iMessage: So funktioniert die Kontaktschlüsselbestätigung

Originalartikel

Backup

<html> <figure class=„aufmacherbild“></figure> Seit iOS 17.2 erlaubt es Apple, in iMessage-Privat- und Gruppenchats zu überprüfen, ob man es wirklich mit dem korrekten Gegenüber zu tun hat. So geht's. Apples Nachrichten-App war 2011 der erste weitverbreitete Messenger, der standardmäßig eine sichere Ende-zu-Ende-Verschlüsselung (End-to-End-Encryption, kurz E2EE) bot. Damit hat Apple eine grundlegende Bedrohung von Kommunikationssystemen adressiert: das unbefugte Mitlesen von Nachrichten. E2EE verhindert, dass Dritte Inhalte einer iMessage-Unterhaltung mitlesen können. Um seine Nachrichten-App sicherer zu machen, hat Apple mit iOS 14 dann einen Mechanismus namens BlastDoor [1] [1] eingeführt, der Angriffe mit schädlichen Dateianhängen in der Nachrichten-App erschwert. Ein Angreifer kann zwar iMessage attackieren, aber in der Regel nicht aus der App ausbrechen und das ganze Gerät kompromittieren – wobei es in der Vergangenheit schon Beispiele dafür gab, etwa durch die Spyware Pegasus [2] [2]. Mit iOS 16 hat Apple außerdem einen optionalen Lockdown-Mode (Blockierungsmodus) [3] [3] eingeführt, der bei Aktivierung eine weitere Härtung gegen Angriffe unter anderem in der Nachrichten-App beinhaltet. Dieser Modus deaktiviert eine ganze Reihe potenziell gefährlicher Funktionen – also solche, bei denen Daten aus fremder Quelle verarbeitet werden. Allerdings bleibt noch eine relevante Bedrohung bei iMessage: die Kommunikation mit jemandem, der vorgibt, jemand anderes zu sein. Wer über iMessage Vertrauliches teilt, sollte sich sicher sein, mit wem er es zu tun hat. Das ist aber nicht immer ersichtlich: Vielleicht hat das Gegenüber ja eine neue Telefonnummer, und die alte, bei

iMessage registrierte Nummer ist jetzt an jemand anderen vergeben. Oder ein Angreifer nutzt eine Nummernportierung oder übernommene iMessage-E-Mail-Adresse gezielt aus und kann sich so unbemerkt in Unterhaltungen einschleusen. Das können gezielte sogenannte SIM-Swapping-Angriffe gegen privilegierte Zielpersonen (etwa Journalisten, Politiker oder Dissidenten) sein, bei denen die Nummer des Opfers übernommen wird. Aber auch „normale“ Endanwender können betroffen sein. <hr /> URL dieses Artikels:
<small>

```
https://www.heise.de/-9622945
```

</small> Links in diesem Artikel:
<small>

```
<strong>[1]</strong>&amp;#160;https://www.heise.de/hintergrund/Pegasus-Der-Spion-der-auf-das-iPhone-kam-6206945.html
```

</small>
<small>

```
<strong>[2]</strong>&amp;#160;https://www.heise.de/hintergrund/Analyse-Wie-die-iPhone-Spyware-Pegasus-vorging-7073968.html
```

</small>
<small>

```
<strong>[3]</strong>&amp;#160;https://www.heise.de/ratgeber/Praxis-Wie-iOS-16-und-macOS-13-fuer-mehr-Sicherheit-sorgen-7322163.html
```

</small>
<small>

```
<strong>[4]</strong>&amp;#160;https://www.heise.de/ratgeber/iOS-17-iPadOS-17-und-watchOS-10-16-Tipps-fuer-den-Praxiseinsatz-9308593.html
```

</small>
<small>

```
<strong>[5]</strong>&amp;#160;https://www.heise.de/ratgeber/iOS-17-Co-Neue-Funktionen-in-Apple-Apps-ausreizen-9309783.html
```

</small>
<small>

```
<strong>[6]</strong>&amp;#160;https://www.heise.de/tests/iPhone-15-15-Plus-15-Pro-und-15-Pro-Max-im-Test-Leichte-Verbesserungen-9313305.html
```

</small>
<small>

```
<strong>[7]</strong>&amp;#160;https://www.heise.de/hintergrund/Ausprobiert-Wie-der-iPhone-Satellitenfunk-Leben-retten-kann-7393605.html
```

</small>
 Copyright © 2024 Heise Medien </html>