OARtech
February 11, 2004

Introductions - What are your summer projects? What would you like to see for future meetings?

Miami - Network architecture strategy study with the Burton group. Interested in doing register/quarantine/patch product for fall.

Owens CC - Telecom switch installation, Banner 7 upgrades, 10 Gb backbone, interested in intrusion detection

Kent - Perfigo trial for network authentication, patch certifications

Wright State - Zoned security structure for the network, Finalizing approvals of security policy, and Upgraded to Gb core with Cisco 3550, 4500. Implemented quarantining infected machines with Packetshaper, forcing infected machines to Microsoft update.

DeVry - Finished wireless access and a major project corporate wide is converting from AS400 to Oracle DB java based applications. They are currently working through the bugs.

OSU - Experimenting with a new forensic tool that allows forensics remotely. Will be doing a presentation on it at Infragard next week. It gathers data from a console on the network that allows access to file shares, etc.... So far it seems to be doing a good job. They would like to see various types of authentication solutions.

Columbus State CC - Implemented a new student email using Netmail and are looking at interfacing their email and Datatel systems. Implementing lab logins for students. Rolled out a test wireless environment and looking at Bluesocket for security. Also looking at port security on Cisco gear. Would like to see solutions similar to Bluesocket not only for unsecure, but secure ports as well.

Antioch - Wireless in dorms that have not been wired. Using 802.1x with PEAK authentication. Looks like it will work and will scale well.

Ohio Northern - Alterus (?) product to push images to labs. Netreg – looking at Carnegie Mellon implementation. Looking at putting out a CD in the fall.

U of Dayton - segmenting academic and dorm networks. Trying to move away from homegrown Netreg to an authentication method. Also deploying wireless.

OhioLink - received some technology grants through OSC and OLN to do project for an institutional repository, federated authentication (using shibboloth), and expanding courseware.

Otterbein - They are finishing a Cisco rollout. Also have wireless projects, and user and mac registrations.

Ohio U - Working regional connectivity. Mail will be moved to load balance blade system. They are current using Bluesocket.

Clark State - Working on phase 2 of web registration, security policy, Datatel cleanup in financial aid, and looking at flash media server.

Case Western - Finished 10Gb backbone upgrade. Looking at VoIP deployment.

Question from the floor - Who else is using VoIP? One site said they had it working fine. Another dumped it because it wasn't stable and they didn't have their data network power ready for data phones and had echo problems. Both were using Cisco.

Shawnee State - Putting wireless in using 802.1x, and are currently waiting on policy from management to implement. They are subnetting the campus network and implementing active directory.

U of Akron - Working on Webdev with SSL, 10 Gb at the core with Gb to buildings. They are having problems with spanning tree with the large wireless and wire networks (using btdu command to control spanning tree problems). Upgrading access points to Cisco 1200 series w 802.11g. Pretty complete coverage. Starting to do trunking with the access points.

Mt Vernon Nazarene - Trying to use VoIP test with virtual office users. Using NEC and they have not been successful. Wireless initiatives stalled due to security issues. They do use Netreg. This fall they will be creating a CD and passing it out. They also plan to do more with Netreg.

U of Toledo - Working on new redundant Gb backbone, with 6513, 6509, and will be upgrading infrastructure and 2 new buildings.

Distance Learning Program (not sure which campus) - They have split to their own DS3 with a main initiative with TFN to make video conferencing more stable across the state and campus.

Oberlin - Virus scanner on email server is cleaning mydoom and blocking zip attachments. They have been scanning for people listening on the backdoor and only finding a few. They have very limited VoIP in remote sites via DSL and

VoIP phones. Summer projects include moving all Netware to a cluster on a SAN. Major networking project is putting more security divisions between dorms and campus network.

Bowling Green - Working on upgrading core and distribution switches. They are covering green space with wireless and using Bluesocket.

Kenyon - Working on rewiring residential buildings and adding wireless in those areas. Implementing Barracuda Anti-spam and have been very conservative with policy and looking at BackupExec to backup data.

Heidelberg College - Working on Banner upgrades with the web products. Using an internal firewall in the 6509. In the fall they will be handing out a CD.

Ohio Dominican - They have moved to Cisco infrastructure. VLANs are dynamic and are mac based. Students will be registered in the spring. Registration is modeled off Netreg, but homegrown. Several new buildings are coming up. They are looking at VoIP for telecom in some new buildings. Looking at upgrading their security card system.

NASA - They changed a 30-day evaluation of Bluesocket to a 60-day pilot and out of the pilot using are Bluesocket to deploy across the buildings and have been pleased with it. They are willing be available as a resource if people would like to ask questions.

Sinclair CC - They are replacing a Checkpoint firewall system with new Nokia Checkpoint firewall. Using mac filtering for wireless in the classroom. Put out an RFP for wireless security and guest access. Narrowed the RFP responders to 3. One they are looking at is AirSpace. They would be interesting if anyone else has looked at them. Starting to do Gb to servers in the data room. They use Exchange in a cluster with SAN and have had some problems. They would be interested in any input on this. Looking at front end for registrations.

Clark State CC - Working on Gb backbone upgrade, SANs upgrade, and increasing speed on a 45 Mb link between campuses.

Denison University - Working on email upgrade, and backbone upgrade. They are using Bluesocket for wireless access and for guest access on some wired lines.

Questions to floor - Who is using a Netreg like solution? Show of hands was a few. One site is using Cisco, but is moving away from it. One is using ACS for dialup and it seems to be working fine. Another has homegrown, they timestamp the registrations and they expire to force people to register. One uses Netreg - they clean it out at the beginning and end of the school year for students, their faculty/staff have static IPs.

