A revised Jabber proposal   SMT/nnn

Bob Dowling, Tony Finch
2nd December 2005

This paper follows up the discussion on SMT/190, the original Jabber proposal, and seeks to address the concerns raised at the SMT on the 22nd of November. Definitions and concepts can be found in that paper and are not repeated here.

Why the University should offer an Instant Messaging service

Instant Messaging is a very common form of communication between students. As such it is an obvious choice to layer certain forms of University activity over. Experience in other locations indicate that IM is used for:

- Quickly sorting out timetabling of supervisions or meetings.
- Asking questions of supervisors or course givers.
- Subject-related discussion for a group of students.
- As the messaging component of VLEs in conjunction with other modern communication tools such as wikis, bulletin boards and blogs.
- Using the presence feature to locate people to save wasted trips.
- Collaboration between researchers both inside and outside the University.
- Side-band for phone calls to spell out items such as URLs.

We can offer a significant "value add" by running the IM server ourselves, especially for communication related to internal University matters.

- We can tie online identities to individuals very tightly using CRS IDs and one or more established password systems. Recognised identities, common across multiple systems create reputations that cause people to behave more appropriately.
- We can provide links between the IM system and other University systems such as lookup and Hermes.
- We can keep logs that will help in the case of complaints or abuse or harassment.

Why Jabber?

The currently popular IM services are all closed and centrally controlled. The University cannot run a system based on AOL or MSN and have any control over identities. If an "rjd4" or "fanf2 appear on MSN you cannot know who they are. If they turn up in the University system you can.

The Jabber specifications and development process are open. There is a wide variety of client software available. Anyone may deploy a Jabber server which may or may not federate with the public Jabber network.

Jabber is particularly popular with internal corporate chat servers because there is no need to involve outside parties. The highest profile publkic Jabber deployment is Google Talk which is promised to federate with public Jabber servers. Jabber has plenty of momentum.

The various other IM worlds are mostly "closed world" systems (albeit with some gateways tacked on as an afterthought). AOL and MSN IM systems are akin to the original AOL system that was swept aside by domestic access to the Internet. The parochial AOL and MSN IM systems face the same fate.

Implementation proposal

Jabber security is based on TLS and SASL, as used for email protocols.

Dedicated Jabber clients authenticate via SASL to the Jabber server. For this they need to quote a password the Jabber server can directly test. This paper proposes that the Hermes password be used for this and that the Jabber server receive copies of the Hermes passwords in the same way as the Hermes systems do.

A Jabber web client could be run from a dedicated web server which applied Raven authentication. Jabber traffic would flow through it to the Jabber servers authenticated by SASL external authentication. This would provide web access to Jabber clients and access to people without Hermes accounts or who choose not to use their Hermes accounts.

We propose that our users' JIDs would be <CRSID@chat.cam.ac.uk> and that MUC identities be <GROUPNAME@group.chat.cam.ac.uk/CRSID>.

Jabber servers are identified using SRV records in the DNS. Cambridge runs a very conservative DNS zone and these would be the first SRV records added to the Cambridge zone. The SRV records act analogously to MX records for email; the client looks up the Jabber SRV record for "chat.cam.ac.uk" and is directed to a server "chat.csx.cam.ac.uk", say. Ultimately there would be a handful of SRV records for the various aspects of the service we might choose to run.

We propose the following release milestones:

- Single server, basic one-to-one chat.
- Multi-user chat
- Additional server to provide web client.
- Gateways to MSN, (AOL & Yahoo possibly too).
- Finish documentation and publicity.
- Announce full service.

Expected use

The SRCF IRC service has more than 200 simultaneous users at times. We don't have any other statistics from them, nor of current MSN etc. use within the University. Predictions are, therefore, hard.

We propose that we measure number of distinct users per week as our primary usage statistic. Given that IM is a tool of the young we would expect to see the vast majority of our user base in the undergraduate population and not in high-profile projects run by senior ("old") members of the University at least at first. However, measures of its use to collaborate with other academic institutions might provide useful data.