Sender: OARTECH Mailing List <OARTECH@oar.net>
From: Terri Beamer <BEAMER@DENISON.EDU>
Subject: OARtech February 13 meeting minutes
To: OARTECH@LISTS.OAR.NET

OARtech Minutes
February 13, 2002
by Teresa Beamer and Bill Mayhew

Patricia asked for introductions with two questions: What is the blocking policy, based on the recent SANS advisories about SNMP? What about single sign on?

Attendees:
AF Inst. Of Tech, Cecil Martin - Block most, uses active directory - firewall authentication
Anitoch University, Bruce Friend - Blocks only some, merging three groups, no single sign-on
Bowling Green State University, Mike Smith - Blocks many, Solaris LDAP with messaging direct
Case Western Reserve University, Eric Chan - Blocks many, looking at LDAP, no current plans
Cedarville University, Gabe Cluster, Alan McCain - Blocks very few, looking at single-on but no plans
Clark State Community College, Hugh Evans, Steve Hurley - Blocks selective, looking at Novell LDAP
Denison University, Teresa Beamer
DeVry Institute of Technology, Dave Leitch
Edison Community College, Jeff Collett, Bert Waldrop
Heidelberg University, Kurt Huenemann, Sean Joyce - Pix, Packet Shaper, only some filtering
Kent State University, Ransel Yoho - Mostly open, blocks certain things, looking at LDAP and RADIUS
Keynote Speaker, Robert Behlen, Jr
Lorain County Community College, Lisa Guerrero, Chris Strobbe - Blocks some, single-sign-on not known
Miami University, Tim Gruenhogen - Blocks minimal, looking at LDAP Novell NDS; recognizes need for a bigger product
Mount Union College, Tina Stuchell
NASA Glenn Research Center, Dave Pleva
NEOUCOM, Bill Mayhew
Notre Dame College of Ohio, Mike Kiec

OARnet, Ruth Crites, Fred Crowner, Aaron Lafferty, Jack Maher, Brian Moeller, Linda Roos, Pankaj Shah, Gene Wallis - As carrier, does only a few things to assure subscribers do not spoof or advertise disallowed IP
Ohio Department of Administrations Services, Michael Yerian
Ohio Northern University, Bob Beer, Jeff Rieman - Blocks selective, resnet servers, Campus Pipeline for single sign-on to some systems
Ohio State University, Mowgli Assor, Steve Romig - Blocks a few things, has implemented DCE in email server and using for AAA to other servers
Ohio University, Curt Flood, Royce Holiday
Ohiolink, Anita Cook - Please read the firewall doucment on OARtech or OhioLINK web sites.
Otterbein College, Jeff Kasson, Tim Pindell
Shawnee State University, Mike Pinson - Block minimal, modified on campus, off campus dial- in uses a different system, WIN2K AD
Sinclair Community College, Roslyn Taylor - Block all, open on request IP verification
University of Cincinnati, Jim Downing, Diana Noelcke - Blocks many, no single sign-on
University of Dayton, Tim Harrington - Blocks many, looking at Novell / LDAP - not this year
University of Findlay, Mike Pifer - Nortel firewall, Netscape directory server with Iplanet, Psync password synchronizer
University of Rio Grande, Chrissy Booth, Kingsley Meyer - Packeteer, uses windows active directory
University of Toledo, John Heiden - Blocks 1/2 the recommended, uses acdtive directory for some services
Wright State University, Patricia Vendt - Blocks/ packet shaper, planning to contract with Gartner to do a study
Xavier University, Mike Bowling - Blocks many, no single sign-on

OARtech Administrative Services

Ruth: Please be sure to sign up on the check-in sheet. Counting the participation is important. Please sign up for OARtech at lists.oar.net. Please be sure to keep your email address current. OLN conference: The 2002 IT conference, "Energizing Higher Education Through Instructional Technology," on March 4-5.
See www.olg.org for further details.

