OARtech
April 14, 2004

Meeting called to order at 10:10 by Tim Gruenhagen

Today we are looking for a nomination for Vice Chair for OARtech. The chair does the coordination for meetings and runs the meetings.
Nominations:
Mike Pincent
Mogli Assor

Introductions - Questions - Do you authenticate user access to the network? Do you track MAC addresses and/or tie them to user IDs? Do you enforce any policy as part of a login process?

Miami - no authentication at login time, or machine address tracking - only track mac address to port. They have shared segments in the residence halls. Will be installing switch and wireless in the residence halls this summer. Will be using Blue socket for the lowest common denominator login. Installing 802.1x as well this summer. They do IDS with tipping point.

Denison University - We use Novell logins in the labs and on main campus. In residence halls we register mac addresses. With wireless we use Bluesocket.

Shawnee State -They are an active directory shop. They require everyone to login against the directory. To enforce policy everyone has to login.

Kent State - Will be doing a trial with the Perfigo box for authentication. Will also be using their scanning product. Would like to put the Perfigo box in the residence halls to keep track of the mac addresses. They do use IDS at the border. The authenticate wireless using Bluesocket in pilot project.

Owens CC - looking at wireless and looking at Perfigo and Bluesocket. They are using "honor system" for visitors. They are also a Novell shop.

Bowling Green - They use a Netreg type system for mac registration for wireless using Bluesocket. They were using Cisco IDS, but are now looking at other products at this time.

NE CC - They use User id and password for resources and are looking at active directory.

Rio Grande - everyone logs in against active directory. In dorms use Foundry to lock mac addresses to ports. Do not register macs at this time. Don't have wireless at this time, but looking at policies.

DeVry - They have active directory authentication, wireless authentication via mac address registration. Wireless cards must be registered at the helpdesk.

Ohio Northern - Wired network using registered mac addresses, looking at Netreg. Looking at Ateris (?) for pushing software out to users. No active ids.

Wright state - They only login at labs with Novell, users aren't required to login at desktop but they manually register mac addresses for Novell access. Students must login through the firewall in residence hall. Do use IDs. Currently looking at a new security strategy.

U of Dayton - They authenticate wireless with Bluesocket. Their wired systems use mac registration with Netreg. They are a Novell shop and when people login they scan systems for vulnerabilities. Use Tipping Point IDS. They are getting ready to split dorm areas from academic area. They are looking to use Cisco's registration tool. Hoping to go to 802.1x in the future.

Oberlin - Transition right now. Historically completely flat network, and registering mac addresses. Attempting to implement more routing to separate student net from rest of campus. They have wireless on campus are looking at authentication. They have 2 directory systems: Active and LDAP. They do have Netware as well. They're environment is 50% Macintosh and 50% Windows PCs.

OARnet - How they handle DoS attack - When a link comes up on monitoring as full, they check netflow statistics and then contact the source and destination of the attacks. They are using a national program that keeps track of compromised hosts and attack sites. 70% of the performance problems are generally due to someone doing something nasty. Cisco has been in the past putting ports that can handle more traffic than the card in the device so you can overload the fabric of the equipment.

There was some discussion on DoS attacks and the signatures of them (e.g. lots of little packets being sent to cause the buffers to overflow). Tools that OARnet provides to help find problems are Netscout, and Netflows. If you can find the address that is attacking, OARnet can block that address. Problem with this is the spoofed addresses.

How long are the blocks left in place? They will contact the sites, then leave in place until the site lets them know that they have corrected the problem or they will leave it in a place for a short time and remove watching to see if the attack continues. You can see your own tickets in remedy allow you to see the status of your tickets.

Members have problems finding the tools and the passwords necessary to use

those. OARnet indicated they will put a link off the support pages for getting to the tools and will distribute the necessary password.

OARnet is looking at bringing up a pilot to help with security issues.

