung zu arbeiten, sodass die Nutzenden von mehr als 1,5 Milliarden Apple-Geräten weiterhin anfällig sind. Die einzige Möglichkeit sich zu schützen besteht derzeit darin, die AirDrop-Erkennung in den Systemeinstellungen zu deaktivieren und das ‚Teilen'-Menü nicht zu öffnen.

Die Forschungsergebnisse wurden in einem wissenschaftlichen Artikel veröffentlicht, der im August auf dem renommierten „USENIX Security Symposium" präsentiert wird.

wissenschaftliche Ansprechpartner:

M.Sc. Christian Weinert
Cryptography and Privacy Engineering Group (ENCRYPTO)
Department of Computer Science
weinert@encrypto.cs.tu-darmstadt.de

Dr.-Ing. Milan Stute
Secure Mobile Networking Lab (SEEMOO)
Department of Computer Science
mstute@seemoo.tu-darmstadt.de

Originalpublikation:

Alexander Heinrich, Matthias Hollick, Thomas Schneider, Milan Stute, and Christian Weinert. PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop. 30th USENIX Security Symposium, 2021.
https://www.usenix.org/conference/usenixsecurity21/presentation/heinrich

URL zur Pressemitteilung: https://www.tu-darmstadt.de/universitaet/aktuelles_meldungen/einzelansicht_311168.de.jsp