Kommunikation, Sicherheit im Chat und im Telefonat: Jabber

Immer wieder kommen neue Protokolle, neue Messenger, neue Ideen auf dem Markt. Jeder springt auf den Zug auf und dann auch manchmal gleich wieder ab. Kommunikation in den heutigen Tagen ist eines der wichtigsten Themen. Vor allem sichere Kommunikation. Doch was ist wirklich sicher? Wollen wir das es sicher ist oder ist uns das egal? Meinen wir damit abhörsicher oder einfach nur das es „sicher EINFACH funktioniert? Diese Frage möchte ich in diesem Betrag gerne beantworten.

Nachdem ich mich doch viele Tage immer wieder mal mit dem Thema (theoretisch so wie auch praktisch) auseinander gesetzt habe, kann ich definitiv sagen das Sicherheit und das es einfach funktioniert einfach nicht zusammen passen. Im Endeffekt ist sichere Kommunikation doch einfach zu bedienen. Aber der Weg dort hin ist dann doch etwas steinig und der normale Benutzer möchte sich damit nicht beschäftigen.

Alle unverschlüsselten Plattformen in ihrer Form scheiden natürlich sofort aus. Proprietäre Protokolle wie Skype detto. Un abgesehen ob man nun was zu verbergen hat oder nicht, muss das denn sein? Man brüllt ja auch nicht seine privaten Probleme laut und verständlich in die eigene Ortschaft hinaus. Signal scheidet für mich auch aus. Der Schlüssel wird hier ohne zutun generiert. Ich habe nicht die Möglichkeit meinen eigenen Key hier zu verwenden. Zumindest wird man nicht danach gefragt und auch suchen nach solcher Funktion blieb erfolglos.

Back to the Root's

Im Endeffekt hat das Rennen wieder mal Jabber gemacht. Warum? Hier ein paar Gründe:

- Es ist fast egal auf wann für einen Server man sich registriert. Vielen können hier schon IPV6.
- Jeder öffentlich Jabberserver spricht mit den anderen, man ist also keinesfalls Domänenanbhängig
- Jeder kann seinen eigenen Jabberserver mit seiner eigenen Domäne betreiben
- Die Kommunikation kann zu 100% verschlüsselt sein (GPG/OTR/TLS)
- Zertifikate muss man selbst generieren
- Video und Sprachqualität stehen Anbietern wie Skype keinesfalls nach (Google benutzt auch XMPP aber gleich wie Facebook, geschlossen)
- Durch Transporte Verbindung auch in andere Netzwerke wie z.B. ICQ möglich. Da Facebook netterweise seine Jabber API abgeschaltet hat, geht dies hier für FB leider nicht mehr.

Um was es ganz genau geht kann man auf der Ubuntuuseres Wikiseite nachlesen. Ich persönlich empfehle diesen Artikel einmal durchzulesen. Er ist sehr aufschlussreich dokumentiert.

Gehen wir nun gleich zur Praxis über. Ich habe einige Clients getestet.

Die Wahl des XMPP Clients (Kubuntu 16.04/OSX/Windows10)

Nun gut wir wissen jetzt was für ein Protokoll wir verwenden sollen. Aber was ist mit dem Client? (K)ubuntu kommt mit Telepathy als Backend daher. Als Frontend gibt es die halbfertigen Programme Empahty (Unity/Gnome) und das KDE Messengingservice. Solange man nicht Telefonieren möchte und kein GPG benutzt tun's die beiden. Warum hier immer wieder auf halbfertige Software gesetzt wird ist mir ein Rätsel.

Folgende Clients wurden noch getestet:

- PSI (wird nicht mehr weiter entwickelt, Audio/Video funktioniert nicht)
- PSI+ (Testsieger, wird aktuell entwickelt, stabil, volle Features inkl. Whiteboard, Audio/Video, Konferenzen, uvm.
- Kopete (wird nicht mehr weiter entwickelt... finde ich persönlich schade, Audio und Video funktionieren nicht mehr)
- Jitsi (Java programmiert, frisst sich beim Schließen in der Taskleiste fest, wenig Chatfeatures, nicht kompatibel mit KDE, das heist aber nicht das es auf Uniy oder Gnome3 nicht sehr gut funktioniert, Vorteil: Provisioningfunktion, Gespräche werden mit SDES/SRTP ZRTP verschlüsselt)

Nachdem Jabber ja durch Transports mit anderen gut kann vielen weitere Tests mit Mulitprotokollmessenger weg.

PSI+

PSI+ ist der Nachfolger von PSI. Pakete gibt es für sämtliche Betriebssysteme http://psi-plus.com/wiki/de:downloads http://psi-plus.com/wiki/de:downloads Die Installation wird für Kubuntu 16.04 beschrieben.

