

# Jabber vs. Silc

24.10.2005

Auf den ersten Blick sind Silc und Jabber zwei sehr ähnliche Systeme, im Großen und Ganzen haben sie auch einen ähnlichen Funktionsumfang. Im Detail unterscheiden sich beide Systeme aber in einigen wichtigen Punkten.

## Jabber

Jabber ist vorrangig ein Instant Messaging System ähnlich ICQ oder dem AOL Instant Messenger (AIM). Anders als AIM, ICQ oder auch MSN ist Jabber ein freies System, welches man nicht nur kostenlos nutzen, sondern auch einen eigenen Server oder ein ganzes Servernetz betreiben kann. Ähnlich wie Email können sich User Nachrichten austauschen und das über die Grenzen des eigenen Servers hinweg. Dafür gibt es die sogenannte Jabber-ID, eine eindeutige Adresse, mit der man die jeweilige Person eindeutig adressieren kann. Eine Jabber-ID besteht aus dem Usernamen und der Serveradresse. Zum Beispiel ist meine Jabber-ID alex@jabber.systemli.org. Auf dem ersten Blick sieht sie aus wie eine Email-Adresse und vom Prinzip her funktioniert sie auch so. An Hand der Serveradresse wird festgestellt, an welchen Server die Nachricht zugestellt wird und mit dem Username wird der User identifiziert.

Wird eine Nachricht an mich geschickt, stellt der Server zuerst fest, an welchen Server (jabber.systemli.org) die Nachricht geht. Wird die Nachricht über den gleichen Server abgesetzt, dann weiss der Server, wo er mich findet und stellt die Nachricht an mich zu. Wird die von einem anderen Server verschickt, setzt sich dieser Server mit jabber.systemli.org in Verbindung und fragt, ob er die Nachricht zustellen kann. Sowohl die Verbindung zwischen Client und Server als auch zwischen den Servern kann verschlüsselt werden, um ein Abhören der Nachrichten zu verhindern. Neben dem offenem System ist das der Hauptvorteil von Jabber.

Ein anderer wichtiger Teil von Jabber besteht in der Online-Anzeige, das System zeigt an, welcher meiner Freunde gerade online ist und mit dem kann ich dann einen Chat starten. Die Online-Anzeige funktioniert aber nur bei Leuten, denen ich es erlaube, dass sie meinen Online-Zustand sehen dürfen. Wem man Zugriff gewährt, ist jedem seine eigene Sache, der Datenschutz ist also gewahrt. Die Nachrichten, die zwischen zwei Personen ausgetauscht werden, erscheinen umgehend beim Partner, offline versandte Nachrichten werden auf dem Server gespeichert und zugestellt, sobald man sich mit dem Server verbindet. Chats mit mehreren Personen sind ebenfalls möglich, die Chaträume können mit Passwort versehen und so der Zugang geregelt werden.

## Silc

Obwohl Silc alle oben genannten Funktionen beherrscht, liegen seine Stärken eindeutig im Gruppenchat. Die Möglichkeiten zum Instant Messaging, also dem Nachrichtenverschicken zwischen zwei Personen und die Onlineanzeige sind eher rudimentär entwickelt, bzw. nicht so praktikabel wie bei Jabber. Silc ist eher ein Ersatz für IRC (Internet Relay Chat) und genau dort liegen auch seine Stärken. Während IRC aus der Anfangszeit des Internets stammt und viele Unzulänglichkeiten hat, ist Silc dem deutlich überlegen, vor allem in den Punkten Abhörsicherheit und Useridentifikation.

Silc beherrscht nicht nur eine verschlüsselte Verbindung, sie ist sogar zwingend. Anders als bei Jabber, wo sich User durchaus unverschlüsselt anmelden können, geht bei Silc nichts ohne. Die Verschlüsselung ist von einem User zum anderen, also selbst die Betreiber des Silc-Servers können nicht sehen, was über ihren Server geht. Chatrooms können zusätzlich abgesichert werden, User eingeladen oder ausgeschlossen werden, ohne dass diese Chatrooms vom Admin eingerichtet werden müssten. Jeder User kann einfach einen eigenen Raum einrichten, in dem er dann Op(erator) ist und andere User zu Ops hochstufen, herauskicken oder die Einstellungen für den Raum einstellen kann.

Der wichtigste Unterschied zu Jabber besteht darin, dass User sich nicht durch Username und Passwort authentifizieren, sondern mittels Key. Diese Keys funktionieren ähnlich wie PGP, wo es einen öffentlichen Key zum Verschlüsseln und einen privaten zum Signieren und Entschlüsseln. Beim Verbindungsaufbau tauschen Client und Server als erstes ihre Keys und bauen dann die Verschlüsselung auf. An Hand der ausgetauschten Keys können die User feststellen, dass der Server nicht manipuliert wurde und der Server kann User eindeutig unterscheiden, selbst wenn sie sich den gleichen Nickname gegeben haben. Streift man die Nicks wie im IRC sind im Silc unnötig. Haben zwei User den gleichen Nick, hängt der Server einfach ihren Rechnernamen zur Unterscheidung an die Usernamen heran.

Durch dieses System ist es unmöglich, dass sich jemand als jemand ausgibt, der er oder sie nicht ist oder dass ein manipulierter Server untergeschoben wird, der das Abhören der Nachrichten ermöglicht. Die gesamte Kommunikationsstruktur ist in sich geschlossen und vor allem abgesichert. Bei Jabber besteht zwar die Verschlüsselung, aber die User authentifizieren sich nur mit ihrem Usernamen und Passwort, wenn das erraten wurde oder sonst irgendwie entschlüpft ist, kann die ganze Kommunikation kompromittiert werden und keiner würde es merken. Einige Jabber-Clients bieten eine extra Verschlüsselung, um dieses Problem zu umgehen.

## Was ist das bessere System?

Keines von beiden, beide haben Vor- und Nachteile. Jabber ist eindeutig im Vorteil, wenn es um die Handhabung und Instant Messaging geht, Silc ist besser beim Gruppenchat und hat das ausgefeiltere Sicherheitssystem. Was die Software angeht, da ist Jabber ebenfalls besser aufgestellt, es gibt für so gut wie jedes Betriebssystem Clients, oftmals kann man zwischen mehreren auswählen. Silc-Clients sind nicht so zahlreich, am ehesten hat man noch unter Linux oder BSD eine gewisse Auswahl.

Clients:

Gaim - Windows, Linux, BSD

Colloquy - MacOS

Silky - Windows, Linux

Es gibt weitere Clients, die aber entweder nicht besonders userfreundlich oder nicht mehr weiterentwickelt werden. Eventuell sollte man sich silc einmal ansehen, wenn man die Shell nicht scheut.

Alexander Heidenreich

Zu Fragen, Anregungen und Kritik könnt ihr mich unter dieser Email-Adresse erreichen: [alex@blacksec.org](mailto:alex@blacksec.org)

Dieses Dokument darf frei weiterverbreitet werden, so lange ein Link oder sonstiger Verweis auf die Originalquelle enthalten ist.