Notes on Securing a VMS DECNET Node

E.H. Harvey, Jr.

July 1988
DISCLAIMER

This document was prepared as an account of work sponsored by the United States Government. While this document is believed to contain correct information, neither the United States Government nor any agency thereof, nor the Regents of the University of California, nor any of their employees, makes any warranty, express or implied, or assumes any legal responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by its trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or the Regents of the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof or the Regents of the University of California.
Notes on
Securing a VMS DECNET Node
Everett H. Harvey, Jr.
Lawrence Berkeley Laboratory
University of California
Berkeley, CA 94720

This article describes some techniques for securing a DECNET node from unauthorized use. It is given in a cookbook-like style and is not meant to be a comprehensive guide to security issues, but it is intended as an aid to many system managers. Security becomes much more of an issue when a network is involved because the number of potential (mis)users grows rapidly. The first section shows you how to secure your DECNET node. The second section gives some ideas about allowing world-read access to files. The last section just gives a recommendation to use even if you do not have a network.

1 Secure Your DECNET Node.

Many VAX computer systems have been configured with a default DECNET account. This leaves the system open to outside (network) penetration. This note gives a simple method for removing some of the security risks, but at the same time allows general phone and mail access by all users of the network. The recommended method of transferring text files is to mail them to the recipient.

The default decnet account usually has the user name DECNET. The first thing to do is disable this account by changing the password. No one will be using this password, so make it a long string of at least 14 random letters and numbers. Use the AUTHORIZE utility to change it.

The following examples use a (non-random) "abcdefghijklmn" password.

$ set default sys$system
$ run authorize
UAF>modify DECNET/password=abcdefghijklmn
$ EXIT

This will effectively disable your default DECNET account. Now you need to enable PHONE and MAIL. To do this you use NCP to define a username and password for these two network objects. When you use NCP to specify the non-privileged decnet account username and password to the executor be sure that the password does NOT match the actual valid one created by the AUTHORIZE utility. As a reminder I have used the string "not_valid_here".

$ run sys$system:ncp
NCP>define object PHONE user DECNET password abcdefghijklmn
NCP>set object PHONE user DECNET password abcdefghijklm
NCP>define object MAIL user DECNET password abcdefghijklm
NCP>set object MAIL user DECNET password abcdefghijklm
NCP>define exec NONPRIV user DECNET password not_valid_here
NCP>set exec NONPRIV user DECNET password not_valid_here
NCP>exit

• Needless to say, you need system manager privileges to do these operations.
• Be sure and remove any FAL accounts (if you have any).
• Remove any NETPRIV account (unless you really need it).
• Test mail and phone access after making these changes.

On large networks, problems can arise that require some network debugging. These can be as simple as two nodes with the same address or as obscure as some strange hardware problem. For these reasons, it is necessary for a network administrator to be able to look at network operations of routers. (routers are computers that direct network messages to other computers. End nodes do not route messages. If you do not know your node type use the NCP command SHOW EXECUTOR CHARACTERISTICS and look at the TYPE field.) For routing nodes (but not end-nodes) it is useful to allow TELL NODE operations such as:

$ TELL NODE DECVAX SHOW KNOWN NODES

I therefore recommend adding a username and password pair to a non-privileged account for the NML.EXE object.

$ run sys\system:ncp
NCP>define object NML user DECNET password abcdefghijklm
NCP>set object NML user DECNET password abcdefghijklm
NCP>exit

where the passwords are the legal ones as for mail and phone.

2 If You Need World-readable Files.

Some installations may feel that the above environment is "too secure" in that world-read access is restricted. While I personally do not recommend allowing world-read access, the following suggestions may be useful for those sites that absolutely want some world-read access. Before implementing these following steps be sure to read the rest of this article. In general, you should worry even
more about security if you choose to take these additional steps. Education of users and a more vigilant approach to security is necessary. I strongly recommend that you carefully study the guidelines on security provided by Digital Equipment Corporation.

The idea here is to not allow write-access anywhere and to restrict read-access to those files where it is really needed. It is hard to enforce this strictly and all of your users should be educated on what not to do. This should at least include not allowing write-access and not putting things in files that they do not want seen. In general they should restrict files to no-world-access as much as possible. This last idea will be hard to sell in an environment which is pushing for world-read over the network!

Create an account in the system UAF using AUTHORIZE for the object FAL. Use a long random-character password greater than 13 characters in length. In the example I use the "abcdefgijkmnn" password again. Of course make sure the account has only NETMBX and TMPMBX privileges and has the flags set /FLAGS=(DISCTLY,CAPTIVE,LOCKPWD). Also disable batch and interactive access with /NOBATCH and /NOINTERACTIVE. Create the account with a different UIC (both group and member) from the default decnet account and from any other account on your system. Choose a group that is different from any other group in use on your system.

After the account is ready, create the default directory with a command

\$ CREATE/DIRECTORY SYS$SYSDEVICE:[FAL] -
   /OWNER=[ggg,mxx]/ PROT=(W:RE)

where the OWNER MEMBER of the UIC is DIFFERENT from the authorization UIC. If disk quotas are in use make sure that this group does not have any disk quota on any disks.

Some files should definitely be protected and must be checked.

\$ SET PROTECTION=(SY:RWE,OW:RWE,G,W) SYS$SYSTEM:RETUAF.DAT
\$ SET PROTECTION=(SY:RWE,OW:RWE,G,W) SYS$SYSTEM:SYSUAF.DAT
\$ SET PROTECTION=(SY:RWE,OW:RWE,G,W) SYS$SYSTEM:VMSMAIL.DAT

Any system-wide login command files should be protected with WORLD:E access only.

Now you are ready to define the FAL account in the DECNET database. Use the same password set in the FAL UAF account.

\$ run sys$system:ncp
NCP>define object FAL user DECNET password abcdefgijklmn
NCP>set object FAL user DECNET password abcdefgijklmn
NCP>exit
Test remote file access from another node after making these changes. Try to create a file in your own directory by using a copy command prefixed with your node name. This test should fail to create the file.

$ copy/log testfile node::.*

Now a user on an outside node can read any world-readable files! Any other worries? Well, maybe there are things you don’t want them to read. Set them to no-world access. This includes directory files if you do not want people to "browse". If a directory file has WORLD:E access then browsing is eliminated, but access to a known file name is still possible. Even worse, if you have world-writable directories files can be created on your computer. World-delete protection means just that too!

There are also many other things you may want to research. Most of them center about information that do you not want read; for instance: do any world-readable command files have a remote node username/password combination? Another common thing to worry about is employee home address and telephone numbers. The list of course goes on and depends upon the particular situation.

3 Everyone Should Do This.

If you have not started breakin detection and accounting, you probably should have. In the SYSTARTUP.COM file, before starting up DECNET, you will want to have lines like the following:

$!
$! Turn on audit alarms - disable logging to Console.
$!
$ set audit/alarmlenable=(breakin=(all))
$ define/user sys$command OPAO:  
$ reply/disable=(security)
$!
$! Enable accounting.
$!
$ set accounting/enable
$!

There is a command file in the system manager account called SECAUDIT.COM which is useful for scanning the operator log file for breakin attempts. The DCL command SHOW INTRUSION will show only recent breakin attempts.

Best of luck to you!

Supported under U.S. Department of Energy Contract DE-AC03-76SF00098