Fachhochschule Wedel
Seminararbeit

Studiengang:
B.Sc Wirtschaftsingenieurwesen

Geschütztes Chatten über Jabber Server

Erstellt von: Bejan Amin, wing102729

Betreuender Dozent: Prof. Dr. Michael Anders

Fachhochschule Wedel

Feldstraße 140

22880 Wedel

Tel. (04103) 804824

E-Mail: an@fh-wedel.de

Inhaltsverzeichnis

Einleitung

Laut Prognosen sollen bis zum Jahre 2021 etwa ein Drittel der Weltbevölkerung via Instant Messaging-Anwendungen Nachrichten verschicken. Wie bereits der Begriff „Instant Messaging“ suggeriert, ermöglicht es den sofortigen Austausch von Nachrichten über ein Netzwerk, meistens über das Internet. Mit IM-Diensten können Nutzer über aktuelle Zustandsinformationen von anderen Nutzern feststellen, ob diese momentan anwesend (= „online“) sind und ermöglichen diesen gleichzeitig den Austausch von Nachrichten. Generell unterscheidet man bei den Mitteilungen zwischen zwei Varianten: Das Instant Messaging als private Kommunikation über ein Netzwerk zwischen zwei Nutzern und die Kommunikation zwischen mehreren Nutzern als „Chat Session“.

Weltweit hatten im Jahre 2017 im Bereich des Instant Messagings der *Facebook Messenger* und *WhatsApp* die meisten monatlich aktiven Nutzer. Danach folgten die Messenger *WeChat*, *QQ*, *iMessage*, *Skype*, *Viber*, *Line*, *Snapchat*, *Telegram* und *Kakao Talk*. Die Messenger-Dienste *WeChat* und *QQ* sind eher im asiatischen Raum verbreitet. *WeChat* kann man nicht nur zur Kommunikation, sondern auch zum Bezahlen nutzen. *KakaoTalk* ist eine südkoreanische App. Es existieren aber noch zahlreiche weitere Anwendungen. Die Frage stellt sich, ob diese Dienste sicher sind? In den etablierten Medien bekommt man immer wieder von Daten-Skandalen von Facebook und Co. mit, deshalb machen sich u.a. auch immer mehr Menschen Gedanken um ihre persönlichen Daten. Der Bedarf an sicheren Nachrichtenversand wird in den nächsten Jahren wahrscheinlich noch weiter steigen. Von 160.000 Überwachungsprotokollen aus den NSA-Dokumenten von Snowden ging es bei 121.134 Protokollen um Instant Messaging – das Abhören von Instant Messengern ist also ein Schwerpunkt für Geheimdienste.

Experten stellen seit Jahren die Frage, ob es überhaupt eine sichere und leicht bedienbare Anwendung zur weltweiten Kommunikation im Internet gibt und haben bislang noch keine eindeutige Lösung gefunden. Diese Seminararbeit beschäftigt sich mit der geschützten Kommunikation im Bereich des Instant-Messagings über Jabber Server mit dem OTR- und OMEMO-Verschlüsselungsprotokoll gegenüber herkömmlichen Messenger-Diensten.

Sicherheitslücken bei verbreiteten Messenger-Diensten

Viele Menschen verwenden herkömmliche IM-Dienste, wie in der Einleitung bereits angesprochen. Leider haben diese Anwendungen entweder oft Sicherheitslücken und/oder es existieren datenschutzrechtliche Bedenken. Im Folgenden werden die zwei am weitesten verbreiteten Dienste genauer im Hinblick auf die beiden Aspekte Sicherheit und Datenschutz betrachtet:

Facebook Messenger

Beim Facebook Messenger herrscht Klarnamenpflicht. Wenn man nicht seinen echten Namen angibt, dann kann dies zu einer Sperrung des Accounts führen. Außerdem sendet man automatisch seinen Standort bei jeder Nachricht mit, wenn man die Funktion nicht vorher deaktiviert hat. Es gibt eine Ende-zu-Ende-Verschlüsselung, also eine Verschlüsselung, bei der die Nachricht auf dem Sendegerät verschlüsselt und erst wieder beim Empfänger entschlüsselt wird. Aber diese bezieht sich nur auf den Klartext und nicht auf die Metadaten, die eigentlich viel wichtiger und wertvoller sind. Des Weiteren muss man jeweils pro Chat eine Einstellung vornehmen, um die Ende-zu-Ende-Verschlüsselung zu aktivieren – dies nennt sich bei Facebook dann „geheimer Chat“. Darüber hinaus macht Facebook den meisten Umsatz mit dem Verkauf von Nutzerdaten, was ebenfalls bedenklich ist. Zudem werden bei der Installation auf dem Smartphone viele Rechte verlangt, z.B. um auf das Mikrofon zuzugreifen. Damit macht man sich aber leider angreifbar und es kann zum Abhören missbraucht werden.

