OARtech meeting
April 12, 2006

Introductions

Oarnet update
Dennis Walsh
Oarnet is in the process of reorganizing the academic services group. They are also waiting on pricing decisions for some new services. A new representative has been highered to take over a lot of Linda Roos' work. Her name is Ann Zimmerman. They are trying to improve communications with their customers. A lighting event for the ETECH organization has occurred. A person has been assigned to work with K-12, cities, and other partners. Oarnet does offer a hosting and co-location for storage and servers.

Paul Schopis
Slides are available at http://www.osc.edu/oarnet/oartech/presentations.shtml
ETECH traffic will be treated as IntraOhio traffic (k-12, public stations, etc).
They are setting up a peering relationship with ETECH to help with redundancy and disaster recovery.

Last Mile Update
Hebrew Union, Southern State CC, North Central, John Glenn Institute, and Oberlin are working to connect their last mile. They are again having capital issues with having to justify all the purchases which are delaying some purchases.

The helpdesk has been changed to a 2 tier support structure. This helps with triage on the tickets before it goes to engineering.

New directions
Merit approached Oarnet to build fiber into Toledo to peer with Merit and thus also allows peering with Merit Orano, NYSERNET, and provides Chicago access.
At the Quilt level they are trying to build interconnects that allow access with those concerned about the NLR and I2 issues. They have fiber into other areas Oarnet could make use of to take advantage of the different peering opportunity. Oarnet is able to take advantage of the OMNIpop to build peering relationships across the US. The Quilt is currently evaluating commodity services (Note: Quilt contracts do provide bandwidth for Oarnet schools as well).

Pdna (Plant Lab)
This is virtualization of the network to simulate networks situations. It gives some fairly serious resource to researchers and thus provides researchers a playground. It allows them to do a "real" simulation rather than emulation.
Different projects include:

HOPI - Hybrid Optical Packet Infrastructure which leverages the network layers to construct a virtual "Light Path"
UCLP - User Controlled Light Path gives end user access to optical resources, and uses Ethernet in Sonet Framing.
Dragon - Uses GMPLS and allows dynamic Lambda switching.
GENI - Based on Planet Lab and employs the notion of virtual routers.

OarnetTFN uses MPLS for recovery and partitioning. They are the only gigapop using logical routers in production.

The proposal is to leverage the planet lab virtualization and use pieces from the all the projects listed above. This would allow you to update a specific piece and build modular constructs and thus give you flexibility in updates and additions. It would use basic building blocks of Control Plane/Service Domain, Forwarding components talking to the Optical switch, Layer 2 switch and Layer 3 with a management/monitoring piece to control the blocks.

The assumption is that the physical structure of the fiber would stay the same.
So the infrastructure to support this already exists and thus can be leveraged.
See slides for diagrams of how the building blocks would be connected.
Functionally it would work as follows: Resource managers on the routers that use multicast resource advertisement to build the routing structures for the network. 1. Request to build a resource 2. Authentication/authorization 3.
Resource exchanges on the real need 3. Resource request (protocol) 4. Resource response and yes the resources are available 5. Code transfer occurs between the routers 6. New infrastructure is setup the optical, layer 2, layer 3 or
overlay 7. Have a separate network as a new dedicated domain. This would allow you to reconstruct services in optional paths in disaster situations and can be used to build global paths and be used to address resource allocation problems.

They are currently looking for funding for this project.

Nominations for Vice Chair and Secretary Mike Pinson, Shawnee State University will take over as the new Chair in June Bob Beer, Ohio Northern was nominated for Vice Chair Terri Beamer, Denison was nominated for Secretary Nominations will be left open to allow for submissions on-line. Voting will occur at the June meeting.

Network Security Update
Steve Romig, OSU
Malware

Slides available at http://www.osc.edu/oarnet/oartech/presentations.shtml

He is in charge of the incident response team at OSU. He will be talking about the problems they have seen in non-university equipment. If they find a compromised system it is knocked off the network until it has been fixed. They have done a good job of educating their network administrators so see few problems in the university own systems. Most of the problems they see come from the non-university owned systems and generally come from social engineering attacks.

Interesting stats - 90% of compromised systems are bots. Most of these are NOT detected by anti-virus because the AV is not-running, not up-to-date, or just not detected. They sometimes have to convince the user that they have been infected since AV is not detecting it, but OSU can see the traffic. Most machines cannot be disinfected easily, thus they generally request that the user rebuild the system. Systems are not detected through the "usual" means of outside reports, denial, and scanning. Most are hard to spot, but are very common. A light week at OSU is finding 100 machines

infected. They do special looking for botnets on their campus. A lot of the bots are controlled through IRC.

Steve recommends the information from Kaspersky's web site on cyber crime and anti-virus. They say that Cyber crime makes more money than security. 76% of people don't update their anti-virus daily and 45% open suspicious email at least some of the time. You can probably assume this is happening via peer to peer or IRC or Chat as well.

