# Somar™ DumpAcl™ Version 2.5 Help Contents


Send problem reports and comments to 72202.2574@compuserve.com.
For information about other Somar products, visit the Somar Software Web site at http://www.somar.com.

## Overview

Somar DumpAcl is a program for Microsoft® Windows NT™ that will dump the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable listbox format, so that holes in system security are readily apparent. Somar DumpAcl also dumps user, group and replication information. Somar DumpAcl is a must-have product for Windows NT systems administrators.

Windows NT contains the mechanisms for providing strong system security, using permissions to control access to files, registry keys, printers, shares and other securable items and auditing to log successful and failed access attempts. However, it can be very difficult to determine if permissions and audit settings have been set correctly, since there are so many files and registry keys on the typical system. The situation is analogous to having a building with unbreakable locks on each of 10,000 doors. The problem is not with the locks themselves, but rather with one person walking around on a regular basis and checking that none of the 10,000 doors is unlocked.

Somar DumpAcl provides a solution to the problem of too many files and registry keys to check on a regular basis, by producing a concise and readable report of permissions and audit settings. By reviewing this report, you can determine if users have more access to the file system, registry or printers than you want to allow. You can then use file manager, registry editor or print manager to set permissions differently.

Some users have suggested just setting permissions on the root directory or registry key (e.g. C:\ or HKEY_LOCAL_MACHINE) and letting those permissions be propagated to all child directories/files/keys. In general, however, it is not acceptable for all directories, files and/or registry keys to have the same permissions. In fact, trying to make all permissions the same may prevent Windows NT from running properly.

See Security notes for further general discussion of computer security.

## Installation

1) Place `DUMPACL.EXE` and `DUMPACL.HLP` together in any directory.

2) The first time `DUMPACL.EXE` is run, it will create the following registry key:

```
HKEY_CURRENT_USER\SOFTWARE\SomarSoftware\DumpAcl
```

3) Somar DumpAcl makes no other changes to your system.

## Uninstallation

1) Run `DUMPACL.EXE` with `/u` as a command line parameter. If successful, a message box will be displayed indicating that the `SomarSoftware\DumpAcl` registry key has been deleted.

2) Delete `DUMPACL.EXE` and `DUMPACL.HLP` from your computer.

## Command Line Options

The command line can contain one of the following:

1) The path of a previously saved report in Somar DumpAcl native file format (*.DCL). The report in the specified file will be loaded and displayed. This type of command line allows opening a previously saved reports by double-clicking in file manager (assuming the DCL suffix has been associated with DUMPACL.EXE).

2) A series of batch command line parameters. Somar DumpAcl can distinguish this type of command line from the preceding by the presence of at least one "/" on the command line. The parameters can be specified in any order.

### Required parameters

| | |
|---|---|
| /rpt=*report type* | Type of report to produce: |
| dir=*drive:\path* | Directory report |
| registry=*hive* | Registry report (hive can be HKEY_LOCAL_MACHINE or HKEY_USERS) |
| printers | Printers report |
| shares | Shares report |
| users | Users report (table format, all fields except groups, groupcomment and grouptype) |
| groups | Groups report (table format, all fields) |
| policy | Policy report |

| | |
|---|---|
| /outfile=*drive:\path* | File in which to store report. This file will be replaced if it already exists. |

### Optional parameters for all reports

| | |
|---|---|
| /computer=*computer* | Computer for which to dump information. Ignored for directory reports (since computer is implied by computer associated with redirected drive). Default is to dump local information. |

| | |
|---|---|
| /saveas=*format* | Fomat in which to store report: |
| native | binary format, can be later loaded back into Somar DumpAcl |
| csv | comma separated columns |
| tsv | tab separated columns |
| fixed | fixed width columns, padded with blanks |
| | Default is to save as native format. |

### Optional parameters for permissions reports only

| | |
|---|---|
| /noowner | Do not dump owner. Default is to dump owner. |
| /noperms | Do not dump permissions. Default is to dump permissions. |
| /showaudit | Dump audit info. Default is not to dump audit info. Ignored if audit information cannot be displayed because the current user is not a member of the Administrators group. |
| /nogroup | Do not perform grouping. Default is to perform grouping. |
| /nogroupdirs | Do not group directories. Default is to group unless /nogroup is specified. |

### Optional parameters for users/groups reports only

| | |
|---|---|
| /notruelastlogon | Do not query all domain controllers for "true" last logon time. Instead use last logon time from specified computer. Default is to query all domain controllers, which can be time consuming. |
| /nosid | Do not dump SID as part of users report. Default is to dump SID, which requires some additional and possible time-consuming processing. |

**Examples:**

`dumpacl.exe c:\temp\users.dcl`

Start Somar DumpAcl interactively, load and display a report that was previously saved in native format in `c:\temp\users.dcl`.

