

John Hine
School of Engineering and Computer Science
Victoria University of Wellington
31 May 2009

INTERNET2 SPRING MEMBER MEETING

Arlington Virginia, USA
27-29 April 2009

I attended the Spring Member Meeting of Internet2 in Arlington Virginia from Monday 27 April through Wednesday 29 April. These meetings are held twice a year and I have attended a meeting every twelve or eighteen months in recent years. Attendance at this meeting was supported by the KAREN Capability Development Fund and Victoria University.

Internet2 (<http://www.internet2.edu>) is a consortium of 300+ universities and research organisations in the United States. It has a focus on new research and education applications enabled by advanced research and education networks. As well as applications there is a strong emphasis on middleware as the common set of services required to effectively support advanced applications.

Approximately 640 individuals representing 280 organisations attended this meeting. There were many concurrent activities and I had to choose selectively to identify sessions of potential benefit to New Zealand. The complete programme with a number of the presentations can be found at <http://events.internet2.edu/2009/spring-mm/>.

Internet2 Research Advisory Council

I attended the public part of the Research Advisory Council's meeting. The Research Advisory Council is responsible for advising Internet2 on matters relating to support for research, both network-focused research and disciplinary research that makes use of the network as a tool.

The problem of co-ordinating distributed support for projects was discussed. Like the network itself many distributed applications obey Metcalfe's Law - their value increases significantly when "everyone" becomes a user. In their early stages such distributed applications may have little or only indirect value for an organisation and hence it is difficult to garner support for the development of the application. As in New Zealand, the United States struggles to obtain funding structures to support distributed applications and middleware.

Ken Klingenstein, University of Colorado, gave an excellent example. It turns out that the advantages of a single sign on using technology such as Shibboleth is multiplied when the user needs to use one time passwords. Rather than managing multiple sets of one time passwords for multiple applications the user needs only a single one time password for his or her identity provider (IdP).

For the first time during the meeting we heard of a growing collaboration between the Internet Society and Internet2. The Internet Society oversees the Internet Engineering Task Force (IETF), the group that "Makes the net work." The Internet Society is interested in adapting some of Internet2's identity and trust management to the lower level protocols of the Internet. The IETF feels this technology may help solve problems caused by firewalls for real-time applications such as video.

Guy Almes, Texas A&M, indicated that many university CIO's are more interested in making a single sign on work with the likes of iTunes. Research is often given a lower priority.

Identity Management

Identity and access management were a recurring theme at this meeting, whether it was sessions about developing the technology or new applications that made use of established identity federations. It is clear that identity management is now an established technology and most organisations are focused on leveraging it for their benefit.

With respect to the technical side of Shibboleth there was a clear message that IdP 1.3 - the software used for identity providers - is dead and everyone should now be using IdP 2.1. Microsoft Geneva will be fully Shibboleth compliant.

EduRoam is a different technology that allows users to authenticate to a local domain using their home site credentials. It has been adopted by GEANT for use throughout Europe. They have adapted EduRoam to make use of nationally based federations, as opposed to institutional identity providers, to perform the authentication.

There are now about 1000 shibboleth deployments worldwide and 25 national federations, as well as additional state and sector federations.

The Internet2 community is moving to build applications that make use of Shibboleth and identity federations. The Suisse presented both a ftp and webdav service (<http://www.cyberduck.ch>) that is Shibboleth aware and a one time password service that integrated with their identity provider. Two collaborative environments based on federations are described below.

The InCommon Federation supports a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States. Ken Klingenstein reported that InCommon membership has grown to 150 organisations and nearly three million users. There is heavy engagement with the US government, particularly the National Institute of Health (NIH). All of Google's applications are Shibboleth compliant and can interface with InCommon. The driver here is the provision of student services. The silver profile has now been approved and is expected to become the standard. This profile requires credentials with very hard to guess passwords and better credential management, reasonably verified personal information about each Subject, unique Subject identifiers that are never reassigned, and secure business and operational processes.