WhatsApp Messenger

Beim WhatsApp Messenger muss man sich mit einer Handynummer registrieren und eine SMS bestätigen. Auch hier gibt es eine Ende-zu-Ende-Verschlüsselung, die sich auch nicht auf die Metadaten bezieht. Die Verschlüsselung muss aber nicht vorher aktiviert werden. Außerdem werden die Adressbücher der Nutzer auf einem Server gespeichert und können miteinander verglichen werden. Den WhatsApp Messenger gibt es auch für Internet-Browser. Die Browserversion hat aber auch Sicherheitslücken. Es ist u.a. relativ leicht möglich das Profilbild und den Online-Status von jedem Nutzer herauszufinden, obwohl man die Telefonnummer des Nutzers nicht gespeichert hat. Da sowohl der WhatsApp Messenger als auch der Facebook Messenger zum gleichen Konzern gehören werden auch Daten von WhatsApp-Nutzern an Facebook weitergegeben, auch wenn diese gar keinen Facebook-Account haben.

Einige Grundlagen zu Jabber bzw. XMPP

Der „Jabber Instant Messenger“ war der erste Instant-Messenger für das Kommunikationsprotokoll XMPP. Dieser Messenger wurde aber eingestellt. Jabber fungiert heutzutage nur noch als XMPP-Service. Man kann daher Jabber und XMPP gleichstellen bzw. man kann sagen, dass Jabber eher die alte Bezeichnung für XMPP ist. Die Grundidee hierbei ist wie bekannte IM-Dienste, wie z.B. Skype: Man hat eine Freundesliste. Dort trägt man Freunde, Bekannte etc. rein. Anschließend kann man sehen, wann diese Personen online sind und dann mit ihnen Nachrichten austauschen, also Chatten.

Es ist aber wichtig zu wissen, dass es nicht nur ein Jabber-Programm gibt. Jabber ist nur ein Synonym über den Dienst über den man kommuniziert. Man muss sich also auf keinen Anbieter festlegen und kann aus einer großen Anzahl an Client-Programmen wählen. Egal für welchen Anbieter man sich entscheidet: Man kann, ähnlich wie bei E-Mails, auch mit Nutzern der anderen Anbieter kommunizieren. Durch diese anbieterübergreifende Kommunikation ergibt sich ein weiter Vorteil. Jeder kann sich seinen Anbieter frei aussuchen. Die großen Dienste (wie Skype) haben manchmal fragwürdige und seitenlange „Allgemeine Geschäftsbedingungen“ (= AGB). Bei XMPP hat man kein Problem einen Anbieter zu finden, der den Vorstellungen von Datenschutz und Privatsphäre von vielen Menschen entspricht, deshalb verwenden auch z.B. viele Firmen XMPP zur Kommunikation.

Das Kommunikationsprotokoll XMPP für jeden einsehbar, es ist „open source“ und wird aktiv weiterentwickelt (im Gegensatz zu manch anderen IM-Protokollen wie OSCAR). Jeder Benutzer hat eine Jabber-ID, die entspricht dem Aufbau einer E-Mail-Adresse (also benutzername@server.xyz). Wissenwert ist, dass man für den Betrieb eines XMPP-Netzwerkes mindestens ein XMPP-Server benötigt. Dieser kann in einem Intranet als alleinige Kommunikationsstelle existieren oder über das Internet zu anderen XMPP-Servern Verbindungen aufbauen.

Ein Beispiel für ein XMPP-Netzwerk mit drei Servern ist in Abbildung 1 zu sehen:

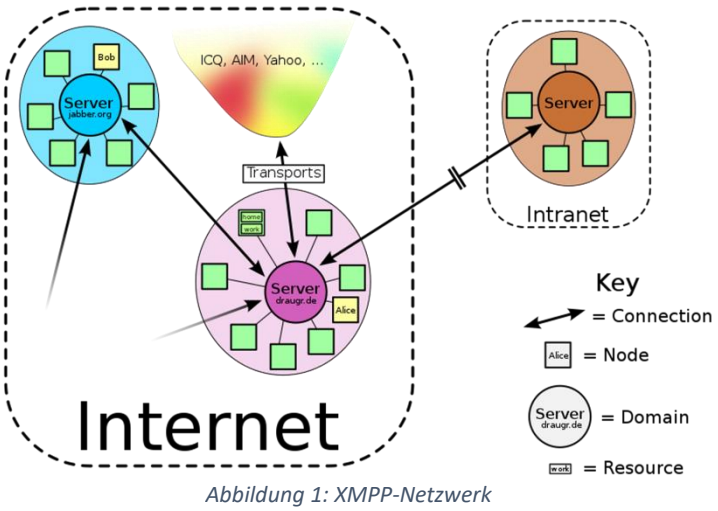

Abbildung 1: XMPP-Netzwerk

XMPP-Clients

XMPP-Clients gibt es für fast jedes Betriebssystem und in fast jeder Programmiersprache. Sie unterscheiden sich aber u.a. hinsichtlich der Sicherheitsfeatures, z.B. gibt es ein XMPP-Client für Linux und Windows, namens Pidgin. Hiermit kann man die Verschlüsselungsprotokolle OTR, OpenPGP und OMEMO mittels PlugIn nutzen. Generell ist Pidgin beliebt und wird oft als Clientprogramm verwendet, da man die Funktionen durch PlugIns stark erweitern kann. Außerdem kann man mit Pidgin auch andere Kommunikationsprotokolle nutzen, also nicht nur XMPP. Dies interessiert uns aber in diesem Fall nicht, da wir uns nur mit XMPP beschäftigen.

Ein relativ guter Client für Mac ist beispielsweise Adium, das eine OTR-Verschlüsselung bietet und auch ohne vorher ein Plug-In installieren zu müssen. Andere Verschlüsselungsprotokolle bietet Adium aber nicht an.

Es gibt zahlreiche Listen im Internet, in der verschiedene XMPP-Clients u.a. nach Betriebssystem und Funktionen verglichen werden. Die „XMPP Standards Foundation“ pflegt z.B. so eine Liste.

XMPP-Transports

Ein XMPP-Transport ist ein Dienst innerhalb eines XMPP-Netzwerkes. Hiermit ist es möglich, andere Messenger-Dienste (z.B. ICQ) zu verwenden und mit deren Benutzern zu interagieren. In Abbildung 2 sieht man ein Beispiel mit Alice und Bob. Alice nutzt ein XMPP-Client und Bob ist bei ICQ registriert. Alice übergibt dem Transport ihre ICQ-Anmeldedaten, also ihre ICQ-Nummer und ihr Passwort. Danach meldet sich der Transport im Auftrag von Alice bei ICQ an und das ICQ-Netzwerk „denkt“, dass Alice ein normaler ICQ-Client ist. Der Transport überträgt schließlich alle Nachrichten zwischen den beiden. Bob bekommt von diesen Ablauf nichts mit. Ihm erscheint es so, als ob er direkt über ICQ mit Alice kommuniziert. In Alice Kontaktliste wird Bob als „normaler“ XMPP-Nutzer dargestellt, obwohl Bob mit dem ICQ-Netzwerk verbunden ist.

Außerdem ist in Abbildung 2 noch OSCAR zu sehen. OSCAR ist ein IM-Protokoll, das nur für die beiden Messenger-Dienste *ICQ* und *AOL Instant Messenger* verwendet wird.

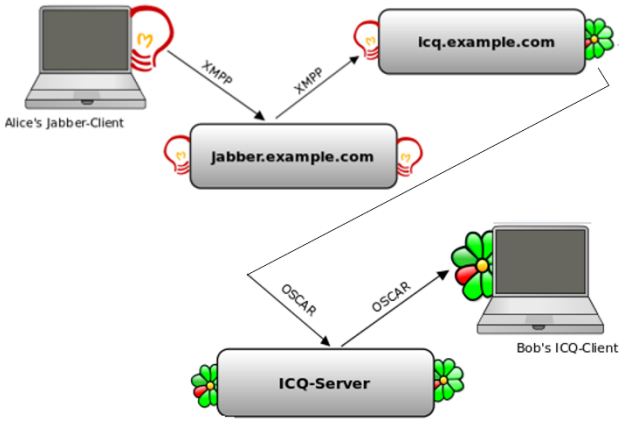

Abbildung 2: XMPP-Transports

Off-the-Record Messaging (OTR)

