Introductions

TFN/OARnet Updates
Paul Schopis

There are pending fiber builds to Kent State and NEOUCOM due in at the end of this month. BGSU is now on. They are waiting for Youngstown State. Kenyon is connecting via Time Warner.

All Schools are connected to TFN via uplinks from legacy POPs. OIT is looking to use the legacy POPs, which would make a strong case to keep the old POPs connected. Some of the old circuits are being ordered out now. Looking to have the main trunks retired by June.

Research support is coming on line now with OSC Springfield with a 10 Gig Lambda. There is a BOR grant for best practices, and file transfer testing for DR. From the networks point of view this is just large fast file transfers. The current network can be monitored by out of band methods which have interested some of the statistical researchers.

SchoolNet and OIT are possible Partners. SchoolNet's design is complete with the current parts ordered. OIT is still looking at their options.

OARnet experienced their first failure on a fiber break on ring 3 between Cincinnati and Xenia. Initial reports were that is was caused by a squirrel, but after investigation it was found to be caused by a farmer who had a dispute with AEP and removed the fiber from the poles. The fiber was lying across the road and had traffic running over it. The network recovered as expected with no customer outages.

Peering is being changed. They closed peering with AADS (Ameritech), Indy POP, and Detroit POP and are going to use fiber rings to get Equinix and Starlight. They are working with CIC Schools to build a fiber link in Chicago to help build the link throughout Chicago and give OARnet access to several areas and cut the cost significantly. This also allows us to easily peer with Merit.

Time Warner is contacting schools that may also have SBC contracts. What are the recommendations? They are working with Time Warner to get the cross connects into place. Either will work, but you need to keep OARnet in the loop. You can buy service from whoever you want as long as you can get to the POP and OARnet can get the cross connects into place. Comment came up that Time Warner Cable and Time Warner Telco are two different organizations. They currently do not have anyTime Warner Cable sites connected at this time. Kenyon will be the first.

Is the disaster recovery project available to other schools? Currently, it is all a demonstration of the technology, understanding the costs, and proof of concept. Initial transfers are very heavy, but the later transfers aren't as big. They are trying to understand the tradeoffs.

OARnet hired a new director, Pankaj Shah, and he will be coming on board at the beginning of March.

Security Forum
Patty Vendt, Mike Snider

We will be using a content management system provided by Rio Grande. Accounts will be created from a request from the official OARtech representative. The URL is https://security.rio.edu/. If you want to moderate a forum let them know. Currently 11 accounts are in place. The site uses Postnuke (www.postnuke.com) with PHP and MySQL. This is public domain software written in PHP and is platform independent. This particular site is being run on a Windows system. It has lots of modules that can be added to it. It has a polling module and survey module that we may be able to use. If you want an account let Patti or Mike know by sending email to patricia.vendt@wright.edu. They are looking to have a few key accounts for each university and will restrict access so security information can be discussed. Phone number and email if you have questions or comments is listed at the bottom of the sign-in page. Mike did a demo of the site.

Currently Rio is using WordPress for a blogging server. Mike did a demo of the blogging site at Rio.

How are you doing the newsfeeds? They are using RSS feeds. He has built in the Cert news feed and from his perspective it makes it easy to maintain.

Can it be used for a course management system? It could but Rio is not using it for that because they have another product specifically meant for course management (Rio uses CT).

They have it using LDAP for authentication for their campus users.

Has Postnuke seen the security problems that PHPnuke has seen? Most of the exploits that have been seen have been in the third party modules. There is a security site that you can see patches and warnings on the software.

This is fully open software, and they release updates about every 3 months.

How many simultaneous users do you expect to see? They expect 80 users editing content when their site goes production. They have rebuilt their site using Postnuke and expect to go live with the new site very shortly.

Patti has made accounts for each of the official OARtech reps. Contact Patti for the password.