There is a Directory Services workshop coming up on March 22. The instructor is from Georgetown. The course is flexible and will be tailored to specific requirements voiced by the attendees.

www.oar.net. Click on Academic. There are some new features. In particular, take a look at new documents, such as the Memorandum of Understanding.

Linda Roos: In the SEGP and Internet arena. Xavier and Findlay are soon to start sending traffic. BGSU is the most recent to sign up.

Video conferencing began on January 2002. The fee is $960/year to be able to use the conferencing multipoint bridge. There is an additional requirement to have certified staff. The next training class will take place on March 26-27. It is recommended to have a back-up person on site. Testing is also required to meet certification. There is also an introductory course on H.323 available.

Gene Wallis

Internet 2 usage reporting - This system is still very much in a development process. The software is changing as well as is the way people are connected. Gene showed a typical installation of an I2 site with a DS3 to see how the statistics could be interpreted. There are also graphs available on the statistics system for the Permanent Virtual Circuits (PVC). Even on a "backup PVC" you will have some traffic that comes through because of the ATM overhead. 1 PVC is the backup that can take over if the other PVC goes down. This allows you to see your I1 statistics vs. your I2 statistics when running over 1 DS3 line.

Hope to demo the next version of the stats package next meeting. It will allow you to load numbers into a spreadsheet. It will look much different than the current stats package.

Gene displayed the logical map of the network. Notable is there is only one OC3 to AADS. Gene's been working for over a year with AADS and Qwest to get a second circuit installed. The current OC3 is at 140 megabits of traffic. PACS is a peeing location in Virginia. It is an offshoot from the original PACS in California. There is currently about 80 megabits to PACS. MAE-east will be coming on line later this year. There is a connection to Genuity in Cleveland now.

Gene showed the physical diagram of the backbone switches in network. It shows 7 Cisco 8540 as core network. Gene remarked that basing the network on switched virtual circuits is a good thing, which helps assure the network works. He pointed out that some routers have separate input and output links. This is because router-on-a-stick is handy configuration methodology, but having more than one stick is needed in practical terms. Gene showed the

logical diagram for the I2 network. It overlays the above physical switch network. It is a separate structure from the I1 network.

Gene was interrupted so Pankaj can do his presentation as he had to catch a plane.

Pankaj Shah, IPV6 Education and Training Labs

Object is to provide related information and training via virtual access and will host an IPV6 lab through ITEC Ohio with six different operating systems. They will slowly roll in some of the Ohio schools; will be looking for early adopters.

Timeline:
Negotiations with Cisco 12/2001
Receive Equipment - January 2002
Installation - Feb 2002
Testing - Mar 2002
Early Field Trials - Late March or Beginning April 2002
Widely available for Ohio Schools - May 2002

Showed diagram for lab.

Windows in the future.

Windows on the Future to be on April 15th at Fawcett center. The American Consortium for distance learning will be taking place at the same time. The groups will combine efforts to display performance measurement and monitoring. See the web site for more information: www.itecohio.org. Will have 3 separate tracks - end-to-end /measurement; Applications; Educational Effectiveness.

What is ITEC doing on End-to-End measurement? They are currently working on a grant proposal to look at the End-to-End beacon. The idea is to create an inexpensive box, which can be placed at strategic locations to help in troubleshooting end-to-end problems. It is being looked at as a possible measurement tool. The beacon can run several different protocols for testing. The first protocol to be used on them is H.323. The purpose of the box is to be able to improve troubleshooting without the need of a real costly MCU. ITEC is working with a company in Cleveland called Websprocket.

Back to Gene
Paul is out of town as he working with the I2 staff to evaluate the next

generation of equipment for I2. He is participating in a sort of an equipment bakeoff. Looking at what the next generation will look like (OC48 and above connections). Abeline is looking to go from OC48 to OC192 backbone using Qwests wave service. Abeline is hoping all gigapop operators will have at least OC48 or possibly gigabit Ethernet available.

