Kai Jendrian

Sicheres Instant Messaging

Alternativen zu WhatsApp und iMessage

Die Platzhirsche unter den Instant Messengern haben in der Vergangenheit große Schwachstellen im Hinblick auf die Vertraulichkeit der übertragenen Nachrichten offenbart. In diesem Beitrag wird zunächst ein Blick auf mögliche Alternativen geworfen und anschließend die App Threema genauer vorgestellt.

1 Sicheres Instant Messaging

Im Zusammenhang mit den zahlreichen Erkenntnissen aus den Enthüllungen von Edward Snowden ist das Vertrauen in die Anbieter von Kommunikationsdienstleistern stark gesunken. Dieser Vertrauensverlust betrifft durchaus auch die Platzhirsche im Bereich des Instant Messaging, die sich in den vergangenen Jahren nicht nur bei Jugendlichen als SMS-Ersatz durchsetzen konnten. Bei beliebten Diensten wie iMessage von Apple[1] und WhatsApp, das inzwischen zu Facebook gehört, ist nicht auszuschließen, dass der Dienstanbieter Kenntnis von den Inhalten der übermittelten Nachrichten erlangt.

Wer weiterhin den Komfort von Instant Messaging nutzen, dabei aber die Vertraulichkeit der ausgetauschten Nachrichten sicherstellen will, muss sich also nach einer Alternative umsehen, die einen Nachrichtenaustausch ermöglicht, bei dem alle Nachrichten Ende-zu-Ende verschlüsselt sind.

Ein wesentliches Kriterium zur Wahrung der Privatsphäre bei Nutzung von Instant Messaging ist dabei die Möglichkeit zur Verifikation der ausgetauschten Schlüssel durch die Benutzer. Nur so lässt sich sicherstellen, dass der Dienstbetreiber selbst nicht über einen Man-in-the-Middle-Angriff[2] Kenntnis von den Inhalten der ausgetauschten Nachrichten erlangt.

1 http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf
2 http://de.wikipedia.org/wiki/Man-in-the-middle-Angriff

Kai Jendrian

Security Consultant bei der Secorvo Security Consulting GmbH, lizenzierter Auditor und Mitglied im Board des deutschen OWASP Chapters. Beratungsschwerpunkte: Information Security Management und Anwendungssicherheit.
E-Mail: kai.jendrian@secorvo.de

2 Sichere Alternativen

Als Alternative böte sich zunächst ein Produkt an, dass für den Austausch von Nachrichten auf das bewährte OTR-Protokoll[3] zurückgreift. Hierzu gibt es eine Reihe von Apps, die häufig auf etablierte Chat-Infrastrukturen (Yahoo, Facebook, ...) setzen und über diese Infrastrukturen eine verschlüsselte Kommunikation implementieren. Leider setzt das OTR-Protokoll eine synchrone Kommunikation voraus, so dass immer beide Kommunikationspartner online sein müssen. Einer der großen Vorteile von Instant Messagern ist jedoch die Unterstützung eines asynchronen Nachrichtenaustauschs. Hierbei wird eine Nachricht solange auf einem Server des Anbieters zwischengespeichert bis der Kommunikationspartner sie empfängt.

Für diese Form des Instant Messaging gibt es zum jetzigen Zeitpunkt drei Apps, die nach heutigen Erkenntnissen als sicher gelten. Es handelt sich um Textsecure, Surespot und Threema.

2.1 Textsecure

Textsecure[4], das von dem bekannten Sicherheitsexperten Moxie Marlinspike[5] entwickelt wird, ist leider momentan nur als Android-App verfügbar. Aus Sicherheitssicht bietet Textsecure viele Vorteile: Das Kommunikationsprotokoll[6][7] lehnt sich an OTR an und ist offen dokumentiert, sogar der Source Code[8] ist als Open Source frei verfügbar. Ohne eine iOS-Version, die immerhin angekündigt ist, steht diese App derzeit leider nur einer Auswahl von Smartphone-Nutzern zur Verfügung; daher verzichten wir an dieser Stelle auf eine ausführlichere Betrachtung.