`dumpacl.exe /rpt=dir=c:\users /showaudit /outfile=c:\temp\users.dcl`

Run Somar DumpAcl batch mode, produce a report of directory permissions for the `c:\users` directory showing owner, permissions and audit settings, with grouping enabled, and store the report in native file format in `c:\temp\users.dcl`.

`dumpacl.exe /computer=\\server1 /rpt=users /saveas=csv /outfile=c:\temp\users.txt`

Run Somar DumpAcl in batch mode, produce a report show all user information in table format for users defined on `\\server1`, and store the report in comma separated columns format in `c:\temp\users.txt`.

## Known bugs, limitations and planned enhancements

1) Somar DumpAcl does not indicate whether directory permissions are inheritable. File manager always makes directory permissions inheritable so this is not a severe limitation. That is, of the permissions in the list below, type (b) is always the same as (a), if you used File Manager to set file system permissions:

a) Permission applies to directory itself (Dir column of Somar DumpAcl report)
b) Permission will be inherited by newly created subdirectories in directory (not shown by Somar DumpAcl)
c) Permission will be inherited by newly created files in directory (File column of Somar DumpAcl report)

2) The WIN32 SDK is not clear as to the interpretation of printer access masks and so there are likely bugs in the Somar DumpAcl report for printers. This issue is being worked.

3) There are categories of securable items besides those currently dumped or mentioned above. Some of these categories may be added in the future. User suggestions are welcome.

4) The groups report may be enhanced to show the full user name. Several users have requested this enhancement.
There are some issues with implementing this feature that are still under investigation. As a workaround, you can dump both users and groups in table format, export to a database, and join and produce a report in the database.

5) Unless you are a member of the administrators group, find and filter by account may not find all files or other items to which the account has the specified access.

For example, suppose write access is granted to group1 for file1. User1 belongs to group1, but DumpAcl cannot determine the the members of group1, because you do not have sufficient permission (not a member of the administrators or account operators group). Or suppose you cannot even examine the permissions for file 1 (not a member of the administrators or backup operators group). Either way, DumpAcl will not be able to determine that user1 has write access to file1.

If the account specified in the find or filter by account dialog is from a trusted domain, or any of the files or other items have permissions granted to a group from a trusted domain or to a local group which contains users or global groups from a trusted domain, then it is necessary to be administrator on both the local and the trusted domains in order for the find and filter by account to always find all files or other items for which the account has the specified access.

6) DumpAcl attempts to store all information in memory. If you have a large filesystem and disable grouping, or permissions are not set in a consistent and orderly way, so that grouping is ineffective, then the amount of information to be stored may exceed available memory. The result will be an out-of-heap space error. You have 3 options at this point:

a) Enable grouping.
b) Reset permissions so they are consistent and grouping is therefore effective.
c) Perform multiple dumps, one for each subdirectory of the original directory tree root.

The long range solution is for DumpAcl to store data on disk.

## Permissions and Audit Settings for File System Entries

If the Grouping Enabled option is selected, Somar DumpAcl shows as little of the file system as possible. Permissions for a subdirectory are the same as for the parent directory, unless the permissions for the subdirectory are explictly shown. Permissions for all files in a directory are the same as the permissions in the file column of the directory, unless the permissions for the file are explictly shown. The CREATOR OWNER account is ignored in comparisons of permissions, since this pseudo-account is converted to the account of the user who creates a file in a directory.

