OARtech Minutes
August 9, 2006

Introductions

Oarnet updates
Paul Schopis
Slides available on OARtech site:
http://www.osc.edu/oarnet/oartech/presentations.shtml

Hebrew Union College, Edison, Tiffin, Washington State are completed.
Malone will be coming up. UT-MUO merger the ring was broke in half so that UT will operate their half of the ring, Oarnet will operate the other half and it is now 2 separate rings.

Closing ring 4 and 5 using KDL (a Kentucky fiber company)

Missed some of the meeting, please see the slides on the OARtech web site.

New directions that Oarnet is looking into include connecting via a 10Gb path to Merit to create a direct interconnect. This would provide peering with several regional nets as well as the other big 10 schools and SLR (Southern Light Rail). They are trying to prevent loss of connectivity if the national organizations (I2 and NLR) go belly up.

I2 and NLR merger talks have broken down again and NLR's peering request has been turned down. Oarnet is staying neutral in the talks.
There was a NewNet advisory group which was chaired by Paul. They came back with a recommendation that whatever they do to the net that it be transparent, and have a vetting group for requests and proposals. It also recommends that they use the I2 representative on each campus and have terms and term limits for representatives.

There was some discussion of the I2 and NLR issues.

PacketNet (NLR) is now functional and NLR did make a request that if you are connected to both I2 and NLR that you set a route preference for NLR. However, the GigaPOPs have said they will pick the best path, not give preference. Battelle is looking at purchasing NLR. We do not know what this means for the NLR. I2 NewNet may be functional as soon as December. Oarnet is working on a connection to I2 via One Cleveland. Paul showed a diagram of the physical network for I2 and a diagram of the NLR infrastructure. The 2 are very similar in their footprints.

Clark state and Capital have upgraded their connections.

Ann Zimmerman is now manager of Academic Services. She now has a full staff of account managers. They are trying to make campus visits around the state. They are also trying to concentrate on the video conferencing. Video Conferencing pricing has changed and they would like the campuses to look at Oarnet's multipoint services.

CALEA Update
Paul Schopis
Community Assistance to Law Enforcement Agencies Slides available on OARtech site:
http://www.osc.edu/oarnet/oartech/presentations.shtml

CALEA began with telecommunications and is being expanded to include other forms of communication. Everyone is trying to find out what it means to each of the institutions. They recommend that you have your legal counsel look at the documents and determine whether you need to be compliant. No one knows what you have to do to be compliant by May 14, 2007. You at minimum must file a security plan on how your campus will be compliant.

Oarnet's attorneys have determined that Oarnet will need to be compliant and that OSU did not have to be compliant because Oarnet is their only network source. Oarnet is using this information to create an FTE and deploy net flow throughout the network. This was needed to be done anyway. The Juniper equipment will support remote port mirroring so they are hoping to use these. Oarnet will remain engaged with the Quilt (which has people working Capital Hill) and remain engaged in talk with in EduCAUSE and Statnets. One possible scenario is that we should still file our security plan, and that any equipment upgrade required can be added at the normal replacement cycle.

CIOs have not yet talked to Oarnet to determine what they expect Oarnet to do. Paul indicates that we may want a working committee to keep track of the information coming out of the various discussion groups.

Chris Allison from Miami indicated that he heard different information at the Networkers conference. He heard that CALEA may only mean changing the equipment at the entry to campus to enable real time wire tapping. He indicated that it would very beneficial for a statement from Oarnet that indicates that they are a private provider.

If Oarnet is your sole source ISP, you may be CALEA compliant as they connect directly to the internet, not the college. If you are dual homed you may need to be CALEA compliant unless your other vendor puts their equipment on your campus. Other factors include: Whose fiber comes to your campus, Who operates the network equipment and where it is located, and Can just anyone use a terminal in your library.

There was some discussion that Cisco gave a device with the technology that would be needed for CALEA to China. This would indicate that the technology is available. Cornell has a flow chart for their response available on the web that may be a good reference for writing your own plan. Another idea brought up would be to ask the Attorney General's office to determine their take on CALEA.

Patty is willing to be a liaison from the IUC (Inter-University Council) security group that is following this process so we can get that information to OARtech. Security plans will be addressed in a future meeting.

Kurt Eckert will mail out a list of URL for sample security plans. To see Wright State's plan go to http://www.wright.edu/security and click on data compliance.

Have changes occurred on the campuses in light what happened at OU? Some schools are looking at their security and trying to tighten it up. Some are starting to define new security positions. Some have only recognized the need for more funds for security, but nothing has been done. Some schools have done nothing, but are more alert to security issues.

How would OARtech feel about Oarnet being more active in forcing sites that are repeat offenders with BOTnets, etc... as identified by REN-ISAC. The general consensus is that OARtech would support Oarnet turning off these sites after having notified them of the problems.

There is a concern about being able work with H323 video and that it doesn't play well with firewalls. So often this equipment is put outside the firewalls, and this is a security concern. It was felt that the security issues will force the products to become more secure. Instead of telnet and ftp you can have people use scp and ssh, but there is no real alternative for H323. It was suggested that OpenVPN can make UDP tunnels.

There is a project for streaming video for sports. Traditionally, ONN would take satellite trucks to the sports events to televise the video. They are now going to test doing the video via TFN. Miami University is a test site. Bandwidth used would be 10Mb and would be broadcast quality video.

