VACCINE for DOS

Anti-Virus System

User Manual
October 1997

This manual documents the virus detection software VACCINE for MS-DOS. For additional information on viruses, please refer to the *Data Security Reference Guide* supplied with the software.

Copyright © 1997 by Sophos Plc

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior permission in writing of the copyright owner.

Any name should be assumed to be a trademark unless stated otherwise. *InterCheck* and *Sophos* are registered trademarks of Sophos Plc.

Sophos Plc • The Pentagon • Abingdon • OX14 3YP • England

Email enquiries@sophos.com • http://www.sophos.com/

Tel +44 1235 559933 • Fax +44 1235 559935

9 8 7 6 5 4 3 2 1

Part # mavdez01/971008

This document is also available in electronic form from Sophos.

Technical support hotline:
Email technical@sophos.com, Tel +44 1235 559933

Contents

VACCINE quick start guide

If you dislike reading user manuals, this chapter is for you. Reading it will enable you to start using VACCINE immediately.

If you wish to use all the facilities of the product, please refer to the rest of this manual. Likewise, if you are using VACCINE to fingerprint files on a file server, please consult the section 'Installing VACCINE on a file server' in the 'Installing VACCINE' chapter.

Note that when you enter a command, your computer will not start executing it until you also press *Enter*. For example, to get a list of files on your floppy disk, insert the floppy disk into the drive and type:

```
DIR A:
```

The computer will not execute the command until you press *Enter*.

If you have any questions regarding VACCINE, please contact our technical support.

Preparing the materials you will need

To install VACCINE on a floppy disk (recommended) you will need:

- The VACCINE and SWEEP floppy disks (supplied with this package).

Important!

- A write-protected system floppy disk, like the one supplied with MS-DOS by the computer manufacturer. This disk should have the DOS 'FORMAT' program on it.
- A spare floppy disk of the maximum capacity of your drive A.

Please note that it is essential that you have a write-protected, virus-free, system floppy disk from which you can bootstrap (start) the PC.

Installing VACCINE

Switch the PC off.

Insert the write-protected system floppy disk into floppy drive A.

Switch the PC on. Wait until the bootstrapping is complete and the prompt

```
A>
```

is displayed on the screen.

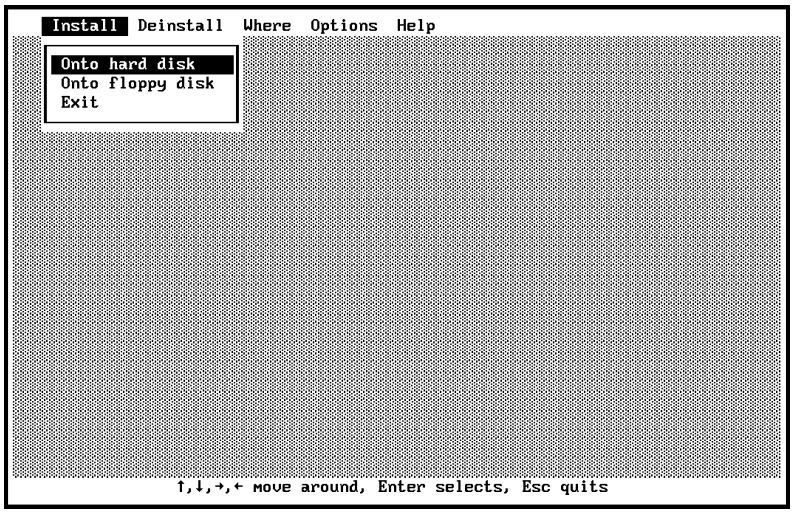
Insert the VACCINE floppy disk into your floppy drive A. Now type

```
INSTALL
```

followed by *Enter*. The INSTALL utility allows you to install VACCINE onto a floppy disk or a hard disk. It also allows you to de-install VACCINE from the hard disk.

We recommend for security reasons that you install and use VACCINE on floppy disk (see the section 'Where should the VACCINE modules be kept?' in the 'About VACCINE' chapter for explanation).

INSTALL is menu-driven, mouse-aware and offers on-line help. After confirming that you have done a clean bootstrap as described above, the main menu is displayed.



Select the 'Onto floppy disk' option and you will be guided through the installation process. For advanced installation options refer to the 'Installing VACCINE' chapter.

Installing VACCINE on a compressed hard disk

If your hard disk has been compressed using one of the compression tools such as *Doublespace*, refer to the section 'Preparing a bootable floppy disk when using disk compression' in the 'About VACCINE' chapter. The rest of the VACCINE installation procedure is identical.

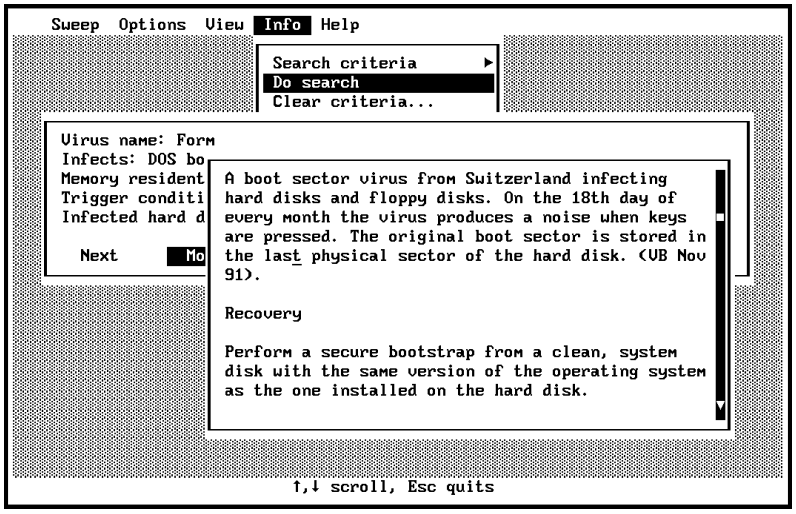
If SWEEP discovers a virus...

During installation SWEEP will check the PC for known viruses: if a virus is discovered by SWEEP, **don't panic!**

Note the name of the virus or virus fragment reported. Make sure that the PC has been booted off a clean system disk, run SW, then select the 'Info' menu from the top bar. Select 'Search criteria' followed by 'Name or alias', type in the name of the virus and then select 'Do search'. When information about the virus is displayed, select 'More' and follow the

instructions in the recovery guidelines. You can call Sophos' 24-hours-per-day technical support by telephone (+44 1235 559933) for more information. Consult the section in this manual on 'Treating viral infection' for further details.

For example, the recovery information for the Form virus would be displayed as:



If DIAGNOSE reports a change...

If DIAGNOSE reports a change, do not automatically assume that it is due to a virus. **Changes to executable files** can be caused by actions such as installing a new version of the software, while **changes to a boot sector** are more likely to be due to a virus.

For more information consult the 'What can cause changes?' section in the 'About VACCINE' chapter.

About VACCINE

This chapter explains how VACCINE detects viruses on your computer system.

How does VACCINE work?

VACCINE is used to monitor the integrity of all executable items on a PC. Since viruses necessarily modify executable code, their presence on a system will be detected as a modification of one or more executable items.

The main advantage of this approach is that **any** virus can be detected, without the need to update VACCINE. The main disadvantage is that the user will be notified of the change as well as where the change occurred, but not which virus (if any) has caused it.

VACCINE is also a powerful tool for auditing and change control; it can be used to detect even a single bit change to a program, data file, disk sector or memory region, as well as changes to the overall configuration of a system, e.g. the existence or non-existence of particular files, subdirectories and so on.

VACCINE modules

The VACCINE system consists of 4 modules:

- SWEEP virus-scanning module for checking disks for the presence of any known viruses. This

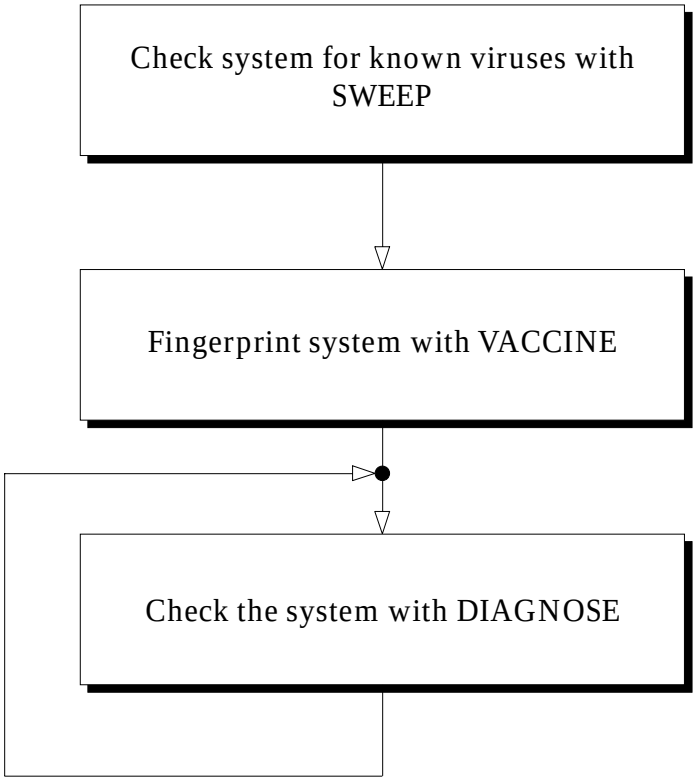
module has a useful life-span of approximately four months from delivery.

- VACCINE system fingerprinting module. Used to take fingerprints of the system and store them in the file DIAGNOSE.FIN.
- DIAGNOSE system checking module. Used to check the integrity of fingerprinted files, disk sectors and memory regions.
- FILEMAC file checking utility module. Useful for checking the integrity of individual files.

How is VACCINE used?

Overview

The SWEEP module is used initially to check your system for any known viruses. Having established



Sequence of events when using VACCINE

that the system is 'clean', VACCINE is used to fingerprint all executable items. The DIAGNOSE module can then be used at regular intervals to check the fingerprints.

Note that SWEEP has a limited life-span: any viruses which were not in existence when a particular version was released will not be detected. VACCINE has no inherent expiry date: all viruses, present and future, can be detected.

Checking for known viruses

For DIAGNOSE to discover a viral attack, you should start with a 'clean' computer system on which all files are genuine and free of viruses. This can be achieved by a complete initialisation of the system disk and configuration of the system. In most cases however this would be inconvenient or impractical and so the SWEEP module is provided to establish that the disk is free of known viruses.

Fingerprinting and checking a system

Once you have established that your system is clean, use the VACCINE module to fingerprint critical items on the system disk.

Important! Critical items include all executable files (EXE, COM and BAT), program overlays (usually OVL), system files (SYS), the DOS bootstrap sector and the master bootstrap sector of the hard disk.

Any modification to the fingerprinted files, their deletion, or the addition of any other files matching the description of critical files, will be detected and reported by the DIAGNOSE module. Likewise, any changes to fingerprinted sectors or memory regions will be reported.

The fingerprints are stored in the DIAGNOSE.FIN file in encrypted form.

Which system items should be fingerprinted?

Although the primary targets for viruses are **executable files, system files and program overlays** (COM, EXE, BAT, SYS and OV? files), checking is not limited to programs: any file (text or binary) can be included the check. Likewise, particular **disk sectors** or **groups of sectors** can be specified directly. Absolute or logical sectors can be specified. Most memory-resident viruses install themselves by modifying the 'interrupt table' - a list of numbers held in memory and essential for proper working of the operating system. VACCINE allows fingerprinting of **memory regions**, which can include the interrupt table for added security.

How are the fingerprints calculated?

Fingerprinting is normally performed using Sophos' proprietary high-speed authentication algorithm based on ANSI X9.9. By specifying '-8' in the command line, the ISO standard 8731 (Part 2) algorithm can be selected instead. In either case, complex one-way cryptographic fingerprints are calculated. Any modification whatsoever made to an item causes its fingerprint to change completely. It is practically impossible to 'engineer' changes in such a way as to leave the fingerprint unaffected.

Hint: When VACCINE is used on a PC where executable modules change frequently (programming groups, software testers etc.), only unchanging executables such as system files, spreadsheets, word-processors, compilers, assemblers and linkers should be fingerprinted. For convenience, these 'fixed' executables should be kept in one subdirectory, while changing executables are kept in different subdirectories. These 'fixed' executables tend to be the most often-used programs on a system. Since most parasitic viruses infect on executing a program, a virus infection can still be spotted promptly, when it infects one of these programs. For more information

see the section ‘Using VACCINE in a changing environment’.

You can also fingerprint all or part of the ‘interrupt table’ held in memory locations 0000:0000 to 0000:00FF hex (the number before the colon means memory segment 0000 and the number after the colon means the offset within that segment), but beware that legitimate changes to the table can cause false alarms. For example, the PRINT command changes the interrupt table, as do various memory-resident utilities and network shells. It can be useful to single out interrupts 13H, 21H, 25H and 26H as these are most likely to be altered by the virus. They correspond to memory locations 0000:004C to 004F, 0000:0084 to 0087, 0000:0094 to 0097 and 0000:0098 to 009B.

