OARtech Minutes
10/08/03
By Teresa Beamer

Introductions - Question was how did your site handle the virus/worm problems?

Denison University - We have a registration system that registers all PCs as they connect to the network based on the Boston College model. We changed our registration page so that it automatically scanned the PC and if it was infected or not patched, it was redirected to a page where the student can disinfect and install patches before they register. Used ideas from University of Connecticut and University of Minnesota.

Ohio Northern - Gave out CDs

Heidelberg - Gave out CDs, they have one core switch and don't distinguish between faculty/students. Intend to put a firewall between faculty and students.

Kent State - Gave out CDs, have registered students, managing infections at the internet border and redirect the infected hosts to a web page that gives them the fixes. Been using RPC scan from University of Connecticut. Will be forcing students to upgrade their systems.

Oberlin - Use Netreg to registered IPs. Students were not allowed to register systems without an employee having scanned and patched the system. All machines were required to be touched by Computing before they could be registered. Also applied policies on the switches to block ICMP. Site license for McAfee and installed it on all machines. They run a flat IP network though Resnet is restricted to specific IPs ranges. Announced there would be a $25 fine for infected computers, but have not charged it. Found machines with 800 viruses.

Cedarville University - Blocked ports with ACLs, had students call in problem reports. Gave out CDs. Looking at implementing Netreg.

Mt Vernon Nazarene - Students are issued laptops that are owned by the university. They were fine until the students showed up for night classes. Walked around with CDs. They have small campuses so were able to get around to them. Also putting in SUS to force patches whenever they connect. Putting in firewalls to prevent spread between campuses.

Lorain County Community College - Don't have student machines to deal with. Watched and went around to faculty machines. Gave faculty a link to install their own patches.

Hiram College - They have a segmented network with vlans. Applied access lists to block ICMP. Blocked dorm DHCP scope from the faculty/staff scopes. Watched the net with a sniffer and force shutdowns when they saw an infected system. Looking at a couple of Cisco products.

OARnet - Gene - contacted schools where infections were coming from, their machines are fairly well protected, but found the a few that were infected and cleaned them. Tried some corrections but they didn't work as well as they hoped. They saw the virus problems on both I1 and I2 links.

What about packages that need RPC for actually running? Blocks did stop some apps.

Sinclair Community College - Found that ICMP 2000 GPO requires Ping to apply group policies. Running Microsoft utility to detect vulnerability and going out to the machine to apply the patches.

Comment: RPC from University of Connecticut is much better then the Microsoft utility.

Wittenberg - Segmented by vlans/building. Had to shutdown the network. Was on the phone with packetshaper for problems at the time the virus hit. Problem was primarily on-campus computers, as students had not returned yet. Contracted with 3rd party to help cleaning. Currently bringing up SMS server and have a McAfee site license. Use VMPS and Dynamic ports. They grab a mac address when registering and block in the VMPS tables. Used VMPS to take care of the unknown systems. Thinking about a quarantined net to put people on.

University of Cincinnati - Used Boston College example with policies/scans the machines, used CNR to setup scopes. This is a similar process as Netreg. If they find someone on campus with it would scan the machine. If there is another virus, they wipe the mac addresses and force users to re-register and get scanned.

AFIT - Didn't get hit hard with this virus, as they don't have a residential system. Each PC is automatically scanned daily and login scripts to detect vulnerabilities so all machines were up-to-date. They also have their own mail relay that scans mail.

Clark State Community College - Mostly Novell with firewall - natted - Norton. They were not hit hard with this virus. They are looking at how to manage updates for their campus systems.

Baldwin Wallis - They blocked ICMP, and other ports. Had a student write a script to see who was hitting the ports and records the machines. They have Norton for the campus and force automatic updates every few hours. Found another virus that was putting routers CPU load up. The virus hit port 6667.

Kenyon - Network link blocked, gave out CDs and had anti-virus clinics.