Showed a possible bandwidth management model
"crustacean" security: hard on the outside and soft in the middle This isn't a good policy. The better approach is may be to harden individual system or groups of systems. In general he'd like to see the border router tied directly to the core network. The problem is trying to apply all the policy in one location. The same applies to bandwidth managers. It is difficult to apply bandwidth policy in one lump. IPV6 can cause problems with the crustacean model as well. Don't use NAT you will regret it!!!! You lose all control; you will be building yourself a problem.

We would like to talk about speed testing. The beacon is an RMON probe that would allow you to do speed testing, Quality testing, as well as eventually FTP and other protocols, etc... Allows you to look at the quality hop to hop and give you reasonable testing for where the problems are occurring.

Debbie Keller (via phone) White paper

The white paper was originally created to help the upper management and has evolved to include information to help the computing staffs with their planning. She feels that the paper needs to find a different design. OhioLINK, OARnet, OLN, OARtech representatives are anticipated. No traveling, conference calls, all via email and conference calls. If you want to volunteer, write to dkeller@uakron.edu. Also send opinions on what you like and do not like about the White paper.

When does this have to be rewritten? Minor re-write at 2002, Major re-write 2003. Kingsley Meyers, and Bill Mayhew volunteered.

Debbie had a separate request - she is teaching a class and is looking for volunteers for students to interview to see what it is like to work in this field. Email her above if you are interested.

ENSS - Jack Maher/ Brian Moeller

Brian Moeller is new staff. He came from OSU was on the OSU response team. He did the incident follow-up after the initial investigation. He would meet with the department after the incident to discuss how the systems were broken

into and how break-ins could be prevented in the future. They developed a firewall on a flash card that uses stateful packet filtering. The card has about 80% of the functionality of a commercial firewall. They use commercial generic hardware to build the firewall. They've made two production runs of firewall systems since January 2002. They haven't done any formal performance testing, but the unit has been used on a 750-user network. There are no drives in the system. Ruth or Christopher can work as contacts for information on the firewall project. Brian is heavily involved in CISSP and the FBI infraguard program.

This summer a group of security specialist did a survey to determine the security risk assessment of columbus. Downtown 33 access points with a large number of them with no protection.

How much traffic does their HW handle? Have tested it with 700 users and gotten good response. It is an Intel P3, 933 Mhz cpu with 2 Ethernet adapters, and a smart card reader. To configure it you edit a configuration file. It is BSD based. If you're interested contact Ruth or Chris, or call ENSS directly.

They've done a wireless risk assessment of Columbus. In less than an hour, they found 33 wireless access points, 25 of which were not running WEP.

Anita Cook, Ohiolink

For the record - She hates firewalls. They are really busy, and they want to know what is happening on your campuses. The usage peaks are much higher than ever seen before in January. If possible, make browser time-outs longer to accommodate the [slow] speed of database access. A Compaq Storage Array Network has just been installed so that disk space can more easily be divided up to the machines where it is needed. Work on cluster searching is under way. Cluster searching has been in development for over a year and should be ready for use now. Due to state budget revisions, some less popular databases will need to be dropped. Some databases are being picked up voluntarily with funding from member institutions. III authentication: no changes anticipated. No current plans to integrate LDAP at this point, but they are able to function with an Oracle database. Now that Compaq (nee Digital) is joining with HP, tru64 UNIX running on the RISC platform will disappear in 2006. First plans are just now being looked over for dealing with this.

Thanks for the valentine hearts go to Julie and Ruth.

Lunch.

Bob Baylen, US Attorney, Southern District of Ohio
Federal Computer Crimes

He gave a summary of his background. Gregory Lockhart was not able to come due to surgery.

Ohio has 2 US Attorney districts: northern and southern districts. Bob is from the southern district. He will be talking about federal computer crimes. The numbers show that Internet users and e-commerce usage has increased immensely. Everything we do has something to do with computers.

A recent survey from the Computer Security Institute shows that there have been a very high percentage of security breaches. These breaches have been hitting close to home with things like the Lovebug virus. Attacks on the defense department have occurred via international juvenile hackers and students. Attacks have occurred to corporate America and government agencies to both email and voice message systems. Physical theft of laptops and computers can also be open to attack.

