

# Warum Jabber?

Raphael Michel  
<raphael@geeksfactory.de>

27. Juni 2010

## Inhaltsverzeichnis

<b>1</b>	<b>Vorwort</b>	<b>1</b>
<b>2</b>	<b>Warum nicht...</b>	<b>2</b>
2.1	ICQ	2
2.2	AOL Instant Messenger	3
2.3	Windows Live aka MSN	3
2.4	Yahoo-Messenger	4
2.5	Skype	4
2.6	schülerVZ Plauderkasten	5
2.7	Facebook Chat	5
<b>3</b>	<b>Jabber, weil...</b>	<b>5</b>
3.1	frei	5
3.2	offen	5
3.3	dezentral	6
3.4	verschlüsselbar	6
<b>4</b>	<b>Ja(bber), ich will!</b>	<b>7</b>
4.1	Server	7
4.1.1	Google Talk	7
4.2	Client	7

## 1 Vorwort

Dieses Essay soll Aufschluss darüber geben, warum auch dem unerfahrenen Computernutzer ans Herz gelegt werden sollte, zum Chatten das freie System Jabber, basierend auf dem Protokoll XMPP, zu nutzen, anstatt auf proprietäre Dienste wie ICQ, Windows Live oder Skype zurückzugreifen. Es wird nur auf die Aspekte des Chattens eingegangen, obwohl mittlerweile nahezu alle Chatnetzwerke die Möglichkeit zu (Video-)Gesprächen

bieten. Hier gilt in Hinblick auf Datenschutz meist das selbe, aber auf Unterschiede wird nicht näher eingegangen.

## 2 Warum nicht. . .

### 2.1 ICQ

ICQ wurde 1996 von israelischen Studenten entwickelt, zwei Jahre später wurde es von AOL für fast eine halbe Million Dollar gekauft. Anfang diesen Jahres (2010) wurde es von AOL für weniger als den halben Kaufpreis an die russische Firma Digital Sky Technologies verkauft.

In einem eigenen Test liefen alle Chatdaten durch einen Server, dessen IP-Adresse auf America Online, Inc. in den USA angemeldet ist. AOL hat also die Möglichkeit, alles, was wir über ICQ schreiben, mitzulesen, zu speichern und sonstwie zu verwerten. Die technische Möglichkeit besteht!

Menschen, die an das Gute in den Konzernen glauben, argumentieren jetzt, dass sie es zwar technisch könnten aber doch nie tun würden und es illegal wäre. Wäre es das? Nein.

In den ICQ-Nutzungsbedingungen<sup>1</sup> findet sich folgendes:

„Sie stimmen zu, dass Sie Ihr Urheberrecht sowie jegliche andere Eigentumsrechte an gesendetem Material durch das Senden aufgeben. Des Weiteren stimmen Sie zu, dass ICQ Inc. befugt ist, nach eigenem Ermessen jegliches gesendete Material oder gesendete Informationen in jeder Art und Weise zu benutzen, beispielsweise, aber nicht ausschließlich, indem es das Material veröffentlicht oder verbreitet.“

Auch behält sich ICQ vor, persönliche Daten, die es außer dem gesendeten Material hat, an Strafverfolgungsbehörden weiterzugeben. Aber selbst, wenn man AOL vertraut, dass sie mit den Daten, die sie sammeln dürfen vertrauensvoll umgehen, ist die zentrale Struktur dieses Netzes gefährlich: werden diese zentralen Server von einem Hacker geknackt, kann er gleichzeitig alle ICQ-Chats dieser Welt mitlesen, da ausnahmslos alle Chats hier „vorbekommen“.