Interrupt 13H is the BIOS disk services interrupt, interrupt 21H is the DOS general services interrupt, interrupt 25H is the DOS absolute disk read interrupt and interrupt 26H is the DOS absolute disk write interrupt.

How often should the fingerprints be checked?

System integrity should be checked using the DIAGNOSE module as often as is practical, for example whenever the computer is switched on. Alternatively, DIAGNOSE can be invoked on a spot-check basis, whenever a possible attack or data corruption is suspected, or at intervals dictated by relevant guidelines. In particular, DIAGNOSE should be used to check the system before carrying out a backup operation.

What can cause changes?

DIAGNOSE can determine that an item has changed, but it cannot determine what caused the change or whether the change was legitimate or not. Human assessment of any changes is required at this stage to

distinguish between legitimate changes and a virus attack. In most cases, this will involve the examination of recent actions on the PC such as the installation of new software.

If all changes can be accounted for, the PC should be refingerprinted using VACCINE.

Changes to executables

Executables can change for a variety of reasons other than an attack by a virus. The most common reason is the installation of a software upgrade. Some software packages store their default settings within executables files, thus changing them whenever the settings are changed.

When examining changes reported by DIAGNOSE, it should be investigated whether they are due to installations of upgrades or other legitimate changes made to the executables. A typical indicator of a parasitic virus attack is a report of changes in a large number of unrelated files.

Appearance of files

If new files are reported on the PC, an examination of past activity should determine the reason. The most common case is the installation of new software.

The appearance of COM files which cannot be accounted for could indicate an attack by a companion virus.

Disappearance of files

The disappearance of files is not normally an indication of a virus attack but, more probably, a consequence of deleting or deinstalling executables.

Changes to bootstrap sector

Any changes to the master or DOS bootstrap sectors should be treated with suspicion as they often indicate a virus attack. However, some utilities such as access control packages, disk compression utilities and IBM's boot manager legitimately change the contents of the bootstrap sector.

An investigation as to whether such software has been installed or used on the PC should clarify whether or not any change to the boot sector was legitimate.

Where should the VACCINE modules be kept?

Maximum security will be achieved by:

- Keeping all the VACCINE modules and the file containing the fingerprints (DIAGNOSE.FIN) on a write-protected floppy disk which also contains the operating system.
- Always storing this floppy disk in a safe place.
- Always bootstrapping (starting) the computer system from this floppy disk before using the DIAGNOSE module.

Important! Even if VACCINE is kept on the hard disk, it will still detect most viruses. However, stealth viruses such as 4K and Joshi may not be detected if the hard disk is infected and is used to bootstrap the system.

See also the 'Secure bootstrapping' section.

Using VACCINE in a changing environment

When VACCINE is used on a PC on which executable files change frequently (programming groups, software testers etc.), only those executables that should not change, such as system files, spreadsheets, word-processors, compilers, assemblers and linkers, should be fingerprinted.

For convenience, these 'fixed' executables can be kept in one subdirectory, while changing executables are kept in different subdirectories.

For example, if 'fixed' executables are kept in the subdirectory 'FIX', the list of items to be fingerprinted could be:

```
+80 0 0 1 ; Master bootstrap sector
C:|0 ; DOS bootstrap sector
C:\FIX\>*.COM ; All COM files in FIX
C:\FIX\>*.EXE ; All EXE files in FIX
C:\FIX\>*.OV? ; All OV? files in FIX
C:\FIX\>*.SYS ; All SYS files in FIX
C:\COMMAND.COM ; Command line interpreter
C:\IBMIO.SYS ; Operating system
C:\IBMBIO.SYS ; Operating system
C:\CONFIG.SYS ; Driver list
C:\AUTOEXEC.BAT ; Initial batch file
```

As these files will be run frequently, a parasitic virus would soon infect one of them, which would be detected next time DIAGNOSE was run.

Preparing a bootable floppy disk when using disk compression

Utilities such as *Doublespace* (delivered with MS-DOS 6), *Stacker* and *Superstor* allow transparent dynamic compression of whole drives. Compressed drives are not accessible if the bootstrapping is performed from a standard system floppy disk.

MS-DOS 6 Doublespace

To create a bootable floppy disk use the

```
FORMAT A: /S
```

while *Doublespace* compression is active. In addition to the two hidden system files (`IBMBIO.SYS` and `IBMSYS.SYS` or similar), the operating system automatically creates the third file `DBLSPACE.BIN` which contains the compression code.

After bootstrapping from such a system disk, the compressed drive can be accessed normally.

Stacker

The creation of a bootable floppy for *Stacker* is somewhat more complex than for MS-DOS 6. *Stacker* uses a device driver which is loaded through `CONFIG.SYS`. Proceed as follows:

1. Format a bootable DOS system disk using the command

   ```
   FORMAT A: /S
   ```

2. Copy the file `C:\STACKER\STACKER.COM` to the floppy disk

3. Copy the file `C:\STACKER\SSWAP.COM` to the floppy disk

4. The file `CONFIG.SYS` on the hard disk should have the two lines which refer to the STACKER and look like:

   ```
   DEVICE=C:\STACKER\STACKER.COM C:\STACKVOL.DSK
   DEVICE=C:\STACKER\SSWAP.COM C:\STACKVOL.DSK /SYNC
   ```

These lines should be copied into CONFIG.SYS on the floppy disk, but the references to C:\STACKER should be replaced with A:\. The above file would read:

```
DEVICE=A:\STACKER.COM C:\STACKVOL.DSK
DEVICE=A:\SSWAP.COM C:\STACKVOL.DSK /SYNC
```

It is important that no other parts of those lines are changed.

After bootstrapping from such a system disk, the compressed drive can be accessed normally.

Superstor

1. Create a bootable floppy disk using the command

   ```
   FORMAT A: /S
   ```

2. The files `SSTORDRV.SYS` and `DEVSWAP.COM` should be copied to the floppy. The `CONFIG.SYS` file on the floppy should contain

```
DEVICE=A:\SSTORDRV.SYS
DEVICE=A:\DEVSWAP.COM
FILES=20
BUFFERS=20
```

After bootstrapping from such a system disk, the compressed drive can be accessed normally.

Common questions

How can VACCINE detect all viruses, existing and future?

Virus scanners work by searching the system for copies of known viruses. This is the approach used in the SWEEP module. Such programs can only recognise viruses that they know about and cannot detect new viruses. Unlike these virus-specific packages, the VACCINE and DIAGNOSE modules do not depend upon recognition of particular known viruses; instead they use the more fundamental approach of testing the integrity of those parts of a system which any virus must attack in order to propagate. This is the only reliable method of virus detection and is future-proof.

Does it matter what method of fingerprinting is used in checking system integrity?

Yes. A fingerprint of a data item such as a program or a disk sector can be thought of as a type of checksum. The security of using such a method relies implicitly upon the mathematical properties of the checksum. Simple checksums or cyclic redundancy checks are unsuitable because they are not mathematically ‘one-way’, i.e. it is possible to engineer changes to a file in such a way that its checksum or fingerprint remains unchanged. Suitable checksum or fingerprinting algorithms must be cryptographically

based to ensure good one-way behaviour and even then, some algorithms are stronger than others. A good fingerprinting algorithm for virus detection must be such that even given ample time for research and development, the programmer who writes a clever virus will not be able to design modifications (for example to the bootstrap sector) in such a way that the fingerprint will remain unchanged.

Are there published standards for methods of fingerprinting data?

There are two: ISO Standard 8731 Part 2 and ANSI Standard X9.9, both of which are used worldwide to ensure authenticity of data in banking transactions. These two methods each produce 32-bit checksums with all the mathematical properties required for secure virus detection.

Does VACCINE comply with either of these standards?

It complies with both. By default, VACCINE uses the ANSI Standard X9.9 method in conjunction with Sophos' proprietary block cipher algorithm SPA. A command line option allows the user to select the ISO Standard 8731 Part 2 method. The ANSI method is used by default as it is faster, but both methods are secure; they bring with them the assurance of the most rigorous international scrutiny and testing, with years of proven use in the banking world.

How and why does VACCINE protect the DIAGNOSE module?

An elementary attack on any virus detection software would be to modify it so that it fails to detect changes. This can be done in a number of ways, ranging from modifying the error messages in the software, to refingerprinting corrupted items. A virus can easily perform these manipulations automatically. VACCINE uses a unique and sophisticated system of two-way cryptographic

protection for its DIAGNOSE module, which defeats attempts to modify status messages or fingerprints without the authorised user being alerted.

What makes VACCINE particularly suitable for use in large organisations?

VACCINE has an extensive range of command line qualifiers which allow data security managers to tailor their organisation's use of the product, as to suit their needs and working practices. Furthermore, all help messages, security reports, screen presentations and user manuals can be customised to suit the requirements of large customers. Finally, Sophos is an established supplier of high-quality cryptographic systems: our customers include banks, governments, industry and the armed forces.

Can VACCINE be used on a file server?

Yes. VACCINE can be used to check any DOS drives, including file server drives.

Has VACCINE been evaluated by an independent authority?

Yes. VACCINE has been certified to Confidence Level UKL1 by CESG, the Communications Electronics Security Group of GCHQ.

Points of technical interest

A fingerprint is a value calculated from the contents of a file, sector or memory region. VACCINE and FILEMAC fingerprint files using a cryptographic authentication algorithm as described in the standard ANSI X9.9. Based on the Sophos proprietary algorithm SPA, the authentication algorithm uses a 64-bit key (derived from the password) and each byte in a fingerprinted item is used in the construction of a 32-bit fingerprint or MAC (Message Authentication Code). Changing even a single bit in the item will alter the resulting fingerprint completely.

The fingerprints produced by VACCINE are stored in encrypted form in the DIAGNOSE.FIN file. Fingerprints calculated by FILEMAC are displayed numerically in hexadecimal format on the screen.

Encryption and decryption are performed using a 64-bit key (one bit - BInary digiT - is a single ‘1’ or ‘0’, and is the smallest unit of data with which a computer can work). This means that there are 2-to-the-power-64 possible keys, i.e. more than 18,000,000,000,000,000,000. There is no known way of cracking the encryption other than trying all keys. Assuming that a supercomputer could try one key every one-millionth of a second (an optimistic assumption), it would take some 500,000 years to try all keys. On average, the time needed to crack a key would amount to some 250,000 years of computing. On an IBM-PC it would take in excess of 10 million years.

The ISO standard 8731/2 (ISO 8731/2-198- ‘Banking, Approved algorithm for message authentication, Part 2: Message authenticator algorithm’), is identical to the draft British Standard Specification for approved algorithms for message authentication in banking.

Installing VACCINE

This chapter explains what you should do when you first receive your copy of VACCINE.

Floppy disks

The VACCINE software is delivered on permanently write-protected disks. The disks should contain the following files:

`INSTALL.EXE`	automatic installation program
`VACCINE.EXE`	system fingerprinting module
`DIAGNOSE.EXE`	system integrity checking module
`FILEMAC.EXE`	file fingerprinting module
`CHNGBW.EXE`	screen configuration utility
`READ.ME`	text file with additional information not in this manual

In addition, SWEEP files are provided on separate disks:

`SWEEP.EXE`	module for testing for known viruses
`SW.EXE`	interactive shell for running SWEEP
`SW.DAT`	virus database file used by SW
`SU.EXE`	Sophos Utilities disk editing program
`READ.ME`	text file with additional information not in this manual

Note that VACCINE in this manual refers to the complete set of four modules, while the individual modules are referred to as VACCINE, DIAGNOSE, FILEMAC and SWEEP.

Display the READ.ME file using the command

```
TYPE A:READ.ME
```

or print it using the command

```
PRINT A:READ.ME
```

Secure bootstrapping

Important! It is most important to ensure that no viruses are memory-resident before running anti-virus software. This procedure is known as 'secure bootstrapping'. It is comparatively simple for stand-alone PCs and slightly more involved for networks.

Warning! Failure to carry out a secure boot will result in some stealth viruses, such as *4K* and *Joshi*, not being detected.

The procedure involves executing only code which is known to be positively clean (free of viruses) during the bootstrap process.

Bootstrapping stand-alone PCs

Important! Switch the PC off. Do **not** use *Ctrl-Alt-Del* as this is intercepted by some viruses.

Insert a clean, write-protected**,** system floppy disk into drive A.

Switch the PC on and let it bootstrap from the floppy. After the PC has bootstrapped, it will display the prompt

```
A>
```

Your system is now ready to run any software under clean conditions.

Device drivers

In most cases you do not need to load any device drivers in order to access hard disks. However, if your system needs to load any device drivers, such as ANSI.SYS, or to execute any software on startup, the file CONFIG.SYS must refer to copies of the drivers held on drive A. In addition, any software executed on startup through AUTOEXEC.BAT must also be present on the floppy disk.

CONFIG.SYS normally refers to other files, which are loaded into memory before the system is started, using statements such as

```
DEVICE=filename
```

Clean copies of all these files should be transferred onto the floppy disk and CONFIG.SYS on the floppy disk should be modified, if necessary, to ensure that it refers to the files on the floppy disk, rather than the original copies on the hard disk. For example, any statements in CONFIG.SYS, such as

```
DEVICE=C:\DOS\ANSI.SYS
```

should be modified to read

```
DEVICE=ANSI.SYS
```

on the floppy disk so as to ensure that all of the operating system is loaded from the write-protected floppy disk.