2.2 Surespot

Bei Surespot handelt es sich ebenfalls um eine Open Source App, die sowohl für Android als auch für iOS bereitgestellt wird. Allerdings verzichtet diese App auf die Möglichkeit zur Überprüfung

3 https://otr.cypherpunks.ca/
4 https://whispersystems.org/blog/the-new-textsecure/
5 http://www.thoughtcrime.org/
6 https://github.com/WhisperSystems/TextSecure/wiki/ProtocolV2
7 https://whispersystems.org/blog/asynchronous-security/
8 https://github.com/whispersystems/textsecure

von öffentlichen Schlüsseln[9] durch die Benutzer – eines der zentralen vertrauensbildenden Eigenschaften, weswegen sie in diesem Beitrag nicht weiter betrachtet wird.

2.3 Threema

Bei der dritten Alternative handelt es sich um die App Threema[10], die sicheres Instant Messaging über einen schweizer Anbieter ermöglicht. Threema ist keine Open Source-Anwendung, so dass die Nutzung das Vertrauen in eine korrekte Implementierung durch den Hersteller der App erfordert.[11] Auch wenn der Source Code von Threema nicht offengelegt ist, wurden von Threema detaillierte Informationen zur App veröffentlicht[12].

Threemas Hauptvorteil jedoch ist die benutzerfreundliche und transparente Implementierung der Schlüsselerzeugung und des wichtigen Schlüsselaustauschs zwischen Benutzern. Auch sonst deutet vieles darauf hin, dass bei Threema die Verschlüsselung vernünftig implementiert ist. Beispielsweise wurden kryptographische Funktionen nicht selbst programmiert, sondern es wurde die verbreitete Bibliothek NaCl[13] von Dan Bernstein[14] verwendet. Als vertrauensbildende Maßnahme bietet die App auch an, den verschlüsselten Nachrichtenaustausch zu validieren[15].

3 Nutzung von Threema

Threema ist so gestaltet, dass auch Benutzer ohne kryptographische Kenntnisse die App einfach nutzen können.

9 https://www.surespot.me/documents/how_surespot_works.html
10 https://threema.ch/de
11 In dem folgenden Podcast aus dem Januar 2013 äußert sich der Autor von Threema: http://monoxyd.de/podcasts/DieWahrheit017-SmartphoneMessenger-Threema.mp3
12 https://threema.ch/de/faq.html
13 http://nacl.cr.yp.to/
14 http://cr.yp.to/djb.html
15 https://threema.ch/validation/

3.1 Installation

Die Installation gestaltet sich sowohl auf iOS- als auch auf Android-Geräten sehr einfach: Die App muss aus dem jeweiligen Store heraus installiert werden, und anschließend kann der Benutzer loslegen.

3.2 Einrichtung einer ID

Bevor die verschlüsselte Kommunikation genutzt werden kann, muss ein Schlüsselpaar erzeugt werden. Die Erzeugung eines solchen Schlüsselpaares wird von der App beim ersten Start automatisch eingefordert. Das Schlüsselpaar wird erzeugt während der Nutzer das System bei der Generierung von Zufall unterstützt. Der private Schlüssel wird auf dem Gerät gespeichert und der öffentliche Schlüssel kann danach für den Schlüsselaustausch genutzt werden.

Da keinerlei Informationen zum privaten Schlüssel auf Servern des Dienstleisters gespeichert sind, sollte jeder Nutzer ein Backup seines Schlüsselpaares durchführen.

3.3 Suche nach Kommunikationspartnern

Wenn gewünscht, kann die Threema-ID mit einer E-Mail-Adresse und/oder einer Mobilfunknummer verknüpft werden, um automatisch nach Kontakten zu suchen, die ebenfalls Threema nutzen.

Im Gegensatz zu anderen Messengern wird bei Threema dafür jedoch nicht das Adressbuch zur Suche an den Dienstleister geschickt. Bei gewünschter Synchronisation wird von jedem Eintrag lediglich ein Hash der E-Mail-Adresse und der Mobilfunknummer an den Dienstleister übermittelt, der bei den registrierten Nutzern auf Übereinstimmung der Hash-Werte prüft. Bei einem Treffer wird die entsprechende Threema-ID an die App geschickt und dort in den Kontakten hinterlegt.