Microsoft has a good blog on anti-malware. They have a malicious software removal tool that currently runs on 250M computer/month. Of this last month found 250k infected with Alcan worm. Of the computers with no support packs 50% have a rootkit installed, and of systems with SP1 or SP2 installed 20% have rootkits. This tells us that SP2 was pretty effective in preventing rootkits, but you still have 1 in 5 computers that have rootkits.

Rootkits replace software on an OS so it will not show the infected material and thus hide the infections. Now they are replacing not just a program or library, but are replacing the OS. There are good methods of detection for rootkits, but it is a cat and mouse game. Joanna Rutkowska writes about rootkits and how to detect them. She also recommends a blackhat site for information. The Holy Father (a person) writes rootkits, one is called Hacker Defender. He even has sold them with services that the copy of the rootkit would be undetectable for a particular time. The bad guys are still doing this type of thing. The technology is there. University of Michigan worked on a project called SubVirt. This is a proof of concept that you can hide a virtual machine that could not be detected.

Invisiblethings.org is Joanna Rutkowska's site about rootkits. It talks about using cross-view detection so that you look for the same material via different ways and compare the results to determine if the machine has been infected with a rootkit.

BOT - a software agent the installs on your computer to make it part of a botnet
BOTNET - a network of bot infected machines. The bots talks to each other frequently through IRC.
Owner (bot herder) can send commands to the bots through the botnet.
Used for spam, phishing, installing spyware/adware, keystroke logging, building botnets, denial of service and click fraud. They can scan the systems for software keys to sell for expensive software.

Most are spread via social engineering using IM, email, p2p, and MySpace virus (e.g. LOL - not a virus!). A bot can respond so that it sounds like a person but is not really a person.

These are very hard to detect. You can detect the commands to the bots using snort rules. However, they do change the commands periodically, or they don't always have to give commands. They can encrypt the traffic and hide that traffic completely. You can see if the system is connecting Command and control servers (C&C) and look at the flows for connections to C&C. Then warn the user of the infection. There is not a lot of discussion about the detection of botnets because they want to keep the information on what is detected from the bad guys and slow down the development of changes to hide the bots.

In detecting a botnet, you would have something at the border that detects the traffic (e.g. Snort). Talk about it on the botnets mailing list to determine how to write rules to detect the bots. Connect via an onion routed network (can generate anonymous traffic) and see what the server is doing. Join a channel - example topic was "aimspread look at this sad killing" points to http:/www.freewebs.com/omgsadkilling/killed.com. The channels can be completely different tasks and partitions the botnet to different machines.
You can look at flows to see what machines on campus connect to them.

When OSU finds a machine that is infected, they have the machine rebuilt.
Microsoft even admits now that rebuilding is best. Some are now looking at kernel mode rootkit/bots that will probably not be very hard to detect because they can infect so many and so easily with social engineering. Others are talking about infecting the BIOS or video memory or other device drivers.

References:
Microsoft anti-malware engineering team blog:
http://blogs.technet.com/antimalware/
Kaspersky: http://www.viruslist.com/en/analysis
Tibbar: http://tibbar.blog.co.uk
Joanna Rutkowska: http://invisiblethings.org

Here is a site you can run malware through a check by several different anti-virus products to see if anyone knows what it is: http://virustotal.com

Steve likes using VMware on Linux for an isolated environment for testing malware. He is currently using a virtual pc environment. But if you have malware sitting around you need to set these so you cannot run them by mistake.
Mac now can run windows machines natively so you have to be careful that you don't run the malware by mistake.

Lunch

SANS EDU
Ransel Yoho, KSU

How many have been to a SANS EDU conference? No hands were raised. Ransel indicated these were very beneficial conferences. He passed around a poster that shows the SANS Threat Map.

In March he attended the "Hacker Techniques, Exploits & Incident Handling". He found it very good training. The EDU classes are 70% of cost of regular classes.

VMWare - Windows provides a VMplayer free that allows you to bring up virtual machines (VM) so you can isolate malware testing. He showed 3 virtual machines on his laptop. One running windows, and one running Linux. He used the Linux VM to scan the windows VM. He made changes to the windows firewall settings to demonstrate the scanning. Virtual appliances are also available to run on the VM. An example would be a "safe" browser that isolates the browsing session.
The VM software is available on http://www.vmware.com/ has been vetted.
Pulling VM from the community could bring in a compromised virtual machine.

VMWare allows you to create virtual networks. You can see the interface definitions in ifconfig.

Soekris Engineering embedded computer information http://www.soekris.com They are using a board from Soekris to but together machines that are fast for about $300.

Bill Blake, Clark State
Noki N770 small portable computer
Runs Linux with Opera as a browser. It has 802.11b, g and Bluetooth. He was able to get WPA and WPA2 working. Has audio, microphone, video support (mpeg1, mpeg4, real video). New version will be out with VoIP. Not really a network tool, but is a small tool that would be very portable. Cost was $350.

Bowling Green University is doing a Resnet Symposium event for discussing tools and issues associated with managing resnets. For more information see http://resnet.bgsu.edu/2006/

Meeting adjourned