Instant Messaging mit XMPP

Norbert Tretkowski

Email: norbert@tretkowski.de
XMPP: norbert@tretkowski.de

Linux User Schwabach
07. April 2016

Agenda

- Grundlagen
- Features
- Clients
- Erweiterungen
- Sicherheit
- Messenger & Datenschutz
- LUSC XMPP Server
- Demo

Rückblick

Quelle: https://gallery.lusc.de/

Grundlagen

- eXtensible Messaging and Presence Protocol
- Entwicklung 1998 gestartet, 1999 unter dem Namen Jabber veröffentlicht
- Seit 2004 offizieller IETF Standard (RFCs 6120, 6121 und 6122) unter dem Namen XMPP
- XMPP Standards Foundation verantwortlich für die Standardisierung des Protokolls und dessen Erweiterungen (XEPs, XMPP Extension Protocols)

Accounts

- Anlegen eines Accounts (Jabber-ID) ist nötig
- Account kann direkt im Client angelegt werden
- ID: nobse@lusc.de/phone
  - nobse: Benutzer
  - lusc.de: Domain
  - phone: Resource
- Priorität (-128 bis 128)

Routing

- Clients können Prioritäten setzen
- Client mit der höchsten Priorität erhält Nachrichten

Nachricht

```
<message to='wampire@lusc.de'
    from='nobse@lusc.de/phone'
    type='chat'>
  <body>Moin!</body>
</message>
```

Features

- Kein Single Point Of Failure (dynamisches Netz)
- Offene Entwicklung
- Transports
- Sicherheit
- Kein Vendor Lock-In (siehe Revolv)
- Kein Walled Garden
- Simultane Logins
- Abwärtskompatibel
- Multi-User Chats

