PEPP VNC Security Issues

This page gives you more information about a few details of running VNC to display real-time seismic data related to security. This material is important if you intend to give any student access to the vnc display.

Passwords:

Computer security is becoming an increasing concern everywhere. For this project we are very conscious of this because we are hoping this will grow as people find out about us. The wider the audience the greater the concern about security as we more and more removed from the individuals involved.

The first point is a ground rule. We DO NOT want you to widely advertise the login password of the account we assign you. For now participants in the program will be given a regular login on the aesn machine, and with that entry any self-respecting hacker could do almost anything to bring the machine down if they chose to. Consequently, teachers, please DO NOT give this password to your students.

Now there is hope here because there are two different passwords you need to obtain entry to the system via VNC: the account password, and the password you give the vncserver. The vncserver password can be more widely distributed with less concerns than the account password. The reason is that we are working on a process to lock down the vnc display so that if one enters through a running vncserver they cannot access the full suite of unix programs. This will prevent a student with internet access at home from connecting to the vnc display and doing something malicious.

In any case an important rule is: CHANGE ALL YOUR PASSWORDS FREQUENTLY! This is especially true of the vncserver password. If tell one student assume the whole school knows it. We would advise you to change it at the end of the school day if you ever give it an entire class. It is your judgement call what to do if you give it to a select group of students, but keep in mind kids exchange information like this often so it would be wise to devise a scheme to change the password often or routinely shut down the vncserver at the end of the school day. We just ask you to recognize that an open vncserver is an invitation to any budding young hacker to do a long list of nasty things.

Given this, you need to know how to do three different things:

1. Changing your account password:

Use the telnet method described in the introductory page (vnc introduction) or ssh (see below) to connect to aesn. Issue the command:

```
passwd
```

and the system will prompt you to enter your new password. You have to type it twice to make sure you didn't make a typo in the first try.

2. Changing the password for VNC

Login to aesn using your account and password (as described immediately above) and just type:

```
rm .vnc/passwd
```

This will delete the file that contains an encrypted form of the vnc password. After this you will need to restart the vncserver like you did the first time you ran vnc (see vnc introduction)

3. Shutting down the vncserver

The most certain way to stop unwanted access to your account via vnc is to kill the vncserver when you aren't actively using the system. To do this you need to know the "display number" of the currently active vncserver (typically something like :1, :2, etc.) Again you will need to use a telnet or ssh communication procedure to login to aesn. Once logged in you will need to issue the following commands:

```
cd .vnc
vncserver -kill :1
```

where the :1 would change if the currently active vncserver was assigned a number other than 1. (e.g. vncserver -kill :20).

Note, of course, that you will have to go through the startup procedure again the next time you want to use vnc on aesn.

Use of ssh instead of telnet:

A more paranoid suggestion is related to the inherently insecure nature of transmissions via what is commonly called "clear text". That is, most internet software is rapidly moving toward the use of encryption to keep "sniffers" from grabbing communications traffic that is especially sensitive (e.g. when you change your password). A serious concern is that telnet traffic is insecure and easily grabbed by relatively unsophisticated

hackers. The best solution in interactions with us is to use packaged used on unix machines called "ssh". If you interact with aesn often, we urge you strongly to install ssh on your machine. A useful page describing how to do this and pointing to a source can be found on ATT's documentation for vnc at vnc and ssh.