From: Teresa Beamer <BEAMER@DENISON.EDU>
Subject: Minutes from October 10th OARtech meeting
To: OARTECH@LISTS.OAR.NET

OARtech Minutes
October 10, 2001

Introductions
Everyone introduced themselves.

Minutes were approved.

Whitepaper, Debbie Keller

There were no substantial changes, but the paper was reorganized. It now has a summary written by OhioLink and an added section on PDAs. Wireless is included in the local campus networking. Video conferencing has been added. Authentication has been added to Security. The bandwidth information has been added as Appendix A. Thanks to Bill Mayhew for his work in writing changes. Whitepaper was approved.

Patty Vendt, Revising Documents

Because of the length of time to get the paper re-written, we need to begin thinking about a new method of re-writing. Consider "How this white paper could be reviewed and changes made". OARtech has also gotten a request for another white paper on Video conferencing. If you have suggestions send email to patricia.vendt@wright.edu. We will discuss this at the December meeting.

Christopher Cook revised the OARtech charter to have it conform to the Osteer charter. They are trying to make all the charters to conform to the same model. What changed in the charter was the Organizational structure that was approved in June. The new charter was approved.

Ruth Crites
Announced a new Enterprise services manager to replace Larry Buell who has now permanently retired. He has been with OARnet for only about 3 months. He is a Graduate from Xavier, spent some time in the armed forces, then with a few commercial jobs. His charge is to develop an income-producing group within a non-profit organization.

You have received your OARnet survey. Please fill these out they do make a

difference in OARnet's planning for the future. Surveys were sent to the presidents, cio, Osteer member and OARtech member. They want input from multiple people at your institutions.

Snort, Bill Mayhew
The Lightweight Intrusion Detection System

Other detection system - the heavy weights - tend to be expensive such as statefull firewalls like Checkpoint's Firewall One and commercial network intrusion detection systems such as Network Flight Recorder that used to be freeware, but has gone commercial.

A good book on protocols, look for a three volume series by William Stallings. Some of the good web resources include Snort's own page, the Computer Security Resource Center's pages, Security Focus's web site:

www.snort.org
www.securityfocus.com
csrc.nist.gov
www.sans.org
www.cert.org

To setup your Intrusion Detection System (IDS) monitor you get a generic Intel CPU with an Unix-like OS with libpcap (e.g. red hat) and add the software - Snort. They used Linux as they were wary of the Windows operating system. Download the Snort software, then untar file, and compile it. The procedure will check your operating system and c, set up the configuration, and make the executables. Then you need to tune the rules.

NEOCOM use it mainly to check themselves. They setup their remote switch by using an x-over cable between two interfaces to feed data from one port into another port. They fed the traffic on a trunk line to the patched port. They then setup a third port in the management Vlan that connects to the local switch with the IDS station on it.

On the remote-switch:
set vlan 2 port 3/2
set vlan 2 port 3/3
set span 1 2/1 create

On the local-switch:
set vlan 2 port 4/1
set vlan 2 port 4/2

To help you watch your logs there are lots of Perl programs available. Snort can send a Windows pop-up via smb and use an MSQL database and can send information to syslog. Tip: keep systems in synch with NTP.

Snort contains rules and then has alerts that are in a hierarchical order. An example of a rule:

```
alert tcp any any - 10.1.1.0/24 80 \
    (content: "/cgi-bin/phf"; msg: "PHF probe!")

alert tcp any any - 192.168.1.0/24
```

Bill has found that snort doesn't always stay up and occasionally dies so you sometimes have to have the system restart the process.

What kind of person do you need to have to run Snort ? Someone who knows your network, can understand the scripts, and understands the output. Actual setup doesn't take a lot of time, rule development can be time consuming, and dealing with the logs and reviewing the information is very time consuming. Since this is a free product, support is best effort.

Comment from the floor: You could possibly use Sawmill to help you to analyze the logs as that is the most time consuming task. Another person has found that it's easier if you dump all your logs to one place using syslog. He uses a product that will dump the syslogs to a database.