Otterbein - hit hard, contained within campus with access rules. Shutdown all dorms and separated them to a separate resnet. Implemented SUS for campus machines. Issued CDs with patches and McAfee Stinger.

Antioch University - have a lot of Mac users. The systems with Zone Alarm did not get hit. They had to go around and patch the system without Zone Alarm.

Ohio University - 20,000 students across 5 campuses. Noticed the problems this summer so devised a plan for when students returned. Put ICMP blocks in dorm areas, and rate regulated ICMP for other areas. Students when they got their key they got a CD. Used NMI to provide network information as to where mac addresses are connected and determine what port they were on and port automatically blocked. Information stored in a database and information on blocked ports given to helpdesk. When students call to indicate they have cleaned system then turned back on. NMI continues to check so if system becomes re-infected or student didn't clean it would get blocked again. Use Bluesocket box to control the wireless areas. Uses NMAP sweeps for port 707. Will be using Nessus scanning for other vulnerabilities. They do not use registration of mac addresses because of vmacs. Would like to register to the user instead of to the machine.

University of Toledo Distance learning group - was not hit hard as they keep their machines patched.

University of Toledo Network - in 2 days turned off 700 machines. Rate limited ICMP traffic. Implemented all Cisco recommended ACLs. Did sweeps for port 707.

Shawnee State University - prevented worm from coming on campus - setup a center for students to bring in computers and scanned/cleaned the systems for them. Register mac addresses and fixed to a particular ports. Implementing 802.11x on wireless with Cisco so students must register wireless equipment.

OSU - only had about 4000 machines blocked then the students came back. Blocked all the regular ports. Scan their flow logs every 4 hours

looking for infected hosts and blocked them when they are infected. Now that students are back they distributed CDs. Resnet is separated from rest of net with firewalls.

(Don't know what site) No resident students. Audit the network every year and install patches on campus machines. This helped a lot. Equipment must be purchased and approved by computing services.

University of Dayton - Intrusion detection found the first infection. They isolate the helpdesk to prevent PCs coming in there from infecting the rest of the net. Verify that machines are scanned and infected. They are seeing AOL Chat problems dropping. Comment - this is a recent discussion on packeteer list.

Whitepaper - Questioned Osteer about the need for the Whitepaper. They indicated that what they need now more of a best practices paper. Maybe more of a web page with links to each best practices to support a policy memo that would come out from Osteer. Next meeting look at what was written last year and determine where we are taking it.

OhioLink - Greg - Looking for a volunteer to look at authentication for services (they are looking at shibboloth), currently have people from OSU, OSC, Kent, OhioLink. They want to look at shibboloth to see if it would work for the authentication needed by OhioLink. If interested send a message to anita@ohiolink.edu

OARnet updates
Linda Roos - will have Paul give report on network monitoring and measurement.

Paul Schopis
Trying to get a better network view with good measurement and to have the tools available to others. Tools used include Looking Glass, Nagios and Stat Scout. Looking Glass allows you to go to any of the routers and switches to look at various pieces of information without allowing you to make changes. Nagios tracks problems and requires staff to acknowledge those problems. Stat Scout is used for keeping track of network traffic statistics. See http://www.eng.oar.net/lg/ for a menu of the tools available. For Nagios see http://mon1.eng.oar.net/nagios/. Stat Scout is also available http://mon2.eng.oar.net/statscout/ log in with OARnet/OARnet.

Adding a new community gateway with Qwest in Cleveland for a 1 year contract to give the network breathing room until other solutions are available. The line was acquired via the quilt contract.

Followed Cisco recommendation to limit the virus at the core and found that dCEF had problems with it. Back up of the changes and tightened up change management policies. Will filter on request but not in the core. Any changes that must be changed massively they have to meet and review the change. The real fix is to patch the hosts and maintain up-to-date virus software. Currently any changes to the network are posted to the web notice page. From the floor - would prefer an email notice.

Did meet with UC and Cincinnati State to look at the Surfnet connectivity to OARnet. Surfnet will run it's ring and OARnet will run the routers.