Abb. 1 | Dialog zur Schlüsselgenerierung

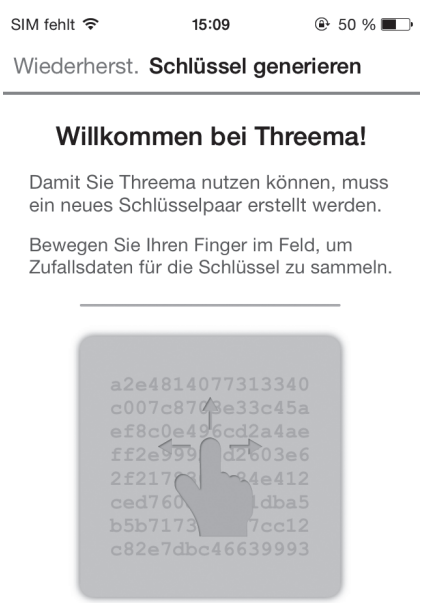


Abb. 2 | Darstellung der generierten ID

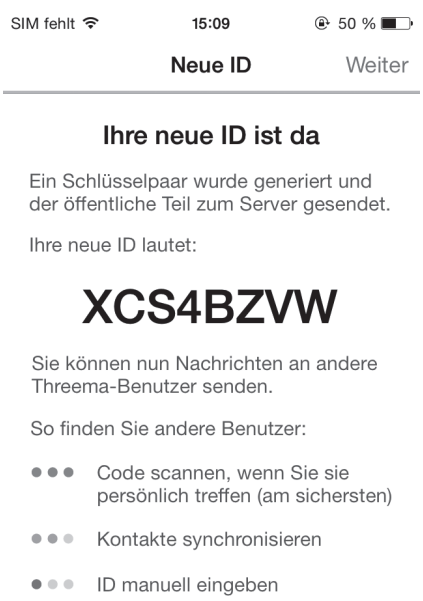


Abb. 3 | Optionale Verknüpfung mit Mobilnummer oder E-Mail

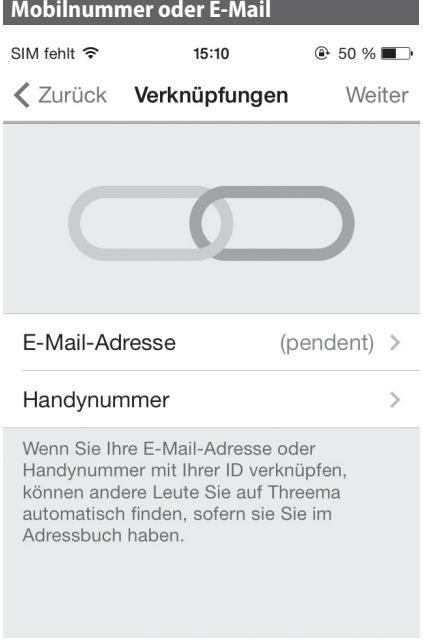


Abb. 4 | Synchronisation der Kontakte

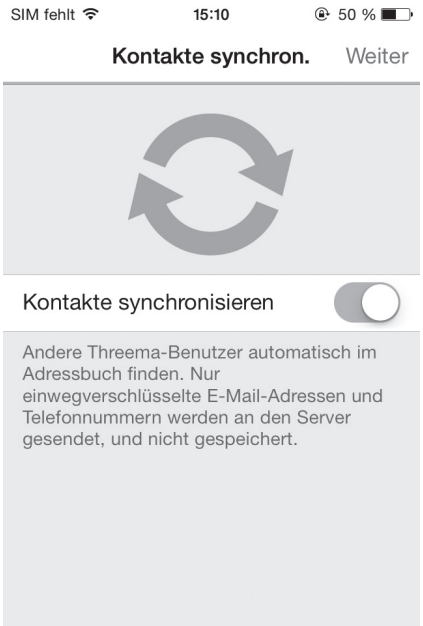


Abb. 5 | ID und öffentlicher Schlüssel als QR-Code

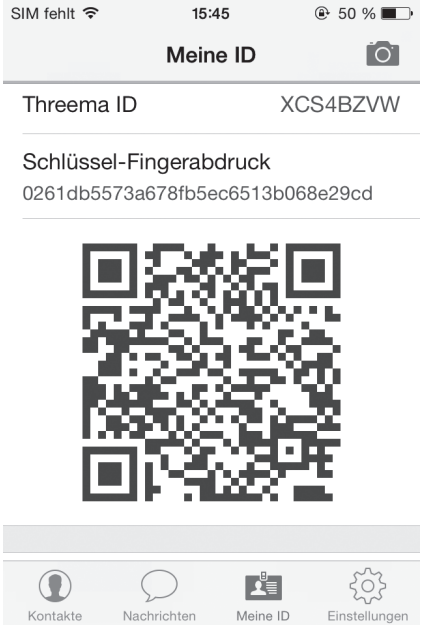
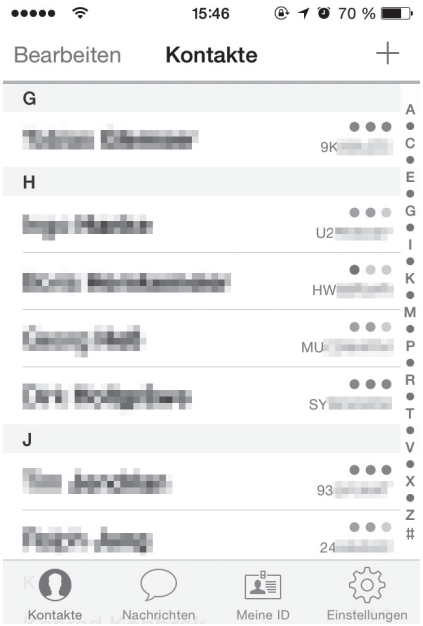


Abb. 6 | Kontaktliste mit Vertrauensstatus



3.4 Schlüsseltausch

Bei einer Kommunikation wird durch Threema immer der öffentliche Schlüssel des Partners bereitgestellt. Wichtig ist hierbei, durch geeignete Maßnahmen sicherzustellen, dass dem Schlüssel des Partners vertraut werden kann. Threema unterstützt diesen Prozess durch die Anzeige verschiedener Sicherheitsstufen in den Kontakten: Ein einzelner roter Punkt in den Kontakten bedeutet, dass keinerlei Prüfung des öffentlichen Schlüssels stattgefunden hat. Zwei orange Punkte zeigen an, dass der zum Schlüssel zugehörige Kontakt im eigenen Adressbuch hinterlegt ist und die E-Mail-Adresse oder die Mobilfunknummer bei Threema hinterlegt und verifiziert wurde. Bei diesem Sicherheitsniveau vertraut der Anwender dem Verzeichnis von öffentlichen Schlüsseln beim Dienstleister.

Das ‚gewisse Etwas' von Threema ist jedoch die Möglichkeit, dass Benutzer bei einem persönlichen Kontakt gegenseitig ihre Schlüssel verifizieren. Diese Verifikation wird bei Threema sehr benutzerfreundlich gestaltet: Die Benutzer müssen nur gegenseitig ihre QR-Codes scannen, die den jeweiligen öffentlichen Schlüssel repräsentieren. Eine erfolgreiche Verifikation wird in den Kontakten durch drei grüne Punkte dargestellt.

