OARtech Meeting
August 10, 2005

Introductions

Oarnet Updates – Paul Schopis

Spam Filtering Project
Oarnet formed a statewide committee to look at what is wanted for spam filtering and sent a survey to OARtech and Osteer. They have a subgroup to look at possible solutions including hosted off-site, appliance-based, and software based products. They plan to have a solution decided by October 2005.
Motivations are to see if there is any cost savings for the consortium to subscribe to a common software or service. Wistnet uses a hosted solution, but Oarnet is afraid it might not scale.

There was a question on the privacy issues for email. FERPA covers students just like written mail. For staff mail, it is not as restrictive.

Last Mile Update
All schools are connected to the backbone. 13 of 17 Phase-2 institutions are connected with fiber-based connections. 8 Phase-3 institutions are in the process of being directly connected. Kent State, NEOCOM and Denison are waiting for fiber completion. They are all waiting for transponders to be shipped from Cisco. Central State and University of Dayton have ordered fiber-based circuits from SBC.

Dark fiber, Local Area Rings and leased circuits are available to get to the POPs. Leased circuits can be gotten via SBC, Time Warner Cable, and SOMACS.
They are looking at these vendors for postalized DS3 RFQ in conjunction with State of Ohio. RFQ was released in June, and expect the completion in October. Several vendors have responded to the RFQ.

Upgrades have occurred on ring 0. The ring is now fully 10 Gig 32 wave capable.
This was a joint project with eTech (new organization that was formed from Schoolnet and OIT). OADMs were added as well as preamps to the ring. Ring 2 will be upgraded next and will bring he south side of ring to 10 Gige capable and will have OADM. The upgrade will occur August 16. Springfield site is being changed from a regeneration site into a POP. They will be using an OADM to provide service. The issues are non-technical due to the fact that SBC, Wiltel, and Quest are all involved in the site. They hope to have it up by Sept. 1st. Schoolnet design is complete, parts are in the warehouse and schedule is outlined.

Issues that have occurred include a pin on the fan tray was shorting the B feed on the DC circuits. They also found a bug in version 5.0 on the optical gear for the POP. Cisco is working with Oarnet to resolve the problem.

The backbone is a transponder service using G.709. Paul talked about why they chose G.709 vs Sonet on the backbone. The G.709 gives them the full use of the channels along with failover. It uses routing for failover. It is a universal transport, is Sonet friendly and uses Sonet management, and is cost efficient.

Are there any indications on the costs for the Time Warner agreement that is to be signed on Friday? They are trying to be competitive, but he did not know the figures. They can go into some of the rural areas that have problem getting service.

PGP Tutorial
Peter Murray, Ohiolink

Some slides can be found in
http://www.pandc.org/peter/presentations/200508-PGP-GPG/

Cryptography is needed to keep information and conversations private, to keep the integrity of the communications, and to verify that you know who the file was from. There are 2 types of cryptography: Symmetric and Asymmetric. Neither type is better. Symmetric is faster, but since the key is shared via out of band, makes it hard to communicate with people you don't know. Asymmetric uses private and public keys.

PGP stands for Pretty Good Privacy and was developed in 1991. PGP is now a corporate entity. OpenPGP is an RFC standard that does not use patented encryption. It uses Gnu Privacy G (GPG). These allow the use of encryptions and decryptions using both symmetric and asymmetric methods. This also has a signature component that verifies the integrity and authentication of the message. It does not necessarily verify that particular person encrypted the message. It also provides a management capability for session keys and asymmetric keys.

How do you know what keys to trust? You can only physically check a finite number of keys. PGP has a notion of a "web of trust" that allows you to sign someone else's key to verify that someone you trust knows the person. So you try to have as large a web of trust as possible. Thus it makes sense for OARtech to build a web of trust among Oarnet institutions.

When you generate a key you want as least 1024 bits in the key. Then you want to generate a revocation certificate after creating a key to allow you to cancel your key if you lose your pass phrase. This certificate should be kept off line. Commands for generating the keys, certificates, etc… were shown in the slides.

When you sign a key make sure you know who you are signing and send the signed key to a key server.

If you are using windows you can use the Windows Privacy Tray. It includes GnuPGP shell extension and others. The Window's privacy tray starts and generates a new key pair. Select a key length of 2048. Use your first and last name as user name. Use a respectable pass phrase so you don't violate the web of trust by making the password too easy to guess.

There are extensions available for Windows, Mac OSX , and Linux. There are some Mail user agent plugins available. Thunderbird is available at http://enigmail.mozdev.org/download.html.

