OARTech Notes for October 9, 1996

Galen Work called meeting to order at 10:02 with introductions around the table. (See appendix 1. Note: some signatures were pretty hard to read; please print if your name on the roster to assure correct spelling!)

Moved to accept minutes from previous meeting. Seconded and approved by voice vote.

Call for any unfinished new business. Kingsley Meyer said, "thank you," for the email responses he received about Win NT utilities for managing large groups of users. He said that he'll wait for the 4.0 release before purchasing the Resource Kit.

Galen Work: reviewed the agenda.

Marlene: TCP SYN attacks. A normal TCP connection comprises a three-way handshake upon opening. A SYN packet is used to request an open connection. The remote host queues the packet and replies with a SYN ack, then waits for the client to give an ACK reply.

Normally, SYNs are queued for 60 to 75 seconds to account for latencies in the network. The hacker attack generates false SYNs from impossible IP addresses. The attack can not be averted. The management approach for now is to use netstat to monitor the attack. Recompile kernels to reduce the timeout and increase buffer space. Consult www.cert.net, comp.unix.security news groups, etc. A patch for Sun systems is reported to be at the alpha stage.

The router at the site under attack needs to be sampled. This then needs to be traced back to MCI. MCI has taken up to six hours to respond with a technician who can install a packet filter.

OARnet updates:

Larry: Recall, one year ago, OARnet had just undergone a major rebuilding of the staff and reorganization. At that time, there was capability to deliver 9 megabits/second to the internet. Current capacity is 135 megabits/second via 3 DS3 connections. Larry is preparing to address Osteer on October 30. Approximately
80-90% of the staff has been rebuilt in the last year. There is heavy

involvement with DAS and Ameritech to roll out the new T1 circuits quickly. There is a meeting every Tuesday morning, and Larry estimates that he and Ruth spend as much as two hours every day managing the project. The initial estimate was for 40 T1s, but more than 100 lines have already been ordered. Ameritech has extended themselves beyond their staffing ability to install lines.

Galen: GTE installed the end points on time, but Ameritech has not turned up the long haul circuits. Kevin reports a similar experience, also in GTE territory.

Ruth: SOMACS update.

Xavier, Franciscan, Shawnee, and six other sites have been installed. Two sites worked immediately, while the others have all needed additional engineering.

Mt. Vernon, Naz., Marietta, Denison, Findlay, Hiram and several others are in the next group. All these have the smart jacks already installed. The hope is for next week to have the circuits up.

Ruth recommends calling or email when one's site gets close to the install date. Q: does the contract have a penalty or sanction for missing the install date? A: No. Larry reiterated Ameritech's under-staffing problem. Q: how are the lines once they've been turned up? A: there have been no problems yet. Ruth recommends watching Ameritech invoicing. Ruth says that adjustments should be made relative to the date that OARnet approves the quality of the line. The installation fee: Ameritech is currently sticking by trying to charge $1429 for the B8ZS installation. Ruth recommends trying to negotiate with Ameritech. Email to ruth@oar.net.

Firewall presentation:

Steve from OSU. He's in charge of the incident response team. They currently have three ongoing criminal investigations. In short, they're a very busy group.

References: Chapman & Zwicky - Building Internet Firewalls

1. TCP/IP Security Issues and Packet filters
2. Outline
3. General Principles - Defense in Depth
4. Defense in Depth

5. General Principles - Don't trust the remote site
6. IP
7. IP
8. IP

Layers of defense. Defense in depth is a strategy that acknowledges that there is a possibility that a hacker could breach any one layer. There should always be a back-up behind any layer.

Restrict FTP to approved FTP servers. Steve has found a lot of what he calls, "accidental FTP servers." People install NCSA telnet or a similar package on PCS and don't realize that it may default to open ftp access to their machines.

Don't trust the source IP port. Don't trust that what you get is really from the host indicated in the packet headers. Apply careful use in access control mechanisms via tcp_wrappers.

Example: Packet filtering. This prevents inside addresses from coming from outside the LAN. Note that a local itinerant host, perhaps plugging into a vacant jack in a classroom, can still spoof a trusted host.