**Dir column (used for directories only)**

| | |
|---|---|
| R | Account can list the contents of the directory. |
| W | Account can add new files and subdirectories to the directory. |
| X | Account can traverse the directory as part of a path. |
| D | Account can delete the entire directory. |
| P | Account can change permissions for the directory and all files and subdirectories. |
| O | Account can change ownership of the directory. |
| All | Same as RWXDPO. |
| No access | Account is denied all access to directory. |

**File column (used for directories and files)**

For files, this column lists the permissions that apply to the file. For directories, this column lists permissions that will be inherited by files created in the directory, unless the creator of the file explicitly specifies other permissions.

| | |
|---|---|
| R | Account can read the file. |
| W | Account can write to the file. |
| X | Account can execute the file. |
| D | Account can delete the file. |
| P | Account can change permissions for the file. |
| O | Account can change ownership of the file. |
| All | Same as RWXDPO. |
| No access | Account is denied all access to file. |

**Audit settings**

| | |
|---|---|
| R | Audit attempts to read file or list directory contents. |
| W | Audit attempts to write to file or add files/subdirectories to directory. |
| X | Audit attempts to execute file or traverse directory as part of a path. |
| D | Audit attempts to delete file or directory. |
| P | Audit attempts to change change permissions for the file or directory. |
| O | Audit attempts to change ownership of the file or directory. |
| All | Same as RWXDPO audit settings. |

See also Special Permissions and Audit Settings.

**Example and interpretation:**

```
Path                    Account         Own Dir   File  Success Failure

c:\DIR1\                Administrators  o   All   All
c:\DIR1\                Everyone            R X   R X
c:\DIR1\                CREATOR OWNER             All
c:\DIR1\                SYSTEM              All   All
```

```
c:\DIR1\DIR2\File1.txt    Administrators  o        All
c:\DIR1\DIR2\File1.txt    Everyone                 RWXD          all
c:\DIR1\DIR2\File1.txt    SYSTEM                   All
```

All directories and files under `C:\DIR1\` have the same permissions as listed for `C:\DIR1\`, except for file `C:\DIR1\DIR2\MyFile1.txt`. Administrators is owner of these directories and files. Also, failed attempts by anyone to access (read, write, delete, execute, change permissions or take ownership) the `C:\DIR1\DIR2\MyFile1.txt` file are audited.

## Permissions and Audit Settings for Registry Keys

Only the HKEY_LOCAL_MACHINE and HKEY_USERS hives can be dumped if a remote computer is specified.

Unless the Show All option is selected on the View menu, Somar DumpAcl shows as little of the registry hive possible. Permissions for a subkey are the same as for the parent key, unless the permissions for the subkey are explictly shown. The Key column shows the permissions for the key itself. The Inheritable column shows the permissions that will be inherited by new subkeys created under the key, unless the creator of the subkey explictly specifies other permissions.

**Permissions**

| | |
|---|---|
| Q | Account can query values for the key. |
| S | Account can create or set values for the key. |
| C | Account can create sub keys under the key. |
| E | Account can enumerate sub keys under the key. |
| N | Account can request notification whenever the key changes. |
| L | Account can create a registry link. |
| D | Account can delete the key. |
| P | Account can change permissions for the key. |
| O | Account can change the key owner. |
| R | Account can read the permissions for the key. |
| Read | Same as QENR permissions. |
| All | Same as QSCENLDPOR permissions. |
| No access | Account is denied all access to key. |

**Audit Settings**

| | |
|---|---|
| Q | Audit attempts to query values for the key. |
| S | Audit attempts to create or set values for the key. |
| C | Audit attempts to create sub keys under the key. |
| E | Audit attempts to enumerate sub keys under the key. |
| N | Audit attempts to request notification whenever the key changes. |
| L | Audit attempts to create a registry link. |
| D | Audit attempts to delete the key. |
| P | Audit attempts to change permissions for the key. |
| O | Audit attempts to change the key owner. |
| R | Audit attempts to read the permissions for the key. |
| Read | Same as QENR audit settings. |
| All | Same as QSCENLDPOR audit settings. |

See also Special Permissions and Audit Settings.

**Example and interpretation:**

```
Path                        Account         Own Key        Inheritable

HKEY_CURRENT_USER           SYSTEM              All        All
HKEY_CURRENT_USER           Administrators   o  All        All
HKEY_CURRENT_USER           Frank               All        All

HKEY_CURRENT_USER\Private   Administrators   o  All        All
HKEY_CURRENT_USER\Private   SYSTEM              All        All
```

All keys under `HKEY_CURRENT_USER` have the same permissions as listed for `HKEY_CURRENT_USER` except for the `HKEY_CURRENT_USER\Private` key and its subkeys. The administrators group is owner of all of the keys.

