Sicher kommunizieren

Tools um vertraulich zu kommunizieren

April 2015

Allgemeines

- Sofern nicht anders angeführt, wurden alle vorgestellten Tools durch unabhängige Security-Audits überprüft
- Sofern nicht anders angeführt, stehen alle Tools unter freien OpenSource-Lizenzen
- Manche Tools müssen passend konfiguriert werden damit sie auch verschlüsseln
  → kommt zur CryptoParty

Abkürzungserklärung

- OpenSource: Software deren Quellcode offengelegt ist, die verändert und weiterverbreitet werden darf
- Jabber/XMPP: ein freies Chatprotokoll
- TOR: OpenSource Anonymisierungsnetzwerk zum verschleiern von IP Adressen
- OTR: Ende zu Ende Verschlüsselungsprotokoll, welches glaubhaftes Abstreiten ermöglicht
- VOIP: Telefonie über das Internet
- SIP: Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung bei VOIP
- ZRTP: Verschlüsselungsprotokoll für Telefonie
- Security-Audit: Unabhängige Sicherheitsprüfung

Good old PGP/GPG

- erste Verschlüsselungssoftware für Allgemeinheit
- sehr sicher (Snowden approved)
- stabil aber alt → nicht am Stand der Technik
- nicht anfängerfreundlich
- Fokus auf E-Mail, aber nicht ausschließlich
- anonym mit TOR
- plattformunabhängig

Internettelefonie mit VOIP & ZRTP

PC
Jitsi

- OS unabhängig
- anonym mit TOR
- auch für Chat mit Jabber/XMPP
- unterstützt OTR
- „all in one“ Lösung
- Android in Arbeit

Handy
cSipSimple

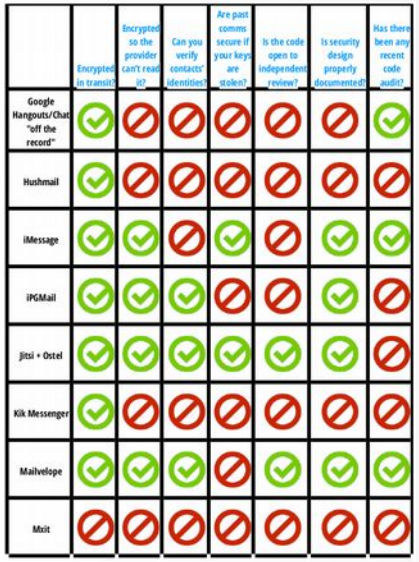
- nur Android
- nur Internettelefonie
- unterstützt alle SIP-Anbieter

Bild: jitsi.org

Verschlüsselungstools für Handys

- TextSecure
- SMSSecure
- ChatSecure
- Threema
- WhatsApp
- Cryptocat
- Retroshare

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM	✓	✗	✗	✗	✗	✗	✗
BlackBerry Messenger	✓	✗	✗	✗	✗	✗	✗
BlackBerry Protected	✓	✓	✗	✗	✗	✓	✗
ChatSecure + Orbot	✓	✓	✓	✓	✓	✓	✓
CryptoCat	✓	✓	✓	✓	✓	✓	✓
Ebuddy XMS	✓	✗	✗	✗	✗	✗	✗
Facebook chat	✓	✗	✗	✗	✗	✗	✓
FaceTime	✓	✓	✗	✓	✗	✓	✓



	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Google Hangouts/Chat "off the record"	✓	✗	✗	✗	✗	✗	✓
Hushmail	✓	✗	✗	✗	✗	✗	✗
iMessage	✓	✓	✗	✓	✗	✓	✓
iPGMail	✓	✓	✓	✗	✗	✓	✗
Jitsi + Ostel	✓	✓	✓	✓	✓	✓	✗
Kik Messenger	✓	✗	✗	✗	✗	✗	✗
Mailvelope	✓	✓	✓	✗	✓	✓	✓
Mxit	✗	✗	✗	✗	✗	✗	✗

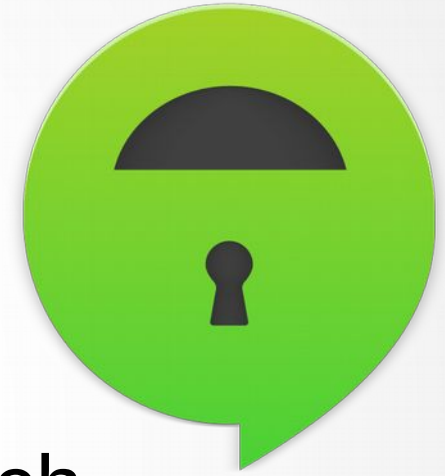
	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Off-The-Record Messaging for Mac (Adium)	✓	✓	✓	✓	✓	✓	✗
Off-The-Record Messaging for Windows (Pidgin)	✓	✓	✓	✓	✓	✓	✓
PGP for Mac (GPGTools)	✓	✓	✓	✗	✓	✓	✗
PGP for Windows Gpg4win	✓	✓	✓	✗	✓	✓	✗
QQ	✓	✗	✗	✗	✗	✗	✓
RetroShare	✓	✓	✓	✓	✓	✓	✗
Secret	✓	✗	✗	✗	✗	✗	✗
Signal / RedPhone	✓	✓	✓	✓	✓	✓	✓