What's a packet header?

- Source and destination IP address.
- Checksum. (quality check, not an integrity control)
- Flags indicating fragmentation, offset.
- Options such as source routing.

What is routing?
The whole point of routing is to move data packets between desired places.

- Based on destination address.
- Get the net part.
- Look up in routing table.
- Forward to the next router (or final destination)
- Path isn't always the same
- Path in may not be symmetrical between source and destination.

IP fragmentation:

- Packets are subdivided to fit into maximum frame size that can be carried on a given transmission medium. Note that
- fragmentation complicates filtering. Note that the port number is only carried in the initial packet. Normally, this isn't a
- problem. There is one attack strategy that exploits fragmentation

to make the fragment look like a valid packet of another type.

UDP:

- Unverified delivery. Checksum may not be implemented by all vendors. Simple datagram delivery.

TCP:

- Verified delivery. Packets carry sequence numbers in addition to source/destination information. This allows the remote host to reassemble the data stream intact and in the correct order.

- establishing a connection:
  client -> server Sc+data (can filter this because ACK is not set on this packet)
  client <- server ACK(Sc)+data
  client -> server ACK(Ss)+data

ICMP:

- messages for the IP layer
  + echo request/response (i.e. ping)
  + port/host unreachable
  + redirect (only supposed to be from the nearest gateway)

Types of attack:

- Denial of service
  waste bandwidth, fill up hard disks, fill up connection tables
- Unauthorized access
  + authentication
    by IP address
    by plain test, reusable password
  + integrity of data
  + privacy of data

Attack methods:

- SYN flooding - denial of service
  + has to come from a nonexistent host to avoid RST replies
  + sen to a port the victim listens on
  + unique source port numbers
- Defense
  + close random ports when queue is full (most likely a hacker port)
  + decrease time out
  + ISS RealSecure or other auto-RST tools (use a heuristic approach)
  + block incoming or outgoing spoofed ports (while this won't

stop a SYN attack, this is a good idea and is also a good neighbor policy)

- TCP spoofing

  The UNIX remote shell utility is generally a good thing because it allows lots of administrative things to be done without putting passwords out on the network. What is bad is that hackers can exploit this by pretending to be a trusted host from an unauthorized location.

- Method: ICMP redirects.

  spoofing from a third party such as an internet service provider, monitoring an on-going connection.

  Defense:

  Block source routed packets.
  protect routes.
  block ICMP redirects.

  block spoofed, but keep in mind:
  don't trust non-local addresses.
  can spoof from the inside too.

- TCP Sequence Guessing Attack

  Normally, we need to see replies. However, if we can guess the replies, we can make up our own responses.
  A pretends to be T to rsh to V
  Traffic from V to T goes to T
  We shut down T with a SYN attack
  A has to guess sequence #s that V is using. Often this is all too easy.
  A sends initial SYN, rsh command, guesses ACK(Ss).

  Defense: block spoofing.

- Session hijacking:

  Encryption, link integrity. Can't prevent denial of service.
  IP watcher by Mike Newman at OnGuard System. This has built-in session hijacking.

- Host scanning:

  Hacker uses ping or a similar utility to find TCP and UDP services. There is a program called strobe that can do

about 10,000 ports per minute.

Defense: scan detectors. Find TCP half open scans.

o Routing and DNS attacks:

o Packet filtering:
block source routed packets
block redirects
block spoofed
only way to be sure - default deny

For TCP
Allow all outgoing TCP connects (requires ACK bit filtering)
Note: if you have a fast connection, exotic things like
tunneling IP in email is possible!

Allow incoming access to specific ports on specific hosts

UDP
Not connection based, so this isn't easy. Note that DNS and
NFS use UDP. DNS needs to get through a firewall, but normally
NFS should not be going outside your network. There really
isn't a good way right now to block NFS but also allow DNS.

TCP problem children:
Talk: uses both UDP and TCP. Solution: get rid of talk and use
IRC instead.

IRC: usually well behaved, but clients may be buggy. Subject
to social engineering attacks i.e. "I'll send you a cool game",
but that game turns out to be a Trojan horse. Direct Client
Commands are supposed to be for private conversation channels.

