NASA Science Internet

Introduction to Network Security

August 1993

Brad Olive,
NSI Network Security Manager

Prepared for the
NASA Science Internet Project Office
NASA Ames Research Center
By Sterling Software, Inc.
NAS2-13210-648

DO-SEC1042.0

NASA Science Internet

Introduction to Network Security

Brad Olive, NSI Network Security Manager

INTRODUCTION

Every person with access to the NASA Science Internet has a responsibility to the other members of the Internet community of making a good faith effort to keep their system secure. Security begins with the individual user. If a user does not take reasonable steps to protect their own account, their data, they may loose their data, as well as put the data of others at risk. Please forward any comments or suggestions about this document to: *bolive@nsipo.arc.nasa.gov.*

PASSWORD SECURITY

Every new user needs to keep a few things in mind. First, over 90% of the system breakins that are reported are due to easily guessed passwords. The NSI Security Group recommends that sites implement a password program that will not allow the user to select an easily guessed password. There are many programs available that do nothing but attempt to guess passwords using combinations of words from dictionaries gathered from around the world. The dictionary that NSI has obtained has nearly 1 million words including English (American, Australian, British), French, German, Italian, Chinese, Japanese, Dutch, Spanish and Yiddish, to name a few.

A password should never be a word that is found in ANY dictionary. A great way to pick an easily remembered password is to find a phrase that is easy to remember such as “Sitting on tacks is NOT a good idea” and use the first letter from each word. This phrase would result in a password of “SotiNagi”. Of course, this example should not be used. Passwords should be mixed case and have special characters or numbers in them. Never write a password down or give it out - even to a System Administrator.

ACCOUNT PRIVACY

NSI accounts are issued solely for the use of the individual to whom they have been assigned. Use of any other user’s account or loaning account privileges to another is prohibited and will be handled in the same manner a violation of the NSI Acceptable Use Policy.

If you notice anything that appears to be unauthorized use of your account or of someone else’s account, immediately notify the NSI Network Security Manager. Disruptive activity, such as interfering with another persons terminal, or attempting to capture information (including passwords) from other users is prohibited, and will be treated in the same manner as a violation of the NSI Acceptable Use Policy.

FILE SECURITY

Once a user has protected their account with a good password, they should take additional steps to ensure that their account is safe. Account passwords should never be written down or given out. A systems administrator will NEVER ask a user for their password. Anyone asking for passwords should be reported immediately to the local systems administrator.The next step in securing an account is to check that none of the files in the users home directory are world writable unless there is a specific reason. Files that begin with a "." should be protected at all times. When an account is set up, the umask and file permissions are initially set by the super-user, however it is always a good idea to check these files periodically.

USER ACTIONS

Users are also responsible for their own actions. Any user caught intentionally damaging a system, data or another persons account will have their privileges removed.This includes invading another persons privacy by trying to gain access to their personal data. Other prohibited actions include software piracy, wasting bandwidth or any violation of the Acceptable Use Policy.

ILLEGAL SOFTW ARE

All software maintained on systems operated by NSI are protected by various licenses and copyrights. Unless explicitly stated in the documentation, users are not permitted to copy this software. The NSI does not allow illegally copied software to be loaded onto any of its machines.

SECURITY POLICY

Attached is a copy of the NASA Science Internet Network Security Policy. This policy should be reviewed by all account holders.Violations should be reported to the NSI Network Security Manager.

ABUSE OF RESOURCES AND PRIVILEGES

There are may ways to abuse privileges on NSI systems. The following is a list of types of activity that may be considered abusive. As a rule, if it seems like abuse, it probably is. Misuse of resources and privileges includes, but is not restricted to, the following:

Violation of the NSI Acceptable Use Policy .

Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.

Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer , software, data, information, or network in question is owned by NSI.

Sending fraudulent, abusive or excessive computer mail or breaking into another user 's electronic mailbox.

Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper , written authorization.

Any activity that causes resources (including personnel) to be wasted as a result of misuse or abuse.

Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit written permission of the owner .

Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner 's explicit permission.

SYSTEM ADMINISTRATORS

Systems administrators are encouraged to obtain a copy of the NSI_Security_Primer Document and the NSI_Security_Archive Document for information about procedures, tools and other helpful information about network and systems security. These documents are available from the NAIC or via anonymous ftp at nsipo.arc.nasa.gov. They are located in the /pub/security/docs directory. Contact the NAIC at naic@nasa.gov or call 1-800-858-9947

VIOLATIONS, INVESTIGATION AND DISCIPLINARY ACTIONS

Abuse or violation of the policies related to system use will be handled in the same manner as violations of the NSI Acceptable Use Policy.

