OARtech Meeting
June 16, 2006

Meeting called to order by new chair, Mike Pinson from Shawnee State.

Introductions

OARnet updates
Paul Schopis

Three sites are coming up: Hebrew Union College, John Glenn, and Oberlin. Oberlin has their serial card in place and is now on their new line. University of Toledo and Medical College of Ohio have merged. They must restructure and function as one, but have had some problems with the integration. They wanted to be able to control their internal campuses and both UT and MCO are on the same Toledo ring. It was agreed that UT will be operating the ring that services the new UT structure and OARnet will operate the portion of the ring that services BGSU and eTech.

The only public schools today on TFN are Toledo Public and SCOCA.
eTech is having some problems getting fiber into their POPs. They are hoping to have it up by the end of the summer. Oarnet has been contracted to help provide eTech with services. eTech is trying to separate from the OIT network and have found it is a significant amount of work.
Public Broadcasting has brought up WVIZ, WTGN, WOUB, and WOSU on the TFN.

The Merit direct interconnect planning is continuing. They are meeting with MERIT, Level3 and Fiber Co tomorrow. They feel working with MERIT is beneficial as they can back each other up and provide peering. There is some question at this time on how the national consortiums are going to move, so they feel that building peering relationships with MERIT, NYSERNET, SLR, and several other organizations, we will have national connections even if the national nets go away.

There are some DNS issues occurring and it seems to be a subtle form of DOS attack. It causes sluggishness in DNS responses. Oarnet is looking at the best practices and are considering in performing recursive lookups only for Oarnet clients. If you see any problems with this approach, please let Paul know.

I2 and NLR merger talks have broken down again. NLR constituency wants Abilene to peer with NLR. The key component to peering is that
it be mutually beneficial, and that may be lacking in this case.
These 2 organizations will be going into a competitive stage.

NewNet is the new Abilene and will be using dynamic provisioning.
They are looking at putting commodity traffic over NewNet. Internet 2 will maintain the routers, but will have a provider maintain the fiber across the nation. They will have a full layer 3 service with OADMSs at every Gigapop. They are looking at reducing the number of routers in the new structure, but maintain redundancy. Paul showed a map of the NLR and I2. Paths are the same because both are using the same fiber provider. Oarnet is taking a neutral policy in hopes that both organizations will come back together at some point.

How will these issues affect the SEGP schools? The problem is not technology, but governance related. Oarnet is only an affiliate member of I2; the primary I2 schools are the members. The I2 board are University presidents, and NLR board is largely regional network CIOs. The question on what will happen with SEGPs has not been discussed. It's hard to say how the SEGPs will shake out.

Is DAS shutting down the video connections? There is a split between eTech and OIT (aka DAS). There were some ancillary issues that are
being dropped. Effectively as of June 30th, you will not be able to
talk to eTech via DAS. The ATM to IP bridges that DAS ran before will be going away. If you have a service with OIT to talk to local K-12, you need to talk to them to determine how your site will be affected.

EDUCAUSE Security Professional Symposium update Aaron Laferty, Cal Frye, Bob Beer, Brian Moeller, Dan O'Callahan Slides are available at
http://www.osc.edu/oarnet/oartech/presentations.shtml

Aaron Laferty
RINGS
Registration service call RINGS (ResNet Integrated Next Generation Service). It was developed at University of Kansas and written in JAVA and has integration with Remedy Trouble Ticket System. It provides ANSR DHCP (LDAP based JAVA DHCP service) that understands the operating system of the end station. The web site has authentication, activation, policy info and a quiz that you have to pass to get activated. It generates a receipt with the activation code. It checks the stations' update configuration, patch levels,
anti-virus(AV) (they use Sophos), AV scan, detects the IP and configures and enables the firewall. On Mac and Linux, it does OS check, AV install and IP address configuration. The security measures used includes Nessus scans, IDS, IPS, and all the data is fed in to their event processor. The admin tools looks at your LDAP attributes to determine whether you can use the administrative interface.