Novell NetWare

This procedure describes the process for secure bootstrapping of a Novell NetWare 3.11 workstation:

Important! Switch the workstation off.

Insert a clean, write-protected, system floppy disk into drive A. This disk should also contain the NETx, IPX and LOGIN programs.

Switch the PC on.

After the PC has bootstrapped, it will display the prompt

```
A>
```

Run IPX from the floppy disk, followed by NETx. Next run LOGIN **from the floppy disk** with the '/S NUL' command line qualifier. This will prevent the execution of both system and user login scripts. Enter

```
LOGIN /S NUL USERNAME
```

You are now logged into the network. If you need to execute any other NetWare programs, make sure that they are present and run from the floppy disk.

Note that you can only check directories to which you have access. If you wish to access all subdirectories on a server, you must login with read rights equivalent to those of SUPERVISOR.

Other networks

A similar process should be followed for other networks, so that a supervisor can login without executing any DOS programs stored on the file server.

Installing VACCINE on floppy and hard disks

Important! Switch the PC off.

Insert a write-protected system floppy disk (normally supplied by the manufacturer) into floppy drive A.

Switch the PC on.

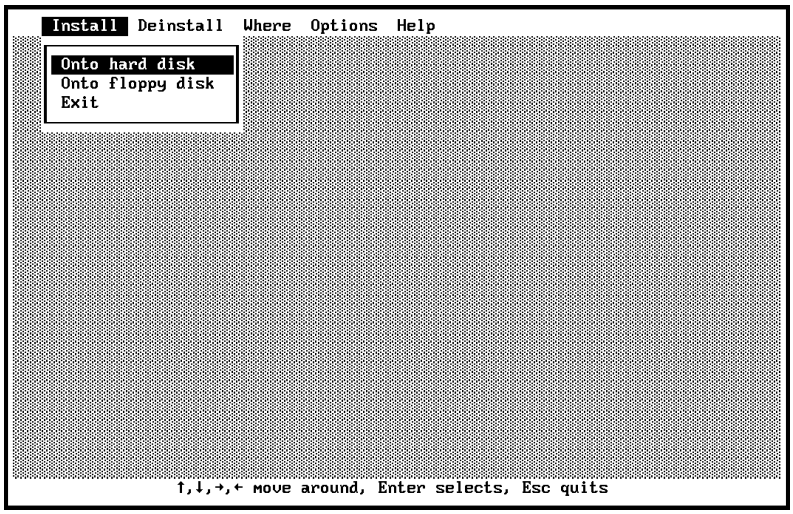
After the PC has bootstrapped, it will display the prompt

```
A>
```

Insert the VACCINE floppy disk into your floppy drive A and type

```
INSTALL
```

The INSTALL utility will ask you to confirm that the secure bootstrapping procedure described above has been followed and then display the main menu. You can explore the options available using either the cursor keys or the mouse.



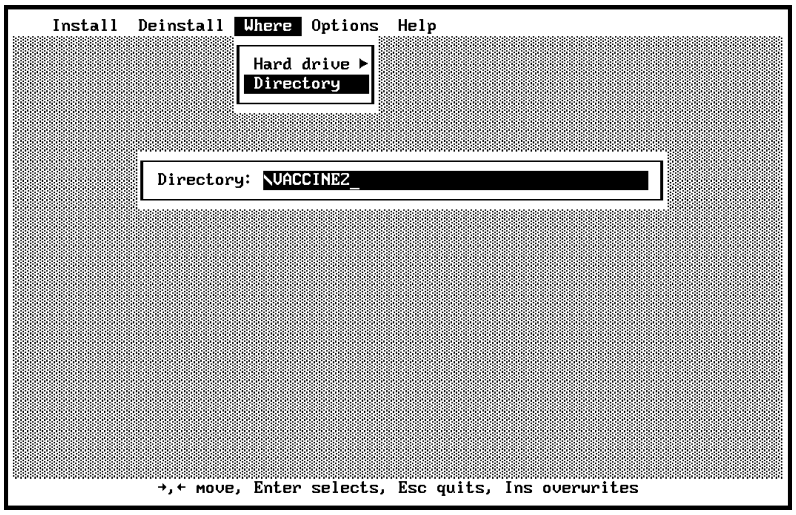
After you have selected installation onto hard disk or floppy disk, INSTALL will guide you through the installation. INSTALL also enables you to de-install VACCINE from the hard disk. When VACCINE is installed on the hard disk, INSTALL will modify the AUTOEXEC.BAT file in the root directory, preserving the original in the AUTOEXEC.BAK file in the \VACCINE subdirectory.

Your attention is drawn to the licence information regarding making copies of the software.

Specifying a different drive and directory where VACCINE is installed

When installing VACCINE on the hard disk, it will by default be installed in the `\VACCINE` directory on the first hard disk. To specify a different drive or directory, choose the 'Where' menu from the top bar and make the appropriate selections.

For example, to install in directory \VACCINE2:



Verbose installation

By default, the installation procedure does not ask your permission before performing every single action. To make it more verbose, deselect the 'Quick installation' in the 'Installation' menu from the 'Options' menu on the top bar.

Configuring installation

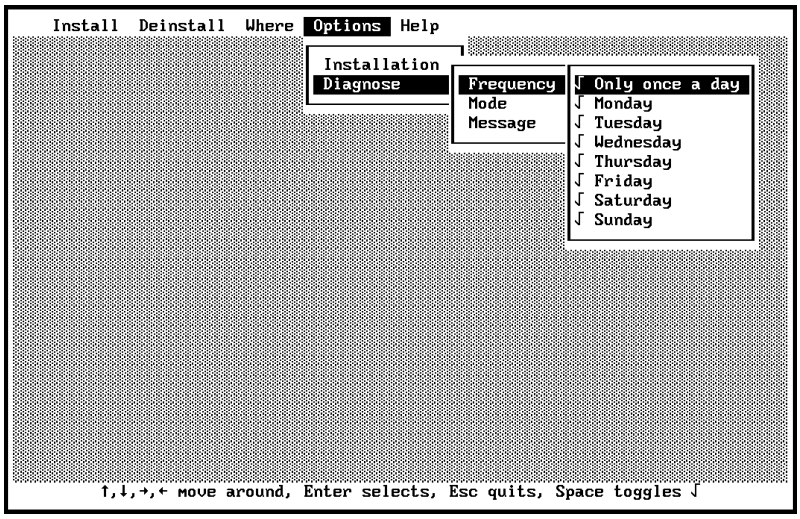
Default options should be used in most cases, but on occasions certain stages can be skipped. Should you wish to skip particular actions during installation (e.g. running SWEEP before installing VACCINE), deselect the appropriate options in the 'Installation' menu from the 'Options' menu on the top bar.

Full Sweep

By default, SWEEP is run in its quick mode during the installation procedure (see SWEEP manual for details). Should you wish to perform a full Sweep instead, select the appropriate option in the 'Installation' menu from the 'Options' menu on the top bar.

Configuring how often DIAGNOSE runs

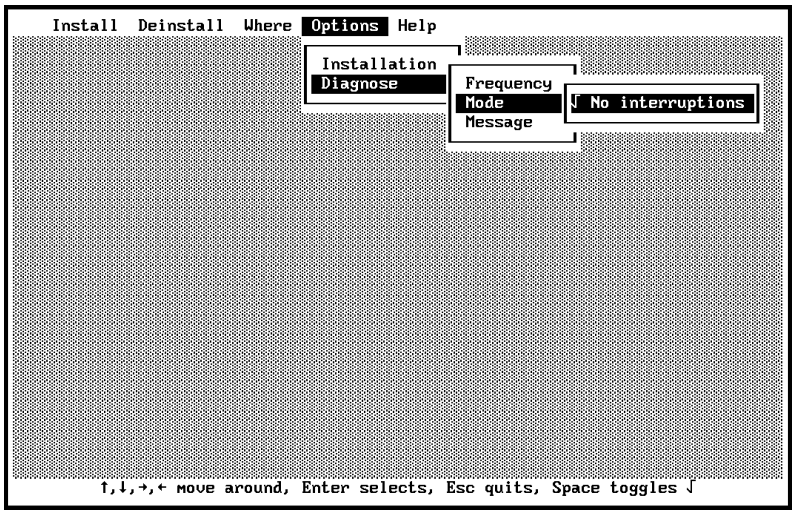
When VACCINE is installed on the hard disk, AUTOEXEC.BAT is modified so that DIAGNOSE runs on chosen days. By default, it will run once every day, but you can select different days in the 'Frequency' menu in the 'Diagnose' menu from the 'Options' menu on the top bar.



Prevent user interruption of DIAGNOSE

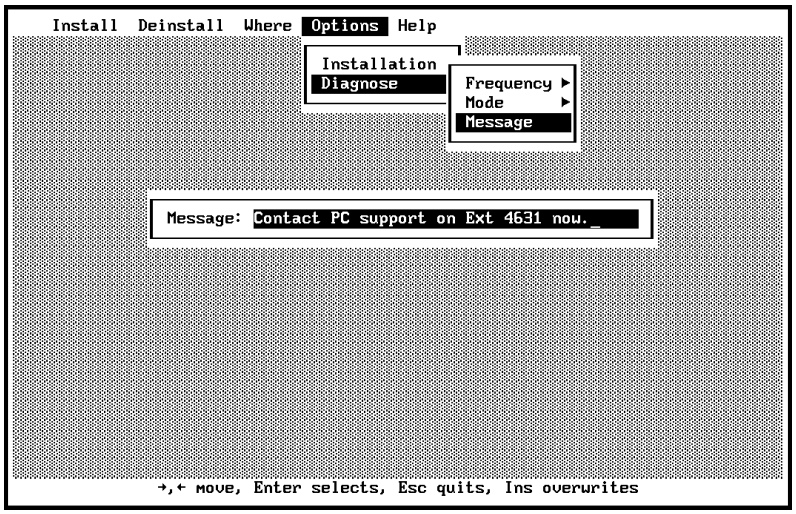
If you select the 'No interruptions' option in the 'Mode' menu in the 'Diagnose' menu from the 'Options' menu on the top bar, users will not be able to interrupt the execution of DIAGNOSE by pressing *Esc*, *Ctrl-C* or *Break* when it is run from AUTOEXEC.BAT.

This setting is not effective when DIAGNOSE is run from within the VACCINE module.



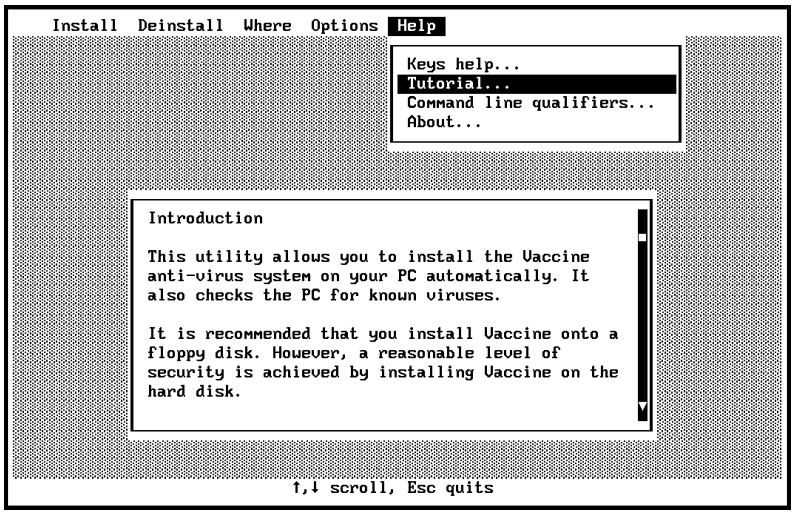
Customising the 'irregularities discovered' message

If you wish to display a particular message when DIAGNOSE reports changes in fingerprinted items, choose the 'Message' option in the 'Diagnose' menu from the 'Options' menu on the top bar.



Help

The 'Help' menu on the top bar gives on-line help as well as a tutorial on using VACCINE.



Installing VACCINE on a file server

The following steps describe how to install VACCINE on a file server running Novell NetWare. The network drive is assumed to be drive F. Installing the VACCINE modules onto a network will enable:

- Users to fingerprint and check their own PCs
- The SUPERVISOR to fingerprint and check critical areas on the file server

It is strongly recommended that the installation, as well as subsequent checking of the integrity of the file server, is performed from a dedicated PC which is not used for any other work except possibly taking backups. A dedicated PC can be bootstrapped from the hard disk without compromising security, but care must be taken that a copy of LOGIN.EXE is available and used from the hard disk.

The checking of fingerprints should be done before taking backups.

Secure bootstrapping

Important! You must perform a secure bootstrap as described in the ‘Secure bootstrapping’ section before installing VACCINE onto the file server.

Installation

Login as SUPERVISOR.