The intrusion updates available on the Snort site are very timely.

Anita, OhioLink
Just a reminder that there are special requirements for OhioLink access. Check the OARtech website for recommendations http://www.oartech.oar.net/library/minutes/.

Radius & U, Shane DaWalt, Wright State

Radius is Remote Authentication Dial-In User Service and is defined by RFC2865.

Each client IP has a secret that the server knows so the password is encrypted with MD5. The server end ether allows or rejects the packet. The code is a request/response type with an authenticator. The client request is a random authentication field. Radius can be setup to do an access-challenge (e.g. secure id)

There are large lists of attributes defined in the RFC. These allow you to get information on the client and allow you to send configuration information to the client. The attributes are set on a per user basis on the server.

They had a problem with radius server - They used Apache and used the modAuthRadius routine. They found out that the Merit server they currently use cached the authenticator. This caused problems with the modAuthRadius routine. The moral - keep your radius server updated.

Radius accounting - RFC2866 updated by RFC28?? Lists all the accounting information that you can see to allow you find out what is happening with each of the sessions.

At Wright state they have a primary and secondary server with Cisco access servers and all create log files. Shane has a Perl script that takes all these logs to a central place and determines the access records. He uses scripts to determine statistics, and un-approved logins.

One reason to use a radius server is to consolidate the username/passwords for the users. When they were looking at LDAP and directory service, it was recommended that they use the radius with LDAP. They use it to authenticate an IP from the dorms and logs the authentication.

In your research have you had any experience with the Cisco radius server? The CCO indicates that they will work with Merit. Merit is extensible.

Note that Cisco is in the process of changing their Radius. OARnet is using it, but will be migrating off of it as it requires another database so becomes more expensive. They will probably be looking at Steel Belted Radius.

Bill Wilson, Remedy
Bill gave a demo of the web interface to the remedy ticket system. They have an interface to the remedy system so OARtech members can track their tickets. The web access will require your client number and the same password you use to access your OARnet stats.

The screen shows your OARtech ticket status, a description of the ticket, the create date and the last modify date, and the request id. It has links to allow sending information to the support center or access the OARnet website. The interface is java based and works with IE and up to 4.75 Netscape (he hasn't tested with 6.1).

Is this available now? Not at this time, as a management decision needs to be made to say it is to be available.

You will be able to go out and see what is active and the state of those tickets. Once the ticket is closed you would no longer have access to it. Some people commented that they would like to see a month's worth of historical information. Bill said it sounds like you need another tool: One to see the current tickets, and another tool to see a longer history. It was agreed that we would like to see the history thru the last month. They could build another tool that would allow you to see longer time period for historical information. Would like users to specify dates for seeing historical data, but all open calls no matter how old.

Would it possible to see the longer description? - We need to ask Gene about what can be made available.

Ruth Crites
Conveyed apologies from Paul Schopis and Jodi Santini that they could not be here to show the weather map due to a meeting on the west coast that had been rescheduled to today.

Patty noticed that only 3 sites have posted HelpDesk information on the notices.oar.net page. It would be nice if we could get more schools to list their HelpDesk information.

HumbleNet Update, Clifford Collins

They have been building a campus network in a test environment. They have it up and running with several devices including routers, firewalls, VPN, concentrators with IPsec, wireless, etc.... They were able to bring up the PDA wireless connections to access email and web.

Servers include www, SSL enabled e-mail, webmail, ldap, syslog, iss and nmap scanners, pgp certificate, radius, oracle, CVS, Samba, etc.... Next things to deploy will include 2nd www, ids, dialup, ipp printng, pager gateway, pki, traffic generators, etc.... A diagram of the network was shown.

They will be testing the home/office model.

Access to HumbleNet you need to send mail to ccollins@enss.net. The url is https://www.enss.net/humblenet/

To use the environment, you can be set up with accounts, etc... to look and

use the HumbleNet to find the best practices.

Ruth was saying that there are now 7 SEGP signed up. Cleveland State and Bowling Green are becoming full I2 members.

