OARtech meeting
December 14, 2005

Introductions

Oarnet Update
There will be a vendor show on Anti-spam will on Friday. ETEC contract has been signed. So TFN will be K-20 network. They are still working on MOU with One Cleveland regional network, and OIT. They are moving forward with 5 more university direct connections. Another announcement from OIT is they have signed off on 10/100 contract similar to the SOMACs contract. Details are not available yet.

Ohio Learning Network
Cable Green
Slides are available on the OARtech website.

Shared services that are available via OLN: Collaborate and Learning Environment (CLE Hosting). Ohio Digital Commons for Education to provide enterprise level learning environments. ODCE (OSC, OhioLink, OLN) asked what are the mission critical eLearning services most institutions are running or will be running in the next 2-3 years? They reviewed this list of services and determine shared services that can be provided statewide. Current services offered include CLE (WebCT vista and Blackboard), object repositories (Ohiolink), ePortfolios and Shibboleth (OSC).

CLE Hosting project
They host for over 110 institutions of higher education in Ohio with over 585K students. Nearly all the campuses require CLE hosting and the items that come with it. Many institutions lack the resources and staff to deliver a robust CLE and content repository services as mission critical applications. The Ohio Governor's commission on higher education in the report at www.chee.ohio.gov calls for more "shared services". The timing for shared services is right.
CLE is better candidate for shared services than the legacy administrative systems because it is not as entrenched. TFN provides excellent networking, and Ohio Commons, OBR, Kent State and UC are eager to lead in this space.

Project has 3 phases and is currently in phase 2:
1. Pilot two and four year public and private institutions of higher education 2. Add additional institutions in FY07 and FY08 3. K-20: Add K-12? For example UC and Catholic Archdiocese

Logistical Goals are to enable any institution no matter size to move into the enterprise level CLE. Financial goal is to save money on services surrounding the hosting - license negotiation, hardware, software, backup, updates, migration and implementation, and training. There are Blackboard and WebCT councils with best practices and training materials meeting monthly online.

A list of the campuses participating was shown. Climate is right for collaboration. There are some schools that are on a basic contract and need to move to enterprise level so the CLE is a reasonable alternative. OLN works as a partner to help with negotiations.

Why do some institutions not join? There is a perceived loss of control and loss of integration with student information systems. But clients retain FULL control. The schools think they can do it cheaper themselves, but when they do the comparison they often find that the share is cheaper. Often there is concern about staff losing jobs, and/or they have the wrong combination of folks at the table.

Costs model is Hosting Fees + License + Integration Costs (optional) = Sub-total - OLN Support = Total cost. They are looking to negotiate with the vendors for buying in bulk to reduce license costs. OLN serves as project manager role.

WEbct and Blackboard are looking to merge. It is currently waiting approval with the government regulatory agency. Open source is becoming a real possibility.
For Sicai, Moodle, and Uportal, OLN is hosting pilots to allow institutions to "kick the tires" of each of the software.

Timeline: Fall 05, discussions with OLN, host, vendor, institution presentation:
Winter 06, All costs known, sign license agreements.

Contact information
Cable Green
Director of Technology, OLN
cgreen@oln.org / 614-995-3240

They are willing to look at open source tools if institutions want it.

Oarnet update
Dennis Walsh

Dennis is the new acting interim director for client services. Linda Roos has left a large hole in Oarnet. To maintain the services that Linda handled, they have created a client/management relationship with staff and assigned specific schools to create a single point of contact for the schools. A list of the institutions as they are assigned to the representatives was handed out. This list will be put on the website and will be sent out to the list.

Paul Schopis
Slides are available on the OARtech website.

There are changes that will be made in engineering and support. They lost an optical engineer, but have acquired another. At this point, they have split the support desk in half. The support desk will take the first level calls, then passes it off to a 1st level NOC

which consults with an engineer that will be assigned weekly with the NOC to determine if it can be dealt with quickly or whether it needs to be handed off to engineering.

Spam Filtering Project was run with a state-wide committee, and came from a survey to OARtech and Osteer. There will be presentations on Friday and the presentation will be posted to the network.

Last Mile update - several schools have connected. Solutions/options: Dark fiber to the POP, local area rings, and leased line options to the POP.
Upgrades have been done to Ring 0, 2 and 3. Springfield POP is being turned into a POP using OADM. All circuits of old backbone have been retired. All ETEC gear has been deployed. The backbone problems they have seen include a power outage at Neilston due to backhoe, but backup power functioned as designed. They had some issues with AC power, due to the provider not being fully ready. They had a manhole fire at Canton that actually melted the cable.
The only school that had an outage due to these problems was Kenyon and that was because Time Warner did not have backup power on their lines. Resource usage info is available at http://statseeker.oar.net and http://portal.oar.net.

