OARtech meeting
June 11, 2003
By Teresa Beamer

Meeting opened by Ransel Yoho at 10:10

Introductions

Security Update - Kent state is going to create a secure web site where minutes will be posted. Looking at meeting 1st Thursday of the month before the OSU Security meeting. A mission statement has been drafted: "Promote policy development, training, and collaboration on information security among OSTEER member institutions by facilitating information exchange consistent with the OARtech mission. An email distribution list will be setup for the security sub-committee. The general idea is a single representative should be on the list from each site.

Low Budget Cyber Vandalism
Mark Chapman, Omni Tech, Director of Info Security Solutions
<mark.chapman@omnitechcorp.com>

You want to be able to protect Information - It's about the Information not the technology. Often non-technical means of obtaining information can be used. We will concentrate on the technical aspects but we need to remember that it is protecting the information not the technology.

Cyber Vandalism is hacking, cracking, threats to the physical resources, committing financial fraud or modifying credentials. Low budget means $1000 or less, often less then $100. He is not endorsing any products only showing a snapshot in time of what can be done. New technologies are always emerging so it can only be a snapshot.

4 areas are becoming convenient, powerful and inexpensive: Electric power, communications, memory, and computation. These areas as they become more convenient, powerful and inexpensive can enable cyber vandalism.

Electrical power can be anywhere when you want it. Batteries and chargers can easily be misused for vandalism and terrorism. We need to think out of the box: e.g. using a small solar power panel to run a wireless PDA off the florescent lights in a remote area to run an illegal web site. Small generators have been available for many years. You need to think of this resource from a security perspective.

Communications resources are becoming anywhere and when you want it. Location information via GPS and motion sensors is readily available. For physical crime, what would happen if you were to put a GPS unit under the hood of all the security vehicles? What if there was use of motion sensors and cameras to view typing of passwords, or codes for physical access to computer rooms. Radio can use local area wireless with motion sensors to determine where people are or if someone has accessed an area. Don't miss the obvious things like binocular attacks. PDAs and cell phones can be used to access networks easily. There are cards available that can change the PDA into a cell phone. Tele-communications is becoming readily available with text messaging. Could this be used to cheat on a test? The point is we don't control the technology any more. Project this picture out 5 years. Convenience can be the opposite of security. Could a user use a camera phone to take a picture of a test and send it to a buddy? A wireless serial port is available that has a range of 3 miles using an amateur radio band that cannot be seen with 802.11 utilities. What if someone convinced you to put it on a console port? You can use this

also to connect to a PC serial port via PPP. USB wireless connector cards are available. Plug it into the USB port on a PC and you can connect via wireless.

Memory is getting smaller, faster and cheaper. Portable memory can be used for stealing and transporting data. Can people do exports from your databases? Key loggers are available that can just plug into the keyboard cables and send it via wireless to another location. What if someone put one in on a cash register between the card swipe and cash register?

Computation is becoming faster and available in more devices. For example look at the computational power on a PDA: there is a version of Linux for a PDA, with Apache tools in your gym running off the lights with a solar panel. You may not even find where the device is located. For about $500 you can setup a server on the PDA that can easily be hidden.

Tools that can be used
He was using a dual screened system and would drag and drop the windows to the screen thus showing only what he wanted showed.

He brought up Word, created a demo document, set a password on the document, and saved to the desktop. When you open the document it prompts you for a password. Lostpassword.com has a password tool kit that can be used to retrieve a password for MS Office. It tested 303,023 passwords in .02 seconds to let you know what your lost password is. Can be used for Outlook and Email accounts. Think what this can do for single sign-on. Can copy the password to the clipboard and paste into the password prompt box. Opened Acrobat document (.pdf) and put a password on this file. Used passware with a whole list of software they support. Showed it using a dictionary attack to determine the password of the document. It also saved a decrypted file unprotected that can be read with the acrobat reader. Also can look at the Internet Explorer settings and looks at the registry and removes the password. He was not using IE to save passwords, but IE still records them even though it doesn't fill them in. The passware found those passwords, even after he cleared cookies, etc.... To explore what can be cracked - do a Google search "how to password crack xxxxx" or "how to hack xxxx". Compare this to the security fixes from the vendor. Comment from the floor: look for pdl files.

Do sites use unencrypted protocols like telnet, ftp? Attackers can use ARP to gather a mac address and there is easy ways to poison the mac address. Ettercap can do sniffing across switched network. Knoptix can also provide same utilities. Used Vmware to show running Ettercap. It sniffed any to any mode and was collecting passwords in the various clear text protocols. It can collect from SSL 1 connection by using man-in-the-middle attack. The point is, if it is a known protocol, someone has a nice program that can view the information. You don't have to read the tcpdump. It does it for you.
Note this can also be done with a PDA from anywhere. Depcon conference is a big hacker conference and the contest is who can make easiest tool. How do you control this - can use ARPwatch to check if someone is using ARP spoofing.

Comment from floor this is a good reason for using sticky learning. It will keep track on the number of addresses that can come from the switch ports. Can set a limit on number that can access the port.