Resouces:
University of Kentucky Resnet: www.resnet.ku.edu NTS Website: www.nts.ku.edu RINGS Source Forge: www.sf.net/projects/rings ANSR Source Forge: www.sf.net/projects/ansr RINGS presentations: www.resnet.ku.edu/opensource

If you are looking for a registration system for your campus, this might be good to look at.

Cal Frye
Baylor Overview
Baylor is an institution with 13,800 students and 2000 employees.
They went through a risk assessment primarily for customer relations and to keep themselves off the news. They chose to go to an outside vendor to get an unbiased look at their systems. They looked at 3 types of vendors, Tier Three is relatively inexpensive, but is something that anyone could do. Tier 2 gave them more information, and gave them more detailed info on the vulnerabilities that were found.

The main lesson they learned is that there needs to be trust and confidence in the firm doing the assessment with non-disclosure agreements. Be sure to have a point person to interactive at times with the vendor. You don't want everyone to know who they are their because of testing social engineering situations. The social engineering was scary stuff and takes a while. They helped to
prioritize the vulnerabilities and look what remediation was needed.
They found the assessment was worth it because it got the attention of the right people and freed up some funding. A multi-year agreement with a single vendor can reduce the overall cost of the assessments.

BOTHerds
The University of Albany in September 2004 had over 800 systems booted from their network due to BOT infections. To solve this problem, they decided this was largely an education issue. To present it differently, they crafted a story that students can identify with and understand where the

risks the effect them might be. They made it attractive with a series of brochures created. It is hoped students would trade them to get the whole series. Student had to pass an online ethics and security test to verify they had read the material.
In 2005 they saw half the problems and an increase in the registrations.

They also took some Technical measures that included using a packetshaper to identify IRC traffic with a whitelist of servers.
Scan IPs not on the whitelist and made sure IRC was blocked, collecting banners if open. They also found that by finding the BOTs Command and Control (C&C) IP helped. The IP based ones are easy to find, to find the DNS ones you have to log your DNS queries and then look for those systems that are really pounding on the DNS servers.

Resources:
Conference site: http://www.educause.edu/Program/8355
Botnet slides: http://www.albany.edu/~ja6447/educause/
University Security Operations Guide: unisog@lists.sans.org
(http://www.dshield.org/mailman/listinfo/unisog)
SECURITY@listserv.educause.edu
REN-ISAC, http://ren-isac.net

Cal is on the program committee for this security conference. He is interested in any ideas for things you would like to hear about. They would like to increase the amount of participation from the smaller institutions.

Bob Beer
He found this conference very interesting, with lots of attendees from Ohio. It's a good chance to see the people who names you see on the lists.

SunGard Security in Banner BOF
SunGardHE should not be used for identity management as there are several security features lacking. Identity management is expected to be built into the network infrastructure. Some of the feature requests include Encryption, Change Tracking, Field level audit trails, product performance and these will affect the performance of the product. To support regulatory needs, you must document any process that touches data, which does transformations and should be looked at in the pre-installation phases of any project.

Some of the miscellaneous Banner discussion included these security issues:
The best/recommend practices are missing, sensitive data is not masked, the auto-generated ID are sequential, third party applications access via privileged accounts which undermines the Oracle security, and the PINS are visible in the GOATPAD form.

Identity Management
This is the authentication and authorization piece of the network.
You need to look at the identifiers and replace SSN. Purdue went with 2 groups of 5 digits for their ids. It has no value except at Purdue.
The provisioning was by department and authorization was done via an ID by Role matrix. They talked about including web training to increase user awareness and require a check of the user's "Level of assurance" before allowing access to a particular resource. The reading policies and training increases the user's Level of assurance.

