Date: Tue, 10 Apr 2001 16:16:05 -0400
Reply-To: BEAMER@DENISON.EDU
Sender: OARTECH Mailing List <OARTECH@LISTS.OAR.NET>
From: Teresa Beamer <BEAMER@DENISON.EDU>
Subject: OARtech minutes for 2/14/2001
X-To: oartech@oar.net
X-cc: petersk@denison.edu, marshall@denison.edu
To: OARTECH@LISTS.OAR.NET
Status: RO

Oartech 2/14/2001

Introductions:

Antioch University: Bruce Friend
Bowling Green State University: Bill Bigelow, Matt Haschak, Shawn Parsons, Tom Roberts, Chris Toth
Case Western Reserve University: Eric Chan
Cedarville University: Gabe Custer, Alan McCain
College of Wooster: Lee Schultz
DAS, Ohio Department of Admin. Svcs.: Mike Yerian
Denison University: Teresa Beamer, Chris Marshall, Kevin Peters
DeVRY Institute of Technology: Dave Leitch
Edison Community College: Bert Waldrop
Heidelberg College: Kurt Huenemann, Sean Joyce
Kent State University: Ransel Yoho
Lakeland Community College: Dave Levine
Lorain County Community College: Tim Bramhall
Lorain County Community College: Norman Lease
Medical College of Ohio: Chris Bauer, Joe Kitting
Miami University: Tim Gruenhagen
Mount Union College: Alex Zumbar
Mt. Vernon: Tim Myatt
NASA Glenn Research Center: Dave Pleva
NEOUCOM: Bill Mayhew
OARnet: Gene Bassin, Clifford Collins, Christopher Cook, Nancy Drugan Koehler, Deborah Sanchez, Pankaj Shah
Ohio Northern University: Robert Beer
Ohio State University: Mowgli Assor
Ohio University: Ken Bailey, Josh Thomas
OhioLink: Anita Cook
Otterbein: Tim Pindell

Shawnee State: Jeff Blevings, Mike Pinson
Sinclair Community College: Roz Taylor
University of Dayton: Tim Harrington, Ron Wagers
University of Rio Grande: Kingsley Meyer, Mike Snider
University of Toledo: John Heiden
Wright State University: Shane Dawalt, Patricia Vendt
Xavier University: Carl Dickhaus

Minutes were approved.

There was some discussion on future topics. Two topics that will be discussed in April include Wireless (two vendors) also what kind of authentication and authorization. Cisco will be providing a wireless discussion for Osteer this may be a possibility for a speaker. Another vendor we may want to look at is Proxim. Another possibility would be Akamai.

June will be more of a picnic, informal. We will have people visit to provide a discussion of what they are doing in their new position.

Cyber Crimes,
Steve Romig, OSU Security Team & Rick Amweg, OSU Campus Police

Non-crimes include free speech issues and policy violations. They are concerned that for non-crimes that the policy be enforced but at the same time protect themselves from lawsuits.

Steve is the manager of the incident response team at OSU and has 2 full time staff, 6 undergraduate students and 1 graduate student. They get involved in the reactive investigation of activities and work with the campus police to do reactive investigations. They also do some proactive work in scanning their own networks and sending the results to the various departments in hopes they will fix the problem. They dump all the information into a database and have students go through and based on policy decide what the team will ignore and what they will act on.

One of the tools they use is SNORT - a pattern matching detection program available at www.snort.org

The incidence response team works with campus police to determine what information they can look at. They must have permission to look at information on a specific person. Most of the detected violations are violations of laws. The students get a warning the first time, then police are sent in for the repeat offenders.

Rich provided a hand out of the applicable statutes. These laws are relatively new, only about 4 years old. Currently there are 2 bills pending - one in the senate and other in house - will apply to the definitions used in child pornography cases. In the past the definitions applied to child pornography has been objects that you can touch - paper, pictures, etc.... The images on the screen are not things that could be touch. The bills redefine the materials. The senate bill is related to dealing with spam. The lawmakers are beginning to become more computer savvy and so we will see some rewrite of current laws to include computer issues.