If you find a violation you should put a banner in place, turn on your audit trails, capture keystrokes, then call law enforcement. The privacy banner should be a generic banner that indicates that there is "No Right of Privacy in This system".

What is the Justice Department's response? It has a division of computer Crime and Intellectual property section of the criminal division in Washington DC. They coordinate the national response, and provide expertise for problems and training. Their web site is www.cybercrime.gov. Each office has a resident "expert" to help coordinate efforts. This person works with business, industry and government groups. They also work with the FBI's InfraGard and RECI (Cincinnati computer crime unit).

The FBI's response has been to set up the InfraGard and the National Infrastructure Protection Center (NIPC). They also have a laboratory Computer Analysis Response Team (CART) with regional computer crime units and every division has a special agent trained in computer crime.

Summary of "Who to Call" information from the handout:
At the local level you can call the Hamilton County Sheriff's Office and Cincinnati Police Division Computer Crime Task Force: RECI at Reci@fuse.net (513)946-6685.
At the Federal level you have the FBI local office (513-421-4310), NIPC

(202-324-0303), Postal Inspection Service (513-684-8000), U.S. Secret Service (513-684-3585), U.S. Customs Service (859-578-4600, 800-BE-ALERT, or 800-232-2538),

Computer intrusion (i.e. hacking): FBI, NIPC, US Secret Service
Password trafficking: FBI, NIPC, US Secret Service
Copyright (software, movie, sound recordings) piracy: FBI
Theft of trade secrets: FBI
Trademark counterfeiting: FBI, If imported, U.S. Customs Service
Counterfeiting of currency: US Secret Service
Child Pornography or Exploitation: FBI, Postal Inspection Service, if imported, US Customs Service
Internet fraud: FBI, Federal Trade Commission, if securities then the Securities and Exchange Commission
Internet bomb threats: FBI, ATF (513-684-3354)
Trafficking in explosive or incendiary devices or firearms over the Internet: FBI, ATF (513-684-3354)

A question was asked about their stance on the NetPD notices for Sony. He was not aware of the notices.

How is the secret service different from the FBI and CIA - the Secret Service protects the presidents, and work with bank fraud, and counterfeit money. They are connected with the treasury department. The FBI is responsible for Foreign Counter intelligence part of the justice department; CIA is off to the side.

Is there anything we can do if we receive unsolicited spam advertising child pornography? Yes, you can forward the mail to the attorney general's office so that they hear about the sites.

The justice department has the "Petite policy": if a matter is taken care of by the state justice, the federal will not prosecute again. The federal system is not setup to deal with juveniles, so unless it is a special case, juveniles would probably be taken care of with state agencies.

The traditional statutes may apply to the crime. As well as other special statutes such as the Unauthorized Access to Taxpayer Information statutes which does not allow IRS employees to access information with authorization.

The main statute for Federal Computer Crimes is the National Information Infrastructure Protection Act (18 USC 1030) that protects the confidentiality, integrity and availability of systems and data. A computer is defined as "an

electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions and includes an data storage facility or communications facility directly related to or operating in conjunction with such device."

How is the Federal Justice working with crimes committed from outside the country? There is a department working on relationships with other countries to ensure that they can get timely response from the other countries.

Section A1 of the statute acts on federal security issues and is probably not applicable here. Section A2 deals with unlawful access to computers without authorization or in excess of authorization. Criminal penalties for the violations get stiffer as the number of offenses increases. Section A4 prohibits fraudulent use or theft of data. The USA Patriot Act eliminated a mandatory minimum sentence of 6 months imprisonment for fraud and theft. Section A5A prohibits damage to system or data where damage is defined as any impairment to the integrity or availability of data, a program, a system or information that causes a loss of at least $5000, effects medical information, causes physical injury, threatens public safety, or is a system used for justice or national defense or national security. A5Aii prohibits intentionally accessing a protected computer (government or financial systems, or systems used for interstate or foreign commerce or communication) without authorization and recklessly causing damage. A5Aiii prohibits fraudulent password trafficking and extortionate threats. Restitution is mandatory in cases involving an offense against property and the defined civil remedy is civil action against the violator to obtain compensatory damages, injunctive relief, or other equitable relief.