Dennis Walsh Fiber status --all backbone segments completed and tested except between Athens to Columbus. By 10/7 will have all network segments up. Integration of the various segments is more complex. Completed integration in Cleveland. They are waiting on contract approval for integration in Columbus, Dayton, Toledo, Youngtown and Cincinnati. Should be done by 10/31/03. Hope to have everyone converted to the new backbone by March.

When will the plan be available to the members as to how the conversion will occur? Currently waiting on some Right of Way approvals. This is not change to sites last mile, but takes the current connection and connects it to the new backbone.

2 committees have finished their work - Lighting committee and Finance committee.

Last Mile committee is putting out an RFP, but OSU legal is reviewing and making suggestions for changes. Looking at some other group to issue the RFP that would include more of the partners. RFP expected to be released by 10/31/03. The RFP will be issued and would have multiple venders responding to it depending on the area of the state they are in. Looking at creating a list of approved vendors. The RFP provides several levels of the various types of services from dark fiber to serviced lines. Looking at 30 days at least before they have the responses from the RFP. Probably won't have pricing until December.

Implementation committee is and oversight committee. Providing Key milestones and other information is available on EPMO. On the TFN website you show should see a link for access to EPMO. The password changes every 30 days. Call Kelly Sites if you need access. The implementation committee received the password via email.

Can sites put some of their own equipment on the network? Yes, but it

must be compatible.

Current network is costing $4000 a day so the sooner we can move to the new backbone the better.

Administrative updates - have weekly team meetings between SBC, OARnet, Schoolnet, Cisco, and ODE.

Trying to increase the awareness of TFN. There is also a broadband commission to see now the broadband can use TFN. Also received call from Ohio Court system Working group to see if they can make use of the TFN network for the court systems.

Funding - Schoolnet is one of the partners and they are providing $3.5 M connectivity to the Schoolnet sites. Would be willing to look at working with higher ed sites to see where there may be a benefits to partnering to help in connecting up the last mile.

Department of Administrative Services is looking for replacement of the SOMAC contract (about to end) and is looking at TFN as a replacement. Received a grant award to fund 3 sites to connect. Also looking at other funding from the PUCO to reduce some last mile costs.

Lunch

Al Stutz
Will be advertising for the OARnet director position in several venues.
2 subcommittees from Osteer exec and Osteer to review the submissions down to a handful which will then be review by another committee with a wider representation.

Juniper Networks
Eric Warner

Juniper is based out of CA in started in 1998. A layer 3 company and is very focused on this area especially with the core. Recently the number of customers in the government and education arena has taken off.

Terry Murray
>From Routing to Robust Packet Processing

Router core is essential is to take a packet and map it to an interface. Get the packet to the correct place. Their product is an IP router, not a multi-protocol router. This talk will deal with IP routing.

They saw 2 issues in routing: control plane and the forwarding plane and

felt these had two different jobs, so they require a clean separation with limited interaction. They felt that routing should be solved with software and use a Pentium 3 processor. Packet forwarding should be solved with custom hardware (ASICs) and provides classification, forwarding, etc.... He showed a diagram that shows how the routing engine communicates with the packet-forwarding engine.

The control plane requirements are that it be stable, scalable, have speed, and be correct. Stability means it has to stay up even when you have failing hardware, attacks, etc.... Software is highly disruptive to recover. Unstable software can lead to a domino effect. The scalability has grown fast with a growing number of routes, neighbors and interfaces. The size of the interfaces is also increasing. He feels that things are not growing as fast today, but they are still growing. Speed allows convergence/recovery to cover momentary outages because of the more stringent requirements for Video and VoIP.

The requirements are at cross-purposes, with early implementations sacrificing speed and scalability to achieve correctness.