Identd: listens on port 113 for available service requests. IRC
makes use of this. Some IRCs won't connect back to you if you
aren't running Identd.

FTP: clients require an incoming TCP connection for data by
default. You can do this with a proxy or else use PASV mode.
Warning, the newer Solaris releases are using higher port
numbers in the 40000 range. Use care when setting up a firewall.

RPC services: They use random port numbers. Beware of making portmapper available. Making portmapper unavailable doesn't protect services. Recommendation, get a replacement port mapper from a security tools site.

Rlogin and rsh: Client port is below 1024. Rsh requires a TCP connection back to client to pass stderr. Uses IP auth, which can be spoofed. Don't allow user .rhosts. Replace this with ssh instead.

X: you're allowing incoming TCP connections to where ever your server is. Uses ports 2000-... and ports 6000-... Again, it is best to use ssh to tunnel the service.

UDP: block in general, but allow to a collection of main hosts. Ignore FSP. Archie - use www instead.

ICMP: Can't generally block... Block redirects from outside to internal hosts. Log and report excessive pings.

Multicast: Can you block it? IP in IP, protocol 4 in header. Once through, can IP multicast to port X affect any non multi-cast services? (Generally no, but are you sure?)

Packet filtering considerations
ICMP error or nothing?

IP dest
TCP, UDP dest port
TCP, UDP source port
TCP flags
IP options

Rule ordering - watch out!

Logging dropped, accepted, forward dropped.

Proper handling of fragmentation and reassembly.

Dynamic rules
Some do content based filtering
Morningstar / Ascend
Checkpoint Firewall-1

Do FTP, could do IRC DCC if they don't already
Use for authenticated access to the net

Favorite security sites: Coast.cs.predue.edu. This is run by Gene Spafford. Www.first.org. In particular, check out the German and Australian team. Mailing lists: bugtrack, etc. Papers: the Morris paper. OSU security meetings on 4th Wednesday of every month. Aegis is an informal security group that meets every other Tuesday for lunch. See www.aegis.gen.oh.us. The Aegis URL could change.

Q: How do you interact with the administrative group. A: Steve is the *the* security team, but works with other groups. He recently added a part time student is hoping to get a GRA soon. There is general cooperation and overlap with the administrative group.

Lunch break at 12:35.

Another fine lunch was provided by OARnet. Salad, lasagna, bread and brownies. Cost $5.00 per person.

Meeting resumed at 13:17

Safe PERL

Presented by Peter Murray at Case Western Reserve Library Information Services.

Case stared out with a secured machine. The staff reviewed proposed code submitted by clients on a line by line basis. The worked until the situation became untenable due to growing demand for services. The result was coming up with a system that would allow uses to write their own code without being able to compromise server security. The desire to integrate a safe version of the ph client, phf, was the impetus for the development. Embedded semicolons and back ticks in user input are potential security problems, allowing users to piggyback UNIX commands in input fields.

Wu-ftp is used to prevent access to the password file.

Perl version 5 introduced a safe compartment for executing Perl code with a new variable name space and operator mask.

The safe module consists of two parts. 1. A suid root cgi C program and a Perl wrapper.

The safeperl.c program: sets resource utilization limits, does safe string copying, de-escapes URLS to usable form. Gets the user ID passed in the URL. The URL would look like this:

http://www.cwru.edu/cgi-bin/AuroraCGI/username/progname/.....

Safeperl.c imposes location restrictions on the script location though use of constants in the source code.

Does a set uid and gid of user; changes to the directory of the user. Sets resource limits and priority.

Perl wrapper:

Perl version 5.001 is required, safe required, several local extensions required.

The wrapper provides facility for generating the standard header and footer. Key is the ropen function that limits the file operations and also prevents pipes in and out.

A mail subroutine allows mail responses to be put out with header showing that the mail came from the script maintainer.

Future plans are to add ability to read files outside maintainer's own directory. Depending on security consequences, writing to any file in the user home directory may be allowed. More intelligent handling of error messages - not just dumped into server's error log.