3.5 Nutzung

Die Nutzung von Threema ist unspektakulär – sie unterscheidet sich nicht von anderen Instant Messengern, da nach Schlüsselerzeugung und –austausch die Kryptographie vollständig im Hintergrund abläuft.

4 Fazit

Es gibt inzwischen sichere Alternativen zu den Platzhirschen beim Instant Messaging. Der Erfolg von jeder dieser Alternativen wird davon abhängen, wie viele Nutzer der jeweilige Dienst auch vor dem Hintergrund der bekannt gewordenen NSA-Zugriffe und der Übernahme von WhatsApp durch Facebook gewinnen kann.

Aus Sicherheitssicht ist es wesentlich, dass ein vertrauenswürdiger Dienst eine echte Ende-zu-Ende-Verschlüsselung implementiert und dem Benutzer eine einfache Prüfung der öffentlichen Schlüssel seiner Kommunikationspartner ermöglicht.

Eine gute Dokumentation der genutzten Kryptographie und eine Veröffentlichung des Source Codes sind hilfreiche vertrauensbildende Maßnahmen der Hersteller. Allerdings darf man nicht vergessen, dass sich das Vertrauen nicht nur auf die App beschränken darf, sondern Benutzer allen Komponenten –vom Betriebssystem bis hinunter zur Hardware – vertrauen müssen.

Zu guter Letzt werden die Benutzerfreundlichkeit insgesamt und die Verfügbarkeit auf allen relevanten Smartphone-Plattformen wesentliche Erfolgsfaktoren darstellen. Die Entwicklung sicherer Alternativen beim Instant Messaging ist sicher noch nicht an ihrem Ende angekommen.