Um zu verschleiern was Client und Server oder Server mit anderem Server austauschen, kann man die Kommunikation über XMPP verschlüsseln. Die Transportverschlüsselung wird im Internet mit SSL bzw. TLS realisiert („https-Verbindung“). Um aber sicher zu gehen, dass eine Nachricht erst vom Empfänger gelesen werden kann, kann man beispielsweise mit dem OTR-Verschlüsselungsprotokoll Ende-zu-Ende-Verschlüsselung verwenden. Diese Ende-zu-Ende-Verschlüsselung bezieht sich hier auch auf die Metadaten und nicht nur auf den Klartext, wie es bei Facebook und Whatsapp der Fall ist. „Off-the-Record-Messaging“ (OTR) kann man ins Deutsche als „inoffizielle, vertrauliche, nicht für die Öffentlichkeit bestimmte Nachrichtenübermittlung“ übersetzen.

Wie bereits bei den XMPP-Clients erwähnt kann man z.B. bei der Verwendung von Pidgin als Client über XMPP das OTR-Protokoll verwenden. Bei OTR werden das symmetrische Kryptoverfahren AES, der Diffie-Hellmann-Schlüsselaustausch und die kryptographische Hashfunktion SHA-1 kombiniert werden.

Man muss wissen, dass man bei OTR die erste Autorisierung sorgfältig durchführen muss und dies kann beispielsweise durch eine „out-of-band authentication“ erfolgen. Dabei teilt man ein Geheimnis über einen „anderen Weg“ mit, z.B. durch ein persönliches Treffen. Einmal authentifiziert werden die benötigten Berechnungen im Hintergrund durchgeführt, beispielsweise für den Diffie-Hellmann-Schlüsselaustausch. Zudem muss ein erster Austausch zwischen den Chat-Partnern stattfinden, bevor die Unterhaltung beginnen kann.

In der folgenden Abbildung sind die Vor- und Nachteile des OTR-Protokolls aufgelistet:

Vergleich:	**OTR**
Encryption	X
Authentication	X
Plausible Deniability	X
Deniability	X
Perfect Forward Secrecy	X
Gruppenchats	-
Datentransfer	-
Nutzung auf mehreren Geräten	(X)
Verschlüsselte Offline-Nachrichten (d.h. die Empfänger*in ist offline)	-

Abbildung 3: OTR Funktionen

Encryption heißt, dass niemand die Nachrichten mitlesen kann. Bei Authentication kann man sicher sein, dass der Empfänger derjenige ist, für den man ihn hält.

Mit Deniability kann nach dem Gespräch nicht bestimmt werden, wer die Nachrichten verfasst hat und mit Perfect Forward Secrecy können Nachrichten nachträglich nicht entschlüsselt werden.

Auf Deutsch kann man die Begriffe wie folgt übersetzen:
Encryption = Verschlüsselung,
Authentication = Beglaubigung,
Deniability = Abstreitbarkeit und
Perfect Forward Secrecy = Folgenlosikgkeit.

Vor allem Deniability und Perfect Forward Secrecy unterscheiden OTR von vielen anderen Verschlüsselungsprotokollen. Die beiden Punkte sind somit auch die größten Vorteile von OTR. OpenPGP hingegen unterstützt z.B. Offline-Nachrichten, aber weder Deniability noch Perfect Forward Secrecy.

Als Nachteil ist z.B. aufzuführen, dass ein Chat mit OTR-Verschlüsselung nur immer von einem Gerät ausgeführt werden kann. Die Nutzung auf mehreren Geräten ist somit nur eigeschränkt möglich.

Vergleich OTR mit OMEMO

Das Verschlüsselungsprotokoll OMEMO kann man z.B. auch bei Pidgin mithilfe eines Plug-Ins nutzen. OMEMO ist –umgangssprachlich beschrieben– die „Weiterentwicklung“ von OTR, denn es bietet theoretisch die gleichen Vorteile und sogar noch mehr (siehe Abbildung 4):

Vergleich:	**OTR**	**OMEMO**
Encryption	X	X
Authentication	X	X
Plausible Deniability	X	X
Deniability	X	X
Perfect Forward Secrecy	X	X
Gruppenchats	-	X
Datentransfer	-	(X)
Nutzung auf mehreren Geräten	(X)	X
Verschlüsselte Offline-Nachrichten (d.h. die Empfänger*in ist offline)	-	X

