OARtech Meeting
June 9, 2004

Meeting called to order by Tim Guenhagen at 10:05am

Nominations for OARtech Vice-Chair
Ransel Yoho, the current Vice-Chair, will be Chair beginning with the next meeting.

Current nominations include Mike Pincent.   Mogli Assor did not agree to the nomination. There were no other Nominations. Nominations were closed and seconded. The new Vice-Chair is Mike Pincent.

Miami - Testing Perfigo, looking to roll it out to dorms. IDS Product they use is Red Siren. Also have Tipping Point to sandwich the firewall to verify traffic through the firewall. They have a PIX 525 - they have had connections cause the firewall to crash. Other major projects include moving to new network structure in their resnet. They are moving from shared to switched equipment with Tipping Point between the resnet and rest of the campus.

Are you going to use the Perfigo agent? They have great consternation about putting an agent on the machines and about the support issues that might arise. It is unlikely that they will require the client.

Denison University – They are currently looking at Perfigo and Bradford Manager. Not sure which way we will go. Currently using Snort and sending logs out to be analyzed. Their 3 main projects this summer are Email server replacement, LANv2 which includes a major Novell upgrade and network security which include firewall upgrades and security review.

Bowling Green - Wireless installation

Belmont Tech - New Information Systems and will be upgrading infrastructure. They are wiring facilities with cat 6 and considering 1 Gb to the desktop.

Kent State - Perfigo trial currently running and they are happy with it so far. They will probably not use the client, but will use the scanning. They like the flexibility of the product. Just putting in a luminous portal and upgrading backbone to 10Gb

Dayton - New CIO so they are going through a Re-org. They are splitting the Resnet from the rest of the network and will be contracting it to a 3rd party (looks like cable company).   They will be putting Tipping Point in front of each of the Dorm areas.

Rio Grande – They have a new MIS system from Student Space and are rebuilding their web site. They did talk with Perfigo, but felt the in line box would not work for their topology (dual gig links from 33 buildings back to the campus main switches). They are looking at TFN to connect to other organizations within the county. OLN gave out grant from WebCt to Vista edition.

Wright State – They will demo Perfigo. Wireless is to be installed. They are looking at clean machine, or other scanning systems. Tested Bluesocket but found it didn't do what they wanted, so will see if Perfigo will do what they want.

Ohio Northern – They are currently in a Perfigo trial and happy with it so far. They are looking at implementing Snort for IDS. Summer projects include increasing wireless areas, and installation of a firewall blade in a 6509.
They will be getting away from directory mail routing to LDAP and are currently using Luminous LDAP for portal authentication.

Case Western – They are upgrading wireless APs from A to G and are in a Peoplesoft rollout.

Sinclair CC – They are rolling out McAfee Orchestrater (sp?), and have just installed another product from them. Testing policy based networking from Enteresys (sp?) using Dragon sensor to set policy to the port level. They are doing a SAN Upgrade. They are using Microsoft's SUS and are very happy with it.

Xavier University - Started trial with Perfigo, and found some problems with network. They have to move trunk lines from ISL to dot1q.

Clark State CC – Using Quava mail system and having problem with sending attachments. They are putting in layer 3 switches to be able to use VLAN segmentation.

Bluffton College – For anti-spam they are concentrating on Barracuda. They are migrating to new hardware for their web server. They are not using IDS at this time.

Lorain Co CC – They do not have residences so IDS not as important. They are putting in a generator for the computer room. They are looking to implement Bluesocket or something similar to control the wireless. They are adding a link to the hospital, upgrading their firewall and experimenting with IDS.

University of Toledo Distance Learning – They are upgrading the hardware in the server farms, installing wireless to the home campus, reviewing video conferencing policies and implementing load balancing, failure over, and redundancy for servers.

University of Toledo – They are testing Perfigo and Bradford Campus Manager, upgrading the backbone with redundancy, and replacing switches in dorms and academic buildings. They are also looking at Tipping Point and Source Fire.

Heidelberg College – They have a 6509 firewall blade to be installed. They will not be looking at Perfigo. They are trying to roll out and move from static IPs to dynamic IPs in dorms and moving servers to new platforms.

Columbus State CC – They have Cisco IDS blades in 6000s with sensors one the outside, but not implemented them yet. They are moving from Cisco AP 1200 to an AirSpace solution, and replacing 3548s with 3550s. Student logins are authenticated against Novell Edirectory and integrated with portal and email to provide single sign on for this next year.