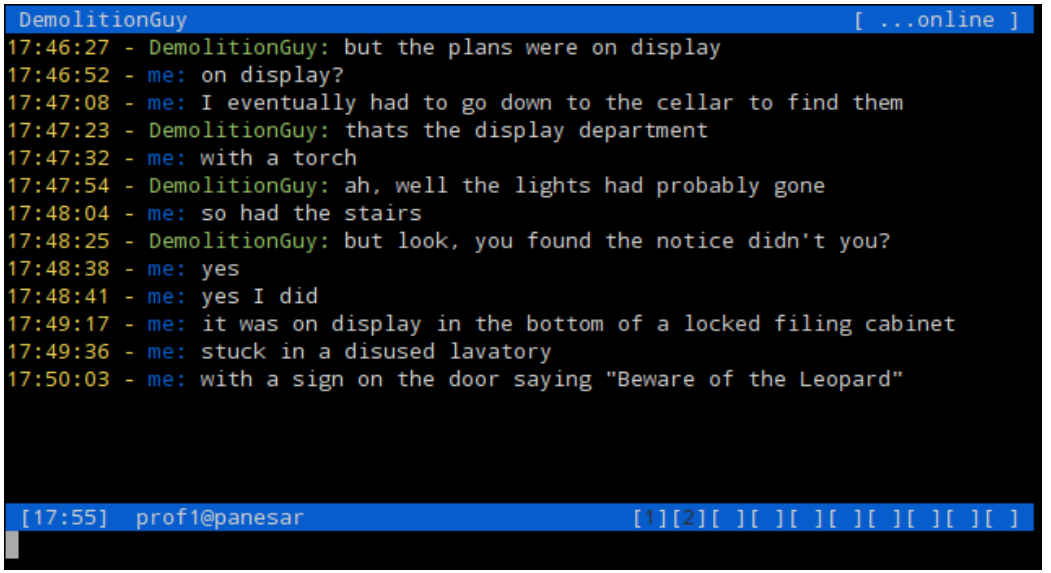
GUI Clients

- Gajim
- Pidgin
- Empathy
- Psi

Quelle: https://gajm.org/

Console Clients

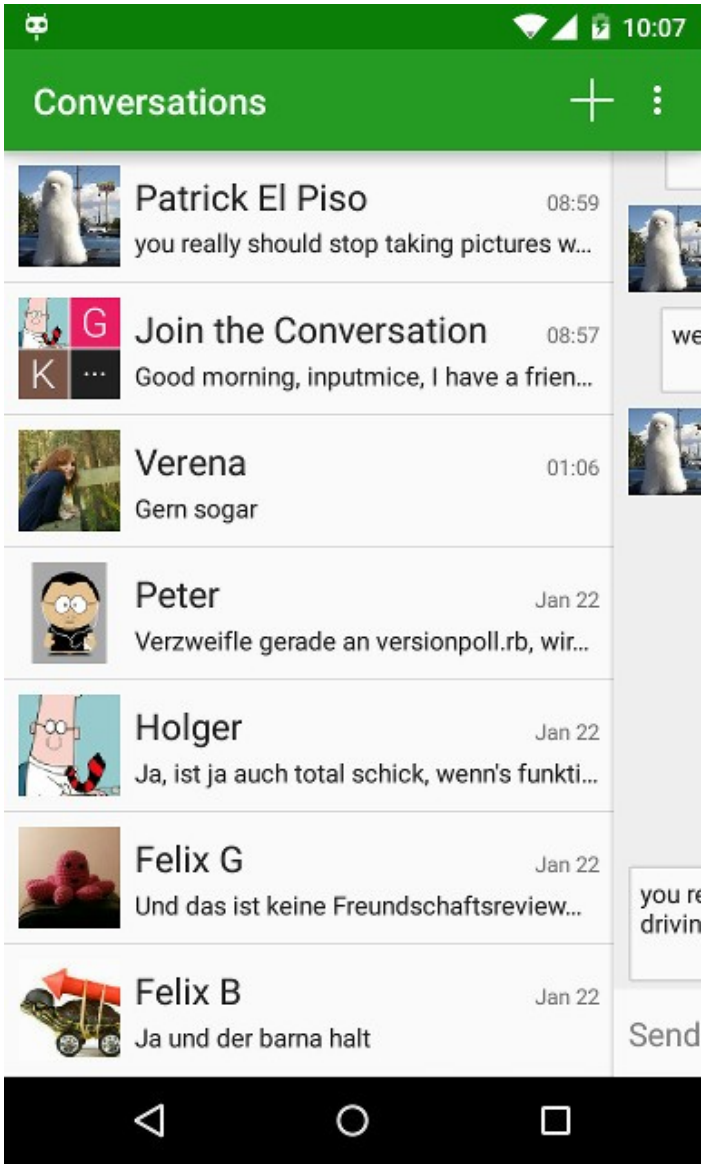
- Profanity
- MCabber
- Bitlbee
- CenterIM
- WeeChat



Quelle: https://profanity.im/

Mobile Clients

- Android:
  - Conversations
  - Xabber
  - Yaxim
- iOS:
  - Monal
  - IM+
  - BeejiveIM



Quelle: https://conversations.im/

Sicherheit

- Client zu Server
  - SSL/TLS
- Server zu Server
  - SSL/TLS (verpflichtend seit 2004)
  - Nicht von allen Servern unterstützt (z.B. Google)
- Client zu Client
  - OpenPGP
  - OTR
  - OMEMO

Transports

- Gateways in andere Netze, u.a.
  - ICQ
  - MSN
  - AIM
  - Yahoo
  - IRC
  - WhatsApp
- Gateways anderer Server nutzbar
- Nicht immer 100%ig zuverlässig, z.B. bei Änderungen am Protokoll

Erweiterungen

- XEP-0163: Personal Eventing Protocol
- XEP-0191: Blocking Command
- XEP-0198: Stream Management*
- XEP-0237: Roster Versioning
- XEP-0280: Message Carbons*
- XEP-0313: Message Archive Management*
- XEP-0352: Client State Information*
- XEP-0363: HTTP File Upload*

(*) Details in den folgenden Folien

Message Carbons

- Eingehende Nachrichten werden an alle verbundenen Clients geschickt
- Ausgehende Nachrichten werden an alle anderen verbundenen Clients geschickt

Message Archive Management

- Nachrichten werden auf dem Server gespeichert
- Neue Clients können auf die alten Nachrichten zugreifen
- Clients die offline waren erhalten trotzdem alle Nachrichten
- Verschlüsselung der Nachrichten bei Nutzung fremder Server wichtig
- Kann im Client deaktiviert werden

Stream Management

- Wiederaufnahme einer Session bei Abbruch einer TCP Verbindung
- Spart Traffic (und damit Akku)
- Mögliche Verwirrung durch Nutzung von Message Archive Management