Ein weiterer Faktor ist die Nutzung alternativer Software. Will man im ICQ-Netzwerk chatten, muss man die von ICQ bereitgestellte, gleichnamige Software nutzen. Diese gefällt jedoch vielen nicht und läuft nicht auf jedem Betriebssystem, daher wurden von unabhängigen Entwicklern dennoch Programme entwickelt, mit denen man sich ebenfalls ins ICQ-Netzwerk verbinden kann. Laut ICQ-Nutzungsbedingungen sind diese jedoch nicht zugelassen:

„Sie stimmen zu, weder (1) Software zu erstellen oder zu nutzen, die nicht von ICQ, America Online, Inc. oder ihrer Partner bereitgestellt wurden, um ihre ICQ-Nummer und Passwort einzugeben oder die ICQ-Dienste zu nutzen ohne

---

<sup>1</sup><http://www.icq.com/legal/policy.html> abgerufen 26.06.10

die ausdrückliche Genehmigung von ICQ; (2) Informationen aus den ICQ-Diensten zu extrahieren, rückzuentwickeln, zu dekompileieren, zu disassemblieren, zu verändern, zu duplizieren, zu kopieren, abgeleitete Werke zu erstellen, zu verbreiten oder anderen die Software, das ICQ-Kommunikationsprotokoll oder jeglicher erhältlichen, abgeleiteten oder extrahierten Informationen oder Teilen darüber zur Verfügung zu stellen; [...] (5) Software oder Teile davon (sowie die ICQ-Kommunikationsprotokolle) in andere Software, Programme oder Produkte, welche mit den ICQ-Diensten oder einem anderen Instant Messaging-, Internet-, oder Onlinedienst kommunizieren, ansteuern oder in irgendeiner anderen Art verbinden, zu integrieren, einzugliedern oder auf andere Weise einzuarbeiten.“

Der Programmcode von ICQ ist nicht öffentlich einsehbar, wodurch keine Transparenz besteht. Niemand außerhalb von AOL kann nachprüfen, ob diese Software wirklich sicher ist.

ICQ läuft standardmäßig derzeit noch unverschlüsselt. Befindet man sich beispielsweise in einem Café mit WLAN, kann jeder andere Gast alles mitlesen.

## 2.2 AOL Instant Messenger

Der AOL Messenger (AIM) ist heutzutage faktisch nurnoch ein zweites ICQ, das nach und nach mit ICQ verschwimmt: Man kann mittlerweile von AIM aus ICQ-Kontakte kontaktieren. Der Unterschied liegt darin, dass bei ICQ die Nutzer über Nummern, bei AOL über Namen identifiziert werden. Ansonsten gilt für AIM das selbe wie für ICQ (siehe oben).

## 2.3 Windows Live aka MSN

Ein weiterer der größten Messenger ist der Windows Live Messenger von Microsoft (früher und auch heute noch besser bekannt als MSN). Hier treffen bedauerlicherweise ähnliche Kritikpunkte zu wie bei ICQ. Alle Chats laufen kurzen Tests zufolge durch zentrale Server und auch Microsoft erlaubt sich in seinen Nutzungsbedingungen, Inhalte zu speichern. Zusätzlich zensieren die WLM-Server Links, die sie für gefährlich halten, um die Anwender zu schützen, es ist aber bekanntgeworden, das auch absolut unschädliche Internetadressen auf der Zensurliste gelandet sind.

Ein eventueller Lichtblick: Laut Wikipedia<sup>2</sup> ist auch hier die Nutzung alternativer Software verboten, in den aktuellen Terms of Use<sup>3</sup> konnte ich dies allerdings nicht mehr entdecken. Dennoch findet sich eine schmale Liste der wenigen „authorisierte Software“<sup>4</sup>. In den Nutzungsbedingungen des .NET Messengers, der eng mit dem WLM verwachsen, wenn nicht sogar identisch ist, steht aber folgendes<sup>5</sup>:

---

<sup>2</sup>[http://de.wikipedia.org/w/index.php?title=Windows\\_Live\\_Messenger&oldid=75969597](http://de.wikipedia.org/w/index.php?title=Windows_Live_Messenger&oldid=75969597)

<sup>3</sup><http://explore.live.com/microsoft-service-agreement?mkt=de-DE> abgerufen 26.06.10

