From: Teresa Beamer <BEAMER@DENISON.EDU>
Subject: Oartech minutes for April 10, 2002

OARtech Minutes
4/10/2002 tlb

Please be sure and sign in, OARnet relies on the sign-in list as a reporting tool to OSC.

Introductions
Air Force Institute of Technology - Tim Fox
Antioch University - Bruce Friend
Bowling Green State University - Chris Toth
Case Western Reserve University - Eric Chan
Cedarville University - Alan McCain, Gabe Custer
Central State Community College - Bryan West
Clark State Community College - Romy Lu, Steve Hurley
Denison University - Teresa Beamer
DeVry Institute of Technology - Dave Leitch
Heidleberg College - Kurt Huenemann, Sean Joyce
Kent State University - Ransel Yoho
Lima Technical College - Damon Hughes, Diane Moots
Lorain County Community College - Lisa Guerrero
NEUOUCOM - Bill Mayhew
OARnet Staff - Brian Moeller, Christopher Cook, Fred Crowner, Gene Wallis,
Jack Maher, Kelly Sitz , Mark Fullmer, Pankaj Shah, Paul Schopis, Weiping Mandrawa
Oberlin College - Cal Frye
Ohio Dominican - Arron King
Ohio Northern University - Bob Beer
Ohio State University - Mowgli Assor, Steve Romig
Otterbein College - Jeff Kasson, Tim Pindell
University of Cincinnati - Tom Ridgeway
University of Dayton - Ronnie Wagers, Tim Harrington
University of Rio Grande - Chrissy Booth, Kingsley Meyer
University of Toledo- -John Heiden
Wright State University - Pat Vendt, Shane DeWalt

Minutes approved

Video Conferencing OARtech meetings
Christopher Cook recommended that the meetings not be broadcast as it would encourage people not to attending meetings and OARnet would have a problem

proving attendance. Some feel that during bad weather it should be considered. Others feel it would be beneficial for others at the local sites to see the meetings. Do we want streaming or H.323? Some would be interested in participating in the meetings directly, but steaming would be better than nothing. There is some concern that if video conferencing is offered than users would not come but would stay at their sites and then get called away for emergencies thus not participating fully in the meetings. The topic was tabled for further discussion.

Listserv Membership
In order to post you must be subscribed to the list. Is there any concern on the membership of the list and the discussions that might occur on this list? There was no response from the membership in the way of concern.

Nominations for Vice Chair. Chair will be Tim Gruenhagen, Teresa Beamer agreed to be secretary next year. The Vice Chair will serve for 2 years and then move to chair for 2 years. Call for nominations were made. No nominations were submitted from the floor. Nominations can be made via the list. Nominations will remain open.

Bill Miller, OARnet - OARnet put up the remedy interface on the network a couple months ago. He was looking for feedback. A couple of sites have used it and say the interface is good.

Christopher Cook - The Cleveland Institute of music is now a new member of OARnet. See their website at http://WWW.CIM.EDU. The new OARnet fee schedule is out. Chris handed out a summary of the fee structure. The basic fee is now a flat fee for all institutions.

Rio Grande is a new SEGP.

Introductory H.323 class will be offered April 18th. Contact Julie if you have questions.

Statistics - Fred Crowner
OARnet is in the process of putting up a new version of the statistics package. They are still working on getting it to function properly. Fred isn't going to show it today, because they are still having problems with it. The login will be different. The internal workings are much different. The problems are different between sites that have T1s and those using DS3 and aggregated bandwidth. On the larger lines they provide just the real numbers on usage and knowledge of the bandwidth limit was left up to the site. Content of the reports will be the same. There are some changes or

possibility for changes in the displays on the screen. They are aiming to cut over June 1st. They are told you can easily feed the data down into a spreadsheet to allow the sites to work with their own data. Fred asked a question of the group on the hourly utilization charts - does anyone use the standard deviation lines? What do you want to see on the screen - one complex report or several tabs with the simplified reports? After they get the package working they will be looking at how to distribute the data for each site. The raw data cannot be extracted directly. So the "raw data" has been manipulated before each site can see their data since interfaces change. They have to see how far down to the raw data they can go.