There was some discussion of the evolving structure of identity management federations. The rather tidy hierarchy that had been expected is not what is developing. Instead federations are all of overlapping, hierarchial and independent. For example, "anyone" can join the UK federation and several US universities have taken advantage of this.

New issues are also being identified. There is a fundamental issue of who can say what in a world with millions of asserting parties. As an example consider a promotional code, e.g. as a loyal customer you are issued with a discount voucher. How is the voucher limited to your use only? There are still many legal issues influencing policy and interoperability. Some federations are being very careful, others are putting the responsibility on the users. How will cloud computing and IAM interact? Will students develop a relationship with their university or with Google? If someone is running a blog and claiming expertise as a member of a university's staff how will the public be able to verify that claim.

A speaker from SWITCH, the Suisse national network, gave some good insights into the effort required to establish and support a federation. SWITCH worked closely with individual institutions, produced tailored documentation, tutorials and a test environment. SWITCH finds that 2 FTE are

required to keep their federation going (39 IdPs, 325 SPs and 17 partners). A further 2.5 FTE are employed on new developments. It is probably also important to note that SWITCH was initially created to develop and support the Suisse R&E network. In contrast, REANNZ is fully consumed trying to build their customer base to make KAREN sustainable.

Ian Young from the University of Edinburgh and the UK Federation had a number of useful observations on the development of identity federations. The UK had a “toy” federation for two years before they deployed the current production federation in 2006. Ian observed that where you have a small number of organisations they are likely to have similar goals, but as the number of organisations grow their objectives become more diverse. It is better to minimise regulation of federations and encourage smaller, self-regulating communities within the federation. The UK federation has only three policies:

- All members of the federation must observe best practice in the handling and use of your digital certificates and private keys.
- All identity providers must make reasonable attempts to ensure that only members of your institution are provided with credentials permitting authentication to your handle server, and that the assertions made to service providers by your attribute authority are correct.
- All service providers must agree not to aggregate, or disclose to other parties, attributes supplied by identity providers.

There was a discussion about the scaling of federations. This included both their size in terms of the number of entities, whether they should span multiple legal entities, etc. EduGAIN, the GEANT federation, addresses the problem of multiple European legal systems by allowing anyone to publish any meta data. Their approach was described as “supporting interaction between consenting adults”. Bluntly, the burden is on the user.

Campus Infrastructure

A number of issues around the development of campus infrastructures were discussed. A general problem, even in “cyberinfrastructure developed” countries, is that researchers will use what is at hand rather than participate in new services and hence contribute to their design.

As an example of the type of support that researchers often require the problems of “network bypass” were discussed. Network bypass refers to bypassing one or more components of the campus network, most often the firewall, but potentially other components. In the extreme, researchers may wish they had a direct connection between two labs.

Everyone seems to be suffering from the problem of increasing complexity of the campus infrastructure, applications and requirements all leading to increasing costs. A discussion attempted to differentiate between internal and external complexity. External complexity arises from the need to participate in middleware levels imposed by R&E networks, e.g. BeSTGRID in the New Zealand context. The importance of individual organisations participating in decisions at the level of the R&E networks was stressed. Engagement was key to ensuring there was a smooth dovetail between the organisational business requirements and services provided by the R&E network.

The Great Plains Network, <http://www.greatplains.net/>, is experimenting with sharing computing, storage and expertise. The New Zealand community should look at this and start considering such services.

A number of organisations have held successful cyberinfrastructure days involving the entire campus. It seems the correct time to hold these is after several early adopters can be identified so that researchers are talking to researchers. This was the model tried at Victoria's e-Research Symposium.

Regional Optical Networks

There was some discussion around the appropriate structures and frameworks for evolving regional optical research and education networks. The Quilt has surveyed the business plans of a number of regional optical networks with the goal of enriching their own business plan. The Quilt is prepared to share their survey information with other networks including internationally. See http://www.thequilt.net/business_case_project.html.