<sup>4</sup><http://messenger.msn.de/Help/Authorized.aspx> abgerufen 26.06.2010

<sup>5</sup><http://messenger.msn.de/Help/Terms.aspx?mkt=de-de> abgerufen 26.06.10

„Zur Anmeldung zum Dienst oder dessen Nutzung dürfen Sie nur Software von Microsoft oder autorisierte Software von Drittanbietern verwenden. Eine Liste mit autorisierter Software von Drittanbietern finden Sie unter <http://messenger.msn.de/Help/Authorized.aspx>.“

## 2.4 Yahoo-Messenger

Ein weiteres Netzwerk ist das des Yahoo! Messengers, kurz YIM. Seit neustem ist es möglich, Textnachrichten zwischen dem Windows Live Messenger und YIM auszutauschen, dennoch handelt es sich um ein eigenes Netzwerk. Auch hier ist die gleiche Kritik anzubringen, wie bei ICQ und Windows Live. Das Netzwerk ist zentralistisch aufgebaut und alternative Software zur Nutzung ist unerwünscht<sup>6</sup>:

„Auf die Messenger-Dienste darf ausschließlich durch die Messenger-Software zugegriffen werden.“

## 2.5 Skype

Noch recht vorbildlich unter den großen proprietären Messenger-Diensten ist Skype. Skypes Fokus liegt deutlich auf Telefonkonferenzen und Videotelefonaten, aber mittlerweile breitet sich Skype als beliebte Chatsoftware aus. Da über das verwendete Protokoll nichts bekannt ist, gibt es im Gegensatz zu ICQ und Co. (bis jetzt<sup>7</sup>) nichtmal alternative Software zur offiziellen. Diese läuft jedoch auf Windows, Mac OS X sowie Linux.

Skype nutzt eine starke Verschlüsselung, sodass Abhören für dritte nach aktuellen Kenntnisstand nicht möglich ist. Dennoch hält Skype auch die Verschlüsselungsmethode geheim, sodass nicht sicher ist, dass Skype wirklich abhörsicher ist und nicht auszuschließen ist, dass die Firma Skype die Möglichkeit hat, die Daten zu entschlüsseln. Der Leiter der Sicherheitsabteilung sagte 2007 in einem Interview<sup>8</sup>:

„Wir stellen eine sichere Kommunikationsmöglichkeit zur Verfügung. Ich werde Ihnen nicht sagen, ob wir dabei zuhören können oder nicht.“

2008 wurde bekannt, dass die österreichischen Behörden inkl. der Polizei Skype abhören können. In China steht nur eine modifizierte Variante von Skype zur Verfügung, von der bekannt ist, dass sie abgehört und zensiert wird.

Skype ist teilweise dezentral, d.h. nicht alle Chats und Gespräche laufen zwangsläufig über zentrale Server in den Rechenzentren von Skype, sondern oft direkt von Teilnehmer zu Teilnehmer. Bei Gesprächen konnte ich das in einem kurzen Test bestätigen, bei Chats konnte ich aufgrund der Verschlüsselung sämtlicher Kommunikation nicht genau feststellen, ob es der Fall ist.

---

<sup>6</sup><http://de.docs.yahoo.com/info/mtos.html> abgerufen 26.06.10

<sup>7</sup><http://www.heise.de/developer/meldung/Skype-Anwendungen-mit-kopflosem-Skype-entwickeln-1028427.html>

<sup>8</sup>Interview mit ZDNet: <http://tinyurl.com/skype-zdnet> abgerufen 27.06.10

## 2.6 schülerVZ Plauderkasten

Unter Schülern findet sich als Chatsoftware auch teilweise der integrierte Chat von schülerVZ namens „Plauderkasten“. Ich habe keine speziellen Regeln finden können, daher nehme ich an, dass die allgemeinen schülerVZ-AGB<sup>9</sup> gelten („Die AGB gelten für sämtliche Inhalte, Funktionen und sonstige Dienste [...], die wir derzeit und zukünftig im schülerVZ anbieten.“). In den AGB findet sich in den für uns interessanten Bereich jedoch kein Satz, der auf den Plauderkasten anwendbar ist. Ebenso scheint sich die Datenschutz-Erklärung<sup>10</sup> nur auf Profile zu beziehen.

