MOBILE INSTANT MESSENGER - SICHERE ALTERNATIVEN ZU

WHATSAPP

„Facebook didn’t need to buy WhatsApp to read your chats.“

Bas Bosschert
Sicherheitsberater, SysAdmin, Unternehmer, 2014

PIRATEN PARTEI

ELZPIRATEN EMMENDINGEN

INSTANT MESSAGING = NACHRICHTENSOFORTVERSAND

- 2 oder mehr Teilnehmer unterhalten sich über Textnachrichten *(**chatten**)*
- Nachrichten kommen unmittelbar beim Empfänger an *(**Push-Verfahren**)*
- Teilnehmer müssen mit Computerprogramm *(**Client**)* über ein Netzwerk wie das Internet oder einen Server miteinander verbunden sein
- Meist ist auch das Übermitteln von Dateien, Audio- und Videostreams möglich

MOBILE INSTANT MESSENGER

Programme, die auf mobilen Geräten Instant Messaging ermöglichen, z.B.

- WhatsApp (450 Millionen Nutzer)
- iMessage
- Blackberry Messenger
- Threema
- Telegram
- ChatSecure
- SureSpot
- TextSecure
- Skype, Xabber,...

WARUM ALTERNATIVEN ZU WHATSAPP?

- 19. Februar 2014: **Facebook kauft WhatsApp** für 19 Mrd. US-Dollar (13,81 Mrd. Euro)
- 21. Februar 2014: Threema verdoppelt seine Nutzer innerhalb eines Tages auf 400.000
- 21.-24. Februar 2014: ca. **1,1 Mio. Nutzer** installieren **Threema**
- 04. April 2014: Threema führt weiterhin die Top-Charts der kostenpflichtigen Android-Apps bei Google Play an

WARUM ALTERNATIVEN ZU WHATSAPP?

- Auch **andere (sichere?) Messenger** wie SureSpot, Telegram und TextSecure erzielen eine **größere Aufmerksamkeit**.

Wunsch nach sicheren Alternativen zu WhatsApp!!

WAS MACHT EINEN MESSENGER SICHER?

- Steht der Quelltext der Software offen zur Verfügung (Open Source) oder wurde er zumindest von Experten in einem Security-Audit o.ä. überprüft?
  - Open Source ermöglicht die unabhängige Überprüfung des Quellcodes auf Sicherheitslücken.
  - Open Source alleine reicht nicht aus – der Quellcode muss auch fundiert überprüft und etwaige Mängel behoben werden.

WAS MACHT EINEN MESSENGER SICHER?

- Wird eine anerkannt sichere **End-to-End-Verschlüsselung** verwendet?
  - Unsicher: Neue, ungeprüfte Verschlüsselungsprotokolle. Allgemein proprietäre Messenger.
  - Sicher: Umfangreich geprüfte Eigenentwicklung des Herstellers oder offene Protokolle wie z.B. OTR (Off-the-Record).

WAS MACHT EINEN MESSENGER SICHER?

- Ist eine **Authentifizierung** möglich?
  - Kann sichergestellt werden, dass die Nachricht wirklich von der Person stammt, von der sie zu kommen scheint?
- Ist eine **glaubhafte Abstreitbarkeit** möglich?
  - Kann nachträglich nicht bewiesen werden, dass der Absender bestimmte Nachrichten tatsächlich versendet hat?

WAS MACHT EINEN MESSENGER SICHER?

- Wird verhindert, dass frühere Nachrichten nachträglich gelesen werden können, falls der Schlüssel in fremde Hände gerät?
  - **Perfect Forward Secrecy (PFS)**: Jede Nachricht wird mit einem neuen Kurzzeitschlüssel verschlüsselt. Dadurch können alte Nachrichten nicht im Nachhinein gelesen werden, falls der Schlüssel in fremde Hände gerät.

WELCHE FUNKTIONEN & KRITERIEN SOLLEN DIE MESSENGER ERFÜLLEN?

1. **Unterstützung verschiedener Plattformen:**
Android, iOS, Windows Phone, BlackBerry, Symbian,...