Make drive A current and place the SWEEP disk into the drive. SWEEP all drives present on the network, for example, if you have drives F:, G: and H: type

```
SWEEP F: G: H:
```

Copying the SWEEP and VACCINE files to the server

Now copy all files from the SWEEP disk and the VACCINE disk into a chosen directory on the server (for example \PUBLIC) by typing

```
COPY *.* F:\PUBLIC
```

Ensure that normal users have read-only access rights to the chosen directory. Use the NetWare utility FILER to set this. Refer to the NetWare documentation for further details. Users’ PATH must also be correctly set up to include the chosen directory.

All network users should now have access to the VACCINE modules held on the file server.

Fingerprinting the server

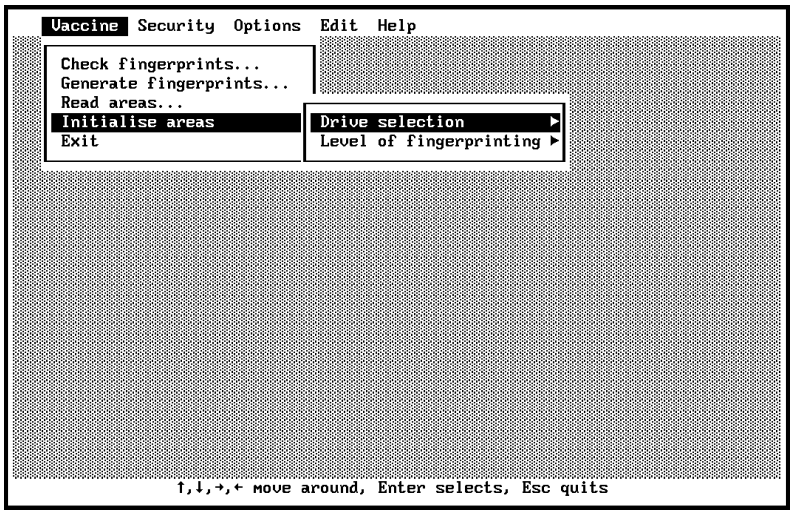
You can now fingerprint selected executables on the file server. It is advisable to store the file with fingerprints on the dedicated workstation. Make drive C current and make and select a subdirectory, for example ‘VACCINE’.

```
MD C:\VACCINE
CD C:\VACCINE
```

Run VACCINE (from the file server) by typing

```
VACCINE
```

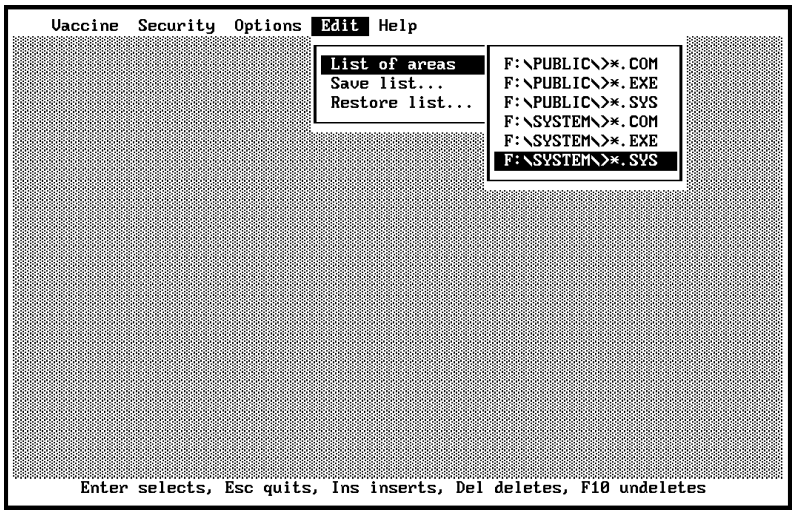
Select the ‘Initialise areas’ option in the first menu. Then specify the drives and the level of fingerprinting by selecting the appropriate entries.



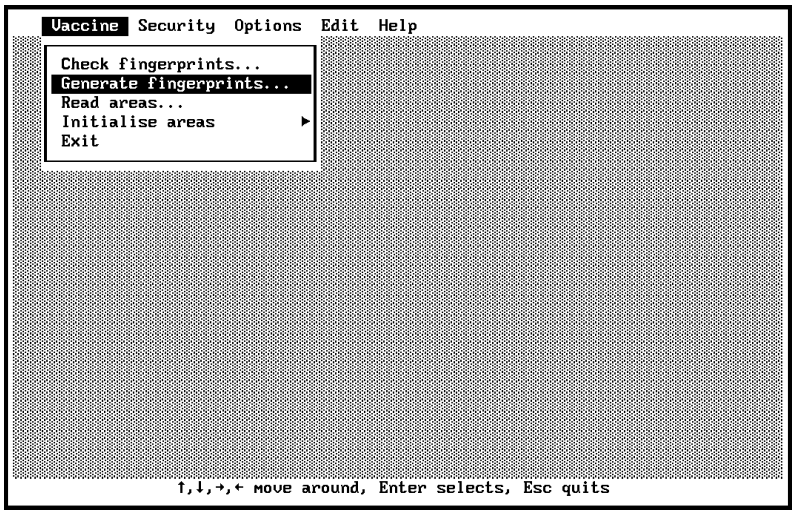
If users may install and modify their own programs on the file server, it may be necessary to customise the default list of items to be fingerprinted. Select ‘Edit’ pull down menu on the top bar and select ‘List of areas’. The list of all items which will be fingerprinted will be displayed. You can edit existing entries by highlighting them and pressing *Enter*, insert new items (by pressing *Ins*) or delete existing entries (by pressing *Del*).

For further details see the ‘Using the VACCINE module’ chapter.

You should fingerprint all critical areas of the file sever which contain fixed executable code. In the following example, all COM, EXE and SYS files in the \PUBLIC and \SYSTEM directories, as well as any child subdirectories (symbol ‘>’ denotes recursion), will be fingerprinted.



Once the list of areas is complete, select ‘Generate fingerprints’ from the ‘Vaccine’ menu on the top bar.



Wait until fingerprinting has been completed, then exit VACCINE by selecting the ‘Exit’ option in the ‘Vaccine’ menu.

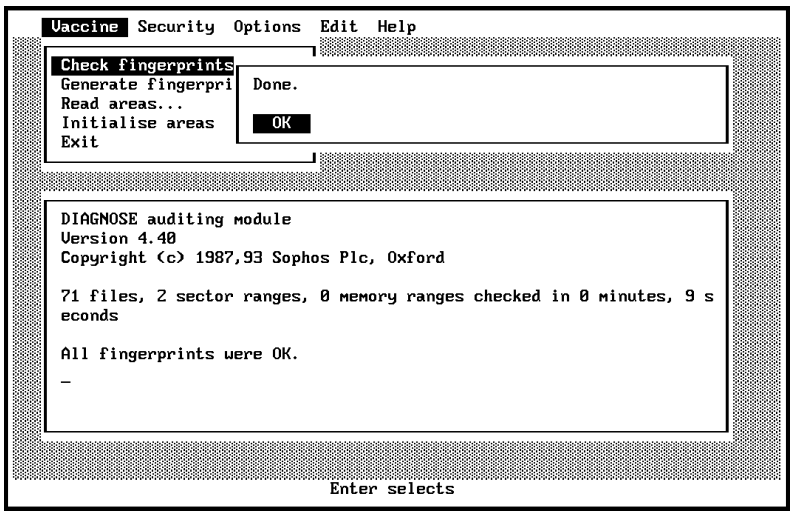
Files which cannot be fingerprinted

Some files on servers may cause an error to be generated when they are opened (some system files as well as any files marked as execute only). You can either exclude them while editing the list of items by using the exclusion operator ‘<’ or you can let

VACCINE do it automatically for you: after editing the list, select ‘Generate fingerprints’. If any files could not be fingerprinted, VACCINE will report them and offer to refingerprint the system. When you select ‘Generate fingerprints’ once again, these files will be excluded.

Checking the fingerprints

Run DIAGNOSE to check the fingerprints. When DIAGNOSE is installed on the floppy or hard disk by the automatic installation program, it will be invoked through the AUTOEXEC.BAT file. DIAGNOSE can also be executed either from the DOS command line or from within VACCINE whenever the integrity of the system needs to be checked.



Important! It is strongly advised that a secure bootstrap is performed before running DIAGNOSE (see ‘Secure Bootstrapping’ section).

Using the VACCINE module

The VACCINE module is used for initial fingerprinting of your system, as well as for running DIAGNOSE interactively. Whenever VACCINE is run, the system should be known positively to be ‘clean’, i.e. free from viruses residing in memory. This must be achieved through secure bootstrapping as described in the ‘Secure bootstrapping’ section in the ‘Installing VACCINE’ chapter.

To start VACCINE, make the directory in which VACCINE is installed current:

```
CD \VACCINE
```

and then issue the command

```
VACCINE
```

What should be fingerprinted

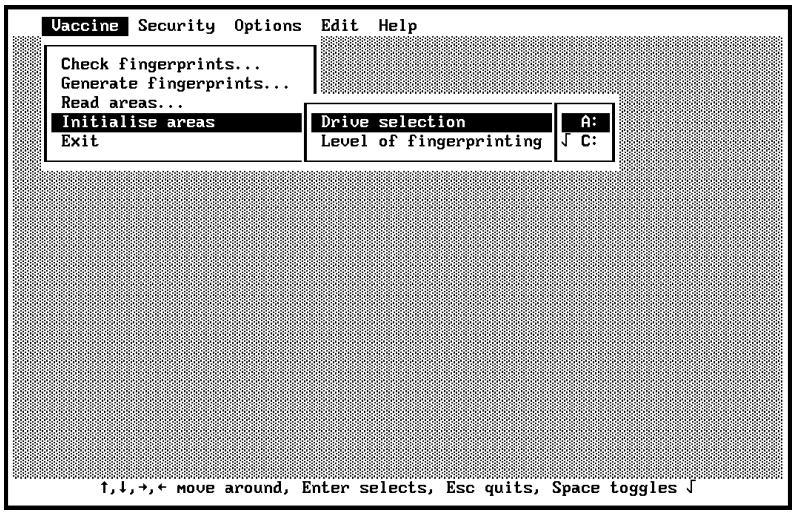
Ideally fingerprint the complete contents of every executable item on the PC and monitor for change. Unfortunately, this is not always possible since the time to perform the fingerprinting and, more importantly, checking, is proportional to the amount of data fingerprinted and can become prohibitively long.

A compromise is to fingerprint parts of the system which are known to be affected by the large majority of common viruses. VACCINE allows you great flexibility in specifying the areas of the system which

will be fingerprinted. You should start by choosing one of the default sets of areas which can then be edited to suit the application.

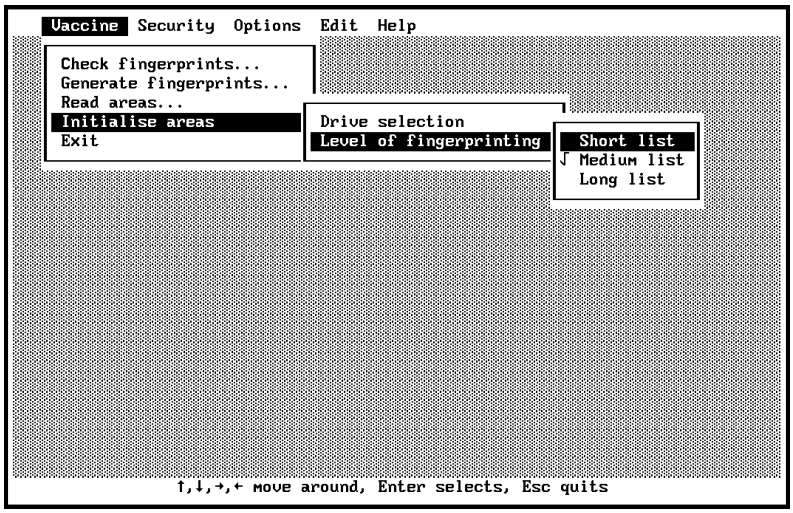
Selecting drives

First specify the drives which will be fingerprinted by selecting the ‘Drive selection’ option from the ‘Initialise areas’ menu from the ‘Vaccine’ menu on the top bar.



Selecting the level of fingerprinting

Next select the ‘Level of fingerprinting’ option from the ‘Initialise areas’ menu from the ‘Vaccine’ menu on the top bar. Three options will be displayed.



The short list contains just the bootstrap sector(s) and the files COMMAND.COM and AUTOEXEC.BAT. The medium list adds the headers of COM and EXE files, along with OV? files, while the long list checks complete COM, EXE, OV? and BAT files as well as the boot sectors.

The longer the list you specify, the longer it will take to fingerprint and check your system. However, you will have a correspondingly greater degree of security.

Remember that the default lists are for convenience only; you can modify them freely to suit your requirements by using the 'Edit' menu on the top bar as described in the next section.

