OARtech minutes for 8/9/2000 meeting

Meeting started at 10:05 with introductions from each of the attendees. They were to state their names, school and what their most interesting projects were:

Ken Bailey, Shawn Ostermann, Ohio University - Cisco Upgrade
David Barber, OhioLINK
Teresa Beamer, Denison University - Wireless, Banner Web
Robert Beer, Ohio Northern University - Campus Pipeline Upgrade
Eric Chan, Case Western Reserve University
Clifford Collins, OARnet
Anita Cook - OhioLINK
Ruth Crites, OARnet
Fred Crowner, OARnet
Carl Dickhous, Xavier University - Changing to a Cisco based switched network
Tim Gruenhagen, Miami University - Time Warner service from Road Runner.
Kurt Huenemann, Sean Joyce, Heidelberg College
Implementing SCT-Banner and the Banner Web product
Kim Koeppe, University of Cincinnati - Wireless networking and Gigabit Ethernet
Dave Leitch, DeVRY Institute of Technology - Blackboard and Windows 2000
Dave Levine, Lakeland Community - Wireless networking
Denin Logan, John Heiden, University of Toledo
Wireless, VoIP, Video on Demand
Bill Mayhew, NEOUCOM - Wireless, SCT Banner Web
Kingsley Meyer, University of Rio Grande
Gigabit Ethernet, Polycom video conferencing, Windows 2000
Jodi Santini, OARnet
Patricia Vendt, Wright State University
Cisco Upgrade, Wireless pilot, Webmail for Students
Gene Wallis, OARnet
Mark Yarnell, Shawnee State University - ATM and Office 2000
Ransel Yoho, Kent State University
Blackboard, Phone/Data/Video over regular campus ATM lines
Unknown - Increase redundancy and introducing dual routers.

Approval of June minutes.

White Paper Changes
OhioLINK Technical Advisory Committee (OTAC) has requested a change in the technical White Paper aimed at the CIO / CFO audience. The White Paper will be divided into sections and provide more information, including staffing good

practices. Organization charts have already been requested from each institution. We will take those organization charts and make a composite determining good staffing practices. Other sections that need expansion include adding an executive summary, expand the bandwidth and desktop sections, and developing the local cable plant section.

Patty Vendt asked for a "point person" to coordinate the changes to the White Paper. It was suggested that it be split up by topics. Volunteers to coordinate each topic are as follows:
Bill Meyhew, NEOUCOM, for hardware and desktop
Denin Logan, University of Toledo, for Video Conferencing, H.323.
Tim Gruenhagen, Miami University, for Cable Plant and bandwidth needs.
Patty Vendt, Wright State, for Security

Remember to bring an organizational chart for your organization to the next meeting.

Authentication and Authorization
David Barber is Joint Technical Planning Director (JTPD) for OhioLINK, OSC, OLN, and OARnet. In that role, he works on technical issues of joint concern to the four organizations such as authentication systems for multi-institutional distance learning programs and centralized information resources. Prior to becoming JTPD, he was OhioLINK's Director of New Service Development. For OhioLINK, he directed the technical development of web information systems such as their Electronic Journal Center and Digital Media Center, and developed OhioLINK's web authentication system.

The joint planning committee are researching the Authentication/Authorization issues from a statewide, and multi-institutional perspective. They are looking at the various aspects, such as security services, institutional environment and problems, multi-institutional environment and problems, alternative solutions, and finding out how to build a foundation for solutions.

The core of the security services would be identification, authentication, and authorization. Where identification consists of providing a unique identifier and authorization is assigning rights to the authenticated identifier. The issues that need to be considered include that there is no sniffing of the data, and that you can verify who really accessed the resource as well as protecting the integrity of the resource.

The institutional environment can be very complex with a wide variety of computers and uses and have multiple registration systems, both internal and

external. Thus making it hard to have tight management of credentials. This becomes even more complex as you expand the view to multi-institutional.

Current uses utilize the centralized resources of OhioLINK to authenticate clients, as well as IP addresses. Neither are able to use stronger forms of authentication. The research is to see what is available beyond IP addresses and to find cooperative or common approach to identification, authentication, and authorization. For instance a student uses the facilities at one institution to access resources at a second, how do you cope? Authenticate at login - does that mean two sets of authorization?