University of Northwestern Ohio – They have an ERP system upgrade, and are putting network into the dorms.   They have upgraded to new exchange version and are looking at Barracuda for an anti-spam solution. They are upgrading servers from 2000 to 2003. They have been building scripts to automate account creation, implemented Web sense, working with SUS to help with patches and implemented a 2003 server for students.

University of Finley – They use DeBreese (?) in student labs to re-image lab machines. They use Spam Assassin. A SAN was approved.

Cuyahoga CC - Backbone will be upgraded with Cisco equipment and they are testing VoIP in the closets.

University of Akron – They are installing UPSs, a Peoplesoft upgrade, moving from Campus Pipeline to Peoplesoft and 3 new buildings are coming on line.

Tiffin University – They have a new technology center with 10 GB backbone. They are looking at Perfigo. They will be moving the server farm to the new technology center.

Antioch – They have a major network upgrade with OARnet. They will be upgrading the Datatel server and adding wireless capabilities. They are playing with Snort.

Kenyon – They have wireless in all residence halls and in public areas, are putting in a Perfigo box trial and will be looking at intrusion protection in the fall.

What are the rules for 3rd party entities on campus doing work for the school? If they were offering services and charging for the services then you would need to talk with OARnet, but if they are doing work for the university then it is not a problem.

Who has used Bradford Manager? Some considering it, but no one has installed it.

Who is using Cisco APs? Many. There are some sites using other products. Is anyone using the module for the 6000 to control the AP? No one has looked at it, Miami is about to.

OARnet Updates
Linda Roos
At the last meeting there was a request for a portal to the tools. They are working on that and will be presenting it at the August meeting. Osteer did approve the fees structure and have made some changes as to the fee to align them more with the bandwidths being used. Invoices have been mailed out. Call Linda if you have questions. They are still waiting for pricing from SBC with OC3 pricing. In order to take advantage of the pricing when they get it, they will have to sign a contract. So it will still be some time before it is available.

Will SOMACs pricing for T1s hold? Probably.

TFN - Dennis Walsh
Turn-up targets- Backbone scheduled to for completion June/July 2004 and all universities and colleges will be on the TFN backbone by fall term. All 15 research institutions will have GB connections by fall term.
41 of 42 fiber spans characterization has been completed.   Akron - Canton fiber scheduled for 6/7/2004.
You can keep track of the install by watching the map on the TFN web page.

The splicing will be completed between Akron and Youngstown by 6/10/2004.   All TFN POPS and ReGENS have been completed and passed the site surveys.
All Cisco Routers have been installed on the backbone.
Several segments have been lighted and tested. Core ring is scheduled for optical installation with a target date of 6/21/2004. Possible tours of the Neilston pop after today's meetings.

They have hired a new optical engineer.

Ring 1 and 2 are scheduled for optical installation by 7/25/2004. Conversion equipment for connecting current schools to new backbone has been ordered. Equipment installation for schools should begin 6/21/2004 and complete installation by 7/28/2004. Notice of site requirements went to schools 5/24/2004.

Last mile committee – The RFP is completed. They are still working with SBC to get that contract settled. Some vendors gave a quantity discount and standalone discount. OARnet is trying to find out how much they need to order to get the quantity discount. Schoolnet is having problems with funding so is delaying they're installations to the A sites. They are looking to install during the 2004 to 2005 school year. Their funding was recalled so they are going to have to determine how to balance their dollars and are probably delayed 6 months. If you want to follow the project closer you can get access to their electronic management tool. Send message to Dennis Dwalsh@oar.net to the login info.

Stat Scout
Paul Schopis

Go to statscout.oar.net login with <call support services for passwords>.

Your get the network monitor console. They are converting names on old equipment to a new scheme. The new scheme uses a code for city, code for type (a - atm, r- router, b-ethernet), then a code for the pop (q-quest, o-oeb, s-sot, r-rhodes tower). You click on the name of the unit you want to look at and you can see the stats for that line. You can look at errors, load, utilization, etc… to see how your line is running.

TFN - Schools that will be receiving optical equipment to connect to the network (currently doing 7 or 8 schools). Basic requirements include physical requirements, environmental requirements, and power requirements. The equipment does require DC power so those with just AC will have to get a rectifier. Tony Eller is their new optical engineer. He has been doing some of the re-testing. Gene Bassin has been very instrumental in coordinating the installation of TFN.

