OARtech Meeting
April 9, 2003
Taken by Teresa Beamer

Meeting called to order by Tim Gruenhagen at 10:00am

Attendance:
Antioch University - Bruce Friend
Ashland University - Brian Wisniewski
Bowling Green State University - Mike Smith
Case Western Reserve University - Eric Chan
Clark State Community College - Hugh Evans
Columbus State Community College - James Beidler, Paul Clark, Tim Malloy, Chris Scanlon, Shane Stewart
Denison University - Teresa Beamer, Chris Marshall
Dept. of Administrative Services - Mike Yerian
DeVry University - Dave Leitch
Heidelberg College - Sean Joyce
Kent State University - Ransel Yoho
Miami University - Tim Gruenhagen
NASA Glenn - Dean Harter, Mike Heryak
NEOUCOM - Bill Mayhew
OARnet - Christopher Cook, Ruth Crites, Nancy Drugan Koehler, Mark Fullmer, Paul Schopis, Al Stutz, Gene Wallis
Oberlin College - Art Ripley
Ohio Northern University - Bob Beer
Ohio State University - Mowgli Assor, Brian Moeller
Ohio University - Curt Flood, Royce Holliday, Terry Kelleher, Brandon Saunders
OhioLINK - Anita Cook
Otterbein College - Greg Hemsoth, Jeff Kasson, Tim Pindell
Rhodes State College - Diane Moots, Sylvia Sargent
University of Dayton - Michael Skelton, Ronnie Wagers
University of Notre Dame - Kurt Eckert
University of Rio Grande - Chrissy Booth, Kingsley Meyer
University of Toledo - John Heiden, Denis Logan
Wright State University - Shane DeWalt
Xavier University - Michael Bowling

Introductions - Using 802.11A or B or other

NASA Glenn - 802.11B
Ohio Northern - 802.11B
Wright State - 802.11B
NEOUCOM - 802.11B
Miami University - 802.11B
University of Dayton - 802.11A and B and looking at G
Clark State Community College - 802.11B
University of Toledo - 802.11B
OSU - 802.11B
Heidelberg College - 802.11B
Oberlin - 802.11B
Ohio University - 802.11B some of A and G
Denison University - 802.11B
Antioch - some of 802.11A, B and G
Columbus State Community College - 802.11B
University of Rio Grande - 802.11B
Otterbein - 802.11B

Brian Moeller, Wireless Security

What is a wireless access point?

OSU took a survey to see what wireless they would find on campus at OSU. They found Cisco, Apple, Linksys, Netgear, and Apple Laptops (if configured wrong can become an access point). They wanted to find out where and how many there were and what to do about policies for wireless, to prove/disprove that wireless implementations are secure or not secure, and to demonstrate what they can do with wireless.

The scanning process used a laptop with a wireless card and a small external antenna, a golf cart, and a map of the campus. They added a GPS to give location data via satellite triangulation, which gave them accuracy usually around 15ft. For software, they used Netstumbler from Netstumbler.com. Free software that looks for the SSID broadcasts, polls access points for configuration, names and any other info. It does not request IP address.

They found that they had a lot of wireless around campus and most did not follow good administrative practices. Many appear to be merely unpacked and plugged in. Most were not running authentication or encryption. They found a total of 122 access points: 45 using WEP, the rest using no encryption. 35 appear to have factory default settings. Channel distribution was found to use 1 and 6 the most, which tends to be due to default settings. They even found a wireless access point behind the firewall with no security.

Their conclusion was that users were not complying with the campus policies. This caused the network to have no integrity or accountability and confidentiality was a problem. Their policies need to be revised to include the ownership and centralized management of wireless frequencies and channels. They should have an authority to assign approve the frequency and channel usage. They would like to see this come through the office of the CIO. However, the CIO's office doesn't have the necessary tools.

Miami has an interim policy that has been waiting for approval. It defines the ownership, but does not have any enforcement.

OSU has the rule that if you are on campus you are required to abide by the campus policies.

University of Dayton says they disregarded the frequency, but if an access point connects to their network they must connect within policy.

OSU has had some interference with microwave ovens and some cells phones. If they do put up some wireless, they want it to work and not have interference from other sources.

Miami only enforces if there is a problem. Many in the room indicated this was the case on their campuses.

Asked for a show of hands for those that had centrally deployed access points, most sites had this. One site said they had centrally deployed access points only.

