Introduction to Jabber XMPP

Jabber is the name of a chat system that works like ICQ, Skype, or Facebook Messenger, for example. However, Jabber has advantages over these other programs because the Jabber protocol (XMPP), as well as most of the available clients and servers are open-source software. That means Jabber does not require communication through one, single service provider (like ICQ or Skype) but users are free to choose from several competing services.

The Jabber client software displays a list of users that are available as communication partners and once a user has been added to a list (and confirmed visibility of online-status to others) then it is possible to see if this user is currently online and available for a chat. Jabber offers similar features as other messengers and can do more than just send and receive text messages. For instance, with Jabber it is also possible to exchange files between users.

The different service providers are interconnected and messages sent by users are transmitted to all servers on the Jabber network in real-time. As a result, users that are registered at one particular Jabber service provider can also communicate with those who have chosen a different one.

Our secure Jabber service at mailbox.org

We at mailbox.org operate our own Jabber server, fitted with SSL/TLS for transport security and state-of-the art feature sets.

All users of mailbox.org can instantly use this Jabber service if they want, simply by stating their user name (username@mailbox.org) as Jabber-ID for authentication. Our Jabber server will automatically accept all valid mailbox.org accounts as users.

Using our Jabber service with your own domain name is possible but does require the correct setting of certain DNS entries. Please have a look at your FAQ "Using Jabber service with your own domain".

Which Jabber client is best?

There is a wide range of Jabber clients available to choose from – which one to pick is mostly down to personal preference. The XMPP standards foundation maintains a comprehensive list which can be found here.

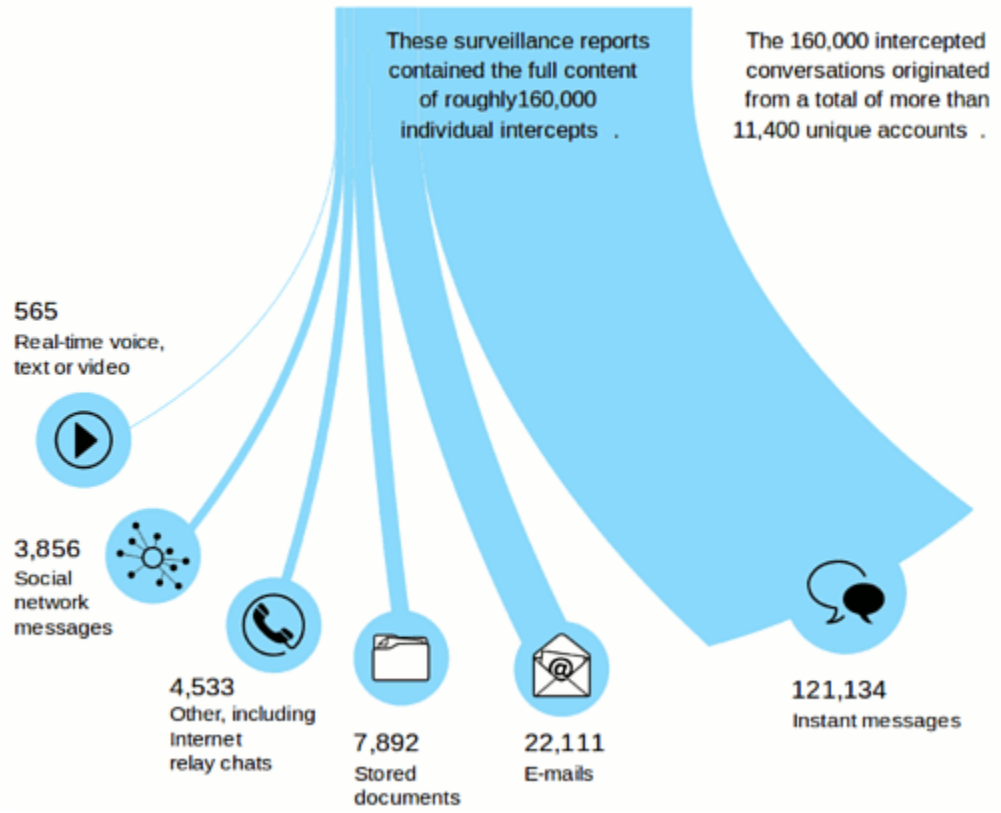
See below for a table we put together to compare the security features of some of the most popular clients:

Jabber Client	OTR Encryption	OpenPGP Encryption	OMEMO	SSL /TLS Config	Enforce DNSSEC
Jitsi (Java)	yes	-	-	-	yes
Conversations (Android)	yes	yes	yes	-	-
ChatSecure (iOS)	yes	-	yes	-	-
Miranda (Windows)	Plugin available	Plugin available	-	-	-
Psi/Psi+	-	yes	-	-	-
Mozilla Thunderbird	-	-	-	yes	-
Adium (MacOS X)	yes	-	-	-	-
TorMessenger	yes	-	-	yes	-

Jabber is not yet integrated into the mailbox.org cloud office interface, but we are working on it!

End-to-end encryption (OTR, OpenPGP)

An analysis of 160.000 surveillance protocols that are part of the NSA documents revealed by Edward Snowden has shown that spying on instant messaging communication is on of the top priorities of today's intelligence services.



End-to-end encryption protects your communication from access by unauthorised third parties. This also includes the provider, which means if you enable encryption, we at mailbox.org can not inspect or read your communication either. When using Jabber/XMPP, there are two encryption mechanisms at your disposal:

- **OTR:** Off-the-Record encryption is available in most clients. Once enabled at both end nodes, the communication will be encrypted automatically. When OTR is active, then the required cryptographic keys will be exchanged in the background whilst the clients are running. In order to ensure the authenticity of encryption keys and prevent any man-in-the-middle attacks, it is necessary to verify the keys using additional information. This is usually done via a third, independent channel. For instance, communication partners may want to exchange a shared password, or a question with a fitting answer, or the actual fingerprint codes of their keys.
- **OpenPGP:** The long-established Pretty Good Privacy (PGP), known for facilitating secure e-mail communication, can also be used for end-to-end encryption in instant messaging with Jabber/XMPP. Communication partners need to exchange their public keys prior to joining a messaging session. The authenticity of the keys is established through OpenPGP and does not need to be verified separately for the use of Jabber/XMPP.
- **OMEMO:** This is a new encryption method for Jabber/XMPP, based on the Axolotl mechanism that is also used by Whisper Systems. Similar to OTR, it offers automatic key exchange as well as forward secrecy. However, unlike OTR it also allows encrypted group chats, encrypted offline messages, and encrypted file transfers. Please note that presently, the only Jabber clients to support OMEMO are *Conversations* for Android and *Gajim.*

Using anonymisation services

The ultimate security for anyone using Jabber/XMPP would be to combine end-to-end encryption with an anonymisation service like Tor Onion Router oder JonDonym. The encryption would protect the content of the communication, whilst anonymisation keeps the meta data, such as the actual communication end points themselves, secure and hidden from spying eyes.

However, most Jabber clients do not support Tor or JonDonym and hence, cannot offer this high level of technical security.

Related Articles

- Introduction to Jabber XMPP
- How to configure Tor Messenger
- Using Jabber service with your own domain
- Setup the Jabber client Adium on OS X
- Features of our Jabber server