Payment Card Industry and DSS
Data security standard was set in 2004 and it applies to everyone who processes credit cards. It applies to any equipment attached to the card processing environment. So if you have a computer on this network, you must meet the standard with the computer as well. The

compliance date to the standard was July 2005, but was not very well publicized. 2 main classes for users: Merchants (us) and providers (banks). There are 4 levels: 1. Any merchant who processes over 6M transaction annually, or has suffered a breach or is considered level 1 by Visa; 2. Any merchant who processes 150k-6M transactions annually; 3. 12k-150k e-commerce transaction annually; 4. Anyone else.

They use the levels to decide what type of the compliance you have to demonstrate to be eligible to process cards. The standard requires regular risk assessments. Upper management needs to understand the risks such as reputation, financial ($500k per incident and an incident can include not following their rules), compliance to level 1 requirements. If you have an incident, you are automatically bumped up to level 1 and will require a risk assessment once a quarter. If you can't meet the standards, you will loose the capability of processing credit cards. Below are the requirements listed in very brief form. These are more like section titles in the standard documents. There are very strict data retention policies. See the standard for detailed information.

Install and maintain a firewall
Do not use vender supplied default passwords Protect (encrypt) stored data Encrypt transmission of cardholder data Use and update anti-virus software Develop and maintain secure systems and applications (patch management) Restrict access (need to know) Assign unique identifiers to all users (various password policies) Restrict physical access to cardholder data Track and monitor access to cardholder data Regularly test security systems and processes Maintain an info security policy

Resources:
On this site: Http:/www.usa.visa.com/cisp Get 3 things guidelines, self assessment, and audit information.

The conference was very good experience with a small group (300 people) and good topics.

Brian Moeller
It would be really neat if people who went to conferences would be willing to bring back the information and do a short presentation at an OARtech meeting to share the information.

Pre-conference session: Exercise in Ethical Hacking
He was blown away by how easy it still is to break into systems.
Brian thought things would have gotten harder over time, but found it is still very easy.

Keynote was Dan Larken from FBI
Started the Internet Crime Complaint Center (http://www.ic3.gov) Internet Crime is the FBI's third priority. They have staff that do nothing but investigate cyber crime. In the past 3 years they have arrested about 6000 cyber criminals.

PKI
This conference has a track of vendors with customers coming together to do joint presentations. The presentations cover decisions, costs, and timeframes. He was afraid the sessions would be vendor ran, but found that the vendor for this talk handled himself well. The session was not vendor specific or indoctrination and dealt with the problems with the vendor as well as the good stuff.

The Botherd is coming
This session presented the problems of Botherds from the helpdesk perspective.

Information sharing the MOREnet way

MOREnet (Missouri Research and Education Network) is similar to Oarnet but a little smaller. At MOREnet, 2 people do nothing but security. Their security office assists customers with incident response, liaisons with law enforcement, and focuses a lot on training of their clients on security.

They have a monthly seminar on several different security issues via the web as well as and annual security conference. They also do their own ethical hacking training. They also have some fee-based services that include Email and virus scanning and also provide security assessments. The training options include contracts with SANS and CISSP training for members.

For more information:
Randy Raw, rawr@more.net 573-882-0749
Beth Young, youngba@more.net 573-884-7200

Dan O'Callahan
Dan attended sessions in the incident response track. The pre-conference session was very good. He found out about Helix which is a free forensics tool that is very powerful. He found the conference was excellent and would encourage attendance. If you are interested any of the Helix information, email him or Patty and they can get it back to you.

This conference was a 2 day conference and was felt very high value for only about $400.

Lunch

No Technical Presentation due to airline problems.

Teresa Beamer was nominated and elected as secretary.

Helix forensic tools are available at http://www.e-fense.com/helix/ It tries not to touch the host computers' hard drive during an investigation.

Yesterday there was a HVAC failure and OARnet lost a T1 mux. They are setting up their own sensors now.

Topics of interest for the next year:
Identity Management
Coordinated Identity
Best Practices for account maintenance especially for students

There was some concern that Bob would not accept the nomination for Vice Chair. Nominations were opened for another candidate. Cal Frye was nominated and elected to Vice Chair.

Meeting was adjourned at 1:20.