Pace Network Security and the End User
Presented at the February 21 and 28, 2006 IMO Meetings
Michael A. Malaspina, Network Services Department, DoIT

Good Morning Everyone! Today I am going to go over the basics of Pace Network Security and the End Users. I would like to touch upon the types of network attacks and some steps we all can take to protect ourselves.

Network Security in the workplace can be compared to Personal Security at home. The network attacker can be compared to a burglar or even a spy. The burglar comes into your home “once” and steals belongings (jewelry, cash, appliances…). Once you determine the point of entry, you can harden the security there. Double locked windows, stronger locks, alarm systems and so on. But it is too late, you’ve been robbed.

The spy comes into your home and may steal belongings, but more importantly may also leave behind listening devices, video devices and other surveillance devices. They may also “take” things from your home in the manner of bills, bank statements, and other documents. This is like the experienced hacker/attacker. At this point, they can keep attacking you long after the initial “break in”. In computing terms, such things as identity theft, compromising data, password cracking, viruses, Trojans…all very serious compromises.

Just like being pro-active in your home and installing alarm systems, locks and taking such steps as shredding your unused papers and keeping documents in a locked safe, we can do the same for our computers and network.

It is very important to keep your Operating Systems up to date with current patches and current virus protection. There is also some third-party software available to help protect your systems. Lavasoft’s AdAware, and Microsoft’s Anti Spyware to name two. But just like having the protections in place at home, if it is not used properly, then it will not protect you the way it was designed. So keeping the .dat files up-to-date is important.

Also, in regard to your files on your computer, there are steps to take to make sure you are protecting the data.

Do not create share folders or shared files on your computer. If there is a particular need to do so, make sure that the share is either password protected or shared only to particular users. Most programs can also be set to have a password in order to open a file. This is helpful.

In mentioning passwords, it is important to note that the new procedure in place to use hardened passwords is critical. When creating passwords for other “Non-Pace” systems, try to use the following this rule: upper/lower case letters with numbers and/or special characters.
There are many systems installed on the Pace network which help us at DoIT to maintain a secure system. Some of these, such as hardened passwords and authenticating to wireless have created grumbling among the Staff, Faculty and Students. “My password is so complicated I can’t remember it!” “Why do we have to log in to the wireless?”

But, these procedures are important to maintain security. Also, with the new system there is a single sign-on, one userid – one password. No more need to keep track of many different passwords. And, remember your password is “your” password. Do not give this password out to anyone, no matter whom. If the person needs access to some of your data, is a better idea to get the data for them and give it to them.

Some systems installed on the Pace Network are transparent to the regular Pace user.

Let’s start at the client and watch as data travels from the user’s PC to the Internet. The user turns on his/her PC, you are then prompted for a username and password on the Pace domain. Once you have clicked “OK” or pressed the enter key, this data travels over the Verizon network connecting the Pace locations together and is compared to a list of usernames and passwords on a server in Briarcliff Server Farm. Once it is established that this is a valid Pace user, you are “logged into” the Pace domain.

Now you open up Internet Explorer (or another browser) and go to the Internet. The data travels over the same Verizon link to Briarcliff. The first stop is an IPS/IDS (Intrusion detection/Prevention) system from McAfee. This device monitors all data traffic to/from the Internet. Inside this unit is a list of signatures of malicious behaviors. Everything from back door program to DOS (Denial of Service) attacks. Your data (opening a web page) is determined to be “clean” and allowed to the Internet. If you had a virus/Trojan on your computer and this data was being sent to the Internet it would be stopped and the event would be logged. This is where most of “illegal” traffic is stopped, including file sharing or P2P (Peer-to-Peer data.)

Next stop, the FireWall (FW). The Pace FireWall has a list of rules that monitors the traffic to and from the Internet. Based on where that traffic originates (Staff, Faculty, students) the rules will either allow the traffic through or deny access. Based on TCP/IP ports and IP addresses, the rules protect Pace from being “open” to the Internet. Depending on the FW rules, data is passed through a filter that determines whether or not the data is “clean”. Your request to open a web page passes through the FireWall and continues to the Internet.

Next stop is the Quality of Service box. The device looks at the data and based on the type of traffic is assigned a priority. Web browsing is assigned a High priority, while other types of data get a lower priority. During the normal business day, students are assigned a low priority to allow data to pass freely to and from the Internet. There is a daytime schedule and a nighttime schedule. At night the priorities are changed to allow students a higher percentage of Internet bandwidth.

Last stop, the Internet router. This device connects us to the Internet through our Internet service provider. There are also rules and configurations on this device to pass the data through to the Internet, and to make sure the data finds its way back to Pace.
Your request now travels the Internet, jumping from router to router until it connects to the server that is running the webpage. The webpage data now travels backwards, using your originating IP address, through the same path, to Pace and passes through each stop. Internet Router, QoS device, FireWall, IDS/IPS and back through to your PC.

Knowing now how the data passes through to the Internet it is surprising how quickly that webpage displays on your PC. Sometimes web pages are either compromised or “built on purpose” to download a Trojan to your PC. These types of Trojans can do numerous things. They can “hijack” your browser – so that as you browse you will continually get “POP-UP” windows appearing. They can change your home page setting so that you can not change it back, and they can add Search bars to your browser. This is why it is important to be running some type of ADaware software. Most virus protection software will also detect this Trojan and stop it from being installed on your PC. Most ADaware software will detect and remove this once it has been installed. This underlines the fact of how necessary it is to be proactive with your updates. If your virus or ADaware software is not up-to-date, these types Trojans will not be protected against.

Again, as with any type of security, you are secure as you make yourself. You get out of it what you put into it. Locks, alarms, safes, these are all important but if you do not lock a door, set an alarm, or use the safe; it is just like not having them. Start a new habit, check your files, update your software definition files, run Microsoft update. Choose a time of day, beginning or end to put aside time to make yourself secure. Educating the user in these steps makes Pace a more secure environment.

I take Network Security very seriously. With the help of my staff, we monitor the Pace Network daily to maintain a secure network. The few devices I mentioned earlier, from the FireWall to IDS/IPS device, create log files that we browse through daily and make sure we haven’t been compromised. These devices will also send us alerts in the case of an active “attack”. We are also always researching new software/technologies that will help us maintain a secure network. Just like a good detective we have to think like the hacker in order to stop or catch them.