Client State Indication

- Unterdrückung von Informationen wenn der Client im Hintergrund läuft
  - Presence (Join/Leave)
  - Typing Information
- Kein häufiges „Aufwecken“ des Clients mit großer Kontaktliste oder in Konferenzen

HTTP File Upload

- Speichern der Dateien auf dem Server
- Funktioniert auch mit mehreren verbundenen Clients und in Konferenzen

End-to-End Encryption

- OpenPGP
  - XEP
  - Funktioniert nicht mit mehreren Clients
- OTR
  - Synchrone Session, Chatpartner muss online sein
  - PITA mit mehreren online Clients parallel

Multi-End-to-Multi-End Encryption

OMEMO Multi-End Message and Object Encryption

- Nachrichten können an offline Kontakte gesendet werden
- Nachrichten können an mehrere Endgeräte gesendet werden
- Gesendete Nachrichten landen auch auf allen eigenen Geräten

OMEMO

- Axolotl (Signal Protocol) Session zwischen Clients
- Ein Key je Client (Overhead erhöht sich je mehr Endgeräte man nutzt)
- Pre-Keys werden auf dem Server gespeichert
- Keine Änderung am Server notwendig (PEP sollte von allen verfügbaren Servern unterstützt werden)
- Clients ohne Unterstützung für OMEMO erhalten die Nachrichten nicht

Messenger

- Die meisten der bekannten Messenger nutzen XMPP, verhindern aber die Kommunikation mit externen Servern
- Secure Messaging Scorecard unter

  https://www.eff.org/de/node/82654
- WhatsApp
- Hangouts
- Threema
- Signal (ehem. TextSecure)
- LibreSignal

WhatsApp

- Contra:
  - Closed Source
  - Client zu Client Verschlüsselung nicht nachprüfbar und nur eingeschränkt (Stand 4.4.2016)
  - Basiert auf Telefonnummern (Verstoß gegen BDSG)
  - Kein Desktop Client, nur Webfrontend
  - Vendor Lock-In
  - Walled Garden

Hangouts

- Pro:
  - Mit mehreren Endgeräten parallel nutzbar
- Contra:
  - Closed Source
  - Verschlüsselung
    - Client zu Client Verschlüsselung nicht vorhanden
    - Nachrichten serverseitig unverschlüsselt
  - Vendor Lock-In
  - Walled Garden

Threema

- Pro:
  - Optional separate Threema-ID statt Kopplung an Telefonnummer
- Contra:
  - Closed Source
  - Nur mit einem Engerät nutzbar
  - Vendor Lock-In
  - Walled Garden

Signal

- Pro:
  - Open Source (sowohl Client als auch Server)
- Contra:
  - Basiert auf Telefonnummern (Verstoß gegen BDSG)
  - Kein Desktop Client, nur Chrome App (alle (Meta)-Daten laufen durch den Closed-Source Browser von Google)
  - Vendor Lock-In
  - Walled Garden (WhisperPush in CM13 nicht mehr enthalten)
  - Nur mit GCM nutzbar (Metadaten gehen an Google)

LibreSignal

- Pro:
  - Open Source
  - Fork von Signal
  - Nutzt Websockets statt GCM
- Contra (zzgl. denen von Signal excl. GCM):
  - Nutzt die Signal Server (kann also von heute auf morgen von extern ausgeknipst werden)
  - Von Moxie Marlinspike als „random software on the internet that should be considered malware“ bezeichnet

SMSSecure

- Pro:
  - Open Source (Fork von TextSecure)
  - Bietet verschlüsselte „oldschool“ SMS
- Contra:
  - Metadaten gehen an den Mobilfunk Anbieter
  - Nur mit SMS Flatrate sinnvoll nutzbar

LUSC XMPP Server

- Irgendwann mal jabberd14 aufgesetzt
- Klausurtag Februar 2006 Migration auf jabberd2 inkl. LDAP Anbindung
- 2007 Migration auf eJabberd, noch heute im Einsatz
- Erwähnte Features sind verfügbar
- Derzeit keine Transports in andere Netze
- Accounts unter username@lusc.de

Demo

- Gajim
- Conversations
- OMEMO
- MUC
- ...

Fragen

?

Quelle: https://gallery.lusc.de/

Links

- https://xmpp.org/software/clients.html
- https://xmpp.org/software/servers.html
- https://lusc.de/dokuwiki/interaktiv/jabber (out of date)
- https://tretkowski.de/talks/XMPP_2016.pdf