Heidelberg - They are an all Cisco shop and redid all wired a year ago. Users log into the NT domain. Not doing wireless officially right now. They will be deploying wireless this summer. Not sure what type of authentication they will be doing. They feel we've made it too hard for students to connect to the network and they would like to make it easier.

OSU - Residence halls don't authenticate. Propose to have them authenticate to the Kerberos system same as they do in the public labs. Residence halls are rate limited. College of Business does register mac addresses.

Kenyon - In the dorms they do not require authentication. On the rest of campus, they use Active Directory.

Sinclair - They authenticate to windows 2000 to servers. They don't have any open access ports, but don't have anything that would prevent a student from unplugging lab machine and plugging in their own laptop. Just completed a wireless RFP. AirSpace was selected purchased from Tangeman.

Case - They register MAC addresses to allow systems a public IP. Wireless goes into private subnet then must authenticate.

Upcoming meeting topics Tipping Point presentation in June? Security is always a good topic. A make and take it workshop for security? Flow tools? Support portal? How to look at your own netflow data? Review the tools that are available from OARnet and do it tutorial style? Tour of new facilities?

OARnet updates
Paul Schopis - Engineering update

CPE - router for the core - Customer Premise Equipment
LDP - label distribution protocol
PE - provider edge equipment
If the packet is labeled it is an I2 packet - if no label then it uses standard routing.

Will compare new design and old design. Old design was an ATM network with equipment at each pop with a router. Used BGP for router difference between I1 and I2. In the new design they wanted to reduce the routers and fees associated with the network. Would like to leverage MPLS in the network. They have to have CPE at the edge with a provider edge (PE) device and a provider core LSP router. They can collapse the P and PE to one device. I1 will use

standard routing. I2 will use label switched with BGP. The new architectures uses PE/P, CPE and GigE aggregators at the campuses. You need CPE device that used BGP for multihop and LDP exchange with the core or GigE switch. The smaller campus' traffic can be taken back to the pop to a router. This allows them to have just 3 devices per pop.

On the national level they are looking at HOPI project. HOPI tries to leverage the optical, layer 2, and layer 3 domains to make use of appropriate use of technology to achieve the best results at the best cost. They are looking at the idea that the service to the campus can be what makes the best sense, as long as it is the same or less cost of installing fiber.

How soon? They hope to have the backbone lit by June with legacy pops connected to the new pops and leveraging it where they can. Until the school is directly connected they will have to put in the CPE to aggregator model. By June they will have the GigE switch at the legacy pops to feed the campus via the current connection method. The equipment to be deployed to the campus will depend on the bandwidth needed for the campus. Sites need to begin looking their needs in terms of bandwidth, jumbo frames, Ipv6, etc.... If you are an I2 school you need jumbo frames, and all bells and whistles. Can probably aggregate 500 MB to each GigE port so will have to look at the needs of the campus to determine the intelligence and bandwidth needs to determine the equipment to be deployed.

Can OARnet get us a list of questions as to what the needs of the campus are that will effect the selection of the equipment?

Dennis Walsh
TFN Status
Fiber Characterization 34 of 42 Spans completed and passed. This is testing to determine the conditions of the fiber they have purchased. After next week's characterization will bring up the 3rd ring. After this next 2 weeks will have all the fiber characterization completed.

Fiber construction projects scheduled for completion by 4/23/2004. They will bring everyone onto the backbone at the same time. Site limitations will basically be their uplink. Site Surveys has been done for 32 of 37 pops and regens are ready for installation. Core routers have been installed and optical switches have been installed on 3 of the major routes. Core ring, ring 3, ring 2, and ring 1 are pending installations. Targeted to be completed by 5/31/2004.

Conversion equipment to provide connectivity between the old and the new network to all schools are planned to be turned-up in June/July 2004. Planning to use GigE connectivity to convert between old to new. As schools connect directly to the new locations they will phase out the old connection

from the old pop. Currently have fiber into 11 schools. Equipment installation these schools should be completed by 6/28/2004.

