

Report on Internet2 Fall Member Meeting

19-22 September, 2005
Philadelphia PA, USA

Background

Internet2 is a United States based organisation devoted to advanced networking. It has approximately 200 US universities and 66 other organisations as members. It runs the Abilene network backbone in the US; supports the development of applications software in support of teaching, learning and research; and develops middleware to support functionality common across applications.

NGI-NZ is an international affiliate of Internet2. VUW is a member of NGI-NZ.

General Observations

There were about 700 attendees, 90% from the US. The audience was a mixture of university CIOs, academics, technical staff, industry and government representatives. There was a much higher percentage of women than I would expect to see at a similar conference in Australasia.

The four days were a mixture of highly interactive workshops and more typical conference presentations, though the level of interaction was always high. There were only two keynote sessions. At all other times there were typically six or seven parallel sessions to choose from. I attended a number of sessions dealing with aspects of identity management as this will be a key middleware component of the NZAREN. I also tried to select a number of sessions that dealt with "successful" use of advanced network technology in universities to improve my understanding of what worked and what didn't and what level of resourcing was required.

As a final observation, this conference expected (dare I say required) attendees to have a laptop or web and email capable PDA. Notices were distributed by email, session evaluations were done in real time and the audience was invited to view on-line demonstrations of the topic of a presentation. I would estimate 40-50% of the laptops in use were Apple Macintosh.

Identity Management

Identity management is primarily concerned with reliably and securely managing identities of individuals over federations of organisations. In the simplest case federations are fixed, e.g. the New Zealand universities. In a more complex situation federations equate to virtual organisations which may be relatively dynamic, forming to address a problem over a period of weeks and then terminating. There are currently a range of technologies that are deemed to be adequately well defined and stable that they are being deployed:

Shibboleth - A system that can be used to authorise actions by an individual who is not a member of the local organisation based on authentication and supporting information provided by the individual's home organisation and local policy. For example, Canterbury University could authenticate an individual as being both a member of their staff and of the MacDiarmid Institute at Canterbury. Based on this the individual would be granted access to MacDiarmid Institute resources at VUW.

Certificate and Registration Authorities - Certificates are required to support Shibboleth and other technologies such as Access Grids and Globus computational grids. A number of interesting points were raised with respect to operating Certificate Authorities (CAs).

- CAs hold individual's and organisation's private keys. Providing a hardened CA to protect those keys is non-trivial. (This is perhaps something that ANCO could run on behalf of the NZAREN members.)
- User applications such as browsers and email clients must recognise certificate authorities to achieve transparent use. The University of Wisconsin-Madison stated that this was a key reason that they chose to use a commercial CA provider. Other institutions argued this was not a significant issue.
- There are several initiatives established to offer low cost identity management including a CA: EDUCAUSE's HEBCA (See <http://www.educause.edu/imsp/>.) and Internet2's USHER. Dartmouth College is building a bridge between these two.

Depending on the outcome of the current PKI Pilot programme with Australia's CAUDIT, NZ could look at Internet2's USHER-lite model for an implementation framework.

Discussions at several sessions indicated that the problems in this area are more organisational than technical. There is a real need for organisations to develop policies to support their participation in federations, but there is often a disconnect between the management that would be responsible for the development of such policies and the researcher(s) that need(s) the technology to participate in a project.

There were several examples of the successful use of identity management technology.

- The most compelling was done by George Washington University on behalf of the Red Cross. It was able to set up a virtual organisation encompassing all workers involved in the aftermath of hurricane Katrina "virtually overnight". This involved placing Shib-lite on all laptops used by Red Cross workers. It enabled the Red Cross to managed authorised access to various databases even though individual workers were authenticated by different agencies.
- The Netherlands has created a federation of its public libraries. Authentication is done by a local library which then authorises borrowing from other libraries.
- The US Government is adopting Shibboleth as part of its core infrastructure. The National Science Foundation is currently conducting a trial with a number of universities to use local authentication for grant submissions to NSF.
- The University of Alaska uses the National Middleware Initiative (NMI) software to manage identities over four campuses (including access to Banner), to synchronise directories and to allow user maintenance of directory information. They accomplished a good deal for 0.5 fte.
- 11 campuses of the Great Plains network have cooperated in a Shibboleth implementation to do inter-institutional authorisation. The project started out as feasibility study and ended up as a pilot. (The full network covers 23 campuses in seven states.) Required up to 3 fte across all campuses. The challenges faced included: policy issues for multiple institutions; entitlements for coarse and fine grained authorisations; strategies for authorising and managing entitlements¹; moving from testbed to production.

¹ There are tools under development to address this issue, but they have not yet achieved the acceptance of the NMI tool suite.

Related to identity management is the question of directories. The number of directories is expanding and maintaining consistency is becoming a significant problem. Commercial solutions have been found to be inadequate and/or too expensive.

The University of Memphis has developed Nexus to manage directories such as Luminous, Active Directory, etc. They have worried a lot about “recovery” and the evolution of business rules. They are open to collaboration with other institutions.

Collaboration

This was a major thread of the week. All of the demonstrations focussed on access grid (AG) like collaboration. Funding for the AG itself has stopped but there are now several commercial offerings, including a free open-source version from Microsoft. An offering from inSORS also seems to be popular. Several sessions at the conference were team presentations with one member local and others coming in from all over the world. In general, these worked very well. There were also discussions of upcoming events many of which involve countries from Africa and the Asian subcontinent. New Zealand was conspicuous by its absence from this discussion.

A number of collaboration tools were presented and demonstrated during the week. A group from Sweden used a café metaphor for finding, meeting and interacting with people. A system named myVOCS gave a reasonable demonstration of how users could create a virtual organisation through a simple web interface and how a user’s participation in a virtual organisation could be supported through a shared diary, document management, etc.

Conclusion

Internet2 has a very wide variety of programmes. The conference itself presented more opportunities than one person could absorb. The New Zealand universities have a lot to learn from attendance at these conferences.

I should mention that this conference also provided an opportunity for me to renew a number of acquaintances from my earlier work with the Internet Society. These included David Lassner (CIO, University of Hawaii), Shigeki Goto (Waseda University), and Ken Klingenstein (University of Colorado and Director of the Internet2 Middleware Initiative).

John H. Hine
Professor Computer Science
Head, School of Mathematics, Statistics and Computer Science
Victoria University of Wellington