VNC on Unix

The use of VNC for remote connections is not recommended by the Cyber Security team and VNC is not a centrally-supported service. The supported solution for remote graphical X11 connections for Unix is FastX. If you choose to use VNC without support, it is your responsibility to follow the guidelines below.

What is VNC?

Virtual Network Computing, or VNC, is a protocol by which one machine can access another's desktop. VNC client and server applications are available for both UNIX and Windows platforms. This page pertains to VNC on UNIX platforms only.

VNC has several security weaknesses. The SLAC Security team recommends that VNC not be used at SLAC. However, if you must use it, there are ways to mitigate some of its weaknesses. You should use **all** of the methods listed below.

If you don't need to use VNC, please delete your ~/.vnc directory.

VNC Mitigations

1. The VNC password is stored within your home directory space, in ~/.vnc/passwd. The password is weakly encrypted but anyone who can read the file can easily decrypt it. Thus, you must ensure that your .vnc directory is not SLAC-readable. One way is to use the AFS commands:

   ```
   fs setacl ~/.vnc system:slac none
   fs setacl ~/.vnc system:authuser none
   ```

   which removes read access by other SLAC users.

   Note that if you had a password in your ~/.vnc/ directory for any period of time before changing the ACL as described above, that password should be considered compromised. You should terminate any existing VNC servers and use a new password if and when you start a new server.

   Furthermore, if you have used the same password any where else, e.g., as your login password for SLAC UNIX, you should also immediately change those passwords.
2. Ensure that your VNC password is a strong one and change it frequently. Do **NOT** use the same password for VNC and any other use, such as for logging in to UNIX or Windows, in case your VNC password is compromised.
3. Add the options -localhost -nolisten tcp when you run the vncserver command to start your Xvnc server:

   ```
   vncserver -localhost -nolisten tcp
   ```

   This will foil scans and connection attempts from random hackers over the Internet.
4. Since the connection between vncviewer (the VNC client) and vncserver is not encrypted, it is essential that you use an encrypted channel such as an ssh tunnel rather than connecting directly from vncviewer to the vncserver. With the version of vnc distributed with RHEL this can be done using the '-via' option. This option automatically creates an SSH tunnel between the client and server machine. For example, to connect to a vncserver running at mydesktop:1, use the command

   ```
   vncviewer -via mydesktop localhost:1
   ```

   For more information about the '-via' option, see the vncviewer(1) man page. For other versions of vnc, see Tunneling VNC over SSH with PuTTY for help setting up the SSH tunnel.