OARtech

June 8, 2005

Introductions

Oarnet updates
Research update
Prasad Calyam

Slides for this presentation can be found on the Oartech site:
http:/www.osc.edu/oarnet/oartech/presentations.shtml

Current research projects include open source network measurement tools software development, voice and video traffic on IP studies, network measurement infrastructure test bed development and maintenance for TFN and characterization of bulk FTP over the internet to find the best throughput.

The H323 Beacon is a tool that can be used to test between set points on the network to find problem links. The TFN will be the beacon infrastructure test bed. They have been collecting data for over a year and looking at traffic patterns and behavior. Active Mon is an extensible and customizable software framework for generation and analysis of active measurements that can be used for routine network health monitoring.
They are planning to deploy and use this in the core of TFN. They will be able to have regularly scheduled measurements that then can be analyzed later. On VVoIP they are developing the E-Model XT that models the effects of human, device, and network factors in a VVoIP environment as well as an understanding of behavior at high-speeds. They built FTP performance testing to determine the limiting factors for large-scale data transfers over the internet as part of the disaster recovery project test bed.

When will the disaster recover project begin moving? Some has been started, but it is moving at a snails pace.

I2/OARnet network performance workshop will be held to learn about the tools. The Workshop will cost $200. Watch for announcements.

TFN OARtech update
Paul Schopis

If you have a DS3 or above each site needs to indicate their bandwidth needs as of July 1. Send that information to Linda Roos at Oarnet. When you doing your estimates make sure you leave enough head room to keep from hitting the caps. They recommend that you add about 30% to what you need. If you find this does not fit your needs, then it can be modified after the fact.

Oarnet is running into 2 different models being considered by some of the full I2 members in how I2 traffic interacts/bursts with intra-Ohio traffic.
Would full members prefer to see burst ability between I2 and intra-Ohio or would they prefer to have this more of a set cap without burst ability capability between I2 and intra-Ohio. I2 inside Ohio is intrastate traffic.

I2 outside of Ohio is I2. Non-I2 traffic was subsidizing the backbone costs for the burst ability that Ohio I2 schools were using to get to use their full pipe in bursts. With TFN, Osteer had indicated they wanted to know the cost of the backbone and not have it subsidized. So they have split the intra-Ohio costs out. You paid for these before, but it was not split out. There was some discussion on how different sites were handling their I1 versus I2 traffic and how to handle the intra-Ohio. There was also discussion to determine why different sites are feeling like they have to pay twice for intra-Ohio I2. The general consensus seems to be the group wants flexibility and burst ability.

OhioLink Digital Resource Commons
Peter Murray

This presentation is on line at
http://drc-dev.ohiolink.edu/presentations/200506-OARtech/

Digital Media Center (DMC) is a digital library collection platform with various commercial collections and institutional collections. It serves as a platform for serving multimedia files with collocation with other similar collections. The problem with it is it is too complicated/cumbersome, hard to find objects, doesn't play well with others, and is not a preservation-quality platform for archival. Users want the service without thinking about the technology and the state wants higher education institutions to work collaboratively.

If they redo the DMC now what changes would be made: Give control to the creators and communities they represent with the ability to accept any media type and metadata schema. Make the service easier and more flexible. The Digital Resource Commons is a new product that is meant to address these problems.

They will be creating the Digital Resource Commons to accept, preserve, present, and mediate administration of the educational and research materials of participating institutions. It would provide repositories of web-mediated journals and dissertations, as well as a learning object repository. One of the problems is they have to provide university identity and affiliation so it looks like the resource is coming from the contributing campuses. They need to encourage scholars to use new ways of publishing and enable clients to discover and work with all the collections and objects and not care what type of object it is.

They will be building a central repository based on the FEDORA Digital Object repository platform (this is not the Linux Fedora). OhioLink will provide the base level of functionality and then turn the development to the community to encourage development of open source for the features they need and then contribute those features back to the project.

Goal: Create the most compelling digital repository platform possible such that institutions will find the DRC a more desirable alternative to building their own systems. End sites would then create content and share that content.