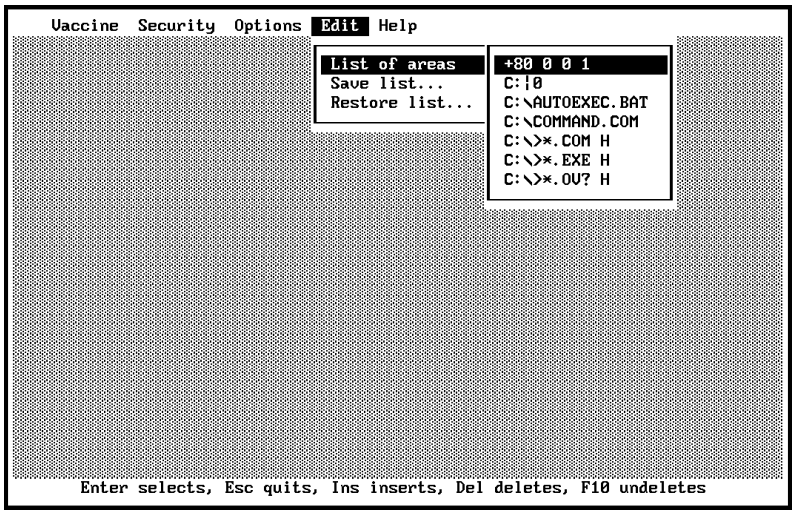
To make your list clearer, you can put in comments, marked by a semicolon ';'. VACCINE will ignore any text on a line after a semicolon.

Hint: The medium list is recommended for most applications.

Customising the list of areas

Modifying the list

Select the ‘List of areas’ entry from the ‘Edit’ menu on the top bar. The list of all items currently selected to be fingerprinted will be displayed. You can edit existing entries by highlighting them and pressing *Enter*, insert new ones (by pressing *Ins*) or delete existing entries (by pressing *Del*).



VACCINE uses a number of special symbols to describe the objects to be fingerprinted.

Filenames are specified using any legal file characters, while the wildcards ‘*’ and ‘?’ have the same meaning as in PC-DOS: ‘*’ matches any number of characters, while ‘?’ matches only one character.

To specify checking of **all files corresponding to a description** (i.e. not just those in the current directory), use the recursion operator ‘>’. This will ensure that all subdirectories from the current specified directory are examined.

To **exclude certain files or directories** from being fingerprinted, precede the description with the ‘<‘ exclusion operator (wildcards may not be used when specifying exclusion).

To specify **logical disk sectors**, use the symbol '|' (the PC-DOS pipe character).

To specify **absolute disk sectors**, use the symbol '+'.

To specify **memory locations**, use the symbol '['.

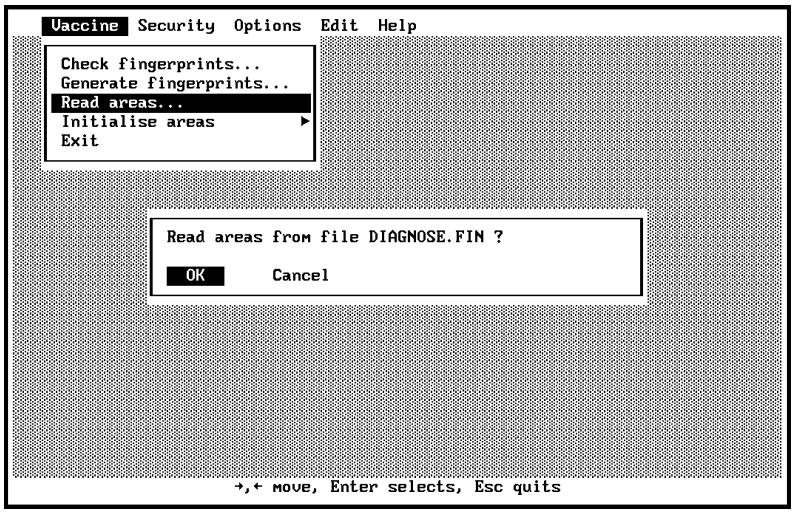
To make the list of items clearer, you can put in comments, marked by a semicolon ';'. VACCINE will ignore any text after the semicolon.

For example, the following is a valid list of objects to be fingerprinted:

```
[0000:0000 00FF] ; Interrupt table
+80 0 0 1 ; Master bootstrap sector
C:|0 ; DOS bootstrap sector
C:|F ; First data sector
C:\>*.COM ; All executable files
C:\>*.EXE ; All executable files
C:\>*.OV? ; All overlay files
C:\>*.BAT ; All batch files
C:\>*.SYS ; All system files
```

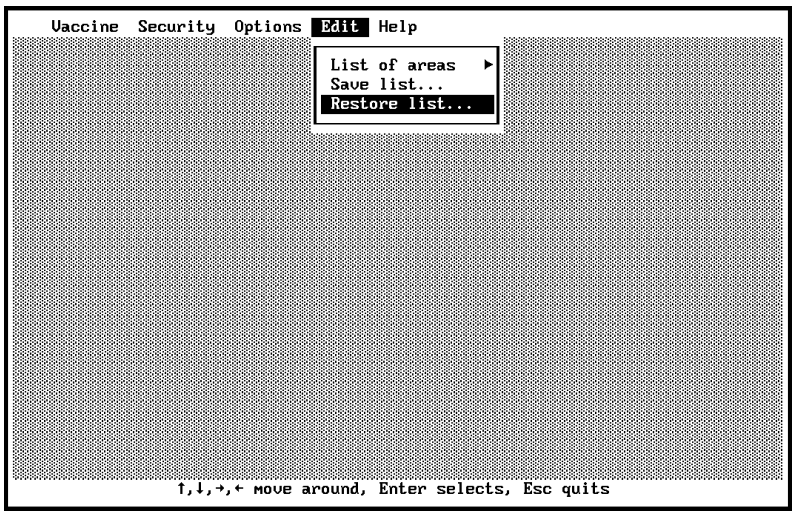
Reading the list from an existing DIAGNOSE.FIN

The list of items which will be fingerprinted is automatically saved in DIAGNOSE.FIN when fingerprints are generated. If you wish to edit the current list stored in DIAGNOSE.FIN, import it into VACCINE by selecting the 'Read areas' option from the 'Vaccine' menu on the top bar.



Saving and restoring the list in text form

You can read in a list of items from a text file, or save the current list in a text file, by selecting the appropriate option from the 'Edit' menu on the top bar. By default, these are saved to the file VACCINE.TMP.



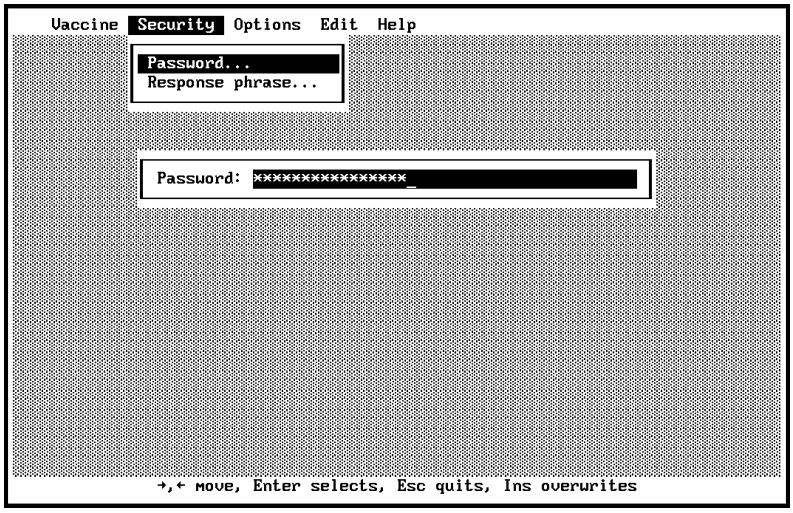
Hint: This is useful if you are fingerprinting a large number of PCs with a non-standard list of items and you do not wish to enter the list every time you install VACCINE on a new PC.

Enhancing security

There are two ways in which you can enhance the security of VACCINE: by specifying a password and by specifying a response phrase.

Password

Choose the ‘Password’ entry from the ‘Security’ menu of the top bar and then enter the required password.



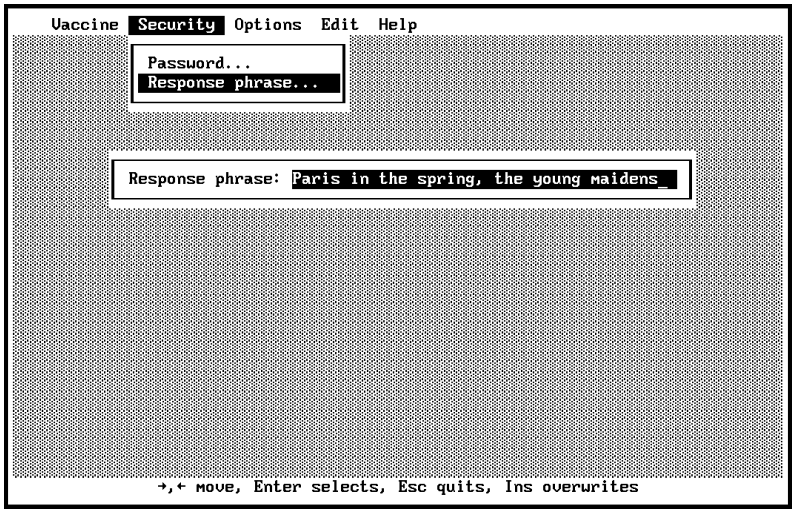
Characters are echoed as asterisks (*) as they are typed in for security reasons.

Even if you do not use a password the fingerprints will still be stored in an encrypted form, but using a standard key.

Note: The password, if used, will have to be entered every time you run DIAGNOSE. The purpose of the password is not to restrict access to VACCINE, but to make it impossible for anyone to modify files and then refingerprint them, without you being aware of it.

Response phrase

Choose the ‘Response phrase’ entry from the ‘Security’ menu on the top bar.



This response phrase will be displayed every time DIAGNOSE is executed.

Note: The function of this phrase is to customise your copy of DIAGNOSE and prevent an attacker from producing a version which looks identical. By using the password **and** the response phrase, you will be ensuring the highest possible security for your subsequent integrity checking.

DIAGNOSE stores the response phrase encrypted securely using your password; when you run DIAGNOSE, you will be asked to verify that the phrase has been displayed correctly.

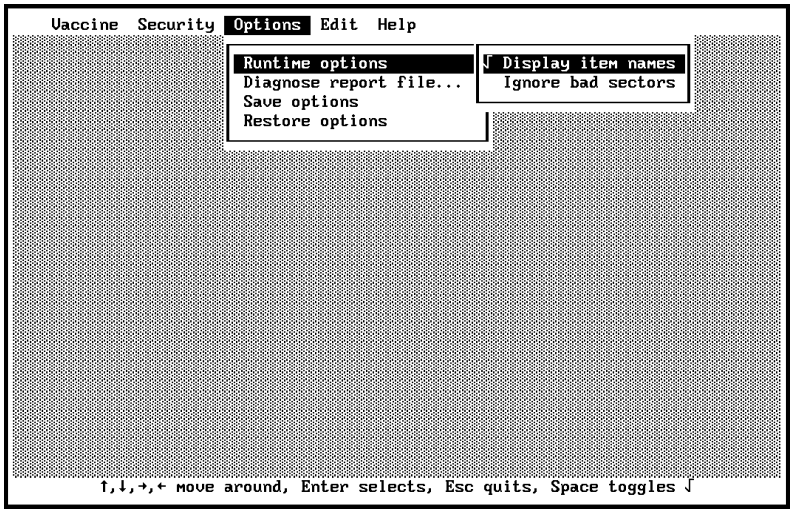
It is recommended that you use an arbitrary, unpredictable long phrase, e.g. ‘I like modern jazz quintets’ or ‘The thorax has a bony-cartilaginous skeleton’ - but make sure the phrase is chosen by you individually. You will not need to enter it when checking the system with DIAGNOSE, but you will need to recognise it.

Options

You can configure both VACCINE and DIAGNOSE using the 'Options' menu. Further customisation is possible by using command line qualifiers as described in separate sections.

Displaying the names of files being fingerprinted

This option applies both to VACCINE during fingerprinting and DIAGNOSE during the checking of fingerprints. When selected, item names are displayed when they are fingerprinted and when their fingerprints are checked.

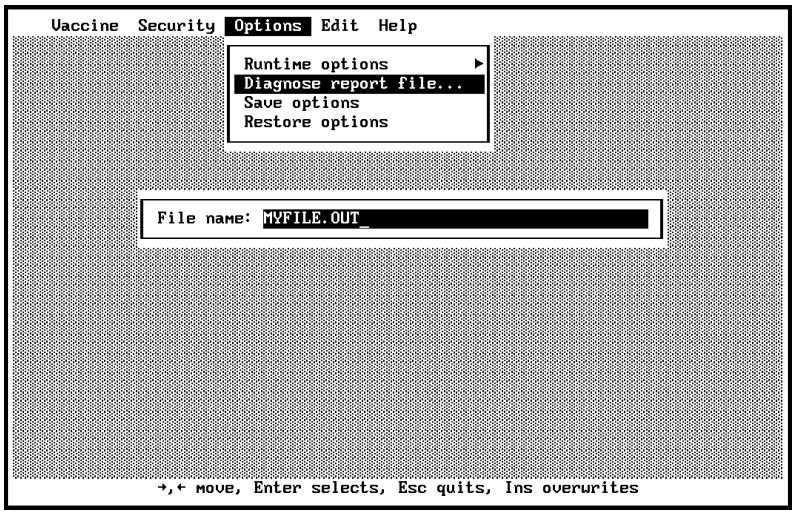


Ignore bad sectors

This option may be useful if you fingerprint disks which contain copy-protected software that intentionally creates bad sectors on a disk.