Abbildung 4: OTR Funktionen im Vergleich zu OMEMO Funktionen

Bei OMEMO handelt es sich aber um eine relativ neue Technik. Daher hat man nicht jahrelang Erfahrung damit und die geforderten Standards wurden noch nicht

ausreichend untersucht. Außerdem befindet sich OMEMO noch in einer „instabilen Entwicklungsphase“, sprich irgendwo zwischen dem „Alpha“- und „Beta“-Entwicklungsstadium. Mit OMEMO sind Gruppenchats möglich (auch wenn dann nicht wirklich Ende-zu-Ende verschlüsselt). Datentransfer theoretisch auch – aber es gibt aktuell noch keinen Server, der dies unterstützt. Bei OTR hingegen sind keine Gruppenchats und kein verschlüsselter Datenversand möglich. Ferner kann man OMEMO auf mehreren Geräten verwenden und auch Nachrichten an Offline-Nutzer schreiben. Bei OTR hingegen nur, wenn der Chat-Partner online ist.

OMEMO bietet also mehr Funktionen und Vorteile. Man sollte allerdings noch abwarten und noch OTR verwenden, bis OMEMO auf die geforderten Standards untersucht wurde und sich in einem „stabilen Entwicklungsstadium“ befindet.

XMPP über TOR

Bislang haben wir uns damit beschäftigt, dass der Chat verschlüsselt ist. Dennoch ist man dann immer noch nicht geschützt, da man nicht anonym im Internet unterwegs ist. Für einen sicheren Chat ist also auch der Aspekt der Anonymität wichtig. Es reicht also auf keinen Falls aus, das OTR- oder OMEMO-Verschlüsselungsprotokoll über seinen XMPP-Chat zu legen, um anonym zu sein.

Deshalb sollte man am besten TOR sowohl bei der Account-Erstellung als auch bei der Verwendung von XMPP, sprich wenn man chattet, verwenden – falls man denn überhaupt anonym sein möchte. Des Weiteren sollte der Benutzername (= die „Jabber-ID“) und das Profilbild in keiner Beziehung zum Benutzer stehen.

The Onion Router (TOR)

Das TOR-Netzwerk hilft also dabei, seine Privatsphäre zu schützen, indem die IP-Adresse des Nutzers verschleiert und die Anfrage verschlüsselt wird. Dabei werden die Informationen vom Absender über mehrere Knoten verschickt, bis sie beim Empfänger ankommen. Durch diese Dezentralisierung und den immer wechselnden Knoten ist es sehr schwierig bis unmöglich herauszufinden, wer der ursprüngliche Absender der Informationen war.

Als potenzielle Schwachstelle im TOR-Netzwerk ist aufzuführen, dass wenn ein Nutzer in der Lage ist eine große Menge an Knoten zu kontrollieren, könnte er die Identität von anderen Nutzern herausfinden. Es ist umstritten, ob die „Five Eyes“ bzw. insbesondere der Geheimdienst der USA (die NSA) dazu in der Lage ist.

Kurze Anleitung für geschütztes Chatten

Aufgrund der Erkenntnisse der vorherigen Seiten sollte man am besten die unten beschriebenen Schritte in folgender Reihenfolge durchführen, um mit einem hohen Sicherheitsgrad Chatten zu können (die jeweiligen Schritte gelten natürlich auch genauso für den Chat-Partner):

1. Tor Browser downloaden & installieren (noch besser mit Betriebssystem Tails)
2. Tor Browser mit höchster Sicherheitsstufe öffnen und das Browser-Fenster weder vergrößern noch verkleinern
3. Mit DuckDuckGo (= anonyme, sichere Suchmaschine, im Tor Browser integriert) einen passenden XMPP-Server suchen und anschließend eine „Jabber-ID“ erstellen
4. Pidgin downloaden und installieren
5. Pidgin öffnen und mit „Jabber-ID“ und Passwort einloggen
6. Tor Einstellungen in Pidgin vornehmen
   - 1. Möglichkeit:
     siehe Abbildung 5

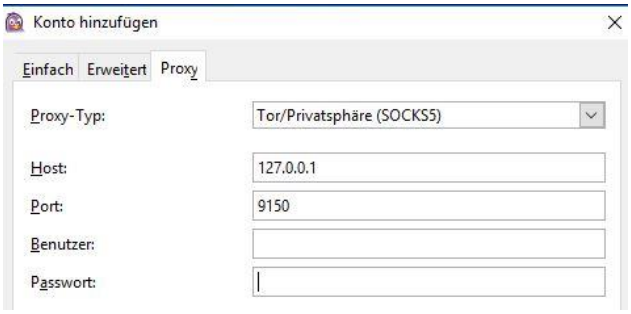

Abbildung 5

   - 2. Möglichkeit über Hidden Service (= onion-Link) des Servers:
     siehe Abbildung 6
     ⇨ Um Probleme mit bösartigen Tor Exit Nodes zu vermeiden wird die 2. Variante oft von den XMPP-Server-Betreibern empfohlen, hier als Beispiel mit „kqiafglit242fygz.onion“