Installation

Benötigt man keine Audio/Videounterstützung Themes oder Iconsätze kann auch das Paket direkt von den Ubuntu Paketquellen installieren. Ich empfehle das https://launchpad.net/~psi-plus/+archive/ubuntu/ppa?field.series_filter=xenial PPA.

```
add-apt-repository ppa:psi-plus/ppa
```

Nun die folgenden Pakete installieren:

```
apt install psi-plus psi-plus-icons-nonfree psi-plus-plugin-psimedia psi-plus-skins psi-plus-sounds
```

Das Programm hat so viele Features und Plugins. Diese hier alle zu erläutern würde den Rahmen

sprengen. Hier ein Kleiner Auszug. Features: * Vollverschlüsselung, auch erzwungen, so kann man sichergehen das nichts unverschlüsselt übertragen wird

- Anpassung an jede Desktopoberfläche mit Hilfe von Plugins und auch Skins möglich
- Freigabe von Musik, Videoübertragung (noch nicht getestet)
- Audio/Videochat (Leider kein SRTP also keine Verschlüsselung)
- Transporte
- Konferenzen (noch nicht getestet)
- GPG/TLS/OTR
- Autoreply
- Gmailserviceplugin
- Übersetzer
- …

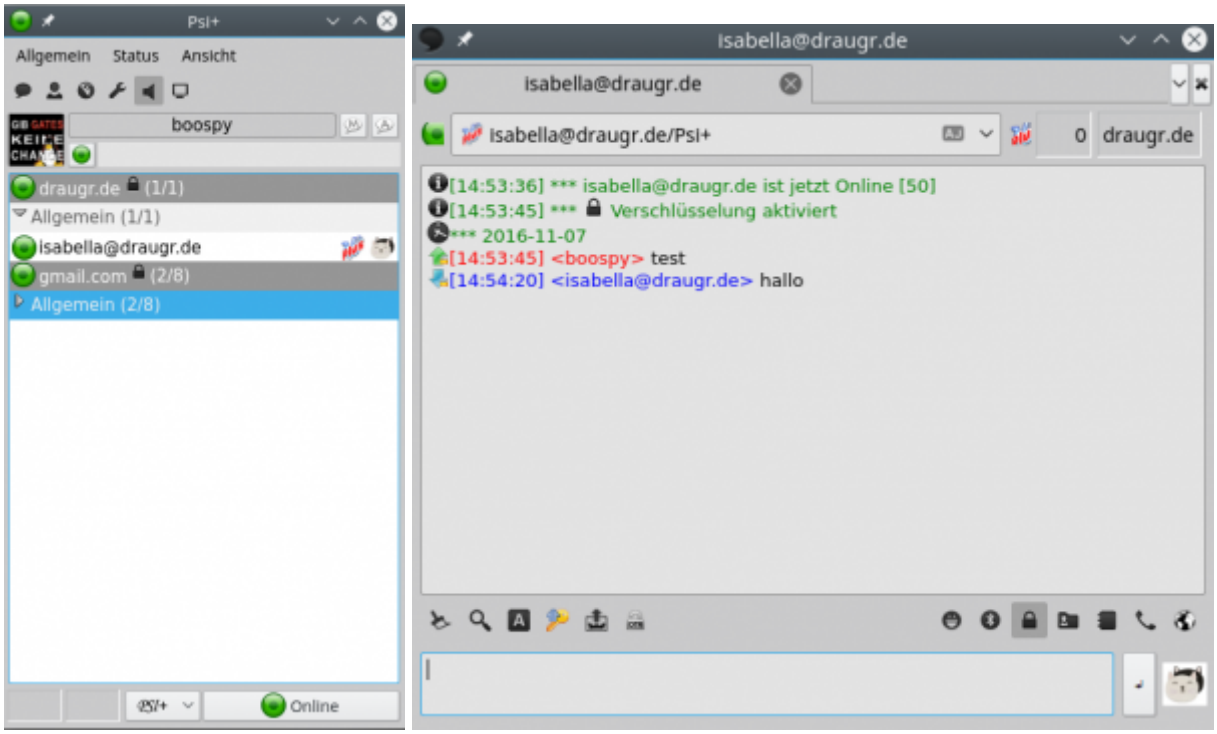
Konfiguration

Zur Konfiguration kann man nicht viel sagen. Die Funktionen sind selbsterklärend. Wichtig ist das man seinen Client für den Dateitransfer konfiguriert. Hat man kein NAT sollte es auch so gehen. PSI+ kommt mit deaktivierten Funktionen. Nur die benötigten schaltet man frei. Z.B. OTR oder die GPG Schlüsselverwaltung.

Um nun doch endlich verschlüsselt kommunizieren zu können verwendet man OTR (einfacher) oder eleganter und sicherer GPG. Ich empfehle und bevorzuge natürlich GPG.

- Web of Trust
- KGpg
- GnuPG

Zum Aussehen: Ich habe mich für das Standardskin entschieden. Zusammen mit den Oxygenicons für die Kontaktliste/Status und die Blackicons als Systemicons, macht das ganze einen Aussagekräftigen freundlichen Eindruck.