2. **Bildnachrichten**

3. **Gruppenchats**

4. **Asynchrone Kommunikation**:
Die Nachricht kann auch versendet werden, wenn der Empfänger nicht online ist, also keine Nachrichten empfangen kann. Die Nachricht wird auf einem Server zwischengespeichert, bis der Empfänger diese empfangen kann. Der Absender muss hierzu nicht mehr online sein.

WELCHE FUNKTIONEN SOLLEN DIE MESSENGER ERFÜLLEN?

5. **Übertragung von Kontakten aus dem Telefonbuch**: Kann dies optional ausgewählt werden oder wird das Telefonbuch automatisch übertragen? Letzteres bietet dem Anbieter die Möglichkeit, soziale Profile zu erstellen.

6. **Leichte Bedienbarkeit**

7. **Geringe Kosten**

WHATSAPP

Sicherheit:

1. Open Source: nein ✘
2. End-to-End-Verschlüsselung: nein ✘
3. Authentifizierung: nein ✘
4. Abstreitbarkeit: nein ✘
5. Perfect Forward Secrecy: nein ✘

WHATSAPP

Funktionen:

1. Unterstützte Plattformen: Android, iOS, Windows Phone, BlackBerry, Symbian, Nokia S40, Firefox OS
2. Bildnachrichten: ja ✔
3. Gruppenchats: ja (nur unverschlüsselt)
4. Asynchrone Kommunikation: ja (nur unverschlüsselt)
5. Übertragung Telefonbuch: automatisch ✘
6. Leichte Bedienbarkeit: ja ✔
7. geringe Kosten: ja (Download + 1. Jahr kostenlos, danach 0,89 € pro Jahr)

THREEMA

Sicherheit:

1. Open Source: nur teilweise (KryptoLibrary NaCl)
2. End-to-End-Verschlüsselung: ja ✔
3. Authentifizierung: ja ✔
4. Abstreitbarkeit: nein ✘
5. Perfect Forward Secrecy: nur über Server-Client-Verschlüsselung

THREEMA

Funktionen:

1. Unterstützte Plattformen: Android ab 4.0, iOS
2. Bildnachrichten: ja ✔
3. Gruppenchats: ja ✔
4. Asynchrone Kommunikation: ja ✔
5. Übertragung Telefonbuch: optional ✔
6. Leichte Bedienbarkeit: ja ✔
7. Geringe Kosten: ja (1,60 € Google Play, 1,79 € AppStore)

TELEGRAM

Sicherheit:

1. Open Source: nur teilweise
2. End-to-End-Verschlüsselung: ja, jedoch nicht ausreichend geprüfte und optimierte Eigenentwicklung mit nachweisbaren Schwächen
3. Authentifizierung: optional
4. Abstreitbarkeit: unbekannt
5. Perfect Forward Secrecy: optional

TELEGRAM

Funktionen:

1. Unterstützte Plattformen: Android, iOS; inoffiziell Windows Phone und Desktopversion
2. Bildnachrichten: ja ✔
3. Gruppenchats: ja (nur Client-Server-Verschlüsselung)
4. Asynchrone Kommunikation: ja ✔
5. Übertragung Telefonbuch: automatisch ✘
6. Leichte Bedienbarkeit: mäßig
7. Geringe Kosten: kostenlos

SURESPOT

Sicherheit:

1. Open Source: ja ✔
2. End-to-End-Verschlüsselung: ja ✔
3. Authentifizierung: nein ✘
4. Abstreitbarkeit: nein ✘
5. Perfect Forward Secrecy: nein ✘

SURESPOT

Funktionen:

1. Unterstützte Plattformen: Android, iOS
2. Bildnachrichten: ja ✔
3. Gruppenchats: nein (in Planung) ✘
4. Asynchrone Kommunikation: ja ✔
5. Übertragung Telefonbuch: nein
6. Leichte Bedienbarkeit: mäßig
7. Geringe Kosten: ja, (Download kostenlos, Zusatzfunktionen kostenpflichtig)

CHATSECURE

Sicherheit:

1. Open Source: ja ✔
2. End-to-End-Verschlüsselung: ja ✔
3. Authentifizierung: ja ✔
4. Abstreitbarkeit: ja ✔
5. Perfect Forward Secrecy: ja ✔

