Chatten mit der Glühbirne

Eine Einführung in Jabber und XMPP
für normale User

Tim Weber
Chaostreff Mannheim
25. Mai 2007

Inhalt

- Worum geht's?
- Terminologie, Unterschiede, Vor- und Nachteile gegenüber anderen Systemen
- Aktueller Status
- Empfohlene Software
- Fragen (auch gern während dem Vortrag)

Worum geht's?

- XMPP: eXtensible Messaging and Presence Protocol („erweiterbares Nachrichten- und Anwesenheitsprotokoll“), XML-Protokoll, bildet die Grundlage für...
- Jabber („Geplapper“): Ein offener Standard für Instant Messaging
- Sinn des Ganzen: Befreiung aus der proprietären Welt von ICQ, MSN und Co., mehr Vielfalt durch freie Verfügbarkeit und Community-Ansatz

Terminologie

- **Jabber:** das Protokoll, aber auch das „Netz“
- **Server:** einer von vielen möglichen Servern
- **Client:** eine Zugangssoftware
- **Presence:** Status eines Users (online, away, dnd, offline, invisible, ...)
- **Roster:** Kontaktliste („Adressliste“)
- **Transport:** Übergang in ein anderes Netz oder Protokoll, auch **Gateway** genannt
- **JID:** Jabber-ID (benutzer@example.com)

Unterschiede bzw. Vorteile

- Protokoll ist frei und offen dokumentiert (anstatt proprietär und zurückentwickelt)
- kein zentraler Server (sondern viele private und öffentliche, die sich vernetzen)
- Einloggen mehrmals gleichzeitig möglich
- Verschlüsselung von Passwörtern und Daten
- Entwickeln eigener Software einfach, da XML und offene Protokolle (und Libraries)
- viele Zusatzdienste verfügbar (Atom/RSS, Terminerinnerungen, Web-Presence, ...)

Nachteile

- Transports in Fremdnetze nicht 100%ig perfekt (geht aber oft auch gar nicht anders)
- Clientvielfalt
- Servervielfalt
- Work in Progress und manchmal veraltete Dokumentation

Aktueller Status

- Kern-Protokoll tut, Transports zu ICQ, AIM, MSN, YM, IRC, GG, IRC, Mail, ...
- File-Transfer, Direktverbindungen (VoIP namens „Jingle“, ähnlich SIP)
- Verschlüsselung: SSL/TLS, GPG, OTR
- Clientsoftware für jede Plattform und für jedes Betriebssystem (afaik) inklusive Windows Mobile, Palm OS und Java ME
- weit verbreitet in Unternehmen oder als Google Talk, GMX/web.de, mabber.de, ...

Empfohlene Software

- Linux/Mac/Windows: Psi (Jabber-only); http://psi-im.org/
- Linux/KDE: Kopete; http://kopete.kde.org/
- Linux/Gnome: Pidgin; http://pidgin.im/
- Mac: Adium?
- Windows: Psi, definitiv

Jabber-IDs

- Da kein zentraler Server, muss der Server in der ID aufgeführt werden.
  - Vorteil: Chance auf Lieblingsnick höher, E-Mail-Adresse verwendbar
- z.B. ist scy@scytale.de meine Mail-Adresse, aber auch meine Haupt-JID

Transports

- gehören zu einem bestimmten Jabber-Server, sind aber oft auch von anderen Servern aus nutzbar; somit braucht nicht jeder Server eigene Transports
- bilden IDs des anderen Netzes auf JIDs ab; Beispiele:
  - 36023058@icq.im.scytale.de (ICQ)
  - scytale%wudnet.org@msn.im.scytale.de (MSN)

Group Chats

- Chaträume mit mehreren Benutzern, werden ebenfalls über JID mit eigenem Host angesprochen; z.B.:
  - c3ma@chat.c3ma.de
  - c3ma%chat.eu.freenode.net@irc.example.org (Transport in den IRC!)

Der c3ma-Server

- nickname@c3ma.de
- momentan öffentliche Registrierung, aber ich bekomm sofort ne Message
- momentan ICQ- und MSN-Transports
- gut für Kongresse etc., wenn man seine Zugangsdaten nicht unverschlüsselt senden will, denn SSL und TLS unterstützt
- alle @c3ma.de-User sehen sich automatisch im Roster
- chat.c3ma.de für spontane Group Chats

Privatsphäre

- aka „Warum sollte ich dir meine Nachrichten anvertrauen?“
- Gegenfrage: Warum solltest du sie AOL anvertrauen, die in die AGBs schreiben, dass du alle Rechte an deinen Texten an sie überträgst?

Kryptodinge

- c2s: TLS / Klartext auf 5222, SSL auf 5223
- s2s: wird unterstützt, wenn der andere Server es unterstützt
- e2e (end-to-end): clientseitiges Feature, Kommunikation wirklich nur von den Gesprächspartnern lesbar
  - GnuPG (mit normalen Keys), z.B. Psi
  - OTR (besser, aber von Psi nicht unterstützt)

Was kann Scy als Serveradmin alles sehen?

- ob du verbunden bist, wann du das letzte Mal verbunden warst
- im Seitenquelltext dein Passwort (manche Auth-Methoden brauchen afaik Klartext)
- deine Kontaktliste (auf einer Unterseite)
- Anzahl offline-Nachrichten, Nachrichten selbst auf einer Unterseite
- **kein** Log der Konversationen
- **aber:** es interessiert mich nicht!!

Lieber eigener Server?

- „klassischer“ **jabberd** in Version 1.2 (alt, aber wird weiterentwickelt) oder 2.0; nicht allzu einfach zu konfigurieren; *ich* hab schlechte Erfahrungen gemacht
- **ejabberd** mit seltsamer Configsyntax, aber recht einfach, Webadmin, viel eingebaut
- **Openfire** (früher Wildfire): Java, Free- und kommerzielle Version verfügbar

Fragen?!