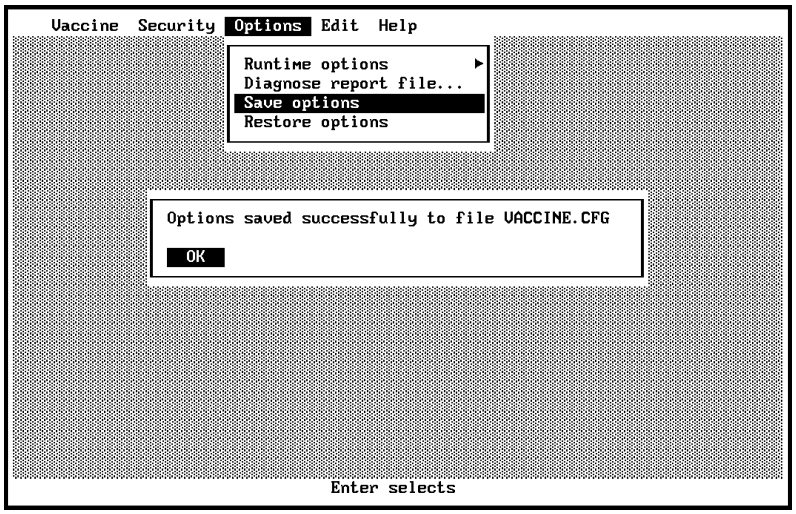
DIAGNOSE report file

If you wish to output the result of running DIAGNOSE into a file, select this option.



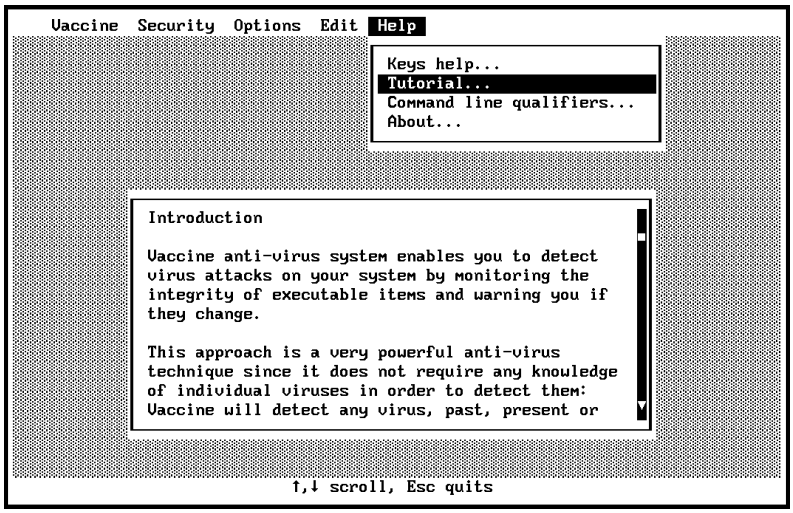
Saving and restoring options

To save the current options or restore the previously saved options from the VACCINE.CFG file in the current subdirectory, use the appropriate selections from the ‘Options’ menu on the top bar.



Help

On-line help is available from the ‘Help’ menu on the top bar. A tutorial on using VACCINE is also available.



Specifying items to be fingerprinted

Files

For high security you should check the following files:

```
All .COM files (executable programs)
All .EXE files (executable programs)
All .OV? files (overlay files)
All .BAT files (batch files)
All .SYS files (system files)
All .DLL files (Windows libraries)
```

To be certain that **all** files corresponding to this description on the system have been checked, you can use the recursion operator '>'. The recursion operator indicates that all subdirectories, as well as the current directory, should be searched. For example, if the entry C:*.EXE is specified, and the disk in drive C contains two subdirectories, only the current directory will be searched for .EXE files. On the other hand, if the entry C:>*.EXE is specified, not only the current directory but also both subdirectories will be searched for .EXE files. Similarly, if the entry

```
C:\MYAREA\MYFILES\>*.EXE
```

is specified, the search will cover the subdirectory

```
C:\MYAREA\MYFILES
```

and all its child directories.

The recursion operator can be positioned anywhere within the area description.

Remember that the more files you specify, the longer it will take to check the system using DIAGNOSE.

In addition, all auxiliary files belonging to programs should be included. For example, the software package LOGISTIX uses the following files:

```
LGX.EXE
LGX.INS
LGX.MSG
LGX.CHR
LGX.OVL
LGX.CAD
LGX.FNT
LGX.HLP
```

These would normally all need to be checked, which could be done by specifying 'LGX.*' as a group of files to be fingerprinted. Any software packages with auxiliary files such as these should be authenticated by specifying all appropriate files.

VACCINE automatically fingerprints not only the contents of each specified file, but also the following file attributes:

```
Read only / Hidden / System
Time of last update
Date of last update
File size
```

Three qualifiers, H, P and N can be used following the filename to control fingerprinting.

H fingerprints only the Header of each file (the first 32 bytes). This is much faster than fingerprinting the whole file and detects most viruses.

P disables fingerprinting of the file's contents; instead only the file's presence is checked and its attributes are fingerprinted. This is much faster than fingerprinting the whole file, but is obviously less secure.

N disables fingerprinting of the file's attributes. This is useful when a file's attributes change often (e.g. the date and time) whereas the contents do not.

The qualifier N can be combined with the H and P qualifiers. For example

```
C:>*.COM H ; only the header will be
 ; fingerprinted
C:>*.EXE P ; the contents of these
 ; files will not be
 ; fingerprinted
C:IO.SYS N ; the attributes of this
 ; file will not be
 ; fingerprinted
C:>*.COM PN ; only the presence of
 ; these files will be
 ; checked
```

See also the section on command line qualifier -M.

Hint: You can **exclude certain files or directories** from fingerprinting by preceding the description with the '<' *exclusion operator*. For example

```
C:>*.EXE
<C:\DONOT.EXE ; will not be
 ; fingerprinted
```

will recursively fingerprint all EXE files except DONOT.EXE in the root directory. If you specify the name of a file without a path, all files or directories with that name will be excluded. For example

```
<ALL.EXE   ; will not be fingerprinted
```

will not fingerprint the file ALL.EXE in any subdirectory in which it is found, e.g. files C:\EXE\ALL.EXE, C:\FIX\DEVELOP\ALL.EXE etc.

The drive, path and file name of the included and excluded items must be **identical**. For example, if you specify 'C:\>*.COM' to be fingerprinted and exclude '<\WS.COM', the file 'C:\WS.COM' will still be fingerprinted. If you wish to exclude it, you should specify '<C:\WS.COM'. Likewise, if you specify '\>*.EXE' for fingerprinting and your current drive is C:, specifying '<C:\NU.EXE' will still fingerprint 'NU.EXE' in the root directory. If you wish to exclude it, you should specify '<\NU.EXE'.

Note: VACCINE **will** NOT fingerprint the file DIAGNOSE.FIN. If you wish to take a fingerprint of DIAGNOSE.FIN, use the FILEMAC module.

Disk sectors

At a lower level than the file structure, disks are organised into 'sectors'. The most important of these are the 'master boot sector' and the 'DOS bootstrap sector', as they contain executable program code which many viruses attack. A floppy disk has just the DOS boot sector.

Sectors can be referred to in two ways: as *logical* sectors or as *absolute* sectors. A *logical* sector number refers to the position of the sector within a particular drive or partition. This is useful when referring to the DOS boot sector, which is logical sector 0 of the partition. The *absolute* specification of a sector is in terms of its physical position on the specified device. While more complex than a logical sector number, it allows any sector on the disk to be specified. This is important for fingerprinting the master boot sector, which can be found at cylinder 0, head 0, sector 1. On hard disks this sector is not accessible using a logical

sector number. On floppy disks, absolute sector 0,0,1 and logical sector 0 are the same physical sector.

Logical sectors

To specify a particular logical sector or set of sectors, use the '|' symbol (the PC-DOS pipe command). It is also possible to specify a byte or group of bytes to be fingerprinted in each sector (for example, if the sector contains variable information). The format of the specification is:

```
drive ssector esector sbyte ebyte
```

where

`drive` is the disk drive, e.g. C:
`ssector` is the first logical sector to be fingerprinted
`esector` is the last logical sector to be fingerprinted (optional)
`sbyte` is the first byte to be fingerprinted (optional)
`ebyte` is the last byte to be fingerprinted (optional)

Note that all values must be in **decimal** format.

For example

```
C:|0
```

specifies that the whole of logical sector 0 on drive C should be fingerprinted, whereas

```
C:|0 10
```

specifies that a fingerprint should be taken of logical sectors 0 to 10 inclusive, and

```
C:|0 10 271 275
```

specifies further that in each of the logical sectors 0 to 10, bytes 271 to 275 inclusive should be fingerprinted.

The following specification would fingerprint logical sector 15 on drive A, fingerprinting only byte number 536 within that sector:

```
A:|15 15 536
```

Note that the start- and end-sectors have been specified as the same.

Specifying 'F' as the `ssector` will fingerprint the first data sector of the partition.

For example

```
C:|F
```

will fingerprint the first data sector of the partition of drive C. Protecting the integrity of this sector is necessary when using system disks on operating system versions prior to DOS 4. A virus could exploit the weakness in the way that the operating system loads the first file on the disk in order to compromise the way that VACCINE fingerprints itself.

Absolute sectors

To specify an absolute sector, use the '+' symbol followed by the drive number, the cylinder (or 'track') number, the head (or 'side') number and the sector number within that cylinder. The first floppy disk drive in the system is number 0, the second is number 1, and so on. The first physical hard disk drive is number 80, the second is number 81 and so on. It is also possible to specify a byte or group of bytes to be fingerprinted in the sector (for example, if the sector contains variable information). The format of the specification is

```
+drive cylinder head sector sbyte ebyte
```

where

`drive` is the disk drive number
`cylinder` is the cylinder number
`head` is the head number

`sector` is the sector number
`sbyte` is the first byte to be fingerprinted (optional)
`ebyte` is the last byte to be fingerprinted (optional)

Note that all values should be in **hexadecimal** format.

For example

```
+80 0 0 1
```

specifies that sector 1 of cylinder 0, head 0 on the first fixed disk (usually drive C) should be fingerprinted, whereas

```
+1 0 0 1 23 1B7
```

specifies that a fingerprint should be taken of bytes 23 to 1B7 inclusive on sector 1 of cylinder 0, head 0 on the second floppy-disk drive (usually drive B).

It can be useful to take two separate fingerprints of the master boot sector, in order to distinguish between legal changes made to the disk partition table and illegal changes made to the rest of the sector. The suggested form is

```
+80 0 0 1 0 1BD ; this is the code
 ; portion of the master
 ; boot sector
+80 0 0 1 1BE 1FF ; whereas this is the
 ; partition table and
 ; boot ID tag
```

Memory ranges

Certain parts of memory are critical for the correct functioning of the operating system and should be fingerprinted for added security. The most important such part is the ‘interrupt table’, which is made up of the memory locations 0000 to 03FF hex in memory segment 0000.

Interrupts can be divided into six categories: microprocessor, hardware, software, DOS, BASIC and general-use. Microprocessor interrupts (numbers 00H to 03H) occupy the locations 0000 to 000F hex.

Hardware interrupts vary according to PC models and are 08H to 0FH (locations 0020 to 003F) on PCs, XTs and PS/2 models 25 and 30. ATs and PS/2 models 50, 60 and 80 also use interrupts 70H to 77H (locations 01C0 to 01DF).

Software interrupts are 10H to 1FH and 40H to 5FH (locations 0040 to 007F and 0100 to 017F).

DOS interrupts are 20H to 3FH (locations 0080 to 00FF).

BASIC interrupts are 80H to F0H (locations 0200 to 03BF).

General-use interrupts are available for temporary use in programs (and viruses!) and are 60H to 66H (locations 0180 to 019B).

Other parts of the interrupt table point to various parts of the operating system.

To specify memory ranges, use the '[' symbol. The format of the specification is

```
[segment:sbyte ebyte]
```

where

`segment` is the memory segment (assumed to be 0000 if not specified)
`sbyte` is the address of the first byte to be fingerprinted
`ebyte` is the address of the last byte to be fingerprinted

Note that all values should be in **hexadecimal** format.

For example

```
[0000:0000 00FF]
```

specifies that bytes 0000 to 00FF within segment 0000 should be fingerprinted, whereas

```
[0230:0010]
```

specifies that a fingerprint should be taken of byte 0010 in memory segment 0230, and

```
[1234 ABCD]
```

specifies that bytes 1234 to ABCD in segment 0000 should be fingerprinted.

