OARtech Minutes
June 8, 2011
Hosted at Columbus State Community College, Delaware Campus

OARnet Network and Technology Updates
TJ Sandor
Slides are available (http://www.oar.net/about/oartech/presentations.shtml)

OMMC Partners have worked through their environmental assessments and all have received approval and their "Finding of No Significant Impact". Horizon has already started laying fiber. One Community has also started building. This will increase middle mile access for everyone.

OARnet is working with Public Broadcasting to roll out HD TV to IP services. They are also working to get an MOU in place with the public broadcasting radio stations. They are redesigning the intra-partner network.

The optical-mesh network, with full mesh lambda capability, has been completed on Ring 0 and Ring 4. The next ring to be updated is ring 1. They are setting up a second 10Gbs internet uplink to the backbone that is slated for the end of the year.

Where will this go? They are working to setup an MOU with Blue Mile out of Columbus.

The state is looking to see if they can take some lambdas to provide public services. They're trying to figure out how to use the extra capacity offering services to communities, perhaps via the jobs program.

OARnet is working on the community cloud service. This service would be available to schools with different service models (Gold, Silver, and Bronze). The BOR-CIO committee has requested that they investigate the Virtual Computer Lab (VCL). A draft proposal has been started, and the draft call of participation has been completed and submitted for approval. This will be a testing for proof of concept for institutions.

Today is IPv6 Day and there is a video mega-conference running today. OARnet has received a /48 from ARIN (1.2x10 24) and can give each institution a /64. All you have to do is request a group from OARnet.

Routing algorithms favor the /64 over the /128 subnets. You can go to ARIN, but you don't have too. If you go to ARIN there will be a cost. If you get your address space from OARnet there is no cost.

The member meeting was cancelled and the next meeting is tentatively scheduled for August 10-11, 2011. More information will be available by then. Hopefully, John Conley, CTO will be able to attend.

Client Services
Ann Zimmerman
(Slides not available)

Two schools are considering 10G, OU and Kent Stat. New members include Muskingum University, and Columbus College of Art and Design.

They have 2 Gigs to Time Warner's eLan. Time Warner is converting services from Time Warner Cable to eLAn. They aggregate the traffic and then hand it off to OARnet.

Columbus State CC, and OSU Delaware have a partnership where they share bandwidth and wireless with virtual desktops. The VMlab test-bed is still available for institutions to test concepts. This will be moving more to the VLC. Columbus State has been doing some testing. They have one graphics class using it to test remote access to labs from home.

OARnet is getting all the new VMware products added to their contract and are extending the contract 2 years. They have been selling lots of it. They are looking at a community college training project from
VMware. The idea is to get students trained on VMware and to sponsor some internships. There was already one school participating in the program.

Internet 2 consortium meeting - OARnet will be purchasing a 10gig connection to I2 to replace the bandwidth that we have been using through Michigan. Full member and SEGP rates will remain the same.

OARnet has had several VMware workshops. Next one will be in
Cincinnati (June 14). See the Oarnet site (http://www.oar.net) for dates and locations. The workshops are sponsored by VMware, IBM and OARnet.

Open discussion

How do you determine use with Microsoft contracts? He has tried calling Microsoft, but they have not called back. If you own the equipment, and are within the IPEDs numbers, show you are willing to work with them. There is a consortium contract on Microsoft licensing. The numbers were significantly better as it is based on the employee count and they combine the numbers of the institutions to get the better pricing. If people are interested in the consortium pricing you can contact James Beidler, Columbus State (jbeidler@cscc.edu).

What about Copyright notices? One institution has seen a drop in notices. Another has seen an increase with what looks like a different service. Oberlin has gone to a block with opt in, no questions asked. Some are blockings, dropping the peer-to-peer, using various tools, Packetshaper, Exinda, Palo Alto, and Packet Logic.