Es handelt sich beim Plauderkasten technisch um eine Web-Applikation, die dadurch für alle Betriebssysteme verfügbar ist. Dennoch gibt es keine API oder Protokolleinsicht und damit keine Möglichkeit, alternative Software zu entwickeln.

## 2.7 Facebook Chat

Auch das weit verbreitete Social Network Facebook bietet eine Chat-Möglichkeit. Auch hierbei handelt es sich um eine Web-Applikation, die mit JavaScript im Browser läuft. Technisch handelt es sich sogar um ein Jabber-Netzwerk, das allerdings keine Kommunikation außerhalb von Facebook zulässt. Es ist dadurch auch zentral und alle Daten laufen durch Facebook-Server aber alternative Software ist möglich – jedes Programm, das Jabber/XMPP unterstützt, kann benutzt werden, Facebook gibt sogar Hilfestellung dazu<sup>11</sup>. Desweiteren wird offen zugegeben, dass Verschlüsselung (außer von Passwörtern) nicht vorhanden ist<sup>12</sup>. Es kann aber jede Verschlüsselungssoftware eingesetzt werden, die mit Jabber kompatibel ist (siehe Abschnitt 3.4).

Facebook ist also rein technisch auch in der Lage, Chats mitzulesen. Die AGB wie die Datenschutzerklärung<sup>13</sup> äußern sich nicht weiter zum Chat.

# 3 Jabber, weil...

## 3.1 frei

Jabber/XMPP ist ein freies Netzwerk(protokoll). Jeder kann es kostenlos verwenden, nachmachen oder sonstwie vertreiben. Es gehört niemanden!

## 3.2 offen

XMPP ist ein offenes Protokoll. Jeder Programmierer kann leicht, bequem und legal Software entwickeln, mit der man im Jabber-Netzwerk chatten kann.

---

<sup>9</sup>[http://www.schuelervz.net/1/terms\\_new](http://www.schuelervz.net/1/terms_new) abgerufen 27.06.10

<sup>10</sup>[http://www.schuelervz.net/1/policy\\_new/declaration/](http://www.schuelervz.net/1/policy_new/declaration/) abgerufen 27.06.10

<sup>11</sup><http://www.facebook.com/help/?faq=16739> abgerufen 27.06.10

<sup>12</sup><http://www.facebook.com/help/?faq=16741> abgerufen 27.06.10

<sup>13</sup><http://www.facebook.com/policy.php> abgerufen 27.06.10

### 3.3 dezentral

Jabber ist ein dezentrales Netzwerk. Wenn du keine Ahnung hast, was das ist, kannst du dir es wie E-Mail vorstellen. Nehmen wir an, du hast einen E-Mail-Account bei Google Mail und dein Freund einen bei Yahoo! Mail. Wenn du ihm jetzt eine E-Mail schicken willst, gibst du die E-Mail an die Server von Google Mail, die sie an die Server von Yahoo! Mail weiterleiten, wo dein Freund sie abrufen kann. Das ist dezentral: Ein dritter Anbieter wie web.de bekommt nichts davon mit. Wenn Yahoo! Mail ausfällt, kannst du immernoch an deine Freunde bei web.de schreiben. Jeder kann also für sich entscheiden, welchem Anbieter er vertraut und sich bei diesem anmelden – dennoch kann jeder, der irgendwo eine E-Mail-Adresse hat, mit jedem anderen, der eine hat, kommunizieren. Dezentrale Systeme sind die diskretesten und ausfallsichersten, weil es eben keine zentrale Stelle gibt, von der alle abhängig sind. Und da es diese nicht gibt, kann dort auch niemand *alle* Nachrichten mitlesen.