October is security awareness month. Oarnet may want to work with the OARtech security group to come up with some focus meetings about sharing what each of the schools have done with educating their community on security. Patty Vendt, Kurt Eckert, Ransel Yoho, Eric Chan, and Aaron Lafferty will coordinate the focus meetings.

What are sites doing about laptop security? Bowling Green sent out an RFP for whole drive encryption, they are still in contract negotiation so they are able to share their information right now. There is interest to find out if the solution is

PKI or PGP compliant. The army is now requiring the TPM modules on PCs. Harvard has stated that there will be no university data that is not on a network server that has not been encrypted. If the data is taken on a laptop, CD, it must be encrypted. Items of interest would be key management, backups, and recovery of keys. Oberlin is looking more at directory level encryption instead of whole disk encryption. OSU was talking about using a token based (secure ID) for authentication so that you can revoke and replace IDs for their HR and financial people. One institution is looking a boot lock password that can prevent using the hard drive without a password (it is a bios level password). Kent state is using Cryptainer and Altiris.

Brian will run a video during the lunch on a bump key. For more information see http://www.toool.nl/bumping.pdf

Lunch

Enabling Authentication & Network Admission Control Great Bay Software Steve Pettit Slides available on OARtech site: http://www.osc.edu/oarnet/oartech/presentations.shtml

Great Bay Software was founded as a subsidiary of Blue Spruce, an integration company. It provides the first step towards NAC/802.1x for non-windows devices and dramatically shortens the time to deploy NAC and network-based authentication. They also help to provide trusted access to non-NAC endpoints. They also provide data for all network attached endpoints with real-time location, identity and historical data. They have reduced 156 man-weeks of discovery and documentation work into 2 weeks. After those 2 weeks they have a survey and the ability to deploy 802.1x. Their software is called 'Beacon'.

They found that non-access devices are being added to the network, without notification. Typically, there are 3.5 ports used per user in a wired implementation.

Endpoint profiling looks at the NAC (windows) systems as well as Non-NAC devices. Their specialty is profiling the non-NAC systems. Scanning can't always pick out the devices and can cause problems with the non-NAC systems. Examples of non-NAC include printers, HVAC, phones, security, etc....

They are building authentication for a non-authenticating host. They reposition the MAC address to the username and use the behavior of the device as the credential. If the behavior changes, then the end-device has changed.

St Clair has used this system.

The system is used for deployment to begin with, and continued use to see the changes that occur in the network and to monitor and manage events (e.g. using information from an IDS). This system will give you more information on the device attached as well as the IP.

Profiling end-points defines the device based on layers 2 through 7 rules sets. They can use port mirroring, flow collection, Boolean rules and inference-based. They can have the device as in-line or out of band as you wish. How much data you feed the system and allow the system to actively communicate with the end-pieces will determine the types of devices/information the system can detect.

Their software does integrate with Cisco's NAC products (Clean Access, etc...). He showed a demo using Clean Access. You click on the device in the list (the link is labeled 'beacon') and you get summary information on the screen that include the manufacturer, location, and the percentage certainty on the type of the device (e.g. 60% certainty that it is an IP-phone). You can see the raw data used to determine the device type.

Their product comes with many devices pre-defined, and they allow you to modify the profiles by adding rules, or adding new devices. It has the capability of finding the game systems on the network. You can
configure the end-points to manage the kind of authentication used.
It can determine that the device is a printer and set the printer in the printer VLAN.

Their product can actually make the change. It can also provide an end-point directory which can interacts with your authentication system. They don't concider themselves a network management company, but their product can be used for some rudimentary management. It will allow you to search to for device based on name or IP address, manufacturer, etc... It can tell you if a switch is 802.1x capable or enabled.

To deploy you can have it on a span port, or you can just feed it flows. If you put it on a trunk port, it can get the DHCP traffic which provides them with a lot of information.

How is this product affected by CALEA? He feels it can provide a history but does not do the wire tapping.

They could integrate with Bradford Manager, but they don't at this time. They have done some integration with Enterasys. They can export the data in CVS format to allow feeds to other systems.

What are the costs of their product?
They have 2 versions available: $24k and $14k list price. The difference between the two versions is the number of nodes it can control.

Contact information:
Steve Pettit   spettit@GreatBaySoftware.com

Ransel Yoho passed on the OARtech vampire tap to new chair.

Thank you gift was presented to Ransel for his work as past chair.

Ohio Law Enforcement information sharing was talked about. One of the campuses has one of the systems installed for their campus security office. The state is trying to gather information that would be searchable by all law enforcement. A system and firewall is put on the campus and the data is pushed up to their central search system. There is some concern about putting non-university systems on the campus network that it may cause some issues because you don't know who would have access. For more information see http://www.oacp.org.

Columbus Infragard meeting was held yesterday. They had a speaker from the Attorney General's office that talked about identification theft and what the State of Ohio is doing about it. They told stories about an individual being arrested even though they didn't do it because someone had stolen the victims' identity. The main focus is victim support and how to restore the user's identity. The speaker was very good and covered a lot of information. They also talked about financial aid identity theft and the department of education has some guidelines out on how to reduce the possibility of theft. Brian will post the URLs to the OARtech list.

Meeting was adjourned at 2:30pm.