Current exploits
There was a question on what are sites doing to control BOTs? One site filters several of the ports, including IRC ports from the dorms. Some block at the switch level. Some are blocking IRC and people who want to use it must request access to it. They use Packetshaper to watch and control the traffic. They are using Perfigo to collect MAC and IP addresses. They don't require the agent on the client machine, but they make it an available option.

Is anyone using NAC? With Cisco's purchase of Perfigo, there is interest in where their CTA is going. CTA is the agent built into third party products for communicating with the Cisco NAC structure. There is no cost for the CTA, but you have to have ACS in place.

Has Perfigo worked well for those that have implemented it? Overall response is yes. There was some discussion of the different solutions available: Perfigo, Netreg, Bradford Manager, etc....

Is anyone running NetDisco? This uses CDP to map out your network and allows your helpdesk to disable and re-enable ports (netdisco.org). It will give you an inventory of Cisco devices and other options that you may currently use

Observer Suite by Network Instruments - Is anyone using this product? No one seemed to be aware of the product.

Lunch

Fport is a good tool for finding what ports are being used on the desktop system.

Shibboleth
Greg Dykes, Kent State

He is most familiar with the Linux pieces so will be talking about those. There are Windows pieces, but he has not tested them.

Name comes from a biblical reference for ID.

Shibboleth does authorization, not authentication. There has been some name changes. The web site doesn't care how you authenticate, but only that you have authenticated and what your role is. The target site is shibbolized. The site checks to see if you have authenticated. User would see a WAYF server "Where Are You From" server, it would go to the Identity site (Origin) to see if the user has authenticated. If they have, then they are allowed to the resource. It uses tomcat on Linux for a backend database. On windows servers you would put a DLL on ISS.

The attributes used are listed on the middleware site object class eduPerson. The attributes is the eduAffiliation attribute and has the following values: Staff, Student, Faculty, Alum, and Affiliate.

He was not able to do a demo as his server was down.The primary software site is http://shibboleth.internet2.edu.

OhioLink is setting up their shib target sites. Once all the universities are setup they will stop using the old authentication process. OhioLink will post the rules for authentication to OARtech list. You are ready when your identification shib is ready. The contact at OhioLink is Greg German. Kent is using Luminus for their central authentication. They are looking at being able to bring remote users into OhioLink resources.

The "Where Are You From" (WAYF) represents the federation or security group you are a member of. It allows authentication based on roles. OhioLink is interested in where the users are from up to the branch level of the university.

Interactive demo on the site is on http://shibboleth.internet2.edu/docs/demo-instructions.html.

What about Luminus? You can set it up to look at your LDAP directories or its own directory. They find they have 2 different LDAPs: the user data LDAP and the program data LDAP. They are looking at deploying Luminus with a shibboleth environment.

What is a WAR file? A tar type of file used to load a tomcat system.

In common or In queue - In queue is a free environment federation for testing. In common is the production federation and it has a cost to join of $1500. This includes the certificates and licenses for the origins. See the shibboleth site for more information. The point of joining a federation is the common points for definition of the values, such as what a student is, what a staff is, etc.... This sets up the trusts so that you know a student is actually a student.

If a user has multiple affiliations what is the role presented to the target? You can set a primary role. All the affiliations will probably be presented to OhioLink.

Pen State is using its shibboleth environment with Napster. So Napster has been shibbolized. Jstor is also shibbolized.

Current licenses say that users should be active student, staff, and faculty. OhioLink will trust the OhioLink member campuses definitions for roles. They do not provide services for Alumni.

This is also some discussion on password changes that are done on the campuses within the federations.

Is there a way to weight the roles so that people with more than one role will get the appropriate role is selected? Remember that all affiliations are sent to the shib target and the provider would then check all the affiliations to determine if one of the affiliations would allow authorization. It is up to the target to make use of the affiliations.

Does the individual have any control on the role that can be sent? They should. The identity servers should allow it. Currently it does not allow that, but you can build it.

Shibboleth is open source software. Current version is 1.2.1a.

New business: None presented.

Minutes were accepted.

Meeting was adjourned.