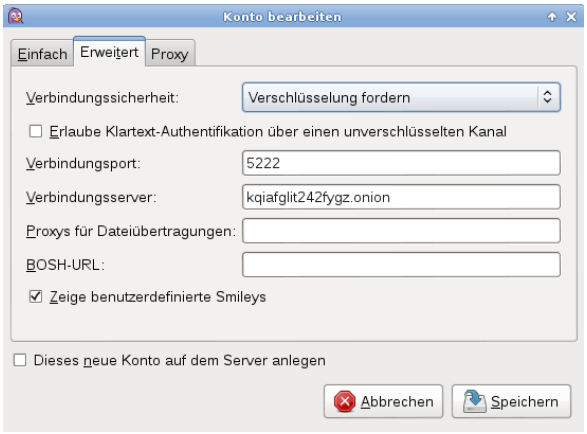

Abbildung 6

7. OTR Plugin für Pidgin downloaden, installieren und privaten Schlüssel bzw. Fingerprint generieren
8. Kontakt hinzufügen
9. Mit dem jeweiligen Kontakt authentifizieren -> ORT-Status ändert sich schließlich auf „Privat“, sobald sich beide authentifiziert haben
   ⇨ bei OTR hat man 3 Möglichkeiten zur Authentifikation: Frage und Antwort, gemeinsam bekannte Passphrase und manueller Fingerprint-Vergleich
10. Nun kann man Chatten ☺

Literaturverzeichnis

- Torben Fritsch: IT-Seminar der FH Wedel bei Prof. Anders vom Sommersemester 2017 mit dem Thema „Geschütztes Chatten über Jabber Server“

- https://pi4.informatik.uni-mannheim.de/pi4.data/content/courses/2006-hws/seminar/arbeiten/12-ausarbeitung.pdf

- https://www.internetworld.de/mobile/messenger-app/verbreitung-messaging-apps-1240805.html

- https://t3n.de/news/top-10-meistgenutzte-messenger-weltweit-2017-839993

- https://userforum.mailbox.org/knowledge-base/article/was-ist-jabber-xmpp

- https://www.heise.de/newsticker/meldung/Facebook-Messenger-Verschluesselte-Chats-verfuegbar-3332724.html

- http://www.spiegel.de/netzwelt/apps/whatsapp-verschluesselung-gut-aber-nicht-komplett-abhoersicher-a-1085726.html

- https://www.welt.de/wirtschaft/webwelt/article164531727/Diese-WhatsApp-Sicherheitsluecke-ist-eine-Einladung-fuer-Kriminelle.html

- https://www.jabber.org/faq.html

- https://pidgin.im

- https://adium.im

- https://otr.cypherpunks.ca und https://otr.cypherpunks.ca/help/3.2.0/authenticate.php?lang=en

- https://github.com/gkdr/lurch

- https://www.torproject.org/index.html.en

- https://list.jabber.at

- https://xmpp.org/software/clients.html

- https://www.jabber.de/was-ist-jabber

- https://www.einfachjabber.de/jabber.html

- https://www.youtube.com/watch?v=yN1gEJisQWA

- https://keinplan.blackblogs.org/wp-content/uploads/sites/577/2018/03/How-To-Jabber-mit-OTR-und-OMEMO-v1_3.pdf

- https://userforum.mailbox.org/knowledge-base/article/pidgin-mit-tor-onion-router

- https://en.wikipedia.org/wiki/Instant_messaging
- https://de.wikipedia.org/wiki/Jabber_Instant_Messenger
- https://en.wikipedia.org/wiki/Pidgin_(software)
- https://en.wikipedia.org/wiki/XMPP
- https://de.wikipedia.org/wiki/Extensible_Messaging_and_Presence_Protocol
- https://de.wikipedia.org/wiki/XMPP-Transport
- https://de.wikipedia.org/wiki/Liste_von_XMPP-Clients
- https://de.wikipedia.org/wiki/Off-the-Record_Messaging
- https://de.wikipedia.org/wiki/OMEMO
- https://de.wikipedia.org/wiki/Tor_(Netzwerk)

(Letzter Zugriff gilt für alle obigen Internet-Quellen: 18.06.18)