Last Mile RFP update - The RFP has been completed and reviewed by committee. They selected the lowest cost options and vendor notification is done by OSU purchasing. The list of options should be to schools 4/16/2004 per purchasing this morning. Letters have been sent to the providers. They will be sending the total spreadsheet to the schools via Osteer and OARtech email lists. Under the new OARnet port fee structure you only pay for the amount you use. The port fee will cover the commodity network, the remaining bandwidth on the line will be for Ohio intranet. SEGPs must purchase the amount of I2 they will use.

Linda Roos
OARnet fee structure for the new network was presented at Osteer and was passed. The new structure includes the following pieces:
Port fee - covers the backbone in Ohio - charged for capacity
I1 fees
Academic services fee
I2 fees

There is some discussion about making the entire state SEGPs for engineering reasons and the costs of the engineering. Because of segmenting the network to handle the SEGP the costs of the network was must higher. The traffic that stays in Ohio is much cheaper then traffic that goes to sites outside of the state. We need to be thinking about how this can be leveraged. For example - OhioLink is currently Ohio I2 now for these same reasons. Under the new model OhioLink will be moved to the Ohio intranet.

Next Osteer is in May and they will be again reviewing the pricing structure.

How does campus BGP affect the Ohio Internet? You are looking at three networks instead of 2 that will need to be controlled (some sites currently have 2 Packetshapers - 1 for I1 and 1 for I2). Can the Packetshapers see tagging so that it can see what network the packet came from?

Lunch

Linda Roos distributed pricing spreadsheet for the fiber network. Invoices have been generated and are currently being reviewed and will be sent out to the sites. The sites need to then get back with discussion on what you need for next year. Official invoices will be generated in June.

Perfigo
Sales representative: Justin Cheen
Engineer: Atif Azim

Presentation will be posted to the OARtech web site.

Perfigo provides a complete end-to-end solution for wired and wireless for authentication, authorization and interrogation. They help with the identifying the problems and then help in correcting the problems. Enforces the policies and the tools to help users to use the tools available. Perfigo is a software company. They can provide on a hardware platform like an appliance if you wish, but you can also purchase it as the software to install on the hardware of your choice if you wish.

Core/Required components: SecureSmart Server, SmartManager, SecureSmart Client, Clean Machines, AP Management. They will be demonstrating these pieces today.

Student/Faculty connect to network either wireless, or wired. User logs in using username/password but system is checked and cleaned and cleared of vulnerability. If vulnerability is found the device is quarantined on an isolated subnet. The system uses roles to determine the resources available to the user.

Can be deployed on DELL, HP, and IBM hardware. It has a very flexible configuration. Can be set as a gateway or not as you please. It is agnostic to hardware and does not care if connection is wired or wireless. Does support 802.1q trunking on untrusted ports. Automatically changes the VLAN based on whether the system is cleaned.

Do they support multicast traffic? Will allow multicast traffic through.

He did a demonstration of SmartManager. You can have control of access on a per person basis. Also provides a guided environment to fix their machine. Authentication supports kerberos, radius, NT, LDAP (v2 or v3), 802.1x, and Windows. Can setup a default role that is applied if the user does not fit any of the roles. Once you create the authentication mechanism, then you can setup a user and their roles based on your policies. You can setup any number of roles you want. You can also have quarantine roles to allow them access to resources to fix their machines. It also can provide IPsec terminations. Can redirect users to URL based on logins and be blocked, etc.... You can allow or deny roaming.

Showed an example of a student role. It is very similar to access lists based on TCP/UDP ports with source or destination addresses. There is a priority based on the order of the rules.

Can the policies be scripted? It is a JAVA based architecture that is accessing their databases. It is possible to script to the databases, but it

is harder to do then the web interface. It is better from the support standpoint if you make changes through the web interface.