## Permissions and Audit Settings for Printers

### Permissions

| | |
|---|---|
| PrintOnly | Account can print to the printer. |
| ManageDocs | Account can delete or pause documents for the printer. If this permission is granted to the CREATOR OWNER pseudo-account, then users have permission to manage their own print documents. Users can manage the documents of other users only if they are members of a group other than CREATOR OWNER which has the ManageDocs permission for the printer. |
| All | Account can print to the printer, manage documents, delete the printer, change permissions for the printer, and change ownership of the printer. |
| No access | Account is denied all access to printer. |

### Audit Settings

| | |
|---|---|
| U | Audit attempt to use printer. |
| A | Audit attempt to administer printer. |
| D | Audit attempt to delete printer. |
| P | Audit attempt to change permissions. |
| O | Audit attempt to change ownership. |
| All | Same as UADPO audit settings. |

See also Special Permissions and Audit Settings.

**Example and interpretation:**

```
Printer         Account          Own Permission  Success   Failure

Laser           CREATOR OWNER        ManageDocs
Laser           Administrators    o  All
Laser           Everyone             Print                 All
Laser           Power Users          ManageDocs
```

All users can print to the printer named Laser, and can manage the documents they print. Power Users can print and manage the documents of other users. Administrators can perform all printer functions, including deleting the printer and changing permissions and ownership. Administrators is owner of the printer. Failed attempts by any user to access the printer (print, manage documents, delete, change permissions or take ownership) are audited.

## Permissions for Shares

Shares do not have an owner or audit settings. Some shares do not have DACL

**Permissions for file shares**

| | |
|---|---|
| Read | Account can read the shared directory and it subdirectories and files. |
| Change | Account can read and write the shared directory and it subdirectories and files, including adding and deleting subdirectories and files. |
| All | Account can read, write, change permissions on and change ownership of the shared directory and it subdirectories and files. |
| No access | Account is denied all access to shared directory and its subdiretories and files |

See also Special Permissions and Audit Settings.

**Example:**

```
Path                              Account           Permission

C$=C:\                                              ==>No DACL

C_DRIVE=C:\                       Administrators    All

temp=C:\temp                      Group1            No access
temp=C:\temp                      Group2            Change
temp=C:\temp                      Everyone          Read
```

## Special Permissions and Audit Settings

| | |
|---|---|
| Axhhhhhhh | Non-standard allow permissions or audit settings, see WIN32 SDK documentation. |
| Dxhhhhhhh | Non-standard deny permissions, see WIN32 SDK documentation. |
| ==>access denied | User who is executing Somar DumpAcl cannot read the permissions or audit settings. |
| ==>no DACL<br>==>null DACL | No DACL was present or DACL was Null, both of which situations are equivalent to "all" permission for Everyone. Normal system ACL editors (such as file manager, registry editor and print manager) never allow no or Null DACL, but other ACL editors might. No DACL is normal for administrative shares (ending with $). |

## Ownership

The owner of a securable item is indicated by an "o" in the Own column when the Show Owner option is selected. Shares do not have an owner.

When Enable Grouping is selected, Somar DumpAcl takes ownership into consideration in attemping to group items. Two items with the same permissions but different owners are grouped provided the owners have explicit permission to change permissions or take ownership of their respectively owned item (i.e. other than as a consequence of being the owner). Otherwise, the items are not grouped.

**Example and interpretation:**

(grouping disabled, or grouping enabled and John and Mary NOT both members of Managers group):

```
Path                              Account         Own Dir        File
```

```
c:\Dir\                         John            o
c:\Dir\                         Managers            All         All

c:\Dir\File                     Mary            o
c:\Dir\File                     Managers            All         All
```

(grouping enabled and John and Mary both members of Managers group):

```
Path                            Account         Own Dir         File

c:\Dir\                         John             o
c:\Dir\                         Managers            All         All
```

(i.e. `c:\Dir\File` not shown because it was "grouped" with its parent directory).