Primary Response, Threat Protection Software Brian Hawes Matt Rees, Sana Security

They work with Nexum out of Cincinnati to help with incident response.

Sana Security was founded in Oct 2000. Taking concepts from the human immune system and applying them to the network security. Philosophy is to create enterprise threat protection software that automatically detects, classifies and responds to complex and evolving threats. They currently have over 250 customers. They create software that is autonomous, aware of environment change, and adaptive.

History of internetworking move from the original networks of military, and government to 2000/2001 with "The Plagues" - Napster/p2p, gaming, worms.
Largely perimeter forces approach was used to combat these things. The university network culture required open back end connections. How do we become "good citizens"? Unwashed masses go largely unchecked uncontrolled and unmanaged. Often networks operate with the policy that "if your network is the source of the problem, we shut you down to save the whole." There are more issues with access anywhere (Wireless, remote access, etc).

Attack evolution has moved to faster and faster infections, and the attacks are becoming more complex and changing. Malware comes from p2p, hacking, nefarious, hacked web, gaming sites and DRM tools (e.g. Sony rootkits) and commercially viable sites.

Strategic solutions can't solve the problem. Antivirus is not enough. It is reactive, too intrusive and difficult to manage. Antivirus does help you to determine the known problems, but does not do a good job with unknown threats.

Sana has a white page on how their primary response product acts in comparison to antivirus. Using gateways doesn't deliver transparency, or remediation, and may require investment in several systems. They limit content and are largely based on "Known Bad". Host checking and clean access is used to direct the users to "virtual sand boxes" or networks. But it is still incumbent on self service tools and assumes appropriate control over the end point and appropriate remediation. Sana feels the current tools fall short of fixing the current problems because the protection is limited, NOT instant and removal is incomplete.

Protection requirement for open networks has to be an end point solution, has to be transparent to the end user, must be simple to deploy, require zero intervention, and must work in real time. Sana's approach uses behavior protection and lockdown from first site through the life of the threat. The product family includes a centralized management system protection with Primary Response Server, and Primary Response Client. Primary Response SafeConnect for standalone protection and Primary Response SafeConnect OnDemand for on-demand protection. These last 2 products are brand new and beta versions are openly available from their web site.

Active Malware Defense Technology V2 is multi-behavioral to provide real-time protection. It looks at the behavior in combination with multiple active attacks to determine and "reverse engineer" on the fly to be able to see an attack from day zero.

Primary Response SafeConnect OnDemand provides instant remediation for unmanaged endpoints. The end user does even know they have been protected. The client instantly detects and removes malicious software securing unmanaged end points connecting via web based email, web applications, SSL VPN, and portals. He showed a diagram of the usage scenario. This increases user productivity, lower total cost of ownership, instant remediation, and ensures compliance on the end points.

Primary Response SafeConnect provides instant and constant protection for business. The beta version is available free. It looks at the heuristics to determine malware attacks and stops them. It is GUI based and can quarantine, remove or restore. They look at many different attack classes, not just spyware, or adware. No need to install multiple products for threats.
SafeConnect pricing for education is $24.95 for 1 yr support and updates.
Currently it is in beta and is feely available. Production version will be available next year. He showed some comparisons between their product and
WebRoot Spy Sweeper. Only remediates as it sees behaviors, not using signatures, and provides zero day protection instead of scanning systems.

Lunch

Brian Moeller
Information Systems Security Association (ISSA) is offering scholarship money for students that are willing to write a paper on security. They are just finishing the criteria for the papers. They will award the scholarships for next academic year. They are also

interested in student chapters of ISSA that might be interested in network security. He will post the final application information and the student chapter information to the list.

Ransel Yoho
Darknet reports are currently available from REN-ISAC as well as the Daily Weather Report with critical notices, Darknet Monitor, and the trends for vulnerabilities and exploits. Occasionally they send out alerts based on the activity they see. If you are interested in being on the list go to http://www.ren-isac.net and see how to register. When you send the information in you have to have at least 2 people vouch for you within a 24 hour period.

OpenVPN
Ransel Yoho

OpenVPN is an opensource, cross platform, client/server, PKI based VPN. Information can be found in http://openvpn.net.

Presentation was postponed due to technical difficulties.

No new business.

Minutes were accepted.

Meeting was adjourned.