Jabber funktioniert genauso: Jeder hat seinen Account bei einem Server, dem er vertraut. Die Jabber-Adressen sehen auch aus wie E-Mail-Adressen, meine ist beispielsweise rami@jabber.ccc.de – mein Jabber-Anbieter ist also jabber.ccc.de (Server des Chaos Computer Clubs).

### 3.4 verschlüsselbar

Jabber an sich ist nicht verschlüsselt. Die meisten Server bieten SSL an, sodass die Kommunikation zwischen mir und meinem Anbieter verschlüsselt stattfindet. Das ist zwar sicher gegen Leute im gleichen Internetcafé, aber dennoch kann mein Anbieter noch mitlesen. Daher gibt es Verfahren, die die Kommunikation auf meinem PC verschlüsseln und erst auf dem PC des Empfängers wieder entschlüsseln. Diese Verfahren müssen von der Software beider Kommunikationspartner unterstützt werden.

Das verbreitetste ist Off-the-Record Messaging<sup>14</sup> (OTR), welches während der Kommunikation ein Abhören oder Fälschen der Nachrichten absolut unmöglich macht, aber dennoch keine Möglichkeit bietet, nach Abschluss der Kommunikation die Echtheit der Nachrichten nachzuweisen. Das bedeutet, dass man sich bei einer OTR-verschlüsselten Kommunikation sicher sein kann, dass man wirklich sicher mit dem anderen chattet, der andere aber anhand der Aufzeichnungen nicht mehr (z.B. vor Gericht) beweisen kann, dass man es wirklich selbst geschrieben hat. Theoretisch kann man dieses Verfahren auch für andere Protokolle wie ICQ oder Windows Live nutzen, aber es wird von der offiziellen Software für diese Protokolle nicht unterstützt – im Jabber-Umfeld dagegen gibt es für die meiste Software entweder eine Unterstützung von Haus aus für OTR oder es gibt ein entsprechendes Plugin.

Auch findet sich gelegentlich der Einsatz von GnuPG bei Jabber, eines bewährten Verfahren zur Verschlüsselung von E-Mails. Es ist aber derzeit weit weniger verbreitet als OTR und deshalb wird darauf hier nicht näher darauf eingegangen.

---

<sup>14</sup>[http://de.wikipedia.org/wiki/Off-the-Record\\_Messaging](http://de.wikipedia.org/wiki/Off-the-Record_Messaging)

## 4 Ja(bber), ich will!

### 4.1 Server

Wie bei E-Mail braucht man bei Jabber einen Anbieter, bei dem man seine Adresse bekommt. Der größte davon ist wahrscheinlich *jabber.org* (<http://www.jabber.org/>), betrieben von der gemeinnützigen Stiftung *XMPP Standards Foundation*, die auch das Protokoll weiterentwickelt. Die Foundation bietet auch eine Liste der bekannten Jabber-Server unter <http://xmpp.org/services/>

#### 4.1.1 Google Talk

Auch Google ist ein Jabber-Anbieter: Die Chatsoftware „Google Talk“ von Google ist nichts anderes als ein Jabber-Client. Jeder Google Mail-Nutzer hat damit auch einen Jabber-Account bei Google. Google Talk unterstützt desweiteren das Protokoll „Jingle“, welches auch Telefonate ermöglicht. Dies wird nach und nach auch von anderer Jabber-Software eingebaut.

### 4.2 Client

Zum Chatten letztlich benötigt man noch eine Software, mit der man Jabber nutzen kann. Da gibt es unzählige Möglichkeiten für alle Betriebssysteme: Pidgin, Psi, Jabbim, Google Talk, Miranda, Adium, Digsby, Empathy, Kopete und viele weitere. Zu all diesen finden sich im Netz zahlreiche Installationsanleitungen.

---

Dieses Dokument ist veröffentlicht unter den Bedingungen der Creative Commons Lizenz by-nc-sa 3.0: <http://creativecommons.org/licenses/by-nc-sa/3.0/de/>

Alle Urheberrechte liegen bei Raphael Michel

<http://www.raphaelmichel.de>