Any jurisdiction through which an offense travels has jurisdiction over the case. For example, if someone from California uses OSU for dos attack then the case could be dealt with in Ohio. There is no jurisdiction over international attacks.

Are other countries doing the same as the US? Some are doing some and some are doing nothing. Most are not moving at the same rate as the US. There are extradition issues that occur with the differences between countries and each country will look at the possible punishment of the crime when deciding on extradition cases.

There are some laws on the books that allow Ohio law to apply in another state, if they have laws on the books that applies to the crime.

Theft - says nothing about computers, but can be applied to any loss of property, ideas, time, etc....

Unauthorized use of property, computer - telecommunications property - paragraph B applies to stealing accounts, and breaking into computers. It grew out of the automotive statutes. This new law is about 4 years old.

Telecommunications fraud - deals with cable television signal fraud and includes computers in its definition.

Tampering with records - OSU is dealing with this more and more. One of the problems with stealing data, in that the perpetrator will take a copy leaving the original there. You have to determine how the theft of that data is valued. Right now it is done on a case by case basis. If someone tampers the data, it will question the validity of the research data if no backups were available.

Telecomm harassment - replaces the old telephone harassment statute. It is

relatively broad and forward-looking and has been looked at by other states when defining their statutes. This crime can apply even if the phone was never touched.

The "denying access to a computer" statute was removed off the books and rewritten into the Unauthorized use of property statute.

There are limits before the FBI will be involved. Getting them to get involved in prosecution is a little harder. They will not be involved in juvenile crime. They will turn it over to the local authorities.

Copying copyrighted material is considered a civil issue. Distributing the material is considered a criminal issue. What about servers - what is the liability? It depends on the specifics of the situation. It depends on the notice of the activity and if notified, they must act on it to reduce the liability. If notification is from outside the US then it would be turned over to police. If copyright is the issue then they will act on it. If computer harassment then they will act on it, but there are free speech issues?

What about log information? Student information is not given out. If request is from outside it depends on the case.

What about scanning? Yes, it is fundamentally illegal, but finding a way to prosecute is very hard. You have to fall back to local policies to stop the activities. A knock on the door quite often takes care of the problem. If their activity continues then the police do the knocking. If the issue is escalated then they could prosecute as illegal activities.

What about the remote scanners that gets put on user's computers without their knowledge? Use it as an educational moment on virus scanners etc....

What is the definition of access? There is none currently in the code. That line has not been defined as yet. It's a case by case situation.

What about scanning the user's computers for maintenance? This falls under the keeping the network running.

OSU has a paper acceptable use policy that each department must sign to get a connection to the network. This gives it permission to check the network for vulnerabilities. They have used this to looking at even the servers/boxes in the departments. The do not do the scanning on student halls. The residence halls have added something to the contract to give them the right to scan

those machines.

When do you determine you need to bring out the "big stick"?

Scanning is looking for network vulnerabilities, not criminal activities. If there is a criminal act that has been reported (someone has called it in) then those are handed off to campus police to investigate. IT has basically free rein in what they have to do if it is to keep the integrity of the network intact.

What do you do when you are looking to fix a problem and find another issue that is clearly illegal? The issue gets handed off to the legal authority. If it falls in law enforcement, it must have court order, etc....

If he is investigating a criminal report on an individual, then he doesn't go out and give a warning because as soon as he turns his back the information will disappear. Instead he would report it to law enforcement and get a warrant and get the system with the information. Note that for child pornography, it supposed to be reported under law. You are not supposed to wait and see what happens.

Who does the copyright designee for OSU - probably the legal department and may actually be an email address.

Investigation of an incident:

Occurred 19:00august 27, 1996
Initiated by a call to Steve from a California ISP that they had been broken into from OSU. He confirmed the activity and found that they had seen several previous incidents for this intruder. They gave him the IRC handle and so checked through logs for that name and found that this person was coming into the modem pool using multiple accounts. Requested a phone trace - required the trunk ids and line to get - legal needed to get involved to get the information. Was a circus in getting the permission for the request it took months to get the information. Ameritech does keep records and can request traces after the fact. When they got the information it came as 3 boxes of greenbar report, even though he requested that it be sent electronically. Today you can get it in hours on a CD. Lesson - work out procedures and information required with your local police and phone company ahead of time.