After the meeting they can provide a tour of the Neilston pop at 251 Neilston, Columbus. The tour will take 30-40 minutes.

Question from floor on how the cut over will occur. Gene indicated that they will not cut over any end sites until the backbone is up. They will leave the existing lines up until new lines are up and stable and will probably do these during maintenance windows.

Access to Looking Glass?
https://www.eng.oar.net/lg/
They have noticed some problems between Safari and Looking Glass.
Contact the support services for the password.

He did a short demo of Looking Glass.

Lunch

Tipping Point Intrusion Prevention
Tim Connolly

He discussed some historical aspects of security and virus protection. A 1972 report discussed that buffer overflows were some of the main problems and breakins. Network security in 1990 used ACLS with shared media, and one large broadcast environment. 1995 had more deployment of firewalls, and switching was put into place. Firewall blocks access to ports, but have no protection with attacks from ports that are used for active protocols. Firewall worked at layers 3 or 4. Some are starting to look at packets for signature type traffic. In 2000 you start seeing IDS being deployed in the networks to find attack traffic. The problem is having so much information and lots of false positives. The attacks still got through and you still had to manually track down the problem.

There is a need for better security. Firewalls don't stop "good" protocols, IDS technology has become overwhelmed by the growth and internet threats have increased. Evolution of LAN security is to split your network in to security zones and to keep malicious traffic within the zones. Traditional IDS doesn't prevent the attacks from succeeding and if using TCP RST can be used to attack other sites with spoofed IPS.

IPS - Intrusion Prevention System

You must do the blocking before it can do harm and it must be an active part of the network. Network based requirements must run with switch-like performance, with high availability and use precise attack filters. It requires specialized, high speed hardware.

Tipping Point's Unity One technology is specialize hardware. Intrusion detection is a young technology so they use field programmable gate arrays so they can be upgraded in the field. Their suppression engines moves through a flow state table for normalization to multi-flow analysis to determine the fragmentation and re-assembly of fragments and run the packets through a 7 layer packet flow inspection with programmable filters. The flows are classified and marked and then can do traffic shaping and rate limiting. He described the pieces of the system and how it works in their box.

Where do you want to put an IPS System? You can put it front of the firewall to protect the firewall. This was used to prevent too many concurrent sessions from blocking the firewall. Often the IPS out front of the firewall is blocked, but not logged because it has too much data. Lot of sites will put it in back of the firewall and in front of the DMZ, in front of the Server environments and in front of “Semi-trusted networks” to zone the type of traffic. You want to put it between the centralized layer 3 core and the layer 2 distribution.

With traditional security model for threats you have to find distributed information to solve the problem. With IPS you can centralize the information to find out where the threat is coming from. They have filters for exploits, vulnerabilities, DDOS, etc…. Attack filter types include application, protocol, and traffic anomalies as well as signature and regular expressions for trojans. They try to write to the vulnerabilities first, then to the protocols, and then to the exploit. Different filters types are used for different types of attacks. The types of filters they have are Vulnerabilitiy (e.g. RPC DCOM Buffer overflow), Exploit-Specific (Blaster, Nachi Worm), Policy (block DCOM Requests), and Protocol Anomaly (Remote Procedure Call Verification). The recommended setting enables filters across all categories that are guaranteed to be suitable for any environment. This allows out of the box to find only the malicious traffic and not block "good" traffic. The system administrator can then tune the system for specific problems over time.

You need to have a management structure so that you can have central management, but be able to have different types of accounts (operator/helpdesk access vs sys admin) and be able to push down policies by segment.

When you deploy a box, it is in line, how does it act on the traffic? You can set the action to any of several settings (block/notify, permit/notify, etc…). If you have it block, it only blocks the traffic that fits the filter, not all the traffic from a specific IP. So you could still do valid application traffic even if there is infected traffic from the same IP with the same protocol. They are also working on a product to block port scans. You can then "blacklist" an IP for a known time period. The product is targeted for November.

If you identify a new vulnerability how do you update your systems? They take raw intelligence feeds; they then do a vulnerability analysis for Sans’ @risk report. For the top 5 they do a vaccine creation and push it out to Akamai's servers. They push the updates out to their boxes if the site has them setup to do automatic updates. Microsoft is a customer for 2 of their divisions.

For blacklisted users can they be redirected to a web site? Has been requested, but doesn't know if it will be there in next version.

Ransel Yoho was welcomed as the new chair and received the chair vampire tap. Tim received, as parting gifts, a mobile pen drive and the traditional socks.