They looked at the scheduling architectures (preemptive and cooperative). Preemptive processes run at the same time and every one gets their time slices. Provided good latency and fairness. Its problems occur when you have to deal with locking shared resources. Cooperative multitasking each process holds the CPU until it explicitly gives it up. Problem with this is you can get a run away process that never gives up the CPU. Found that locking issues were very hard to solve. With cooperative you have to enforce latency values because things may have changed since the process had the CPU.

What they did was create a cooperative multitasking on a pre-emptive scheduling kernel (FreeBSD). PPM - Periodic Packet Management, they call it RPD. This gives you both speed and stability. You also get fast convergence. Dystra is their process that determines the lowest cost path. When things get busy the conservative hold-downs kick in. We sacrifice some speed for stability but only after trying some things to try and still keep the speed.

Some platforms have a redundant routing platform and use graceful restart so that they restart the control plane and not have to restart the forwarding plan so that they don't have to reconverge the tables. Also avoids the network outages both planned and unplanned.

Design goals are a minimalist approach - it deals only with control plane failures and it preserves the forwarding state information. To do this the planes must be separate and on restarting a node you must

preserve the forwarding information across the restart of the control plane. Neighboring routers hide the failed router from all other routers in the network. When the router recovers the neighboring routers rebuild the forwarding database on the recovered router. This allows no change in traffic path and no convergence, no disruption to routing and forwarding, and limits the scope of the outage.

A graceful Restart Engine Switchover allows the change from one Routing Engine (RE) to a fail over routing engine in the box by keeping the forwarding data on both routing engines. This allows in-service software upgrades. This is something they are working toward, as some are not fully implemented.

BFD - Bidirectional forwarding detection - allows a faster convergence of routing protocols. Detecting aliveness at the forwarding plane so the control plane doesn't have to do it. Can be used over direct links and MPLS LSPs or other unidirectional links. Can be run over IP or over Ethernet to determine neighbor failure or hardware failures and can be used for routing protocol aliveness, switch-router, router-host, etc… Is jointly developed by Juniper and Cisco and is an Internet draft with the next revision due out soon.

Rules of thumb for scalability issues - CPU and memory are limited resources. The principles all state that protocol can be represented by in a bounded amount of memory. There is no reason to drop adjacencies, no reason to run out of memory, or crash.

Good things to do under load - but you've got to keep your peers and adjacencies up, be more efficient under load, and don't keep any redundant information. Distribute the right things across the net when it is right to do that. Bad things use more CPU and lose peers and adjacencies.

Building a Robust Forwarding Plane
Must keep up with the instantaneous interface - you must have memory or buffer space if other equipment can't keep up with the forwarding plane. Router size can be huge as you interconnect routers. Over the past 7 years the chip size and speed has been getting better. They don't want to put buffers on the plane that increases the latency time. Big routers have gotten cheaper per unit bandwidth and denser and this is going to continue. They are being slowed down, as they need more memory chips with more pins on the board. The huge monster routers are built on a switch fabric.

There will be bigger routers when needed but you won't find that the $/Gbps go down as fast as the $/Mbps. The big applications that are starting to emerge may change some of the needs. See paper on Juniper's web site.

On WDM the fastest you can currently clock an OC-768 deployment, is 40 Gbit.

Future challenges include the usual scaling trends. Increase in the number of routes and number and size of interfaces. New challenges include scaling the control plan to provide network wide policies over per-hop behavior. This allows you to put a blanket across the network for management. Looking at Flow based processing and the emergence of big applications.

Is there a general trend toward the swiss army all-purpose router at the core? They don't see a swiss army at the core. Put the extra things at the edge and over provision the core.

The forwarding processor really doesn't use the CPU - its all done in the ASIC. When they implemented NAT they use a CPU that you plug in and forward the packets through that CPU.

Next meeting hope to have something on DWDM. We are looking for other suggestions for topics? Send a message to Tim if you have suggestions for future meetings. If you have information on things you have put into place to fight the virus that you would like to share - send the info Christopher cook at OARnet (ccook@oar.net).

Meeting was adjourned.