The White Paper:

There were no comments re: the paper.

Kingsley moved to accept the paper. Seconded. Adopted by a unanimous voice vote. The paper will be presented to Osteer at the October 30th meeting.

OARnet activities:

Gene: presented a map of the network. There is only one notable change:

the Athens POP is now fully activated. Cleveland is still a problem in that both LCI and Ameritech are involved. Things will clean up if Case can be moved. Currently, there is not enough information in anybody's hand to be able to move the line from one POP to the other. Instead, new lines will be installed. Traffic on the backbone has continued to increase at about the same exponential rate.

Gene hinted at an Educom instigated initiative to modernize the internet. CIOs from many large players were present to work on setting initial standards. The White House is expected to make a press release in the near future describing the plans for building the multi gigabit network. An ATM basis with IP v6 transport might be expected. This is not a public announcement at this time. The proposed network would be for education and research not a replacement for the commercial internet.

Q: why are there still POPs, given the postalized T1s? A: At this time nothing faster than a T1 is postalized. For the foreseeable future, high speed connections will retain distance sensitive pricing.

The VbNS tie connection is definitely, "go;" it has been funded. Access to the national MBONE network is one major benefit that will result. The implementation of VbNS and OCARnet are expected to begin shortly after the beginning of the year.

Kevin Earp: The support center has been making steady progress. Calls began to ramp up as the school year began. By the end of the summer, they were able to begin most days with no open tickets pending. They are still in the process of finalizing the Remedy ticket system. They are rolling it out this month. SSDS clients are getting training. Many OARnet clients have been entered into the database. The rest may be entered by the end of the month. The database will hold much relevant data, such as circuit IDs. The system will also hold a ticket history for each site. Kevin feels that the first year has been successful and they have learned much and also learned what they still want to learn. Please call or email Gene with any needs. Q: Has Cisco Works been installed yet. A: They are still working on it. They have found that Cisco Works uses more resources as each user goes on line. They want to avoid becoming their own best customer of resource consumption. Q: what about web access to tickets? A: perhaps by the end of 1996. That is the next agenda item for the consultants.

Greg: Ohiolink:

Ohiolink has had some hardware troubles. There have been a number of

disk failures. Greg has pressured his management to get RAID systems for everything. They have just added the 35th library system. There are 21 million items, with 5.9 million unique. The current rate is 10 million searches on an annualized basis. Power Pages is delivering about 50,000 pages per week.

New business? No new business.

There is no firm agenda schedule for December. The next meeting is December 11th. Please submit comments to Galen.

Appendix 1: Attendance Roster

Name	Representing	Email (if changed)
Bob Walker	Edison Community College	
Jay P. Blum	Thomas More College	
John Ship	Stark state College	
Bill Blake	The University of Findlay	
Galen Work	Wilmington College	
Kingsley Meyer	U. of Rio Grande	
Sheila Hollenbaugh	Wright State	
Dave Leitch	DeVry Columbus	
Kyle Strom	Denison University	
Kevin Luckhay	Denison University	
Andy Longbridge	Board of Regents	
Mary Copas	Board of Regents	
Tim Sell	AFIT	
Patrick Limpach	CWRU	
Bob Beer	Ohio Northern Univ.	
Tim Kincaid	Terra Community	TKincaid@TERRA.CC.OH.US
Patricia Vendt	WSU	
Elliot Jolesch	Oberlin College	
Bill Mayhew	NEOUCOM	
John Gruber	B. G. S. U.	
Mike Bartz	Univ. of Dayton	
Barb Deschapelles	Univ. of Dayton	
Sean Jayre	Heidelberg College	
Mike Andrews	Wittenberg University	
Scott Powell	Wittenberg University	
Peter Murray	Case Western Reserve Univ	
Corinne Bishop	OhioLink	corinne@ohiolink.edu

Jamie Rishaw	Mulitverse	jamie@multiverse.com
Robert Misiak	Multiverse	robert@multiverse.com
Lee Schultz	College of Wooster	
Greg German	WSU/ohiolink	
Gail Carelli	OARnet	gail@oar.net