In this example, permissions are the same for the file and directory, but ownership differs. If John and Mary are members of the Managers group, then John can take ownership and change permissions on the `c:\Dir\` directory and Mary can take ownership and change permissions on the `c:\Dir\File` file (because All permission allows taking ownership). Therefore, Somar DumpAcl groups the file and directory.

Ownership is important because the owner of an item can always set permissions for that item. If Mary were not a member of the Manager group, she could still change permissions on the `c:\Dir\File` file at any time, and thereby obtain access to information that someone thought was only available to Managers. Likewise, if John were not a member of the Manager group, he could still change permissions on the `c:\Dir\` directory at any time to give himself full control (via inheritance) of newly created files in this directory, that one might think (if looking only at the permissions on the directory) would only be available to Managers.

## Miscellaneous Notes

1) Computer accounts shown in the users reports are those with UserName ending in "$". A computer account is needed for a workstation to join a domain. There is a password associated with computer accounts. This password is automatically changed and kept in sync between the domain controller and the workstation. If the passwords get out of sync, users at the workstation won't be able to log onto the domain. Fix this problem by removing the workstation from the domain and then adding it back.

2) The account shown on the Services report is the account under which the service runs. It is usually a good idea to run as many Win32 services as possible under ordinary user accounts, instead of LocalSystem. Many Unix breakins have occurred due to bugs in daemons (equivalent to Windows NT services) running under the root account (equivalent to LocalSystem).

3) Information about users authorized to access the server using RAS can be obtained using the RASUSERS.EXE utility in the NT3.5 resource kit.

4) Windows NT only stored the last logon time on the authenticating logon server. So, if there are two or more domain controllers (primary plus one or more backups), it is necessary to access all controllers and use the latest of the last logon times reported. The Dump Users reports have an option to enable or disable this scanning. The scanning is normally enabled, but you might disable it if you want to compare the last logon times among the different controllers, for some reason.

## Copyright/License/Warranty Disclaimer


Send problem reports and other comments to 72202.2574@compuserve.com.

You should carefully read the following terms and conditions before using this software. Use of this software indicates your acceptance of these terms and conditions. If you do not agree with them, do not use the software.

## License Agreement

This is not free software. You are hereby licensed to: use the Shareware Version of the software for a 21 day evaluation period; make as many copies of the Shareware version of this software and documentation as you wish; give exact copies of the original Shareware version to anyone; and distribute the Shareware version of the software and documentation in its unmodified form via electronic means. There is no charge for any of the above.

You are specifically prohibited from charging, or requesting donations, for any such copies, however made; and from distributing the software and/or documentation with other products (commercial or otherwise) without prior written permission, with one exception: Disk Vendors approved by the Association of Shareware Professionals are permitted to redistribute Somar DumpAcl, subject to the conditions in this license, without specific written permission.

You are specifically prohibited from copying or redistributing the keyfile (`DUMPACL.KEY`) that will be sent to you upon receipt of your registration payment.

Unregistered use of Somar DumpAcl after the 21-day evaluation period is in violation of United States and International copyright laws.

A single registered copy of Somar DumpAcl can only be installed on a single computer. Thus, if you have 3 computers on which you want to install Somar DumpAcl, you must register and pay for 3 copies of Somar DumpAcl.

You may access the registered version of Somar DumpAcl through a network, provided you have obtained individual licenses for the sotware covering all workstations that will access the software through the network.

There is no license required for dumping permissions for network drives or for dumping permissions for remote computers, using the Select Computer capability. Thus, if you have 2 administrator workstations and 10 servers and you only run Somar DumpAcl at the workstations, dumping permissions for the servers via network connected drives, then you need 2 licenses. If you only run Somar DumpAcl at the local consoles of the servers, on the other hand, you would need 10 licenses. If you run Somar DumpAcl both at the workstations and at the local consoles of the servers, then you would need 12 licenses.

Upon receipt of your registration payment, you will be sent a key file (`DUMPACL.KEY`), which is to be placed in the same directory as `DUMPACL.EXE`. This key file will be your proof of registration. The presence of this key file will enable certain functions of Somar DumpAcl which are disabled in the unregistered version. These functions involve the ability to produce hardcopy printouts of the Somar DumpAcl report.

For how to register and pay for Somar DumpAcl, see Order form.