OSU knew what accounts were being used so they did a tcpdump (check with your lawyers on electronic privacy act on how it applies to network traffic). Eventually, they got tired of starting tcpdump by hand and so began to set it

up for electronic notification. OSU found that there were about 10 people, local high school age kids, involved. The tcpdump logs are very tedious to go through so OSU wrote some software to review dumps with a GUI interface and replay the session. Steve showed some examples of the log information and how it looks with the screen replays. Steve's group also wrote a special replay for an x-session.

They found that eventually the perpetrators were accessing military sites. This brought the federal entities in and complicated the investigation making it drag on for several years. Steve started looking at their network traffic and found the perpetrators were using private key and sending mail across in plain text. So when OSU got to the data, even encrypted, they could decrypt the data.

He had names, pager number, phone numbers, private keys etc.... But he still had to get phone trace before he could get a warrant. He found that the perpetrators were much more organized then expected. They were stealing accounts and there were some involved in stealing computer equipment.

The perpetrators were part of a group of the Dark Data Lorz or Lotek hacking group. Steve was updating a players list, where he has a description of each of the players and descriptions of where they worked etc., but not names, or addresses. They discovered that one of the intruders was parking in front of Rick's house every day after school and was dating a neighbor's daughter.

Summer 1997 - They wrote a quake proxy and learn lots about the quake protocol. The hackers played lots of quake as well (1/4 of the logs of tcpdumps was quake). They wrote a quake replay that created a demo recording that you could replay. This shows how much can be gotten via tcpdumps.

They were able to get all the pin registrations. And recorded the calls and then was able to use this to request the warrants. Naval criminal investigation got involved. Once it has been turned into the feds then the feds were calling the shots. They are still waiting for an end to it.

Slides are available http://www.net.ohio-state.edu/security under "talks".

Lunch

Support Center Update
Jodi Santini

Notice.oar.net site - They are still working to get an additional webmaster

for the address. All updates are currently being done manually.
Contact list updates are currently being done. Please update your lists - make any changes and send it back to support.
If they get a request for information, they will call or email the site and check to be sure this person is a contact and then send the information out, or will copy the information to the contact. Include HelpDesk information if you would like to have Oarnet or Ohiolink can know who to refer users for local problems. This information will be added to the notices page. If you don't see your site there, send a message to support@oar.net so they can add it.
Quality assurance information - how do we report these? Akamai servers this last week were compromised so there were some slowdowns there. Traceroutes and pings are very helpful when you find a slow down.

Pankaj Shah - Ohio ITEC Update: Windows on the Future event

Idea is to collect researchers in a forum that will allow them exchange information.
Target audience is VP of research and chairs of EE and IT departments. Would like a good cross section from the institutions. If you know of someone that would be a good speaker for this forum connect to the ITEC web site and give them the information and registration. This also ties into a grant proposal that has recently been submitted.

Do you see ITEC as being an on-going group? Yes. In North Carolina the research triangle where many of the manufacturers working together to further research was started with a group like ITEC. Someday, they may be self-sustaining from work in labs etc....

White Paper:
As of last Friday, the only submission was the security from Patty and PC from NEOCOM. Anita had provided the executive summary. We now have an additional submission for the Quality of Service. Bill will send the revised page tonight. Each site must read the document and respond by Thursday evening with an approved or not vote from each site. This would have the paper available for a meeting on Friday and then for the next Osteer.

Patty proposed that we revise the Whitepaper every other year instead of once a year. Proposal: We request that OhioLink advisory committee consider whether the Whitepaper could be revised every 2 years instead of once a year with a possibility of a technical addendum on the off year. The proposal was seconded. Passed unanimously.