Oarnet does offer a newsread service. It eliminates having to have a local news server. They do it per class C at $100/month but will work with those sites with class B.

Spam mail tends to target group aliases that are not setup as moderated lists. It was noted that if you put email addresses as Gifs on the web pages, the web crawlers can't pick it up as easily. There are also web crawlers that pick up FAX numbers to send unsolicited faxes.

Some sites have received letters from NetPD. And have found students running Morbius and Aimster. These programs seem to be working even if the sites have blocked all inbound originating connections. These letters should be forwarded to the university lawyers; at least the lawyer should be in the loop.

A suggestion for future topics, a discussion about what ports sites are setting for policy of what is limited, and what ports (e.g. Packeteer policies).

Lunch

Scott Peters, Microsolved inc., Tripwire
Local firm that works with security consultants

In today's networking, with everything being interconnected, all servers across the world are vulnerable to a data integrity threat. Many of them are from within the server, because of administrator's limited time to watch and change configurations. For example, within Microsoft, due to a known administrative change, their server was down for 24 hours. After a security breach has been discovered via firewalls, and intrusion detection. Tripwire will determine any changes that have been made to the server, thus allowing you to identify whether a server has been modified. It keeps a record of the last good known state and can lets you know what has changed since that time.

What is integrity as it applies to data and network? All data and servers are in a known state at any point in time. Tripwire will identify changes from those states quickly and allows managers to restore the server back to the known state quickly.

Tripwire is based in Portland OR, with offices internationally. Customers range from larger corporations to small shops the need to know what is happening on their servers. The product is evolving from a security product to an integrity control product. Assuring that the devices and servers keep their integrity.

The time you have the most confidence in a server is right after you set it up, and before it gets put on the network. Once others start using the server you get integrity drift. Backups provide no assurance that the problems caused by something that may also be on the backup, and thus restored when you restore the backup.

Validation is run periodically. Incremental checks can occur as frequently as 1 minute, and complete checks can occur multiple times a day. This can provide protection from hackers, fraud, staff mistakes, etc....

At the beginning it was designed to look for changes caused by outside intruders, but has evolved to use with internal changes as well. As well as to monitor software for authorized use. It is also used in forensic cases to track how an intruder got to where they made the changes.

Tripwire for servers - checks for damage that may be caused by a hacker accessing multiple servers. For the example he gave, a company was able to correct the damage over a weekend instead of several days. It can also determine when an update or patch that may have caused problems.

The software is installed on the server you wish to monitor. Once it is installed it builds a database that is a snapshot of the files on the server.

Supported platforms: Solaris, NT, 2000 (professional and server), HP-UX, Linux. The control console runs on Solaris, Windows and Linux. It monitors file protections, type, etc.... For Unix it monitors 14 different attributes of a file as well as 4 types of encryption hashes. On Windows it can monitor different attributes. On NT and 2000 it will allow you to check the registry, keys, and sids.

To deal with files that are constantly changing, you can selectively check files (e.g. check that a log file only grows, not shrinks). You can select the type of monitoring you wish down to the file.

The Tripwire manager allows you to monitor and control multiple servers with tripwire from one station. You can remotely schedule the change from the manager (e.g. distribute the policy to each server). It allows you to check

different operating systems from one management console. You can have different types of managers. You can have 2 modes, active and passive. Active allows changes, passives allows monitoring and alerts, but no policy changes. The first manager to connect to the server becomes the active manager. Others connected are passive. Tripwire is working on being able to designate which are to be passive or active. Up to 25 machines can be monitored from one manager.

Tripwire has syslog reporting, and can specify what kinds of things to report to syslog and can use SNMP trapping for log messages.

The policies have been developed using a Perl-like language that defines the policies. They currently have a gui that will generate the rules. Tripwire will allow you to see that this file has been changed on these systems, as opposed to going to these systems and looking to see if the file has been changed. Reporting is available to give you summaries.