NEOUCOM users must register their access points, and stations. Thus they only get a DHCP address if their mac address is registered.

It was felt that the person with ownership of the access point would be responsible for any activity that comes through that access point.

How many sites are only allowing registered mac addresses on their network? Only 3 or 4 sites indicated this to be the case.

Ohio Northern uses radius and requires a mac address, but it is a manual process to register them. At OSU they have a mix of types of signup, both manual and electronic.

How many people require a special client? No one. Some require authentication. Some require that the users provide their own VPN client.

Who has looked at the web authentication products out there?

OU has been using the Bluesocket boxes. These act as a gateway box to the wireless networks. It pushes all the authentication issues to software on the gateway. They went through a long evaluation process to find something that would allow anyone with wireless to access the network but would require them to authenticate. They have published their evaluation document: http://www.cns.ohio.edu/hot_topies/itinfrastructure.html.

ReefEdge is a competitor to Bluesocket and has provided a 5-user demo for free. OU found that ReefEdge was still working on their product when they did the evaluation. Bluesocket seemed to be ahead of the ReefEdge in development.

OU drew a picture of their implementation using Bluesocket. They connected the building switches with 200 Mb connection to a Bluesocket wg-1000 and then to the access points. How many buildings setup this way? 11 locations. This configuration has a master that the other devices update their configurations from. What database do you use for authentication? DCE and Radius. Their guest information is all stored in Oracle. Bluesocket will do LDAP, will pass through 802.1x, and will do active directory. Clients bring up their wireless. If they are unregistered then they are allowed to do some things like getting to guest information. OU does not allow telnet, ftp, imap, or other known insecure protocols. They startup a web browser, the Bluesocket box forges the response with its own login page. OU is not running NAT but is running their gateways in a transparent mode. The installation was included in an infrastructure rollout. Bluesocket WS-1000 costs around $5000.

Another vendor is Vernier that does basically the same task, but is less expensive. Xavier is looking at the Vernier product. They cost around $3500. OSU is building their solution based on the Carl Bridge for about $1000 each.

What about the transparent IP roaming? These solutions create an IP tunnel back to the master. Bluesocket has been very responsive when problems have come up and to feature requests.

Another possible vendor with a competing product is SMS/OSC from Tut Systems: tutsys.com - SMS/OSC.

OSU is building their own based on their old Carl Bridges to authenticate back to their Kerberos systems. They had to add the authentication to their firewall. They are using these same boxes for authentication in the labs. Their product is still being beta tested.

Are there any solutions that do encryption? Blue socket does some, but OU is not using it. Miami is looking at it. They are looking to run things through their VPN concentrator to force some encryption. This also requires a client on the desktop. If the user is accessing sensitive materials then it is up to the users to secure it, such with VPN to the server.

OSU's policy discussions are currently going on. They need to define what technologies are approved as well as the encryption scheme. They would recommend at lease WEP and strongly recommend VPN. They require mac address registration and filtering, and authentication for all users that use the network, which includes the wireless. The AUP should apply to all resources. They don't really want NAT or private addressing. OSU requires that users use campus-assigned network addresses to help with capacity planning.   If any problems are seen on the network, they block that address. If it is a NAT address, they could knock a whole NAT based network off.

OU just acquired an /18 IP range to use just for their residential network. Remember that you need to let your library know if you add address space so they can let OhioLINK know of the new addresses.

OSU requires standardization of access point names and employ logs for user authentication information that must be kept for at least 30 days. Wireless access point configurations must have password-protected configurations.

What do you do if they can't afford the extra stuff required for authentication? OSU says if you can't afford to secure it, then you probably can't afford wireless.

A couple of schools are using LEAP for authentication. Xavier has wireless laptops that authenticate to their NDS tree and must be registered into VMPS. They are looking at Venier boxes to provide guest access.

Another school is using LEAP with Cisco's ACS and active directory for Cisco access points. Anyone who brings another type of access point are told they are not allowed to use it.

Some schools are using free-radius and that it provides the necessary extensions.

OU uses a single authentication system for both email and access.

Oberlin is looking at UPN, which would authenticate back to their LDAP servers, using LDAP to provide authorizations as well. UPN is a Terasys product.

Xavier, Denison, and Oberlin also use some form of mac registrations.   Mac authentication only does authentication to the machine not to the user. OU wanted to authenticate to the user.