Charles Morrow-Jones - K-20 Initiative Update
Is Internet 2 the right tool for k-12 to communicate with the I2 entities? Some I2 schools thought that providing a utility grade network connection for k-12 was contrary to the current definition for a high quality research network. Thus came the idea for a National Education Network (NEN). This would be a separate network from I2 and they are talking about using the Abilene network lines. What they see is three networks emerging NEN, Abilene (high speed - content), I2 (research). There is a meeting going on right now to try and put a structure on NEN. The proposal is 6 month to a year behind the I2 proposal.

Paul Schopis - QoS,MPLS and the Inner Child

Overview of Best Effort
Features -
Best Effort offers no guarantees for latency, jitter or loss. It is totally probabilistic. With TCP, if a device finds congestion it will back off. This provides a very bursty environment. UDP hasn't got any controls, and the control must be done by the application. On a network with both TCP and UDP, UDP will always win because TCP will back off.

The probability of delivery depends on the inter-packet arrival times. If the times are equally distributed the probability is high that one can achieve the line speed and thus avoid congestion since the service times are constant. What matters is the first 2 moments of the packet arrival distribution. The parameters you need to look at are the mean, the standard deviation of the service time. Uses a Poseidon function for modeling the traffic.

This means that even under ideal conditions the Internet cannot meet the needs of any application that requires a guarantee for any of the three parameters - loss, latency or jitter. Some days it will work and some days it won't.

Two types of QoS
Expedited Forwarding - uses strict priority, strict per hop latency, and a strict enformanet<?> policy. Anything that doesn't fit is dropped.
Assured Forwarding has a more vbr<?> like behavior. Profile violation is dealt in drop priority way very must like ATM clp<?>.

Currently most of IETF work seems to be in the EF and I2 is following this.

IntServ/RSVP - per-flow service state at every hop. Scalability problems, focus is on multipoint multicast. This is falling into disfavor.
DiffServ - Packets are colored at the edge to indicate the forwarding

"behavior". The focus is on aggregates not on individual flows.

Current trend is Expedited Flow with DiffServ.

One way to ensure queue rates on the router is to verify the ingress is slower than the egress. If the arrival times are faster than the outgoing you start to build queues and thus queuing delay.

The degenerate case - the classic over provisioning model - when you pop over the 1/2 limitation, then you start to introduce queuing delay.

So what does MPLS have to do with this?
Came out of the ATM and Frame relay environments. Multi-protocol and uses the same algorithm. The label n is the nth entry in the forwarding table. There is no learning curve because it is configured into the switch. See everything as an interface. All information is contained in the label. It is the basis for layer 3 traffic engineering.

Problems: How do you control the bandwidth allocation at layer 3? MPLS traffic engineering, but this only works if the glass is half-empty. What happens if all bandwidth is being used?

Solution is DiffServ Aware MPLS - protect the bandwidth so EF traffic is always preferred. It is configurable to avoid queuing delay and can control the jitter window to absorb small delays.

They are currently looking at this on Abilene - Concerned with someone setting the priority up high and thus takes over the bandwidth.

How close is this to reality? Currently available for Cisco products. But it can grow to be very hard to manage. Can use BGP community tables for controlling who has access to a tunnel. Can use it change behavior from the standard TCP behavior.

How useful is this to the campuses? May be useful to the larger campuses, but may not be time efficient for small campuses.

I2 QoS Working Group looking for a diffserv solution for Abilene Premium service. They were testing Diffserv with Cisco equipment with a pre-release version of IOS and found that it worked as advertised in the docs doing MPLS forwarding, Constraint-based Routing, and Link recovery.

Recommended that they proceed with a limited field trial in Abilene.

Is this usable by OARnet? Yes, if you are using MPLS when you move from ATM to Optical, then you don't have to do anything to the routers. You would just use the same MPLS tunnels.

Patty asked if we could get an update at a future meeting an update on Ipv6 and where OARnet sees where it is going.

Web pages have been updated with the presentation slides and last meetings minutes.

Elections for chair are coming up. Nominations will be taken next month. Please get your suggestions to patty (pvendt@wright.edu).

Meeting was adjourned.