If you want the whole interrupt table to be fingerprinted (and not just the PC-DOS part), specify the fingerprinting of

```
[0000:0000 03FF]
```

Note that certain legal programs such as the PRINT command install themselves as memory-resident processes and in doing so usually modify the interrupt table. If the interrupt table is to be included in the fingerprinting list, VACCINE and DIAGNOSE should be run with the same memory-resident software loaded - otherwise the interrupt table will show a bad fingerprint.

Fingerprinting the system

After you have specified which files, sectors and memory regions need fingerprinting, press *F2* (QUIT) and then *Enter*.

The cursor will be on the ‘Fingerprint system’ option. When you press *Enter*, the VACCINE program will fingerprint the files and sectors you have specified and record their fingerprints in the file DIAGNOSE.FIN .

Command line qualifiers

VACCINE accepts certain optional command line qualifiers to control and/or automate the fingerprinting process.

Drive

VACCINE will by default fingerprint drive C. If you wish to fingerprint a different drive, specify this command line qualifier.

For example

```
VACCINE D:
```

will fingerprint drive D. This is equivalent to using the -DR command line qualifier.

-? Help

If this command line qualifier is used, VACCINE will display all command line qualifiers and a short description of their function.

For example

```
VACCINE -?
```

-8 Use ISO standard

VACCINE allows you to choose between two methods of calculating the fingerprints. By default it uses the SPA algorithm, which provides an ANSI standard X9.9 MAC. If the command line qualifier '-8' is specified, for example

```
VACCINE -8
```

then the ISO Standard 8731 Part 2 method is used instead. In practical terms, the only difference is that the SPA method processes data much faster. There are no security benefits in choosing the ISO method, but sometimes compliance with that standard is required.

DIAGNOSE automatically uses the correct fingerprinting method when carrying out its check.

-BW Display in black and white

VACCINE determines whether the monitor is colour or black and white and displays in colour, if possible. If this command line qualifier is used, VACCINE will treat the monitor as being black and white.

For example

```
VACCINE -BW
```

will display all text in black and white.

-CFG= Specify configuration file

The default configuration file name is VACCINE.CFG. A different file name can be specified by using this command line qualifier.

For example

```
VACCINE -CFG=F:\VACCINE\VACCINE.ALL
```

-CO Display in colour

VACCINE determines whether the monitor is colour or black and white and displays in colour, if possible. If this command line qualifier is used, VACCINE will treat the monitor as being colour.

For example

```
VACCINE -CO
```

will display all text in colour.

-DI= Specify DIAGNOSE.EXE

VACCINE will by default run DIAGNOSE.EXE. A different executable file can be specified by using this command line qualifier.

For example

```
VACCINE -DI=F:\PUBLIC\DIAGNOSE.EXE
```

-DR= Drive

VACCINE will by default fingerprint drive C. If you wish to fingerprint a different drive, specify this command line qualifier.

For example

```
VACCINE -DR=D:
```

will fingerprint drive D.

-F= File with fingerprints

VACCINE will by default store the fingerprints in the DIAGNOSE.FIN file. If you wish to store fingerprints in a different file, use this command line qualifier.

For example, you may wish to keep a short list of fingerprints in one file to check on a daily basis and a long list of fingerprints to check on a weekly basis. You can store them in, say, files DIAGNOSE.FI1 and DIAGNOSE.FI2 and invoke DIAGNOSE with the appropriate file name.

The file you specify will not be fingerprinted.

For example

```
VACCINE -F=DIAGNOSE.FI1
```

to fingerprint and

```
DIAGNOSE -F=DIAGNOSE.FI1
```

to check the fingerprints.

-FL= File with the fingerprinting list

This command line qualifier allows you to specify a file which contains the list of items to fingerprint.

VACCINE will automatically read in the list of items to be fingerprinted from the specified file.

For example, you may have a batch file for automatic installation, which will fingerprint a standard list of items. This batch file MYINSTAL.BAT could contain:

```
VACCINE -FL=VACCINE.STD
```

When the user types 'MYINSTAL', VACCINE will read in the contents of VACCINE.STD. The user will not be required to enter anything.

-M= Attribute mask

This qualifier allows a logical-AND mask to be applied to the attributes of files before they are fingerprinted. By default the mask is 1F hex, which excludes the 'archive' bit used by many backup programs. This means that the attribute fingerprint will not change when the file is backed up.

For example specifying

```
VACCINE -M=00
```

has the effect of excluding all the Read-only, Hidden, System and Archive attributes from file attribute fingerprints.

For full information on which bits correspond to which attributes, refer to the sections 'Directory Entries' and 'Fields of the FCB (File Control Block)' in the MS-DOS Programmer's Reference Manual.

-MO Display in monochrome

VACCINE automatically determines the type of monitor. If this command line qualifier is used, VACCINE will treat the monitor as monochrome.

For example

```
VACCINE -MO
```

-P Path through the menus

This qualifier can be used to specify the selection of options in the VACCINE menu structure. **0 selects the first option, 1 the second etc.** For example

```
VACCINE -P03
```

will choose option 0 in the first menu and option 2 in the second menu. '^' is equivalent to the user pressing Esc while '?' allows the user to make a selection. For example

```
VACCINE -P031?^01
```

would ask the user to select the level of fingerprinting and then proceed to generate the fingerprints (selecting option 0 in the first menu, option 3 in the second menu etc).

-R= Response phrase

This qualifier allows the response phrase to be specified in the command line, which can be useful if VACCINE is to be run from a batch file.

For example

```
VACCINE -R=JOLLY_GOOD_SHOW_CHAPS
```

has the same effect as entering the response phrase

```
JOLLY GOOD SHOW CHAPS
```

interactively in the normal way. Note that any underscore characters used in the command line, as in the above example, will be converted into blanks.

-TI= Tick symbol

This qualifier specifies a different menu item selection character (✓) in hex. The default is FB hex.

For example

```
VACCINE -TI=4
```

specifies '•' as the menu selection character.

-W= Password

This qualifier allows the password to be specified in the command line, which can be useful if VACCINE is to be run from a batch file.

For example

```
VACCINE -W=FOR_YOUR_EYES_ONLY
```

has the same effect as entering the password

```
FOR YOUR EYES ONLY
```

interactively in the normal way.

Using the DIAGNOSE module

The DIAGNOSE module performs a check of your system against previously calculated fingerprints. It will detect any changes made to the fingerprinted items, down to the level of a single altered bit.

DIAGNOSE is always used after the VACCINE module has been used to calculate the initial fingerprints, as described in the previous chapter. The fingerprints are stored in the file DIAGNOSE.FIN.

Checking the system

For maximum security, you should check your system after performing a secure bootstrap, as described in the 'Installing VACCINE' chapter.

DIAGNOSE automatically detects whether it uses a password. If this is the case, it will first ask for the password you entered during the initial system fingerprinting using VACCINE.

Once the correct password has been entered, DIAGNOSE will display the date and time of fingerprinting with VACCINE, as well as the response phrase. It will then ask you whether the date, time and the phrase are correct. Type Y for Yes or N for No. (If no response phrase is in use, this question is automatically omitted.)

DIAGNOSE will proceed to check the fingerprints of all files, sectors and memory ranges in its list. If there are any discrepancies between the system when

fingerprinted and in its current state, DIAGNOSE will inform you of the differences.

To stop DIAGNOSE's output on the screen, type *Ctrl-S* (hold down the Ctrl key and press S). To restart the screen output, type *Ctrl-Q*.

Note: As DIAGNOSE cannot check the fingerprint of the file containing the fingerprints, it ignores the files on the disk with the same name as that file.

Running DIAGNOSE from batch files

The return value of DIAGNOSE can be tested by using the 'IF ERRORLEVEL' DOS command. This enables you to take action in case DIAGNOSE discovers an abnormal condition.

Important! DIAGNOSE normally returns:

- 0 if no errors are discovered and all patterns matched
- 1 if the user interrupts the execution by pressing *F2 Esc* or *Ctrl-C*
- 2 if some fundamental error is discovered, such as the absence of the file DIAGNOSE.FIN
- 3 if some abnormal condition is discovered, such as bad fingerprints, presence of files which should not have been on the system etc.

You can test these return values by using the 'IF ERRORLEVEL' DOS command. For example

```
DIAGNOSE -NK
IF ERRORLEVEL 3 GOTO FISHY
IF ERRORLEVEL 2 GOTO SOMEERR
ECHO No problems
GOTO END
:SOMEERR
ECHO Some error has occurred
GOTO END
:FISHY
```

```
ECHO Something has been discovered
:END
```

will print ‘Something has been discovered’ if DIAGNOSE discovers an abnormality, ‘Some error has occurred’ in case of an error, or ‘No problems’ if nothing is discovered. The -NK command line qualifier tells DIAGNOSE not to stop execution if abnormalities are discovered.

Customising the ‘Viruses Found’ report

If DIAGNOSE discovers an abnormal condition, it will produce a warning to that effect. You can customise the warning, for example

```
Contact MIS Immediately on Ext 4321!
```

by placing the appropriate text in the file DIAGNOSE.MSG in the current directory.

You can specify a different file name by using the -FM command line qualifier.

Command line qualifiers

DIAGNOSE can use certain command line qualifiers to configure its operation. These qualifiers can be combined as required and are particularly useful when DIAGNOSE is used in a batch file such as AUTOEXEC.BAT.

-? Help

DIAGNOSE will display all command line qualifiers and a short description of their function, if this command line qualifier is used.

For example

```
DIAGNOSE -?
```

-A Append report

By default, any security report written to a file by DIAGNOSE will be overwritten by a subsequent report written to a file of the same name. Specifying the -A qualifier in the command line

```
DIAGNOSE -A -P=FOO.REP
```

directs DIAGNOSE to append the new report to the old file FOO.REP, rather than overwriting the old report with the new one.

-D= Day or percentage

Though DIAGNOSE is most conveniently incorporated into the AUTOEXEC.BAT file, it may not be desirable to perform the system check every single time the computer is switched on. The -D= qualifier allows you to specify either the probability with which DIAGNOSE will actually proceed to check the system, or the day of the week on which the system should be checked.

For example

```
DIAGNOSE -D=MONDAY
```

will make DIAGNOSE run only when invoked on a Monday. The day of the week can be abbreviated to a minimum of two letters, eg. MO for Monday, TU for Tuesday and so on.

Alternatively,

```
DIAGNOSE -D=20
```

will make DIAGNOSE check the system on average 20 times out of every 100 that DIAGNOSE is invoked. The number specified must be an integer between 0 and 100.

-DE Daily execution

This command line qualifier will check if DIAGNOSE has already been executed that day and if it has, it will not be executed again. The file DIAGNOSE.DAY is created on the current drive and directory and contains the date when DIAGNOSE was last run (YYMMDD).

For example

```
DIAGNOSE -DE
```

A different file can be specified by including '=filename' after the -DE command line qualifier.

For example

```
DIAGNOSE -DE=diagnose.da1
```

-F= File with fingerprints

VACCINE will, by default, store the fingerprints in the DIAGNOSE.FIN file. If the fingerprints are stored in a different file, use this command line qualifier. For example, you may wish to keep a short list of fingerprints in one file to check on a daily basis and a long list of fingerprints to check on a weekly basis. You can store them in, say, files DIAGNOSE.FI1 and DIAGNOSE.FI2 and invoke DIAGNOSE with the appropriate file name. The AUTOEXEC.BAT file would contain

```
DIAGNOSE -F=DIAGNOSE.FI1
DIAGNOSE -D=10 -F=DIAGNOSE.FI2
```

which will run the short fingerprint check every day and the long check 1 out of 10 times (10% probability). See also the description of the '-D' command line qualifier.

-FM= Message file

If DIAGNOSE discovers one or more viruses and the file 'MESSAGEFILE' exists, DIAGNOSE will output its contents to the screen. This facility can be used to customise virus recovery procedures.

If -FM is not used, the default file name is 'DIAGNOSE.MSG'.

For example

```
DIAGNOSE -FM=MYMESS.TXT
```

specifies the file 'MYMESS.TXT'.

-L= Left margin

The -L qualifier specifies the left margin for security reports. The default is 9 spaces, which allows for punching holes in the margin. For example, to specify 3 spaces:

```
DIAGNOSE -L=3 -P
```

-ME= Message

This qualifier specifies the message which will be inserted in the printed security report instead of the default 'MESSAGE NUMBER' text.

The message cannot include blank spaces.

For example

```
DIAGNOSE -ME=Number -P=PRN
```

would insert the text 'Number' into the security report.

-MF= File which will be inserted

This qualifier specifies that the contents of the specified file should be inserted in the printed

security report instead of the default 'MESSAGE NUMBER' text.

This allows the customisation of the report, for example, with the serial number of the computer which generated it.

For example

```
DIAGNOSE -MF=PATTERN.TXT -P=PRN
```

would insert the text in the file 'PATTERN.TXT' into the security report.

-NI No interrupting

The execution of DIAGNOSE can be interrupted by pressing *F2* or *ESC*. If this command line qualifier is used, the execution cannot be interrupted using *Esc*, *Ctrl C* or *Break*.

For example

```
DIAGNOSE -NI
```

-NK No key to continue

If DIAGNOSE discovers one or more bad fingerprints, it will pause at the end of the security report and ask for a key to be pressed before continuing. If you want to disable this, use this command line qualifier option.