Any concern with QoS on a Bluesocket type of system? How will it work with voice or video traffic? OU tries not to have congested links to provide the needed response. Bluesocket does have some VLAN capability and have separate VLANs for VoIP.

ReefEdge currently has the same capabilities as was mentioned as the Bluesocket products.

OhioLINK authentication is an IP based authentication. They have 101 databases that provide access via IP. If the mode of authentication using your methods to get your campus is within your IP range then its okay. If they come in with a different IP then they must authenticate via the library systems. Authentication is verified with the local library system in an unencrypted method. They pull the full record back, verify the information, and then give a cookie to the browser that is good for 2 hours. They would be interested in things like shibboleth. Steve Cantor at OSU has a web site about shibboleth. If you change IPs or add IPs, you must let OhioLINK know.

How many have one username/password for the whole network? A few raised hands. This would make it less likely that users would share their information.

Clark State Community College is using Colleague to automatically create the necessary accounts using the rosters from the classes.

OhioLINK
They have 250 videos converted and later this month should have something to show. Would they be interested in other formats besides Real? Currently that is what they are working with, but they may add other formats in the future. They can provide temporary caches to the campuses for some of the videos.

Packeteer question
The site is using 5.3 code but still seeing their http traffic peak. Seems to be peer-to-peer applications that are tunneling in http. Some of the newsgroups allow http transfers of files that can be very large as well. There was some other discussion on packeteer issues.

OhioLINK
Someone setup movies and setup a chat room to discuss the movies on one of their servers. They rebuilt the server and hacker was still there. They are exploring ways to get rid of it.

Did some looking on fcc.gov to see if a user brought in an access point to your site, could they use it? Under the unlicensed rules, then you must accept the interference with your access point and you are not allowed to interfere with other licensed services. There is proposal to require the registration of the access base stations. Convenience can take precedence over the federal law.

University of Dayton has some off-campus wireless. Have they had issues with interference? Last it was heard they had pulled it back, as they had some problems due to barriers etc.... It turns out to be a high maintenance option.

Lunch

OARnet updates
Ruth Crites
Christopher Cook
May 6th, Introduction H323 class will be offered.
Moved OARtech website to the OARnet site www.oar.net click on OARtech to get to it. Send info to ccook@oar.net if you wish to put information on the site. Username and password for access was given at the meeting.

It was voted to put vendor links on the password protected portion of the pages with a disclaimer.

Al Stutz
Talked about the new TFN manager Dennis Walsh. He will be at the next OARtech meeting and Osteer meeting. As project manager he is totally responsible for the TFN. He is currently working on the segment testing validation data. He is also working on a timetable for the project. The timetable has been complicated as they are in serious negotiation with SchoolNet. The MOU should be signed this next week. We are getting a lot of support from the governor's office and the technical advisor there. OARnet has been put in as a line item on the budget with that money to be used for the fiber network.

He has asked for training for OARnet staff and OARtech for running on the fiber network. They hope to have some more information on the training at the next OARtech meeting.

The pricing committee has been very active in determining the cost structure for the fiber network. They are a sub-committee of the Osteer finance committee. This is a problem in that a lot of the costs are estimates with best guess efforts. They have finally agreed that this is the way to go. They will be able to look at what the component costs are for the network and the OARnet services.

Paul Schopis
They are trying to get an RFI out for the equipment to light the fiber. They hope to have the RFI out in the next 30 to 60 days. They are going with an RFI instead of an RFP to allow the vendors some partnership and research opportunities, and flexibility. This is very hard to do with a formal RFP. Nortel, Lucent, Extreme, Juniper, and Cisco are possible players.

Gene Wallis
The contracts have been signed for the main fiber. Some of the moneys for the appropriations in the budget is for the connection and regeneration sites. Gene showed a map that includes the congressional districts. They are currently working on testing the segments and looking at how to bring together the various pieces of fiber. The next phase of building the structure is to let out the contracts for building interconnects in each of the locations where necessary. They are looking at 15 pop locations and 17 regeneration sites around the states. They have purchased local fiber rings in Columbus (AEP) and Cleveland (AFS) and will be looking at sites associated with these companies. AEP purchased the Prism sites in Columbus so OARnet is looking at using that as the primary pop in Columbus. In Cleveland, AFS has a collocation with Switch and Data where OARnet will probably interconnect. There are similar locations in some of the other cities, but it is not all firmed up. They have had a lot of conversations with some of the schools about how to build fiber into the phase 2 of the plan (getting the primary state institutions).