What are people using for NAC? Enterasys and Bradford were mentioned.
Palo Alto will be able to integrate with Enterasys and Aruba. Palo Alto can really interact with almost any device that requests authentication information.
There was a discussion about IPv6. OSU has implemented it across their core. They found IPv6 on the core is fairly easy. The problem is really getting applications capable. What is envisioned from the network device vendors is dual stack for a while. When the traffic drops on ipv4 to a certain level, vendors will start dropping IPv4 support. You will want to be fully capable at that point.

DNSSEC - Some schools are starting to look at it, but not implemented yet.

How much bandwidth are the shaping boxes (1 G) seeing? Sites are seeing 300-400M. The control traffic is open and the payload is encrypted so you can see the setup to block.

Palo Alto Networks
Jason Wessel
Slides are available (http://www.oar.net/about/oartech/presentations.shtml)

He did an overview of the company and his own experience. The founder moved from Checkpoint, to Juniper, then founded Palo Alto. They have 3500+ customers across 70+ countries.

What is the #1 threat vector out there? Applications are carrying the threats. All applications are prone to misuse: some are used to tunnel to other applications, they have known vulnerabilities, file transfers are easier and cross platform. All these are used by malware that is evasive as they try to prevent being blocked. An example of an application would be BitTorrent. Facebook is no longer just a site, but is now full of applications. Companies are using the social networking to do testing to find new employees. Applications are extending usage (Twitter started small, but now can transfer pictures).

Social networking is no longer a fad as companies are now using social networking to leverage their business, from hiring to branding.

Facebook has over 500 million users compared to LinkedIn's 60 million. YouTube is the 3rd most popular site. Social networking is now a hotbed for malware and they are being leveraged by the malware. The malware is now very targeted and many times hides.

Pal Alto collects lots of data from live networks on various networks (723 organizations, found 931 applications and 1.3 petabytes of bandwidth) for analysis. They are currently seeing lots of media (Netflix, streaming media). He discussed the key findings of the data. The port use is no longer the static mapping that we used to use. With the port hopping software, different protocols can go over any port.

Application control belongs in the firewall. The firewall should not only see the IPS data but be able to control it, not just allow all or deny all. The next generation firewall needs to be able to recognize all applications and be able to control them. You select your risks by naming the applications you are willing to allow through the firewall. To reduce the threat level, the devices need to look and control at the application level not at the TCP level and must be able to detect different components of a threat. It also needs to give you a way of viewing the data.

Next Generation firewalls need to include firewalls, IPS, URL, AV,

Policy, Reporting, and Performance.

There was discussion on how the inspections on SSL packets occur.

How have you worked through the problem of port block verses application? They have gone in saying they are giving full visibility. Some schools have had contractors convert current firewall rules into the Palo Alto.

Where on the network does the devices get put, the edge, between zones, etc? Everywhere. They started at the edge but are moving more to the datacenter.

How do you deal with new applications, what's your lag time? They release application identities 2-3 times a week and they are updated on a regularly basis.

How do you balance the logging of the data with privacy issues? There is a policy so you can granularly keep track of what you want to. You have to explicitly say to capture packet and only do it for malware streams. You see logs like flow data, not tcpdump like data. You can control what the admins are able to see as well.

They can do QoS into a class with guarantees, maximums, etc. But they can only do 8 classes. However, it can mark packets with tagging to be rate shaped by other devices.

How many sites have gotten rid of their Packetshaper when they put in Palo Alto? Several do that when the maintenance on the Packetshaper has expired.

He sees more aggregating of similar types of traffic.

We need a host for the August and December meetings - 8/10/11,
12/14/11. The October 12, 2011 meeting will be hosted at Stark State University.

There was some discussion on how to get more schools to attend again.

Columbus State gave a brief overview of their network. They are almost all virtual, both on the server end and in the labs. VMview required Active Directory so they had to find a way to work between their current directory and Active Directory. They have direct fiber between the campuses. They are working to build a DR site between the
2 campuses. The Delaware systems are fed from the Columbus servers. There will be a tour after the end of the meeting.

Meeting adjourned at 12:24pm.