Defined "kiddy porn". Knowingly possessing any material of child pornography that has been transported in interstate commerce is an offense. Items used in the pornography are forfeit. The justice need all the images of the child pornography, including the disk, cd-roms, etc.... SAVE all of them, but remove it from the network. You must show that the image was sent over interstate or foreign commerce using network logs and pc login logs. If you have pornography being stored on your facility, if you trace it back to a person you know or repeated from the same site, then take an image of the disk and send the image then you can wipe the disk.

How long do need to keep logs? 90 days is reasonable amount, but he was not willing to make a recommendation.

The Electronic Communication Privacy Act (ECPA) protects V-mail and E-mail. It says that it is a misdemeanor to access a facility through an electronic

communication service without or in excess of authority and thereby to obtain, prevent or alter the communications.

How do you determine authorization? If there is a password, it is an implicit notification that you must have the password as authorization.

Exceptions to the criminal provisions for email and voice mail apply to the provider, the user, if message is intended for that user, or the government in some situations. A provider to the public cannot disclose content except in a few instances (consent of parties involved, necessary for rendition of service or property rights of the provider.) Provider an access and disclose messages to a forwarder, and law enforcement if inadvertently obtained and pertains to the commission of a crime or immediate danger to a person. There are no prohibitions on disclosures by private providers. There are 2 levels of access: Subscriber information and content. The basic subscriber information can be subpoena, without notice. Content in storage 180 days or less require a warrant. Content in storage more than 180 days require a warrant without notice to the subscriber or with notice to the subscriber with subpoena or court orders.

Preservation of Evidence: you can receive a call to retain or save information for 90 days and an additional 90 days upon request. Procedures to access voicemail has changed from wiretapping rules to email rules. Subject to the 4 year sunset clause.

The USA Patriot Act was a response to the acknowledgement that technology outpaces the law. September 11th encouraged the government to move on this act. This act changed the Pen Register (collecting outgoing call numbers) and Trap and Trace (collects incoming numbers - Caller ID) rules so that it applies to any device or process that provides the same process, recognizing that pen registers are not just for telephones anymore. It cannot be used to obtain the content, only the numbers. It can get the headers, but not the subject or the message content. Order to authorize the pen registration can be authorized locally and a single order can be use to trace communications that originate in one district but that extend out to others. The DCS 1000 (Carnivore) is used when the law enforcement uses it's own equipment to install a pen register.

New law allows the law enforcement to intercept "computer trespassers" and help victims monitor computer hackers. It is covered by the 4-yr sunset provision. The computer trespasser is someone without authorization but does not cover those with "an existing contractual relationship".

These laws provide very important tools for law enforcement and must be used prudently. If a victim has been hacked then their advice is to 1) Have a banner in place, 2) monitor the attack, 3) preserve the record and 4) contact law enforcement either local or federal. This will require the filling out of an incident reporting form. For a federal offense the damage must be valued above $5000.

For reporting crimes see: WWW.CYBERCRIME.GOV

To contact the US Attorney offices:
Columbus: Deborah Solove, AUSA, 614-469-5715
Cleveland: Robert Kern and Linda Betzer, AUSAs, 216-622-3600
Cincinnati: Robert Behlen, AUSA, 513-684-3711

What about unauthenticated Internet access through the libraries - how does it apply? There is no legal liability to require authentication, but there may be civil liabilities.

What about if law enforcement subpoenas some information that we do not keep, are we going to be charged with negligence? They will take what they can get, but do not require that you log specific information.

Minutes approved.

Are we interested in looking at wireless policies again? Are there any hardware or software topics people are interested? How about an IPV6 program?

OARnet needs to upgrade many of the equipment on the net and will be contacting the various sites that need the upgrade.

There will be some discussion on use of the list and video conferencing of the meetings.

Meeting adorned.