NCCS Cyber Security Training

Version 1.1
10/11/07

INTRODUCTION

The National Center for Computational Sciences (NCCS) computing resources are provided to approved users for research purposes. All users must agree to abide by all security measures described in this document. Failure to comply with security procedures will result in termination of access to NCCS computing resources and possible legal actions.

SCOPE

The requirements outlined in this document apply to all individuals who have an NCCS account. It is your responsibility to ensure that all individuals have the proper need-to-know before allowing them access to the information on NCCS computing resources. This training will outline the main security concerns. Specific use policies are covered in the NCCS Computing Policies document.

PERSONAL USE

NCCS computing resources are for NCCS business use only. Installation or use of software for personal use is not allowed. Incidents of abuse are will result in account termination.

Inappropriate uses include, but are not limited to

- Sexually oriented information
- Downloading, copying, or distributing copyrighted materials without prior permission from the owner
- Downloading or storing large files or utilizing streaming media for personal use (e.g., music files, graphic files, Internet radio, video streams, etc.)
- Advertising, soliciting, or selling

ACCESSING NCCS COMPUTING RESOURCES

Access to systems is provided via Secure Shell version 2 (sshv2). You will need to ensure that your ssh client supports keyboard-interactive authentication. The method of setting up this authentication varies from client to client, so you may need to contact your local administrator for assistance. Most new implementations support this authentication type, and many ssh clients are available on the web. Login sessions will be automatically terminated after a period of inactivity.

When you initially receive your accounts, you will be mailed an RSA SecurID key fob. This device displays a numeric code that changes every 30 seconds. When you first log in, you will be prompted to select a PIN. After that is set up, you will use your PIN followed by the code on the key fob (this combination is called a PASSCODE) to authenticate yourself to the system. All users are given access to a general purpose IBM server that can be used for accessing your home directory and setting up your initial PIN. To access this server, log on to home.ccs.ornl.gov

DO NOT share your PIN or key fob with anyone. Sharing of accounts will result in termination. If your SecurID key fob is stolen or misplaced, contact the NCCS immediately and report the missing key fob. Upon termination of your account access, return the key fob to the NCCS in person or via mail.

DATA MANAGEMENT

The NCCS uses a standard file system structure to assist users with data organization on the systems. Below is a brief introduction to the most common file systems all users should be familiar with.

NCCS computing resources employ standard Unix file permissions as the primary mechanism for data protection. Permissions on all user home areas by default are set to 700. This provides the owner of the directory the ability to read, write, and execute files while disallowing other to do so. Users can change permissions on files owned by them to share data with collaborators. This can be accomplished through the use of the standard chmod command (see man chmod for details). Users are discouraged from changing permissions that would allow other outside of their Unix group to access files (i.e. chmod 755).

Home

All users are given a home directory. This directory has a quota of 2 GB (which can be increased with appropriate justification). This home area is shared between all systems. Since it is not local to the HPC systems and it is very limited in size, users should not run batch jobs that perform large amounts of I/O in their home directory.

Scratch

In addition to the home directory, users are provided a large local scratch area on each system. This file system is local to the HPC system and is much larger than the home directory. User jobs should perform their I/O to this file system. It can be accessed as /tmp/work/<username> on each system. User scratch directories do have quotas, although they are significantly larger than those of home. If a user needs an increased quota on the work directory, it can be given with appropriate justification.

NOTE: Scratch directories are not intended for long-term storage of data. They are temporary 'working' space. As such, a 'sweep' program runs daily and deletes files older than 14 days. However, files younger than 14 days can be deleted if it is necessary to increase space in the file system. Users are advised to store important files (executables/input files/output files) to HPSS as soon as possible. Users are also requested to delete files in their work directories once they have archived them.

High Performance Storage System (HPSS)

Access to HPSS is through the use of the hsi utility. You will be prompted for a SecurID PASSCODE to access the system. Access without the use of a PASSCODE is permitted for automated scripts. Data is less secure in the event of a security incident in this mode. Contact the NCCS if your require access to HPSS without use of a PASSCODE.

HPSS is optimized for large file transfers. Users with large numbers of small files should combine them into a single tar file and then transfer that file. Users should try to make the files they transfer to HPSS at least 1GB.

Sensitive Data

Additional file systems and file protections may be employed for sensitive data. If you are a user on a project producing sensitive data, further instructions will be given by the NCCS. The following guidelines apply to sensitive data:

- Only store sensitive data in designated locations. Do not store sensitive data in your home directory.
- Never allow access to your sensitive data to anyone outside of your group.
- Transfer of sensitive data must be through the use encrypted methods (scp, sftp, etc.).
- Sensitive data may be backed up to HPSS. The permissions on archived data must be 700.
- All sensitive data must be removed from all NCCS resources when your project has concluded.

One Bethel Valley Road
P.O. Box 2008, MS 6008
Oak Ridge, TN 37831-6008
E-mail: help@nccs.gov
Phone: 865-241-6536
Fax: 865-241-4011

DATA TRANSFER

The preferred method of transferring data to NCCS computing resources is through the use of Secure Copy (see man scp for details) or Secure FTP (sftp). This is a secure, encrypted method of transferring data. For large data transfers, it may be necessary to use the BBCP utility. BBCP offers parallel transfers of large amounts of data. BBCP must be installed and configured properly on your local system to be usable. Contact the NCCS if you need assistance in transferring large datasets.

One Bethel Valley Road
P.O. Box 2008, MS 6008
Oak Ridge, TN 37831-6008

E-mail: help@nccs.gov
Phone: 865-241-6536
Fax: 865-241-4011