Note that Somar Software reserves the right to increase the registration fee at any time without notice. If the fee has been increased, and your payment is received after such increase, then Somar Software has the right to require additional payment before accepting your registration and sending you a key file. Once

you have paid the then current registration fee, and Somar Software has accepted your fee and sent you a key file, you have the right to use the version of Somar DumpAcl that you paid for, for as long as you want, without additional payment. Future versions of Somar DumpAcl may require a different key file. You may be required to pay an additional fee to upgrade to such future versions.

## Governing Law

This agreement shall be governed by the laws of the District of Columbia.

## Disclaimer of Warranty

THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SOLD "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OF MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. Because of the varying hardware/software environments in which Somar DumpAcl may be used, THERE IS NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE.

Good data processing procedure dictates that any program be thoroughly tested with non-critical data before relying on it. The user must assume the entire risk of using hte program. ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR REFUND OF PURCHASE PRICE.

## Order Form - Somar DumpAcl V2.5

To print this order form, click on Print Topic in the File pull-down menu.

Current Somar voice/fax numbers and hardcopy mail address and any up-to-date ordering instructions (including current price, in case price has changed) are available at http://www.somar.com/ordering.htm or via email from 72202.2574@compuserve.com. This information is not included here because it may change from year to year.

You can register and pay for Somar DumpAcl by 3 methods:

- VISA/Mastercard/AMEX credit card. Send this form via hardcopy mail or fax, or send information via email (you must accept risks of eavesdropping on email), or place order by voice phone.
- Check in US dollars drawn on a US bank, payable to Somar Software. Send with this form via hardcopy mail.
- CompuServe registration service (GO SWREG, specify ID 2723). Charge will appear on your CompuServe monthly statement. Key file will be sent via email only.

When your registration payment is received, you will be sent a key file (`DUMPACL.KEY`) via email (SMTP MIME or CompuServe attachment). This key file will be your proof of license and will contain your registration name (see below) in encrypted format. When a valid key file is properly installed, the registration name will will appear in the Help'About dialog box and all functions of Somar DumpAcl will be enabled. Optionally, you can also have a 3.5" diskette shipped via hardcopy airmail, containing the keyfile and most recent version of the software.

```
___1 licenses at US$99 each (price subject to change)      = ______

Current California sales tax (8.5%)                        = ______
      (not applicable if key file sent via email only or
       if shipping address not in California, USA)
Airmail shipping and handling                              + _US$5_
      (scratch out if you only want key file sent via email)

Pay by:   Check   Visa    Mastercard   AMEX          Total = ______

Credit card #: ________________________________ Exp date: ______

Card owner signature: ____________________________________________

Registration name: _______________________________________________
(name that will appear in the key file, normally a company name)

Email address: ___________________________________________________

Voice: _____________________ Fax: ________________________________

Shipping address (include country if outside USA):

_____________________________________________________________________

_____________________________________________________________________

_____________________________________________________________________

_____________________________________________________________________
```

## Security notes

### What is security?

A secure system is one that is protected against various natural disasters and human attacks. Security with respect to a computer system is very similar to security with respect to a bank vault. A computer system or bank vault containing valuables (data in the case of a computer system, secret documents or jewels in the case of bank vault) is secure if:

1) No one can look at, modify or remove any of the valuables for which they do not have the proper authority. In the computer context, this requires:

Permissions are set properly.
Computer is physically secured, possibly inside a locked room.
Data is encrypted if computer cannot be physically secured (e.g. portable PC).
Backup tapes are physically secured in a safe, or else encrypted.
There are procedures in place to ensure viruses do not get introduced into the system.

2) No person or natural disaster such as a fire can easily destroy the valuables. In the computer context, this requires:

Permissions are set properly.
Backups are performed regularly.
Copies of backup tapes are stored offsite.
There are procedures in place to ensure viruses do not get introduced into the system.

3) No one can easily disrupt authorized access to the valuables (denial of service). In the computer context, this requires:

Permissions are set properly.
There are procedures in place to ensure viruses do not get introduced into the system.

An example of disrupting authorized use of a computer system is a virus that modifies and thereby corrupts the registry so a database program will not run. The database itself maybe intact (because it was protected by permissions), but the data cannot be accessed until the registry is repaired, which may require reinstalling the database program. This temporary disruption can be as costly as actual loss of data for many mission critical computer systems.