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Silent Phone	✓	✓	✓	✓	✓	✓	✓
Silent Text	✓	✓	✓	✓	✓	✓	✓
Skype	✓	✗	✗	✗	✗	✗	✗
SnapChat	✓	✗	✗	✗	✗	✗	✓
StartMail	✓	✗	✓	✗	✗	✓	✗
Subrosa	✓	✓	✓	✗	✓	✓	✓
SureSpot	✓	✓	✓	✗	✓	✓	✗
Telegram	✓	✗	✗	✗	✓	✓	✓

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Telegram (secret chats)	✓	✓	✓	✓	✓	✓	✓
TextSecure	✓	✓	✓	✓	✓	✓	✓
Threema	✓	✓	✓	✓	✗	✓	✗
Viber	✓	✗	✗	✗	✗	✗	✗
Virtru	✓	✗	✗	✗	✗	✓	✓
WhatsApp	✓	✗	✗	✗	✗	✗	✓
Wickr	✓	✓	✓	✓	✗	✗	✓
Yahoo! Messenger	✓	✗	✗	✗	✗	✗	✗

TextSecure

- sicherer Chat mit OTR
- keine SMS Verschlüsselung mehr
- benutzt Google messaging
- Handynummer zwingend erforderlich
- iOS, Android und Windows Phone
- Gruppenchat durch mehrere OTR Sessions



SMSSecure

- baut auf TextSecure auf
  - → benutzt (noch) Google messaging
  - → Handynummer zwingend erforderlich
- verschlüsselt wenn möglich SMS und MMS
- sehr junges Projekt
  - → noch kein Security-Audit
- unterstützt nur Android
- OTR nur bei SMS übers Internet

ChatSecure

- sicherer Chat über Jabber/XMPP mit OTR
  → serverunabhängig da offenes Protokoll
- anonymes Chatten über TOR möglich
- iOS, Android und Windows Phone
- kein Gruppenchat

Threema

- sicherer Chat, aber kein OTR
- senden auch möglich wenn Partner offline
- NICHT OpenSource
- KEIN Security-Audit
- „anonymer“ Gruppenchat (kein Dateiversand)
- iOS, Android und Windows Phone
- iOS: Chatprotokolle in iCloud gespeichert

WhatsApp

- NICHT OpenSource
- Verschlüsselung nicht dokumentiert
- Provider kann mitlesen
- Kontakte können nicht verifiziert werden
- wenn der Schlüssel gestohlen wird, sind auch alte Kommunikationen lesbar
- unterstützt alle aktuellen mobilen Betriebssysteme

Cryptocat

- Benutzerfreundlich
- baut auf XMPP auf
- Zweipersonenchat über OTR
- Gruppenchat möglich (nicht OTR)
- anonymes Chatten über TOR möglich
- Partner muss jedes Mal neu identifiziert werden
- keine Warnung, wenn sich der Schlüssel ändert
- Chrome, Firefox, Safari, Opera, OS-X, iOS
- Android App in Arbeit

Retroshare

- dezentralisiertes privates Social-Network
- KEIN Security-Audit
- KEIN OTR
- Gruppenchat
- Statusmeldungen
- VOIP mit Plugin
- Youtube ähnliche Channels
- viel mehr Features
- PC, Android(beta)

Quellen

- https://www.eff.org/de/secure-messaging-scorecard
- https://dev.guardianproject.info/projects/ostn/wiki?title=OSTN
- Text Secure: https://whispersystems.org/blog/private-groups/
- Text Secure: https://eprint.iacr.org/2014/904.pdf
- https://github.com/cryptocat/cryptocat/wiki/Multiparty-Protocol-Specification
- https://threema.ch/press-files/cryptography_whitepaper.pdf
- https://guardianproject.info/apps/chatsecure/
- http://www.heise.de/security/meldung/TextSecure-Fork-bringt-SMS-Verschluesselung-zurueck-2595471.html
- http://retroshare.sourceforge.net/wiki/index.php/Documentation:Security_model
- https://security.stackexchange.com/questions/79070/how-do-i-verify-that-whatsapp-is-using-end-to-end-encryption
- https://jitsi.org/Documentation/ZrtpFAQ#faqHow

Copyright

- Der Text dieser Präsentation untersteht keinerlei Restriktionen bezüglich Weiterverbreitung und Veränderung. Do whatever you want with the text of this presentation.
- Die folgenden Folien enthalten Bilder, welche als Marken eingetragen sind, und dürfen nur unverändert in Verbindung mit den hier vorgestellten Tools verwendet werden: F09(Threema), F10(WhatsApp).
- Die Bilder auf folgenden Folien stehen unter der GNU General Public License: F11(Cryptocat), F12(Retroshare).
- Der Urheber(jitsi.org) des Jitsi Logos muss bei Verwendung seines Bildes genannt werden.
- Die restlichen Bilder bestehen nur aus einfachen geometrischen Formen sowie Text und erreichen keine Schöpfungshöhe, somit unterstehen sie nicht dem Urheberrecht (F06, F07, F08) oder stehen unter Lizenzen, welche die Weiterverbreitung und Veröffentlichung nicht einschränken.

ERRATA

Durch einen Fehler meinerseits waren die Angaben auf der Folie 7 zu TextSecure mit denen von ChatSecure vermischt und falsch. Da mir dieser Fehler beim zusammenstellen der Präsentation unterlief hatte ich während des Vortrags ein falsches Security-Konzept dieser App im Kopf. Ich möchte mich bei dem Fragesteller, welcher versuchte mich darauf hinzuweisen, bedanken.