Hacking attempts may be investigated by a system administrator after reasonable evidence has been obtained that the activity was caused by or through a particular account. This may include monitoring the account and its contents for evidence that a hacking attempt occurred from or through the account.

If an account has been compromised, the NSI Network Security office should be notified via phone to assist in the investigation. The owner of the account may or may not be notified of the tracking of the account during the investigation. If it is determined that the account was compromised by someone other than the owner, the owner will be notified of the activity and given instructions on how to proceed.

Upon identification of a policy violation, several things may occur including, but not limited to:

Notification of the user's supervisor.

Suspension or restriction of the user's computing privileges. This action is subject to the ruling of the NSI Project Manager.

The users files, diskettes or tapes may be inspected.

If further disciplinary action is required, the action will be referred to the appropriate department.

It should be understood that these regulations do not preclude enforcement under state, federal, or international laws.

NASA Science Internet
Network Security Policy

NSI is fully interconnected with the Internet and other networks. In general, valid users enjoy unrestricted access. However, access from Internet or other sites to or through NASA/NSI resources is only authorized then that access is in conjunction with valid work or project-related requirements.

The use of NSI is inappropriate when that use:

- ❍ Compromises the privacy of users and their personal data.
- ❍ Damages the integrity of a computer system, or the data or programs stored on a computer system.
- ❍ Disrupts the intended use of system or network resources.
- ❍ Wastes resources (people, network bandwidth, or CPU cycles).
- ❍ Uses or copies proprietary software when not authorized to do so.
- ❍ Uses a computer system as a conduit for unauthorized access attempts on other computer systems.
- ❍ Consists of unauthorized and excessive snooping, probing or otherwise connecting to a node or nodes in a manner which is deemed not to be of an authorized nature.
- ❍ Results in the uploading, downloading, modification ore removal of files on any node in the network for which such action is not authorized.

Incidents of misuse and abuse of NSI by hackers or overly curious network users have necessitated certain limitations to be imposed in order to ensure the continued security and integrity of the network.

As long as the person's activity is related to and necessary for the completion of their work, then that activity is generally considered an authorized use of the network, and is allowed. In cases where a person's work might generate multiple or random network connections, it is advised that such activity be coordinated with the Network Operations Center or the remote system managers so as not to inadvertently cause a security incident.

NSI/1993

NASA Science Internet
Acceptable Use Policy

The NASA Science Internet (NSI) Mission is to provide a computer communications network designed to support NASA science flight missions, discipline research programs, and collaborating scientists affiliate research institutes.

SUMMARY:

NSI supports all NASA science flight missions, discipline research programs and collaborating scientists at NASA Centers and elsewhere.

NSI is not to be used for private gain or profit.

SPECIFIC:

1 Use of NIS must be in support of official NASA programs; all user requests for NSI connectivity must be validated and supported by cognizant OSSA Discipline Chiefs.

2 Use of NSI to support coordination and administrative execution of OSSA research grants is permissible.

3 Use of NSI to support NASA research, related training, and associated technical activities at non-profit institutions of research and education is acceptable

4 Use of NSI for commercial or intellectual gain by for-profit organizations is not acceptable, unless those organizations are using NSI to satisfy specific NASA contract or grant requirements.

5 Use of NSI for research or education at for-profit institutions will be reviewed on a case-by-case basis to ensure consistency with OSSA programs; lack of program approval will result in disconnection.

6 Use of NSI to gain unauthorized use of resources attached to NSI may result in disconnection and legal prosecution. NSI will make every attempt to implement precautions to safeguard against NASA computers, databases and other attached federal resources.

7 Use of NSI for the introduction of worms, viruses, trojans, or other software which maliciously interferes with normal NSI operations is unlawful.

NSI July 92

NSI-CERT contact information:

Report any security violations to the NSI-CERT immediately.

Brad Olive, NSI Network Security Manager NASA Science Internet Network Security Office NASA Ames Research Center MS-233-8 Moffett Field, CA 94035-1000 U.S.A.	bolive@nsipo.arc.nasa.gov nsi-cert@nsipo.arc.nasa.gov +1 415-604-0670 voice +1 800-998-6653 message pager +1 415-604-0063 fax machine +1 415-694-9970 numeric pager

Emergency contact if unable to reach NSI Network Security at the above numbers: NSI Operations +1-800-424-9920 or +1-415-604-3655