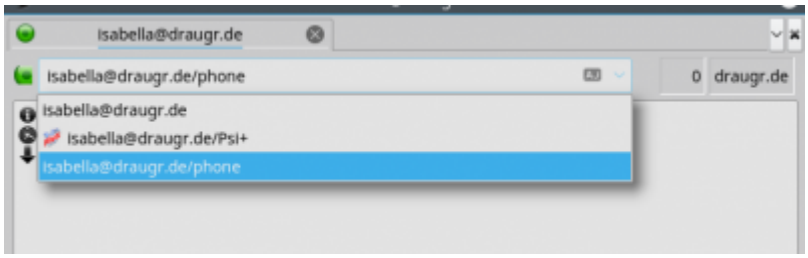


Um die Konfiguration auf ein anderes System zu übertagen muss man lediglich dies Dateien auf sein Zielsystem kopieren. Natürlich müssen etwaige Schlüssel extra übertragen werden.

```
/home/$USER/.config/psi+
/home/$USER/.local/share/psi+
```

Auswahl des Clients (Gesprächspartner)

Ist der Gesprächspartner mit mehreren Clients online so muss man das Ziel auswählen.



Probleme

Hat man eine Kamera mit Mikrofon angeschlossen kommt es anscheinend bei manchen Modellen dazu wenn man einen Anruf tätigt und die Kamera aus was für einem Grund auch immer nicht richtig am System erkannt wurde zu einem langen Timeout, auch ein Neustart der Anwendung dauert lange. Lösung des Problems: USBkabel neu verbinden oder die Kamera unter Telefon deaktivieren damit es nicht mehr vor kommt. Das Problem ist beim Dev schon bekannt.

Mobile Clients

Xabber

- TLS funktioniert nicht
- OTR lässt sich nicht starten
- kein GPG

jTalk2

- Stürzt schon beim Start ab
- kann sich nicht verbinden

ChatSecure

- Plus Secure mit Hauptpasswort
- Mit Googlekonto durch Assistent verknüpfbar (Jabber Default, alle anderen Clients können das auch, nur wird man nicht danach gefragt)
- Vermaschte Verbindung ohne Internet wird angeboten
- Einwegkonto
- Defaultmäßig wird mit OTR verschlüsselt

- Leider wird die App nicht mehr weiter entwickelt, empfohlen wird von ihnen Conversations

Conversations (Sieger)

- Einfach Bedienung
- TLS, OTR und GPG funktionieren einwandfrei
- Gruppenchat
- Synct sich mit dem Desktopclient (natürlich nur immer eine Verbindung)
- Dateien versenden (PGP verschlüsselt)

Je nach Telefon sind Energieeinstellungen (Stromsparmechanismen) aktiv die, die Anwendung zum Trennen der Verbindung auffordern könnten. Sollte das wo der Fall sein, gibt es in Conversations unter Experteneinstellung ganz unten ein Häckchen (Dienst im Vordergrund ausführen). Ob man nun zu einem Mobiltelefon oder zu einem Computer übertragen möchte, hierbei wird man pro Unterhaltung gefragt. Ist man Mobil und am Computer Online sieht der Status in PSI+ so aus:

Nutzt man GPG sollte man sich der Bedienung bewusst sein. Das heist immer zwei Endpunkte. Also PC zu PC, PC zu einem Mobiltelefon, Mobiltelefon zu einem Mobiltelefon. Das sind alles eigenständige Unterhaltungen da ja P2P verschlüsselt wird. Ich beende daher immer angefangene Konversationen und bin nur immer an einer Stelle online, sonst kann es zu Verwirrungen kommen.

Fazit

Trotz einigen Aufwand lohnt es sich über das XMPP Protokoll verschlüsselt zu kommunizieren. Qualitätsmäßig steht Jabber niemanden hinterher, ganz im Gegenteil. Oft wird man nur durch Unsicherheit, (mit der Aussage: alle nutzen Facebook und Skype) Unwissenheit und vor allem auch Faulheit gehindert sich mit einem wirklich wichtigen Thema auseinander zu setzen. Aber nur so lange bis einen die Realität durch z.B. Datendiebstahl und Datenveröffentlichung einholt.

Links

- Toxprotokoll (nicht fertig viel zu viele Fehler) https://en.wikipedia.org/wiki/Tox_(protocol) https://wiki.ubuntuusers.de/Tox/ https://github.com/qTox/qTox/issues
- Telegram (nicht getestet) https://wiki.ubuntuusers.de/Telegram/
- Wire (auch noch ein sehr junges Projekt das seinen Schwerpunkt auf Telefonate setzt) https://de.wikipedia.org/wiki/Wire_(Messenger)
- jabber (ausgereift und verbreitet, alle Funktionen die für Kommunikation benötigt werden)

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