It is a good time for sites to get information to OARnet for what might be available in each location to help with the build in their area. Send information to ccook@oar.net. The philosophy is to have direct fiber to each site. They will be looking at what makes sense for connecting sites in common areas at the same time. Now is the time to get the information on local fiber or other connection media to OARnet. Gene has been talking to some of the local areas about the economic opportunities for community rings.

They will be sending a note to the CIOs, provosts, and presidents at every university to watch for the TFN and to be planning for this to happen and keep it in mind as they look at other vendors for providing Internet access.

Note that the fiber network will affect your firewall strategies.

OARnet will be willing to come to meetings with universities, k-12, city and other organizations to find out about the network and its potential.

Other things you might think about are the branch campuses and remote sites that might benefit from the project. This network is being built to provide the service they provide today but also new services, such as disaster recovery, backups, etc.... Talking to Wright State and Xavier about a test for mirroring administrative data at the supercomputing mass storage units. Cluster Ohio is distributing replaced processors as they upgrade the cluster every 18 months to sites for research. They also do this with Sun systems. You could have backup web sites (continuous, mirrored) as well as hosting websites so sites are always available.

They are looking to have lighted fiber by this fall. There is information on the web sites in the Osteer member password protected area. Some will be moved to the TFN web site.

Paul Schopis - H.323 committee
A draft report has been written and sent to the committee. They will finalize this and send it out to the list. Some of the firewall vendors have gotten better in dealing with the H.323 protocol.

ITEC update - version 1.2 of the beacon has been released with major GUI enhancements. New features have been added with autographing statistics with test report generation. They have committed to the full-scale version (v.2), which can be downloaded off the ITEC web pages. V1.1 can be gotten off the ITEC web page; v1.2 can be gotten from pshah if you are interested in working with the beta version.

Other current projects include helping SBC to reach rural areas. I2 collaborations are working on getting XML based performance statistics from the network boxes. They are doing testing on MPLS for extended IP to see if there is a bottleneck in IP for the very high performance networking. They are continuing their consultation role in Abilene.

Since the last OARtech, they are trying to take the netflow feeds from Abilene to do research on that network data available. The data is anonymized. OARnet says they have ordered the I2 netflow data project equipment to support the flow data statistics. The project has been split out to various schools to get the various pieces up. In the next 30-60 days Abilene data will be available.

Could you include the beacon in the videoconference training? OARnet is willing to consider it.

Could the beacon project be used for other protocols? The H.323 beacon is the first piece of the pipes project that will be a single interface for the possible testing framework. OARnet has talked about putting up an Iperf site. Iperf is a tool used for testing networks in client/server mode doing both TCP and UDP tests to give you a picture of your loss, jitter, etc and to look at performance tests across your internet links. Send a message to pschopis@oar.net if you want an account on the OARnet Iperf test system or maf@oar.net if you would like a test box brought to your campus for testing.

Al Stutz
OSC Search Committee
They are actively negotiating with the preferred candidate. The candidate is very good at collaborative projects and is a mover and shaker in the industry.

OARtech issues.
White Paper - there will have to be an email vote to pass the White Paper as it is supposed to be presented to Osteer in May.

Tim and OARnet have been suggesting a group from OARtech to look at operational issues. This would look at how you would work with the operational issues such as managing your network and how sites deal with the issues that come up, what statistics you look at, how calls are escalated, etc.... This would play into the new network, as it has been defined as a 5-nines network and we need to help OARnet define what this means and the type of reliability and redundancy necessary for the local spurs.

How many have 24 hour staffed NOCs? Only 2. Several sites indicated they have electronic monitoring 24 hour.

There was very little response to the suggestion of a sub-committee. So maybe we should have OARtech membership to look at this. We could have a network operations initiative that should be dealt with at OARtech meetings. This idea was voted on and passed.

New business
OhioLINK is implementing a new function that will require opening new ports in your firewall between your library server and OhioLINK.

Security Sub-committee
The co-chairs are Patricia Vendt <patricia.vendt@wright.edu>, Brian Moeller <moe@net.ohio-state.edu>, and Greg Siebert <gregs@kent.edu>. The mission statement is:

"Promote policy development, training, and collaboration on information security among OSTEER member institutions by facilitating information exchange consistent with the OARtech mission."

Adjourned.