

MOBILE INSTANT MESSENGER - SICHERE ALTERNATIVEN ZU

WHATSAPP

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

Bas Bosschert

Sicherheitsberater, SysAdmin, Unternehmer, 2014

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**
- Juli 2015(!): Threema ist weiter in den Top-Charts der kostenpflichtigen Android-Apps bei Google Play und dem Apple App-Store

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:
möglichst optional.**
- 6. Leichte Bedienbarkeit**
- 7. Geringe Kosten**

	 Sicher	 Threema	 Telegram	 Whatsapp	 Snapchat
End-to-End Encryption	✓	✓	Secret Chats only	✗	✗
Offline Key Verification	✗	✓	✓	✗	✗
Encrypted Local Storage	✓	✓	Secret Chats only	✗	weak
App-level Password Lock	✓	✓	✗	✗	✗
Encrypted Group Chats	✓	✓	✗	✗	✗
Self-destructed Messages	✓	✗	✓	✗	✓
Sends Address Book to servers	✓	✗	✗	✓	✓
Encrypted File Transfer	all files	media	media	✗	media
Open Source	✗	✗	✓	✗	✗
Server Location	DE	CH	RU,CA,UK,SI	USA	Google
Supported Platforms	iOS, Android, Windows Phone	iOS, Android	iOS, Android	iOS, Android, WP, BB, Symbian	iOS, Android
Free app	✓	✗	✓	✗	 Compare Ninja

FAZIT

- **Threema und TextSecure/Signal** sind in puncto Sicherheit und Funktion geeignetste Mobile Instant Messenger für **plattformübergreifende Kommunikation** (Android ↔ iOS).