Peter did an example setup on the Macintosh platform and on a Windows platform.

Recommendation from the floor that windows users create a directory that is encrypted by default that only you can open so you can keep your notes on system access strings.

They would like to see us have another key signing at the next meeting to continue to build the web of trust amongst OARtech.

How long do you make a key last? Some of the people use a 2 year period of time.

Is there a way to have people resign a new key? You would just ask them to resign. Any keys for people you did not have contact with would be lost.

Network Security – Open Discussion

Kent will be implementing the Perfigo (now Cisco Clean access) on their campus.
They did tests with a group of about 100 users. They are happy with the results of the tests. They came across one particular problem in vlans not talking to each other via the clean access box. The problem was caused by a bug in the code.

How are you doing authentication? Via LDAP. Note that if you are using Perfigo it will log passwords in clear text in debug mode.

How is the scanning mode working? They decided not to do the scanning because of the windows firewall. They are requiring the agent on the systems via the captive portal for windows boxes only. There is a Macintosh agent coming down the road. Cisco is merging the Perfigo product and NAC products.

Another school also using the product are informing students of updates needed, but not forcing. Some schools will be requiring Windows SP2 using the Perfigo server. There is a question on exactly what Cisco devices are supported with clean access box.

Some schools will be requiring the agent this year.

Is anyone doing VoIP with SIP to PBXs? A couple schools have been working with it using Asterix (?). Ohiolink inherited the phone switch from Oarnet when they moved out of that building. It has not been modified since. They are looking at what they can do. OSU has been playing with VoIPong which is a VoIP sniffer. It was able to tap into the traffic. They were concerned that it was this easy to tap into the line. This brings into a whole other aspect and concern on physical security. VoIPong is a free product.

Anyone working with VoIP over wireless? One school is playing with it, but just in test mode with Cisco products. Not much security available although it does have LEAP capability.

Lunch

Virtela Communications
Rick Boler and Ryan Mallory

http://www.virtela.net

Virtela is a global network aggregator and integrator and supports a secure delivery infrastructure available anywhere in the world. Where they see they can help universities is with global access and by providing education. They are headquartered in Denver Co. with NOC/SOCs in Colorado, India and Philippines. Their services are managed with MPLS, VPN (both private and IP), remote access services, convergence service with video and telephony, security and remote monitoring and management. They use several vendors for vendor aggregation, network aggregation, and technology aggregation (various protocols).

Virtela provides an increase in country to country interconnectivity to peer between providers. They provide availability and enterprise use of alternative access technologies such as DSL and Ethernet. VPN technology is mature and can result in cost savings with replacement of frame and private lines. Virtela can provide an optimum path internationally. They can help to provide connectivity to a remote site.

They can help negotiate specific terms and conditions from multiple vendors. They try to negotiate the best terms across multiple vendors. They can negotiate SLAs and credits. They can help with the local to global performance across

multiple regions. Seriously consider broadband, but do your homework. They help with the country specific idiosyncrasies, e.g. infrastructure, firewalls, gateways, etc….

Performance is important. You have to determine the QoS level you need. The higher the QoS needs the more cost associated with network. They analyze the paths and choose the best path to fit the QoS selected. They use MPLS CoS to determine the paths. (CoS – Class of Service)

Virtela has 3 platforms – MPLS, Private VPN, and IP VPN. You can use the various platforms based on the needs for that connection. You can use all three platforms and have them work as a fully meshed connection.

They use several access methods like TDM/Frame, MPLS, and Ethernet to regional policy centers through the network to other policy centers to accommodate Dialup, Broadband, or Wireless. They use proprietary algorithms for automatic fail-over. They will fail-over to the same class of service level path. They put their own tags on the traffic to be able to know what the traffic is. They always have primary, secondary and tertiary paths end to end. They do take into consideration the physics of the distances of the path when they agree to the SLA. They partner with local providers within the various regions and thus send traffic via that network within that region. They provide the industry's first Global multi-carrier MPLS service to provide performance and failover. They have partnered with providers for specific levels of performance that are utilized when they get a contract for a particular level of service.

They do real time path analysis to determine the best path. They provide flexibility and performance and failover in the global market. The can provide for end to end class of service (CoS) and each CoS is associated with a QoS based on the SLA commitments. They can provide single CoS that can be upgraded to multiple classes.

Slides are available on the OARtech web site:
http://www.osc.edu/oarnet/oartech/presents/ryan_V3.ppt

New Business: None

Old Business
Minutes from the last meeting were approved.

Meeting was adjourned at 1:40 pm.