Note the importance of *permissions* and *viruses*, which are implicated in all types of security risks. Permissions are the primary protection against malicious users and viruses which run under user accounts. There is no way to protect against viruses which run under administrator or system accounts. So it is very important to avoid running untrusted programs when logged on as an administrator, or to allow untrusted program to be run as services under a system or administrator account.

### What should a well-organized set of permissions look like?

A well-organized set of permissions will produce a short Somar DumpAcl report. In general, the shorter the report produced by Somar DumpAcl, the easier to understand, and so the more confident the systems administrator will be that permissions have been set properly.

### Issue of registry key permissions

Use Somar DumpAcl to produce a report of the HKEY_LOCAL_MACHINE registry hive. Note that Everyone has write and delete access to many keys. So any user who can access the registry locally or remotely can make changes that might disrupt system operations.

Consider the following scenario. A student in an undergraduate university computer lab logs on using another student's account (they found the other students password written in the front cover of that

students notebook) and makes various changes to the registry of workstations and servers in the lab so that these computers no longer function properly, but the malfunction is so intermittent and obscure that only an expert systems administrator would be able to trace the problem to the registry. Since the damage was done using another user's account, there would be no way to identify the true perpetrator. The only way to correct the damage will be to reinstall NT, but then the perpetrator will just come back and break the system again. I am not being paranoid in pointing out this scenario. Undergraduate students are notorious for finding such mischief a great source of amusement, and having plenty of time on their hands to engage in it.

No one I have talked to seems to understand the registry well enough to know whether permissions can be reset so that Everyone does not have write access to so many keys, or whether doing this will cause problems with the normal operation of Windows NT. The registry key permissions seem to have been set in a very haphazard and inconsistent way.

**More info about security**

Visit the Somar Software Web site at http://www.somar.com for a further discussion of computer security issues.

## A useful security technique

Suppose you want users to be able to access a file through a program, but not directly (i.e. not by using file manager, file open dialog or the command line). For example, Microsoft mail requires users to have write access to the WGPO directory, where the postoffice files are stored. You want users to be able to access these files using the mail program, but not using file manager. To do this, set up directories and permissions as follows:

| | |
|---|---|
| \HIDDEN\ | (no access permission for everyone) |
| \HIDDEN\WGPO\ | (read/write permission for everyone) |

Users cannot even list the files and subdirectories in the HIDDEN directory, and therefore cannot access the WGPO directory using file manager. However, programs executed by users can access the WGPO directory, provided these programs specify the full file path during the open.

For another example, suppose you are writing a Visual Basic program that will run on client machines and update an Access or similar database on a file server. You must give all users who will run the program write access to the database file, but you do not want the users to modify the database other than using the Visual Basic program. To do this set up directories and permissions as follows:

| | |
|---|---|
| \HIDDEN\ | (no access permission for everyone) |
| \HIDDEN\DB.MDB | (read/write permission for everyone) |

Users cannot even list the files and subdirectories in the HIDDEN directory, and therefore cannot access the DB.MDB file using file manager. However, programs executed by users can access the DB.MDB directory, provided these programs specify the full file path during the open.

The feature of NT which makes this technique possible is called the Bypass Traverse Checking user right. You can disable this feature using User Manager. Bypass Traverse Checking causes NT to behave differently from Unix. In Unix (and NT when Bypass Traverse Checking is disabled), a program must have list permission for all directories in the path, as well as the appropriate permission on the file being opened.

This technique is vulnerable to users who know how to program in any language, including Basic. For better but also more complex security, use a client server design, where the client executed by the user communicates via RPC or other methods with a service running under a privileged account. Files can then be protected using normal permissions.

**Note regarding this specific example for MS Mail**

When initially setting up mail clients (either Windows for Workgroups or Windows NT workstation), it is sometimes necessary to connect to the WGPO instead of HIDDEN directory. In this case, you can temporarily share the WGPO directory as WGPO$ (trailing $ means the share prevent the share from appearing in the file manager connect dialog), connect to this share from the client, setup the client, modify the .INI or registry settings on the client to connect to use \HIDDEN\WGPO as the mailbox directory, then stop sharing WGPO.