Procedurally, they collect every 5 minutes, 24 hours a day certain data on every interface. Then they have to preprocess the data to clean the anomalies in the data. The next step is to process the data from the bytes to bits and then divide by the sample time to get a minute-by-minute statistic. Conversion of the existing data will take several months. Incoming and outgoing data rates for the various lines are what they will provide unless there is something else sites want. The data they can collect must be SNMP collectable or can be calculated from the collected data. A suggestion from the floor is to have a next button so you can just page through the week without having to go back to menu. The user likes to see the totals per month so they can continue their charts on their use of their lines over time. Send suggestions or requests through the support center support@oar.net.

Kelly Sitts
Windows on the Future is this Monday. She handed out agendas for the meeting. The conference is collaboration between ADEC, I2 and ITech-Ohio. The conference is actually 3 days, but the Windows of the Future portion is only 1 of those days. Break out sessions are broken up by track. Cost is $125.00. See more details on itechohio.net. There is also a list of attendees available so you can see who else is attending.

Gene Wallis
I2 - Cleveland State is now an I2 member and OARnet is waiting on approval from BGSU. So there are 2 more full members of I2 in the state. 10 SEGP members at this point and 1 sponsored participant. With the new design of I2 network, the POP in Cleveland will go away. They are looking at Indianapolis to replace that I2 POP. The Internet 2 group here has been testing equipment under NDA until the decision is made as to the equipment they will use in the new design.

Infrastructure - Biggest changes have been the 2nd OC3 into Chicago is now up and operating. They originally thought they were going to move peers, but have been adding peers instead. At the same time MAE-East came up and they have been adding peers there. They are currently peered with over a hundred other networks. Some of the biggest peers are outside of the country (Canada, Japan, etc...). They are running 350- 400 Meg of traffic.

Gene Bassin - Qwest pops were relying of AC power and are in the process of converting them to DC power to improve power reliability.

Gene Wallis (again)
They have removed all the 7513 out of the remote pops at this time and are replacing them with 7507mx. They are going to channellized interfaces on the equipment. The DC power changes give them more control over the racks in these pops.

When you let OARnet know that you are doing H.323 video conferencing, that information is given to engineering so that the video conferencing can be considered when the changes to the pop are made.

Everything in the network is now up to the current version of the IOS, so all equipment are patched against the snmp hole. They have been removing older equipment as they have been doing the IOS updates. They are re-enforcing and making the networks more resilient as they do the updates. The structure in the main pops has changed, in that they have core router and client routers to provide redundancy to the network.

Satellite and Wireless Update:
Bob Dixon is working with ADEC to setup a mobile satellite station so that they can do demonstrations and short term setups. They have been designing and building this on a trailer so that is can be just rolled up to a site and set up and have a working system in a short period of time. The trailer currently being designed to have "everything but the kitchen sink" on it. Hope to have it available for Farm Science Review conference in September. They are looking to include H323 video conferencing off this unit.

Dark fiber project
OARnet is in the process of generating an RFP for dark fiber installation that they hope to have out by the end of this month. They expect to put out the RFP and see what they get back from industry. They would like to see at least the major corridors covered. They know there is at least some existing fiber in the ground that might be usable.

Are they still working with AEP? No. They started working with them, but in the process the power companies changed their structure. The new group is only interested in looking at the major market areas. They don't seem to be interested in bringing up new market areas. Existing lines will continue to be used, but they will not be adding any new lines through them.

Patty -
The pink handout is a list of the addresses on the OARtech list. Review it and if you have changes let OARnet know.

NetPd notices have been changed to SonyMusic.com. Notices have started going out again this week. The reporting seems has improved.