Collaboration

Several collaborative environments were described that have been or are being built on top of federated identity management. Heather Flanagan of Stanford University described *Confluence*, a collaborative work space between universities for sharing information. Interestingly the demand for *Confluence* came from administrators as well as researchers. *Confluence* supports applications such as *Drupal*, an open source content management system. *Confluence* can be co-managed from any of the participating sites.

Frank Pinxt of SurfNet described problems with their current "group" system. It is based on Sharepoint and Adobe Connect and has 60,000 registered users. They have found that Sharepoint severely limits their ability to be innovative and to introduce new services requested by their users. He described a new system, *CICF*, able to support innovation and offer guarantees such as the storage of data within the Netherlands. They are using *Groupier* as the basis for their new system as it offers the most flexible group management.

Discussion of the new collaborative environments raised several questions that have arisen with some experience of such systems. One is the selective release of information to different services. For example one individual may have several roles and wish that different contact information be provided by the environment to the different services associated with each role. Having worked for a number of years to achieve a single login across several services the question of what is meant by "logout" is now being discussed.

Healthcare

Dr. Barbara Alving, Director of the NIH National Center for Research Resources, presented a plenary on the impact of ICT and research networks in healthcare research. She described it as the first systematic change in clinical research in fifty years. The NIH Clinical and Translational Science Awards (http://www.ncrr.nih.gov/clinical_research_resources/clinical_and_translational_science_awards/) programme requires open collaboration between universities, medical schools and hospitals. It is based on the formation of regional partnerships. Interestingly social networking was seen as a tool for developing relationships between biomedical researchers. The NIH runs its own identity federation.

The United States Veterans Association is employing Internet2 as a testbed. In 2007 the VA conducted 400,000 consultations with veterans using telemedicine. (In New Zealand why aren't the Ministry of Health and the DHBs members of KAREN?) The plenary was supported by a

demonstration of the use of Cisco's telepresence for a "consultation". Cisco's telepresence is actually high definition video with "no" noise running over a dedicated 10 gigabits. Doctors who have used the system regularly comment on quality of the video. High definition allows doctors to look for things such as tremors from, for example, Parkinsons. The system supports remote zoom and camera control to keep the patient on screen, and to enable close inspection. Cisco telpresence can be used with a high resolution camera to do dermatological screening. There is also scope for remote sensors - possibly administered by a community nurse.

South Pacific Developments

David Lassner from the University of Hawaii organised a BoF on Pacific Networking following Monday's reception and dinner. David had a number of developments in the Pacific to report on. There were a number of attendees with an interest in the Pacific but none from any of the Pasifika nations. Items of interest.

- This year the PacRim East cable will be repurposed providing a 1 Gb connection to American Samoa. An extension to Samoa will be added, also this year.
- In 2010 a 20GB cable from Hawaii to French Polynesia will be commissioned.
- Also in 2010 a new fiber will be installed from the Marshall Islands to Guam providing connectivity to PacRim West.
- Other new fiber is planned from Australia to New Caledonia, Guam and Papua New Guinea.
- The OB3 satellite system, <http://www.o3bnetworks.com/>, a medium earth orbiting satellite, will be able to provide multiple gigabit gateways within 20 degrees of the equator.

David is currently trying to raise awareness of the potential of this new infrastructure within the various island governments.

Miscellaneous

All Google applications are now available using the IPv6 network. China has 20 universities using IPv6 only. This is to be expanded to 200 by the end of 2009.

The United States Restructuring and Reinvestment stimulus is an unprecedented opportunity for the Internet2 (R&E Network) community.

Russ Housely, the Chair of the IETF, reported that 8% of all electricity consumed is in some way related to the Internet. He did acknowledge that this is unconfirmed.

Conclusion

In November 2007 I attend the Internet2 Fall Member Meeting. At that time I was impressed by the technology put on show by CallT and the San Diego Supercomputer Centre. The unescapable fact from the Spring 2009 meeting was that, despite being able to build on the shoulders of others, New Zealand is falling further behind in leveraging ICT and KAREN to support its research.