Is there any interest on Campus Manager? One or 2 responded
Is there any interest in Cisco's solution? One or 2 responded
How many are using 10 Gb backbone? Those using it are using 6500 switches. One blade is one port. So you need more density on the blade for 10 Gb. Cisco is starting to come out with a 4 port blade. You also have to upgrade the power and fan assembly on the switches to handle the higher bandwidth.
What kind of wireless deployments do site have? campuswide - about 5 or 6 sites raised hands; Hotspots - about 10 sites. About 6 sites are implementing wireless with other vendors besides Cisco. The latest version of IOS on 1200 is the most stable and can do trunking. One site is using LEAP using aegis client for the non-Cisco NICs. This will kill Novell, and takes over all your network connections. One site is using WLSE from Cisco for monitoring wireless access points. One site is using Interasys and using Interasys's management product. 802.11A only one site is using it in hotspots. One site is looking at a 802.20 test for outdoors connectivity (miles of non-line of sight). Pt-to-pt highspeed wireless: there would be some interest in it.

OARnet updates
Linda Roos
OARnet offices have moved to 424 Kinnear Road. The next OARtech meeting will be held over there. There is a video conferencing certification class to be held. Christopher Cook has moved to another position and so any academic communications should go to Linda. At the Osteer meeting in March the finance committee hopes to have a pricing model for the TFN.

Paul Schopis
Cable and Wireless has gone bankrupt and is terminating their services. OARnet is scrambling to bring up another line with another vendor. The Nagios tool will be fully functional by the end of the month. 2 weeks ago, AFN (a subcontractor for AEP) was doing some work and at the end of the work, OARnet had problems with connections. AEP found there was a timing problem. Then they discovered a timing problem in a switch in that pop. They concluded that the switching backplane was going bad and replaced it.

What can they do with denial of server attacks? Sometimes, you can call OARnet and they will block a problem port, or can call another campus that is putting out the attacks. Would a secondary ISP solve the filled bandwidth problem? A site with 2 ISPs says having 2 ISPs doesn't solve DoS issues because you can just as likely get the problem from the other ISP.

TFN
Currently doing fiber characterizations. The first burn in is scheduled for the Columbus gear the first 2 weeks of March. They will probably bring up the fiber in about April time frame and start moving the current backbone in the June timeframe. OARnet is hiring an optical engineer. They did get another grant to

connect the teaching hospitals to TFN. The last mile RFP received about 13 responses. They saw everything from fiber to wireless. All the responses will probably be accepted. So you could see pricing from several respondents. The list will be out in about a month. Currently looking at their peering contracts. People are leaving the peering groups, as it is becoming a less attractive option. He is interested in whether peering relationships are important to sites, if so, what sites.

Lunch

Bluesocket
Mike Brockney, Sr

Slides will be available on the web site.

WLAN management & security requirements include access control needs through authentication, authorization, encryption, and physical security. Need to manage the bandwidth and control the bandwidth use. The number of access points has increased and needs to be controlled. There is a need to have interoperability between many different types of endpoints and access points, as well as using the different radio protocols. The access has to be simple and manageable. You need to keep it mobile and flexible. Another problem is the finding of rogue APs. Bluesocket partners with AirMagnet, AirDefense, Wavelink, AirSpace to detect and alert. Cisco, Proxim/Orinoco and others are building the rogue detection into the standard APs.

Security standards
WEP Security (Wired Equivalent Privacy) is better than nothing. Is available on all APs and cards with different key lengths and could be used in the home. It is crackable. 801.1x is a standard for port based authentication in wired networks but was adopted by IEEE for wireless. The WEP key is dynamic. The supplicant is the client. The AP checks with the authenticator. Uses EAP (extensible authentication protocol) of different types: TLS, TTLS, PEAP, LEAP. Cisco and Microsoft both have PEAP but the inter- authentication pieces are different and don't necessarily talk to each other. One site uses Microsoft's PEAP with free radius server. Microsoft's PEAP works with both Windows platforms and Apple platforms. You need to be sure your radius server supports both protocols if you have both Microsoft servers and Cisco APs. The same EAP method needs to be supported on the client device and authentication server. There are 3 approaches to EAP - Password based, certificate based, and token based. Early entries were LEAP, MTLS and TTLS. Emerging leaders are PEAP (Microsoft, Cisco, and RSA, and TTLS (Funk and Certicom); there is no specific EAP for PDA clients.

Most implementation require vendor specific APs, NICs and servers as there is not a standard EAP method of operating mode. Software is required on the client

to run 802.1x. You need to be aware of where your vendor is going with their migration. WiFi Protected Access (WPA) has a subset of the 802.11i standard and is using TKIP and MIC to check for man in the middle attacks. For all of the methods you have to look at some type of radius server.

802.11i (WPA v2) has stronger encryptions and can support VoWlan, but not all the details are settled. Bluesocket will recognize the authentications schemes that are available. For instance for PEAP they can recognize that and not require another username/password. They are also looking at adding a worm/virus detection piece that will allow you to put infected systems into a limited area that you control. You can also use IPSec encryption.

There was some interest in mac lookups using LDAP then authenticate.

Bluesocket Futures:
Will continue to support standards PEAP, TTLS, and 802.11i. Will add additional authentication methods to support customer needs. Currently have added PIN, Cosign, Certificate, use XML API for other methods. They continue to innovate around security and mobility such as VLAN mobility and more efficient traffic routing as it relates to mobility. Will be adding load sharing to distribute the load. They will be adding more flexibility around login pages by location/interface.

The Bluesocket box is a gateway that you plug into your wireless VLANS. They don't limit traffic based on application, they limit based on the user, or group type.

mike@bluesocket.com

New Business
Likely presentation will be on Perfigo in April. Also in April will be elections for new vice chair, and secretary.

Question from the floor - has anyone heard of Dell's new switches? No one seems to have any information.

Meeting adjourned.