In considering the alternatives to solve these problems they are taking the approach of a research project as opposed to trying to define a specific solution. These options will be looked at with various groups to see what is feasible and then look to see if something really needs to be implemented. Some of the alternatives included in the study are:
Biometrics and smart cards - expensive and problematic for remote access
Name and Password - currently the most common
PKI - a two-factor system that includes a certificate (public) as something you have given to the user by an institution and a private key or password that is kept by the user as something you know.

There are 2 approaches to PKI, standard PKI and NDLF. Standard PKI is used by Internet 2. It stores information about the user in the certificate and thus must be revoked and reissued each time that information changes. NDLF from the National Digital Library Federation has a link back to a directory and thus you can be selective on the information included in the certificate. NDLF is supported by a smaller group, but CIC (Big Ten) is considering this as a security project, thus including OSU.

Some of the problems with PKI is that it is the "bleeding edge". It's hard to use with public workstations, browsers must know about the certificate authorities unless bridge certification is developed. Bridge certification is under development by the government to allow trust between different certificate authorities.

Passwords will have the same problems we have now where it depends on the user to take their password seriously. Password databases have to be synched and plug-ins that replace the authentication modules in the browsers may have to be developed. As you increase the size by going multi-institutional, this can be come very complex. Currently passwords can be done with centralized credentials and authorization - UK has 200 universities that upload account information to a central database or they can be decentralized making calls to

radius, and/or kerberos like servers.

Some of the foundations for the system must be addressed. Such as policies that enable institutions to trust one another both about who they allow to access the systems and that the systems are being run securely. Will it require 2 types of security, one verified and one not? Every campus would need to provide a source for authentication.

Has there been any discussion of keeping student information private (FERPA) when using PKI or other mechanisms? It has not been looked at yet, they are still in the planning stages. It may require getting the lawyers together.

Many of these issues go straight to the philosophy of the institution in how they maintain their accounts. What kind of quality of service mechanisms will be needed? Electronic media has raised the bar as to needs for how information is used and how much privacy we can provide. The question of minor's access also needs to be considered.

What is being implemented now? Currently name and password is the most common. People trying PKI are reminded of the kerberos - if all the vendors do not support the certificates there is a problem.

After this year, there may be enough data to determine what may be more useful and where the drawbacks are. Vendors will need to be able to issue the certificates, directory services issues need to be developed as well (Windows 2000, LDAP, etc...), and the security aspects also need to be in place. Costs have been all over the place. A couple of years ago OARnet looked at running certificate authority, but the price was $75,000 a year. Not only would OARnet have to run one, but each campus would need to run one or have OARnet run one for them.

Another idea that has surfaced is that of the digital wallet with servers to provide the wallet information.

In summary, the technology is still evolving.

OhioLINK Update Anita Cook - OhioLINK
The NASA images are live now. They can be found in the Digital Media Center and are open to anyone. We are the first state to make these images available. The Sanborn maps are still being worked on. They hope to have these available by Fall. They also have a collection of physics videos. These are 2-6 minute videos on physics demonstrations that will probably be put in several different formats including Real Video and Quicktime so that they can be streamed or

downloaded. Also some video clips are available from Denison and Kent State. All the video material will need plug-ins in the end user stations.

Ruth Crites handed out a security update from Mogli at OSU Incident Response Team. It can be seen at http://www.net.ohio-state.edu/security/talks/updates/20000809.shtml

Questions and Answers

Question from the floor asked if anyone responded to port scans? Your firewall is there to protect and notify you of those scans. If you wish to report a scan send a nice note to the site the scan is coming from and copy OARnet on the note. OARnet notifies the provider and requires a response. There was also some discussion on what you can do if you are being used as a site for a denial of service attack. What can you use to find the culprit machine? It was noted that OhioLINK has 2 sources of books, you might be able to find texts on this problem with full text. Bill Mayhew recommended StatsScout and MRTG. Email any useful links, and references etc... to Oartech Web page maintainers so they can be posted in the Tools area of the Oartech web page.

Ruth Crites, OARnet

Video Conference Conference will be held at University of Akron and are being done with OLN. They will also be holding sessions in Columbus in September and at Wright State in November. Lunch is provided.

MegaConference reminder: October 30-November 1st. If you have people doing H.323 on your campus, the mega-conference would be interested in how your people are using the technology. If you just wish to view the conference, the requirements are are minimal and it will be streamed. If you wish to participate, you need to talk to OARnet to get an MCU Spot. For more information see http://www.mega-net.net/megaconference

Lunch

OARnet Update
Gene Wallis - Engineering
Gene showed the "Next Generation Map" for 2000-2001. Highlights included adding additional pops and line to Cleveland, NW, and SE. Cable & Wireless connection going up to OC12 and can run it fractional. Sprint to 2 OC3, Qwest to OC3, Chicago Nap to OC3, May East to OC3 and in Columbus OC48 Backbone ring

between the Columbus pops. When these changes are implemented OARnet will "break" the gigabit barrier on connectivity. Gene also showed a drawing of the equipment at OEB pop. The heart of that portion of the net is Cisco 8540s though there are still some LS1010s in the network.