FEDORA is an acronym for the project that follows an item through the entire lifecycle of the object with content repurposing. It unifies the architecture for access, management, and integration for the service and applications. It uses WSDL (definition language for defining a web service) and XML. FEDORA 2.1 open source software is due out in June

2005. It is currently being used for collections, repositories, records, document, and asset management. It allows end users to collect and annotate objects and submit it back to the project to be made available.
The FEDORA project defined what a digital object is and what it takes to display that object back to the user. This allows the web site referencing the object to make standard requests that can be fed back to the user from the database in whatever ways that make the most sense for that resource.
The authorization and management is layered over the physical storage so that the users don't need to know the underlying architectures.
Authentication plug-ins can be done with tomcat and will have LDAP tie- ins.

The OhioLink servers will be Redhat Linux servers with an IBM fiber channel SAN with the physical infrastructure as redundant as possible.
They will be adding some developers. They are running this as an open source project to encourage other institutions to participate.

Digital resources commons project website is http://drc-dev.ohiolink.edu/

Speakers contact information:
Peter Murray
http://www.pandc.org/peter/work/
peter@ohiolink.edu
614-728-3600 x338

Can you give an example of this resource? Peter showed a search of the Encyclopedia of Chicago which returned an essay, and a clickable map which would bring up local maps and information on the event including scanned newspaper articles:
http://www.encyclopedia.chicagohistory.org/

If your site is an OhioLink member, your site is eligible to participate or if it is a project with regard to Ohio history you are also eligible to participate.

Lunch

REN-ISAC
Research and Education Networking Information Sharing and Analysis Center Doug Pearson http://www.ren-isac.net dodpears@indiana.edu
24x7 watch desk 1(317)274-6630

ISACs were encouraged, but not funded by the US Government to collect, analyze, and disseminate security threat information on physical infrastructure and computing infrastructures.

REN-ISAC is an integral part of higher education's strategy to improve network security through information collection, analysis, dissemination, early warning, and response. It is specifically designed to support the environment and needs of higher education. It is a component of what a broader Higher Ed ISAC might do. Its subscribers are organizations connected to REN and I2 members are the first major constituency. They develop information products and services designed to provide early security threat and warning information to subscribers. They do not intend to duplicate a service or product, but to enhance.

Their information resources include Abilene network information, Darknet, and global NOC monitoring systems. They also get information from other ISACs and US-CERT, network security collaborations, backbone and member engineers, vendors, mailing lists, and members.
Their activities include information products, incident response, 24x7 watch desk, contact development, tools, and partnerships.

Their products include Daily Weather reports that contain observations of network threat traffic, and a Darknet that looks for scans and malware and reports on what is found. It contains the top scanned-for ports, and highlights any critical issues and provides recommendations for what sites can do to mitigate attacks. It also indicates any new exploits that may have come out. The Darknet report provides a report of the source IPs on your campus that may be attacking other institutions. They also distribute alerts as needed on vulnerabilities that are seen. They also will list malware sites to allow institutions to apply blocks. Notifications are institution specific and contain actionable items and suggestions such as notifying an institution of systems that may have been compromised on their campus. They also provide publicly available reports of common and threat vector ports at http://www.ren-isac.net/monitoring.cgi . They do respond to requests for incident response assistance in the form of specific detailed monitoring, and consultation. They use a closed mailing list for confidential communications, and are also developing a registry of security officers for an institution.

They are working to develop guidance and information products to extend their reach to more institutions and other flows of information. They would like to expand the monitoring and instrumentation and provide black hole and block lists using REN-ISAC as a clearing house for sharing of data. They are looking at expanding their contacts and relationships with other groups and institutions to share information.

Who can participate? They don't turn anyone away. However, they are actively trying to work with the full I2 members. They are also interested in working with Oarnet and the SEGPs.

What are the guidelines that you are using for privacy of the information you collect? They have a policy, but it is currently not on the web, but should be. They are looking at it as a way to protect the network and they do not look at the content of the packets, only the flows.

He handed out contact/registration forms for those that may be interested in participating.

No new Business.

Old Business.

Correction to the minutes was read:

"PGP signing party
Several OARtech members participated in a PGP signing party. Each member confirmed his PGP fingerprint to the other members. Ransel then signed each member's public PGP key, and sent them all the exported public keys. What Ransel really likes

about PGP is that it can be utilized to securely store account information, even via email. PGP is becoming more common and they use it to control root access to administrative machines. If you wish to get the keys, you should get Ransel's key at least so that you can verify information coming from him:
http://net.kent.edu/~ransel/Ransel-Yoho.asc"

Minutes were approved as amended.

Patti indicated that she is waiting on Rio Grande for some corrections/changes before she sends out the account information on the OARtech security site.