CHATSECURE

Funktionen:

1. Unterstützte Plattformen: Android, iOS
2. Bildnachrichten: ja ✔
3. Gruppenchats: ja (nur Client-Server-Verschlüsselung)
4. Asynchrone Kommunikation: ja (nur unverschlüsselt)
5. Übertragung Telefonbuch: unbekannt
6. Leichte Bedienbarkeit: mäßig
7. Geringe Kosten: kostenlos

TEXTSECURE

Sicherheit:

1. Open Source: ja ✔
2. End-to-End-Verschlüsselung: ja ✔
3. Authentifizierung: ja ✔
4. Abstreitbarkeit: ja ✔
5. Perfect Forward Secrecy: ja ✔

TEXTSECURE

Funktionen:

1. Unterstützte Plattformen: Android (iOS und Desktop-version in Entwicklung)
2. Bildnachrichten: ja ✔
3. Gruppenchats: ja ✔
4. Asynchrone Kommunikation: ja ✔
5. Übertragung Telefonbuch: optional ✔
6. Leichte Bedienbarkeit: ja ✔
7. Geringe Kosten: kostenlos

FAZIT

- **Threema** ist in puncto Sicherheit und Funktion imho der geeignetste Mobile Instant Messenger für **plattformüber-greifende Kommunikation** (Android ↔ iOS).
- **TextSecure** ist für die Kommunikation zwischen **Androidgeräten** imho die beste Option.

QUELLEN

Freie Software Offenburg ;)

c't 7/2014, S. 139ff

http://all-about-apps.de/iosandroid-surespot-ein-weiterer-messenger-der-verschluesselt-kostenlos/

http://www.androidnext.de/apps/whatsapp-android-widget/

http://bas.bosschert.nl/steal-whatsapp-database/

http://bas.bosschert.nl/steal-whatsapp-update/

https://de.wikipedia.org/wiki/Instant_Messaging

https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern

https://de.wikipedia.org/wiki/Surespot

https://digitalcourage.de/blog/2014/nach-dem-kauf-durch-facebook-alternativen-zu-whatsapp

https://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients

https://en.wikipedia.org/wiki/TextSecure

http://www.giga.de/apps/android/news/android-und-ios-dominieren-weiter-den-mobilfunkmarkt/

http://www.golem.de/news/verschluesselung-snowden-empfiehlt-textsecure-und-redphone-1403-105052.html

https://guardianproject.info/apps/chatsecure

https://netzpolitik.org/2014/it-has-to-pass-the-greenwald-test-snowden-gibt-empfehlung-fuer-verschluesselte-kommunikation/

QUELLEN

http://www.heise.de/security/meldung/WhatsApp-erweitert-Einstellungen-zur-Privatsphaere-und-bleibt-trotzdem-unsicher-2140499.html

http://www.heise.de/security/meldung/Snowden-lobt-Moxie-Marlinspike-und-Open-WhisperSystems-2140053.html

http://www.heise.de/security/meldung/Verschluesselnde-WhatsApp-Alternative-Threema-So-funktioniert-der-Wechsel-2119643.html

https://itunes.apple.com/de/app/chatsecure-verschlusselter/id464200063?mt=8

http://www.kuketz-blog.de/textsecure-crypto-held-oder-weiterer-blindgaenger-teil1/

http://www.kuketz-blog.de/textsecure-crypto-messenger-mit-verbesserungspotenzial-teil2/

https://missingm.co/2014/02/fighting-dishfire-the-state-of-mobile-cross-platform-encrypted-messaging/

https://netzpolitik.org/2014/wir-erklaeren-den-heutigen-tag-zum-deinstalliere-whatsapp-tag/

https://www.os3.nl/_media/2013-2014/courses/ssn/projects/threema_report.pdf

https://play.google.com/store

http://support.whispersystems.org/

https://threema.ch/de/

https://telegram.org/

http://unhandledexpression.com/2013/12/17/telegram-stand-back-we-know-maths/

http://www.whatsapp.com/

http://www.zeit.de/digital/mobil/2014-02/threema-telegram-surespot-chatsecure-vergleich/seite-all