Lunch

Best Practices - Brian Moeller
Why are logs important? They allow you to look at performance management, planning, and security. It allows you to know what's going on with the network. The logs also help with troubleshooting.

The basics: there are 3 layers of control - Network, Operating Systems, and Application. The firewall looks at the network and can log that traffic. The operating system and applications can create their own logs. You need to know who is on your network and log that information (Authentication). Authorization is the information that tells what the users are allowed to do once they get on the network. Accountability is the process of keeping the records of the activity (Who, What, Where, When and how).

What should you log? Log enough as you can handle and is useful. The logs need to be able to answer the Who, What, Where, When and how questions: Who was involved? What happened? Where it happened? When did it happen? (You need time synchronization between the logs). How was it done/How much was used? Use several logs to prove the same point so you can look at each to build the incident. Use several logs to see what other things occurred during the incident. Example: Workstation cache show suspected activity, Network traffic logs indicate suspected activity, Files not found on workstations, but are found in a recent backup, User maintains innocence, but...telephone records show phone calls....

Log as much as is practical for your needs. Try some dry runs - do something and then try to prove it from your logs. How long should logs be kept? Be practical... general rule of thumb is 3 months of 'quick' access, then another 3 months 'offline'. You may have other rules that will effect how long you must keep your logs (tax records, financials, etc...).

Don't let your log service be public access. Limit to only those that are investigating a break-in. Generally plan on 10% of system capacity for logs. Find a place between logging more that you need and not effecting system performance.

If you use the logs to check the activity before it becomes a problem, you can prevent an incident. Learn what is correct so you know when things are wrong. This allows you to use logs as a problem prevention tool.

If logs become evidence, you must keep copy and keep them protected.

Is the integrity of the logs questioned in a court case? Always, that is why you need multiple logs to verify via the information via multiple places. The issue is the body of evidence in total. Each and every piece of log will be questioned and picked apart. This is another reason to limit access to the logs.

What about printed media and backup storage? Keep 2 copies of evidence; keep it under lock and key. You need to keep a record of what happened with the log (take pictures, have someone watch and verify where the logs came from, etc...).

Slides will be available off the OARtech web site (oartech.oar.net)

Security Update, Steve Romig and Mowgli Assor, OSU
Kazaa/Brilliant/AltNet

Kazaa is peer to peer file-sharing system has partnered with Brilliant (3D advertising). It will allow Brilliant to charge commercial customers for use of "spare" computing resources (Altnet). They didn't really announce this, but it was in some accounting reporting that was picked up. The will provide "compensation" in coupons etc… http://www.brilliantdigital.com/

The Issues OSU sees: Sneaky? Privacy? They are already downloading software down to pc to run their 3D ads. What about Security - bugs, subvert, DDOS attacks - how good is their software? Whose computers? They have no control on private computers, but they are seeing it increasingly on university computers. Whose network? Bandwidth? Even if it uses student computers the bandwidth is OSU bandwidth. How does this effect commercial use for OSU systems?

What can you do?

Uninstall: http://zdnet.com.com/2100-11-875278.html - must be done on all machines. If you Block tcp/1214 there no guarantee that they won't change the port numbers.

Probably need to notify users about this so they know what the university stance is.

Setti at home project, is the same basic thing, but they don't try to hide it and is up front.

There have been recently reports of break-ins on shares of NT boxes and sql servers that don't have administrator passwords set. Microsoft has just recently announced a whole bunch of IIS patches.

It is sometimes hard for the administrators to know what is happening on all machines. The software installs can change the security information even when you have it set a specific way.

Ninzider - will show you the ports you have open and what is running on those ports.

Mowgli
Bot nets - handout was provided.

Sudden spikes of traffic are suspicious. Botnets can spoof traffic to hide what machine it is on. You can look at flow logs to find the machine. In general, the folks that use these are on a private network for development and then they spam it out to users to get them to install it.

If you have a lot of ICMP packets that don't have a return packet from that pc then it's a clue that the system is infected.   Free software is the most common vehicle for distributing bot software.