You can do bandwidth restrictions based on role and can timeout sessions. Can do a heartbeat timer with scans and pings as to logout users once they have disconnected.

You can source your LDAP attribute to map user to specific roles.

Clean Machines - Interrogation
If you machine is on the list for a clean machine the system can be forced through the clean process. Anytime vulnerabilities are discovered, you can clean the list and force machines back through the clean process. You can also force the machine to a URL to explain what has happened. 2 aspects of interrogation: network based and client based. The network based scans can be done based on the roles. Can do different scans based on the type of systems. They have the standard Nessis plugins and you can import your own and the standard Nessis plugins that become available. They also provide a site for updating the plugins. They determine the OS based on the tag on the browser. You can setup your own profile for vulnerabilities by selecting which scans you want done and by selecting which vulnerabilities will force the user to clean their system. If the users are determined to have vulnerabilities they are put in a quarantine roles and then put where they can download the correction for the vulnerability.

Can also have a policy page that people must click on accept or decline a policy.

Perfigo does have a client available for them to access the network. You can require the client based on a role. If a user logs in and has a role that requires the client they can be given the option to download the client and install it on their machine.

You can require users to upgrade their system with patches and provide downloads if they don't have it. This is available for windows only at this time, but they are looking at adding Macintosh and Linux in the future. You can have registry checks and tell the manager how to check for the vulnerabilities. You setup a package with the check necessary and the parameters to check (e.g. file existence, registry keys, etc...). You can setup the checks based on the roles. So students could have different checks than faculty/staff. You can setup a test role to allow a group to test a check before rolling it out to a whole campus.

They had a user from their site login to provide a demonstration of what a student might see. You can customize the login page. The user logged in, checked authorization and then showed that report (this current client had

just some servers running). They provide a redirect to informational pages and, since this was a clean user, it gave them the option of decline/accept the policy. The machine was logged into a clean machine list. Note that personal firewalls can prevent the scans from seeing anything, so you would need to have the client on the system to check those with personal firewalls.

They can log to a syslog server.

They had the user connect and login to a faculty role that require the client and if they did not have the client it gave them the option of downloading it.

Showed the client on the system. There is a limit to the customization of the client. What is the mechanism for the client to communicate? Detects the smart server, and then downloads the checks. Authentication is done over SSL. If you don't make all the checks it puts the system into a quarantine role. It goes from the first package to the next if multiple packages are needed. Once the package has been downloaded it completes the scan and assigns the end role to the client and lists the machine in the clean machines list. You can also get a list of the packages that client downloaded.

If the user is coming in from a wireless site, you can also see the SSID and access point they are coming from. They get this information from the client. They can setup the untrusted network as a NAT gateway, virtual gateway or use a real-IP gateway.

They also have a wireless IPsec client available. They demonstrated the wireless client. You can have the role enforce VPN. The wireless client is available for Macintosh and Linux as well as windows. It shows the networks available as well as rogue access points and will not allow a login to the rogue point and the information on the rogue point is sent back to the manager. They also support PGP. This allows the wireless clients to be used as your rogue access point detector.

They find that they can get 2000 through one box.

What kind of response have they gotten from the end user on the delays and the scans? At one site they used this when users returned from spring break, they did 3 checks and the users had a positive response. Perfigo is trying to make security for the end user "dumb proof".

What about game systems? What happens? You can allow based on mac address and can do a scan and then you can manually put it into a pass through list.
The other approach is to have it registered and put in the pass through list. The same would apply to printers and other non-pc network devices.

If I'm rolling this out tomorrow do I need to upload the static listing of IP addresses? There is an import option for importing mac addresses into the system. You can setup a printer role.

Is there a way to escalate a login? Can you change a role after they have been on a lab machine? Initially can be in an un-authenticated role then when they login and get scanned and get authenticated role.

You can trial the solution. Contact Justin if you wish more information at Justin@perfigo.com.

Meeting was adjourned at 2:30pm