What is his favorite method to determine if someone is using Ettercap? Ettercap. Several other methods were mentioned from the floor. Ettercap will let you do several different methods of attack.

Vulnerability assessment tools can be used to check for problems. Several

sites were using Nessus. Nessus provides a framework for this information. Nessus gives a menu to run attacks against different hosts, network segments, etc... and gives you a vulnerability report. It can be used to gather information on the various network resources. It uses nmap to find the ports being used, find the hole, and connects you to the cert advisory and how to fix the vulnerability. This tool is essential for the network professional, but also to the hackers. Updates are gotten from the Nessus sites periodically. You can set it not to run the vulnerabilities that may crash your server. Recommends that you review the updates before you run them.

Does Ettercap run with a lot of OSs? It does work with a lot of protocols. Is there a Novell password cracker? Novell does a little better job of encrypting passwords. He does not know of a tool to crack Novell passwords available at this time. Often if it is hard to crack the protocol, the hacker will move to the workstation (windows).

Plug and Play allows you to combine inexpensive technologies in creative ways. E.g. LukeJack for phone, PDA, and GPS systems can used to keep track of a car or other item for less then $40.00. Can allow you run a gambling web server in remote unknown locations.

Resource hijacking can be use to steal your technology resources. Are you taking reasonable protections?

Malicious Tampering can be use to replace data in databases and include malicious code. If you use VoIP on a share subnet then a tcpdump can be used to do wiretapping.

What about Peer-to-Peer? Tunneling protocols in other protocols will allow you to connect, and provide access of various types. You should be doing some packet filtering firewalls to take reasonable measures to reduce the risk. You need a policy in place and be able to enforce it. There is no such thing as 100% secure. You try for the 80-20 rule. Try to get 80% secure.

Comment from floor - if you run Nessus on your network you'd be surprised at how many professors have important data that is not secure.

Thanks to Jon Langis and Arif with videoconference connection. They will have this available for future OARtech meetings. They are not recording.

Lunch

OARnet updates

Al Stutz
Paul is now chief engineer with OARnet. OARnet wants OARtech to be involved in the network at the beginning. If you have issues, don't let it stew. Call Paul, or call Dennis. Let OARnet know. Looks like they are on track to have President Bush here for the "first lighting" (they have a link to Chilicothe already lit). This will help with project visibility and project funding.

Dennis Walsh
Project Manager for TFN
Major developments have occurred recently. They were looking to bring net up by April 2004. The new target date for getting the backbone circuits up is Jan 2004. This will save some money as we move main circuits over. They are still standing by the 4-phase schedule. They are still in phase 1 to bring up the network. There are some schools that are starting to look at building out to the connection point instead of waiting for OARnet to provide the link.

OARnet is beginning to look at the costs for last mile connectivity. They should have the RFP by the end of the month. If you have any fiber providers in your area that you would consider using, please get that information to OARnet so that those providers can be notified of the RFP. The structure is usually a local provider that can respond can get better pricing.

Looking at Public Utility funding for more funding for the project. OARnet is seeking funding for those pops in the Ameritech areas. They have come up with a proposal of 10 additional pops in the Ameritech areas that can be funded to extend these pops to the remote areas. This proposal is competing against at least 7 other proposals.

Paul Schopis
OARnet engineering team is focusing on running the fiber network. Do people find the trend software useful? Sent a mailing with this question, but only 3 responses. He wasn't sure how to read it. Is asking the question here to see if he can get more info. Currently looking at MRTG and StatScout.

Another package is RTG -similar to MRTG but will store to disk and keep the granularity over time.

Feedback at the meeting indicated that the average, standard deviations are good statistics.

The netflow project is up and functioning. Some I2 sites have received the equipment.

Working on a looking glass site to allow users to look at the routers on the net for testing. Paul did a demo of the site www.eng.oar.net/lg/. The password was given out at the meeting.

OARnet/OARnet
This site will allow you to do ping, traceroute, back to sites to test from outside your net. They will control the number of users that can use it at any one time and will be restricting it to OARnet members. May in the future make it available to I2 members. They are also looking at using secure ID for router access to increase security on the routers. He went over the router naming.

They are re-evaluating peering. They are looking whether to peer at Washington DC. Does anyone have comments? One comment from the floor is that we need more information.

Linda Roos
This afternoon at 2:00 David Barber will be introducing the grant proposals in the technology initiatives program here at this location.

Christopher Cook
There are some companies that are interesting in testing spam/virus filtering for evaluating this third party product. If you have any more information for the web site send it to ccook@oar.net net. There is a TFN joint committee meeting next Wednesday. If you are on a committee plan to come to the meeting at OARnet.

Patty Vendt indicated that a 45 Mb PVC link through the DREN to AFIT and other Wright Patterson labs is now passing packets. This is a totally parallel non-milnet network to show it can be done. They have been working with milnet, Abilene, and OARnet to get it up. If you are doing collaboration with AFIT you should contact Patty at Wright State to see about participating.

April minutes were approved.

Adjourned.

_____
Oartech mailing list
Oartech@lists.oar.net
http://lists.oar.net/mailman/listinfo/oartech