How to trace the traffic? Go by the volume of traffic - look at switch information within your network. Look for high usage ports within networks - Flow logs, or argus(?) logs are the best way to find the stations. Intrusion detection systems may not be able to catch it. Snort can see "large miscellaneous ICMP" traffic. Might also use the miscellaneous IRC ports.

Analyzing Miscellaneous Software
Steve Romig

Steve worked through a sample case.

They got a piece of "Something", what does it do? In their case it came as an email attachment but was not recognized by the anti-virus software.

1. They ran it through the UNIX "strings" program just to see what they get - doesn't always give you anything, but can sometimes give you something useful, and then do Google searches on what turns up. Try to determine what it does by symbol names, included libraries, files, etc… In this case, nothing useful was found.

You can try running a dis-assembler on it if you want.

2. Try running it - Be VERY careful where you run it. It might do "Bad things", and it might tip off the perpetrators.
   a. Create a clean test machine
   b. Detach the machine from the network
   c. Run the malware there
   d. Don't reuse the machine for other tests.

Use VMWare! to set up virtual machines.   Install the operating system, patches, and applications as needed to setup the Windows machine. Make a snapshot of the virtual disk and squirrel it away. He uses a read-only "airlock" with host-only access.   Then run the malware with no access, use library call tracers: isof handlex, Filemon, regmon (windows only) sysinternals.com.   Take a snapshot of what happens. Use tcpdump and ethereal to see what kind of network traffic it produces.

Create a Fake network. - In this case it attempted to resolve an IP address, so create a fake DNS entry and try it again. It attempted to connect to tcp/80 - so created a fake web server and tried again. The malware then attempted to download nethief_connect.htm Google and Babelfish are your friends! Archive.org - caches pages.

OSU eventually got the zip file. It was the console that controls the whole thing. The zip file had a read me/ license/ registration/ support, etc... Nethief24 with documentation. However, the documentation was written in Chinese. The url was greenstuff.363.net. This url is no longer out there, but when it was there, was all in Chinese. They used Babelfish to translate the Chinese to see what it said. The program was written in Chinese as well.

They found that the malware will generate the backdoor program used to infect other people. It updates the web site once a minute with the current ip, creates the trojan and infects someone. The Trojan runs at login, checks the web site once a minute with tcp/8102 and the console tcp/80 can used to update files, etc.... It works behind a firewall because all connections are outbound. The attacker can specify what stations to use to attack.

They found that only virus detection software in specific areas of the world recognize this malware.

Gene Wallis - Infrastructure Design
This was a discussion of Gene's suggestion of putting a network in front of the firewall for H.323, etc... to get the best performance.

ENSS is providing some firewall support at some sites. They have to open all ports above recommended to that video conferencing unit.

3 technical things that a firewall can do to affect H.323: 1. Network latency (only have a up to .3 seconds for end-to-end traffic) 2. Jitter has a huge effect on H.323. 3. Packet loss, as the firewall gets busy it starts to drop packets.

Paul - OARnet has been testing with latency and found that up to a 5 second latency is okay, but jitter causes a lot of problems. Jitter is directly affected by the frame rate you are using. They tested each parameter independently. You can have both problems at the same time. They will be doing a presentation at Windows of the Future on this.

It is an important point that all sites are at different stages, some have already installed what OARnet says they will not support.

Arif - H.323 and firewall - they are trying to build a system that is meant to run without a firewall. Jitter is critical and you need to determine what is good for you. They are recommending the least amount of equipment as possible between ends. This is the recommendation throughout the world. Worldbank has been converting H.320 to H.323 but they say it will not work behind the firewall.

Brian - the benefits of having a firewall is based on what they need at the time. You can setup the firewall port to pass the appropriate traffic, but if your firewall or the links to it are loaded then you get the jitter and latency.