Tripwire will run on Cisco IOS v8 and above as well. It will do the same checking for the last known state to prevent un-authorized changes. It also can automatically download the last known state for a router that has seen un-authorized changes.

Tripwire demo is available freely from the web site. Educational pricing of $3000 + $1500/yr maintenance and each server is $300 + $120/yr maintenance. Wright State has found it really helps to determine where changes have occurred and are really excited to see the manager that allows you to see those changes in one place. This tool was traditionally free software on Unix, but with the commercial basis, it is available for other operating systems. Doing the policy writing is much easier with the gui instead of writing the policy yourself, but doesn't preclude you from accessing the policies directly. They also have the academic release for free. It is several revisions back, but if you can't get the money, then it works better than nothing.

http://www.tripwire.com - they are willing to come onto your site and provide a demo.

Clifford Collins,
ENSS is building a web based tool that allows you to input a web page url and a email address, and if that web page changes, they can notify you of that change. It will require authentication. How frequently it checks is user settable. It can help determine when web page vandalism occurs. They are also exploring licensing on lectures, that they have acquired mp3s on talks on

many different topics. They are looking on making those available.

Debbie Keller, is a professor for Akron University.
Debbie has been monitoring and running a Cisco academy network class from her pc at the meeting. They are currently doing CCNA and will be doing CCNP in the spring. They have all the material on-line. She has been monitoring and releasing the materials during our meeting. Today they have been taking quizzes, not the final test. Started CCNA a year and half ago. They are accelerated classes so they fit into an 8-week period. So they can get their CCNA in 1 year.

Gene Wallis, OARnet
When will the remedy web page be available?
Today's presentation was a beta test. They have received several requests. They expect to have it up shortly; they will be relocating it before it comes up live. They will shoot for November 1st.

Will it be possible to bring up historical information as well as currently open? This is doable.

On the demo screen we saw there was a field called "Short description" would it be possible to get more detail information on what had been done that could give us more information than just the short description? This is something they have wrestled with a lot. They have opened the system up with only mild security (client id, etc). The ticket system is more critical with a higher degree of the information that should probably not be publicly available. The diary information would need to be sanitized in order to make it available, so they would not make that available. They are planning to use the short description and to make that field as useful as possible. A suggestion was made to add box for next action, so we can see what they are waiting on. OARnet liked the suggestion.

Gene showed a diagram of the ATM switch layer as OARnet has them installed to show how complex the network has become. Its about a 35 switch SVC ATM network. The problem is it doesn't scale anymore. They have to look at what is available in order to increase the size for more bandwidth.

Then he showed the logical network for I2 that runs on the switched network. Their central router is a Cisco 7507MX with 7200's on the edges. This runs on a PVC mesh. Member schools with at least ds3 connectivity connect to this mesh. The SEGP members with smaller connections are peered via the OEB3 router into the I2 backbone. There are still grants available for the smaller institutions that may want look at NSF funding.

Last time OARnet checked about 40% of I2 traffic is peer to peer networking. The problem is we currently have packet shapers that control the type of packet. The problem is that there is no way to control the traffic specific to I1 or I2. We also can't get statistics to know the measurement of how much I2 traffic you have. Another issue that is coming up is how to determine the firewall needs (do you need 2 firewalls: One for I1 and one for I2?). Traceroutes and pings are too limited as test programs to measure the connectivity. OARnet has been asked to report how much I2 bandwidth the SEGPs are using. Currently there is no way for them to do this. They are using Netflow to look at the lines between the core routers. They may have to expand that in order to produce the type of reports that will eventually be needed. This can impact the routers as well as the collection boxes and what to do with the data that is collected are all issues that need to be determined. In summary, they can report I2 traffic statistics only if the site has dedicated access to I2. Currently they need to work through problems with stats on the individual PVCs. The next step is to get the stats on the trend site so you can see the I1 and I2 traffic statistics.

New business - Packeteer is having some performance problems. Half duplex on video conferencing, packet shaping, I2, your going to have problems. You need to go to full duplex.

Meeting was adjourned.