Jodi Santini - HelpDesk
OARnet is looking to bring up a network outages page. Something like what Miami has (e.g. http://www.muohio.edu/noc) in place. Jodi was asking for input on several questions:
What people would like to see?
Who should it be available to? Everyone? Only OARnet members? Passworded?
Information included would be lines down, fibers cut, a calendar of outages and schedules for NAPs.
Would each site want put on the page if your line is down?
The general consensus showed the overall net information should be public.

There was some discussion of setting up a notification address for each campus. But we found there was some confusion on what aliases had already been used for OARnet. It was decided that we needed a look at the existing aliases to see what they are and what should be used.

Paul Schopis - Internet 2
How can we provide a forum that can be useful for both H.323 and H. 320 users?

OARnet is looking at using an Accord unit to provide an H.323 to H.320 gateway. Accord is a company out of Atlanta that can provide a gateway product and have demonstrated multiple windows on a screen showing H.323, H.320, and H.321. They are looking at allowing the setup of conferences "on the fly". This will require software on the users station to manage the conference.

Question was raised as to the use of the interconnect between DAS and OARnet. This is an OC3, but the success for video conferencing for this interconnect is about 80% due to vendor equipment problems.

For a user to setup a conference through the Accord product requires a username and password. Summary of the connections they will have include 24 H.323, 12 ATM and ISDN with 384K bandwidth.

A description of the mega-conference was given.

Clifford Collins - Security update
Clifford gave a summary of the new network security audit that OARnet will be making available. His slide presentation should be available off the Oartech

web site.

There will be 7 different packages to meet a variety of needs, depending on the needs at each site: External scan, Internal Scan, Phone scan, Network Architecture evaluation, basic audit, standard audit, and premium audit:

The external scan is done with Network Associates' Cyber Cop scanner under a 90 day license. This scan is done from ENSS Ops Center. It will encounter and test any firewall or filters in place at the entry point to the campus net. The results are provided on CD without any analysis. Fee is sensitive to the address space scanned.

The internal scan is done from within the campus with the same product. It has the same issues as the external scan but does not test the entry firewalls or filters. Fee is sensitive to the address space and will include travel since it must be done from on campus.

The phone scan uses SecureLogix's TeleSweep product which schedules the service and catalogs the numbers and modem information. It is performed on campus and requires some on-compus telephone lines. The fee will be based on the number of phone numbers scanned and travel to the campus. Results, like those above, will be provided on CD without analysis.

Network Architecture Evaluation will review the configurations and layout of the campus network. A network map will be generated and policies reviewed. The fee will be sensitive the available address space and travel costs. The final report will be provided in written form and presented to management.

The Basic Audit will include the external, internal and phone scans. The fee will be based on the address space and the phone number range. The results will be provided on CD without analysis.

Standard Audit will include all items in the Basic Audit with the Network Architecture evaluation, with a policy review and presentation of the results.

Premium Audit will include the Basic and Standard Audits and also include a risk assessment for the site.

The scanning tool that will be used have the resulting report sorted by various categories. Cliff is interested in how schools would like the data sorted in the default report. The items available for sorting include Complexity, Ease of fix, Host, Impact, OS type, Popularity of hack, Risk factor, Root cause, and Vulnerability ID. The general feeling at the meeting

was order would be best by Operating System, host, and/or vulnerability id.

ENSS is the new security services group within OARnet. It stands for Enterprise Network Security Services.

They are also looking at a scanning product from Purdue that would be aimed more at Education use as well as other alternatives that may make the service more affordable.

Question was asked: How are you going to work with the false positives? Will identify the most common false positives, but it's better for false positives then false negatives.

Some recommended texts on security:

"Intrusion Detection", by Terry Escamilla (is in OhioLINK's IT Database)
"Solaris Security", by Peter Gregory

Oartech Web page - www.oartech.oar.net
Would like suggestions on content people want to see. Some suggestions given: FAQs, Agendas, Meeting dates, Tools, add a link to the outage page, Contact information.

Meeting adjourned 2:45 PM