Mogli - Ultimately it's your network and you have to make the decision yourself. Can you? Yes, but what you open up must be set up for all sorts of access. They are not meant to provide security. Ultimately it comes down to testing. As long as the firewall is not doing any address translation or other heavy load then it should be able to run H.323 fine.

Paul - Some schools have used an MCU that straddles the firewall.

Some schools cannot put a network outside the firewall due to their management policy. They also can't afford to build a second network to support these things.

Patty suggested a committee be created to work with the H.323 protocol and firewall issues: Volunteers are Wright State, Tom Ridgeway from UC, Bill Mayhew from Neocom, Teresa Beamer from Denison, and Brian, Paul, Arif from OARnet.

Tom Ridgeway - They have a PIX firewall with the same issues of bad video. They tried the MCU straddling the firewall, but that needs to be babysat. The PIX firewall version they have now works fine outgoing, but has problems incoming. They are trying to find the most flexibility. Tom is willing to chair the sub-committee.

Gene - the classic firewall design includes a DMZ net. But they usually say web server, email servers, etc... but Gene was just trying to point out that there are other servers that need to go outside the firewall. They have found that running through a firewall that sometimes it will run fine and then all of a sudden stop running. OARnet is trying to make H.323 reliable. With the current state of firewalls you have a hard time making it run reliably.

Chris - When firewalls are involved it can take from days to weeks to get it to work. But for $80/month they don't have resources to throw at troubleshooting both the firewall and H.323 problems.

The charge of the committee is to find a set of best practices.

Patty - This will include protocol issues, firewall issues, etc...

What about the firewall on a flashcard? ENSS has made a bunch of them and they are available. These are low cost firewall but are not full featured.

Gene - just getting the issue out and discussed is good for the community. We are going to have a hard time coming up with a definitive answer that applies to everyone.   None of these things is impossible, but you need to determine what is needed. OARnet does not have the time to troubleshoot your firewall every time they go to setup.

Other issues: What about equipment that runs 10 half that has been recommended by OARnet? Desktop conferencing can't be outside the firewall. When you troubleshoot H.323 do you troubleshoot other equipment on the network? They check through every switch back to the network asking questions about each step.

Discussion will have to move to the list.

Mark Fullmer - Net Flow
Developed tools to look at Network flows:

Packets or frames have common attributes: creation and expiration policies, counters, and routing information. They can be unidirectional or bi-directional, contain other information such as application information, and have aggregated flows.

With IP only you can only see 2 flows (incoming, outgoing). With a flow key can see both the TCP and ICMP flows. To collect the data, you have a flow collector connected to the router. Flows are not generated for the local LAN.

Cisco product is Netflow. Juniper calls it Cflow.

Netflow has 4 unaggregated types, and 14 aggregated types. Each version has it own packet format. The version defines what type of data is in the flow.

Most use Netflow V5. The key fields are Source/Distination IP, Source/Destination Port, IP protocol, ToS, and Input interface. If any of these changes, a new flow is recorded. You have accounting for packets, octets, start/end time, and the output interface. Flow- tools are a collection of programs to post process the Cisco Netflow compatible flows.

A year ago, Abilene came to them and requested that they look at traffic engineering using flow information. The 12 Abilene core routers are configured with a sample Netflow. Ohio ITEC takes the data and captures it. They just recently brought up data between the gigapops and abilene.

Flowscan takes output from flow-capture and graphs it. It allows you to see how your traffic is split up and what applications are being run. They are talking to Enterprise Services about making this available as a service to campuses. The Cisco Netflow software is bundled in the IOS. All you need to do is turn it on. The software to look at the flows is openly available.

He has written reports for Abilene to be able to see what percentage of traffic is created by what flows. http://www.splintered.net/ot/links.html has the sample links that he showed.

About 14 percent of the traffic on Abilene is from SEGP, 75% from I2 participants.

Http://netflow.internet2.edu/weeklly/20020218 shows the distribution of TCP flows.

They are interested in looking for a site to check for test flow data. OSU is using it to help find compromised systems.

Meeting adjourned.