For example

```
DIAGNOSE -NK
```

-NR No response phrase check

This qualifier can be used to let DIAGNOSE run without checking the response phrase.

For example

```
DIAGNOSE -NR
```

This is useful if it is necessary for DIAGNOSE to run without any user interaction.

-NS Do not suppress items checked

Using this command line qualifier will cause the display of names of fingerprinted items.

For example

```
DIAGNOSE -NS
```

-P{=} Print security report

This command line qualifier directs DIAGNOSE to print a security report. If you use the qualifier as -P (not followed by =), DIAGNOSE outputs the report to the device PRN.

Alternatively, the report can be directed to a particular file or device using the qualifier -P= .

For example

```
DIAGNOSE -P=SEC.DOC
```

directs DIAGNOSE to write its security report to the file SEC.DOC.

-SS Super silent running

If this command line qualifier is used, DIAGNOSE will not display anything (not even the copyright message) unless bad fingerprints are found.

For example

```
DIAGNOSE -SS
```

-W= Password

This qualifier allows the password to be specified in the command line, which can be useful if DIAGNOSE is to be run from a batch file.

For example

```
DIAGNOSE -W=FOR_YOUR_EYES_ONLY
```

Has the same effect as entering the password

```
FOR YOUR EYES ONLY
```

interactively in the normal way.

Using the FILEMAC module

This chapter describes the use of the FILEMAC module for producing and checking file fingerprints.

The function of FILEMAC

The FILEMAC module can be used to produce a fingerprint of any file or group of files.

FILEMAC is a flexible cryptographic fingerprinting tool which can be used in a variety of ways for change control, software release identification and so on. It differs from VACCINE and DIAGNOSE in that it displays the actual numerical values of the fingerprints it calculates. FILEMAC is used for monitoring authorised and unauthorised computer system changes, and in particular for implementing challenge/response procedures to audit securely from a central management point the integrity of remote systems.

Running FILEMAC

To use FILEMAC, type

```
FILEMAC filename
```

FILEMAC will fingerprint the file and display the fingerprint (also known as a MAC or Message Authentication Code).

You can use wildcards in the filename, as well as specify more than one filename.

For example, you could type

```
FILEMAC *.123 *.DOC
```

in order to fingerprint all .123 files and .DOC files.

Command line qualifiers

FILEMAC accepts a number of command line qualifiers which can be used to configure its behaviour. These can be combined, in so far as they do not conflict logically.

-? Help

If this command line qualifier is used, FILEMAC will display all command line qualifiers and a short description of their function.

For example

```
FILEMAC -?
```

-C= Check fingerprint

Including the -C= qualifier in the command line allows FILEMAC to check whether the fingerprint it calculates is that which was expected. The value supplied must be an 8-digit hexadecimal value.

For example

```
FILEMAC MYFILE.EXE -C=0BB4E359
```

calculates a fingerprint for the file MYFILE.EXE and checks whether it is equal to the hexadecimal value 0BB4E359. FILEMAC displays the result of the check and returns to DOS a normal code (0) or anomaly completion code (3) as appropriate. This return value can be used to interrupt processing of a batch file in the event of an error.

The -C= qualifier and the -I qualifier cannot be used simultaneously.

-I Individual fingerprints

By default, FILEMAC calculates a single fingerprint for all the files specified in the command line. The -I qualifier enables individual fingerprints to be calculated for each file.

For example

```
FILEMAC *.EXE -I
```

directs FILEMAC to calculate a separate fingerprint for each file with the extension .EXE.

The -I qualifier and the -C= qualifier cannot be used simultaneously.

-K= Starting key

The calculation of a MAC (i.e. a fingerprint) is based on a 'starting key'. Choosing a different starting key will lead to calculation of a completely different fingerprint value. By default, FILEMAC uses a starting key of 0000000000000000 Hex. However if you wish to use a non-zero starting key, for example to implement a challenge/response scheme, the starting key can be set using the -K= qualifier. The qualifier must be followed by a phrase or a 16-digit hexadecimal number.

For example

```
FILEMAC SCR -K=0123456789ABCDEF
```

would use the starting key 0123456789ABCDEF Hex to calculate a fingerprint for the file SCR.

Hexadecimal digits are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F. Keys so specified must have exactly 16 characters, all of which must be hexadecimal digits. The hexadecimal digits A, B, C, D, E and F can also be entered in lowercase.

A key can also be any word, phrase or number, from 1 to 64 characters in length, though for security purposes, keys shorter than 8 characters are not recommended.

For example

```
FILEMAC MYFILE -K=Who_goes_there
```

The case of characters is not important (uppercase or lowercase). Any characters other than letters and digits are ignored and can be used to enhance legibility.

Important! If you use the -K= qualifier you must type the key without blank spaces. Either omit them altogether, if present, or use underscore characters (_) as in the above example; these will not affect the validity of the key.

-NK No key to continue

If FILEMAC discovers a discrepancy between the calculated fingerprints and the fingerprints specified with -C command line qualifier, it will pause and ask for a key to be pressed before continuing.

If you want to disable this, use this command line qualifier option.

For example

```
FILEMAC -C=12345678 -NK
```

-S Silent running

The -S qualifier suppresses the display of file names while they are being fingerprinted.

For example

```
FILEMAC *.* -S
```

will calculate a single fingerprint for all files, but not list their names as it processes them.

-8 Use ISO standard

By default FILEMAC uses the SPA algorithm for fingerprinting. To generate a fingerprint conforming to ISO Standard 8731 Part 2 instead, use the -8 command line qualifier.

For example

```
FILEMAC MYFILE -8
```

Changing default colours with CHNGBW

The CHNGBW utility can be used to configure Sophos software which uses colour output for monochrome monitors.

Note: This is especially useful on some PCs with LCD displays which do not display colour text very well.

Introduction

Run CHNGBW by typing

```
CHNGBW
```

When prompted, enter the name of the program which needs changing. This program must be in the current directory.

CHNGBW will then ask you if you wish the program configured for black and white or colour. Type the desired parameter and press *Enter*.

If you have entered *black and white*, CHNGBW will configure the software without any further prompts.

If you have entered *colour*, CHNGBW will present you with a screen of parameters which you can change. For example, you can specify a different cursor shape, different colour for normal text, different colour for error messages etc. Use *cursor down* and *cursor up* to position the cursor on a parameter and then *cursor right* and *cursor left* to change the value. Pressing *F5* will restore the default

parameter value. Press *F2* when you have finished and select *Yes* if you want the settings implemented or *No* if you do not.

Command line qualifiers

CHNGBW can use certain command line qualifiers to configure its operation. These qualifiers can be combined as required, and are particularly useful when CHNGBW is used in a batch file.

-BW Set display to black/white

Using -BW in the command line specifies that the software is going to be configured for black and white.

-CO Set display to colour

Using -CO in the command line specifies that the software is going to be configured for colour.

-D Install default values

When CHNGBW is used for configuring a colour version of the software, it will read and display the current settings of various parameters.

Using -D will restore the default settings, without reading in the settings in the current copy of the software.

-MO Display in monochrome

If this command line qualifier is used, CHNGBW will configure the program to use the monochrome monitor.

-S Suppress output

Makes CHNGBW operate without outputting any information on the screen, provided that you have also specified -CO or -BW command line qualifiers.

-TI=tick character hex value

Specifies the value of the tick character on the menus ('✓' by default). The value must be specified as a hexadecimal number representing the desired ASCII character.

-U=<top>,<bottom> cursor rows

Specifies cursor size:

- The Colour Graphics Adaptor (CGA) can display a cursor which has 8 rows, numbered from 0 at the top to 7 at the bottom.
- The Monochrome Display Adaptor (MDA) and the Extended Graphics Adaptor (EGA) can display a cursor which has 14 rows, numbered from 0 at the top to 13 at the bottom.
- The MCGA and VGA adaptors can display a cursor which has 16 rows, numbered from 0 at the top to 15 at the bottom.

The desired cursor size is set by specifying the top and bottom rows.

For example

```
CHNGBW VACCINE -U=3,5
```

will set the cursor size to rows 3 to 5 in VACCINE.EXE.

Default cursor settings are 6 to 7 for CGA, 11 to 12 for MDA and EGA and 13 to 14 for MCGA and VGA.

Using VACCINE in a large organisation

These guidelines are intended for use by data processing managers, data security managers and internal auditors. They describe how to use and administer the software package VACCINE within a large organisation.

Policies and responsibilities

Data integrity is becoming of increasing importance; in particular, *every* large organisation should be aware of the threats posed by computer viruses and other forms of system corruption. The allocation of responsibility for these issues varies from one organisation to another, but typically the Data Processing, Information Technology, Management Services or Data Security departments should have the authority to assess and recommend strategies and products, while the mainstream or 'line' management should have corresponding powers of enforcement.

These guidelines will refer from here onwards to the **data security department** and the **data security manager**, to identify the department and personnel concerned with advisory management and installation of procedures. The Internal Audit department plays a special role in many cases, having a specific authority to run 'third-party' checks on the roles of advisory and line management. This can be of particular relevance to the use of VACCINE.

Each organisation should have policies which

- Assign responsibility for the safety of its PCs and other computer systems.
- Give the data security department the power to install protective measures.
- Give line management the power to enforce these measures.

Clearly defined policies, backed up by suitable resources, are essential for rational management of computer system integrity.

When there are no existing data security policies in place, the first action should be the appointment of a person charged with defining the policies and directing their implementation. Sophos organises regular seminars on this subject, which can be of great help in streamlining the complex initial stages in defining a corporate policy.

Defining the Strategy

The data security department should plan carefully its use of VACCINE. There are no universal recipes for the correct level of security and the way to achieve it, but the following pages indicate the type of questions which must be asked. Each organisation will tend to develop its own approach and the VACCINE modules constitute a suitably flexible security tool to allow this.

Questions to ask

Which computers should be controlled using VACCINE?

If it does not already exist, a register should be compiled of all computers falling under the jurisdiction of the data security department for purposes of system integrity. The computers should be grouped by type (PC, Unix system, VAX, etc.) and typically also by department or location. For each

computer the register should contain full details of the machine model, screen type (black / white or colour, in the case of PCs), the removable media type and size (disk: 3.5", 5.25"; tape: 1/2", 1/4", 1200 bpi, 6250 bpi etc.) and location, as well as details of the person responsible for the machine.

Should the computers be classified into different categories of security?

Depending on where computers are situated, what they are used for and which personnel have access to them, it may be appropriate to distinguish between them for the purposes of integrity checking. If this is so, suitable security categories should be defined as part of the organisation's strategy. Particular systems or areas can then be assigned an appropriate category or rating, based on a risk / threat analysis, from which will follow the measures and procedures to apply.

Who should take initial fingerprints?

It is crucial that a system's integrity is certain before the initial fingerprints are taken and not all users will be technically competent to determine whether this is the case. Ideally, initial fingerprinting should be performed immediately after a system is originally configured with its operating system and application software. When this is not possible, the use of the SWEEP module can ensure that the system does not contain any known viruses. In many cases, this checking and taking of the initial fingerprints is best done by a data security manager.

Which items should be fingerprinted?

The answers to this question can vary widely from one application to another. If VACCINE is being installed primarily as a virus detection measure, the important items to check include operating system files, programs, command or batch files, the system bootstrap sector(s) on a disk and certain memory regions, such as the interrupt table on PCs. If the

emphasis is more on change control, only certain specific items such as CAD files, payroll files or software source files may need fingerprinting. Since the duration of fingerprinting and fingerprint checking depends upon the volume of data being fingerprinted, a balance should be struck between the scope of the check and the overhead it imposes.

Who should be allowed access to the VACCINE module?

This question is related to the previous one; if a user has access to the VACCINE module, which takes the initial fingerprints, then he will be in a position to re-fingerprint his system. If it has been decided that only certain personnel should do this, then others should be excluded from access to the VACCINE module. If the users themselves are to run integrity checks (see the following question), they will need to have access to the DIAGNOSE module. However, if only the data security manager will perform checks, it is usually preferable to deny users access to any of the VACCINE modules.

Who should run integrity checks?

Integrity checks with the DIAGNOSE (and/or FILEMAC) modules can be carried out either by the user or by the data security manager. Sometimes a combination of the two is desirable, with the user checking his own machine on a day-to-day basis and the data security manager performing more formal checks less frequently. In more stringent and secure environments, it may be inappropriate for end users to perform any self-checking using DIAGNOSE or FILEMAC. Instead, such tests should be carried out either by the data security department or by an internal auditing team.

In which situations should checks take place?

System integrity checks should be made systematically: on powering up the computer; before taking a backup; before and after installing a new

software package; when a computer changes 'ownership' etc. A policy should be established to determine which situations require integrity checking and which do not. An effective technique is to use batch files (also called scripts, command files or procedures on some operating systems) for such operations and include DIAGNOSE within them, so that it is invoked automatically. A typical point at which to include DIAGNOSE on PC systems is the AUTOEXEC.BAT file, so that a system integrity check is carried out automatically every time the computer is powered up.

How often should checks be made?

In general terms, the more often the checks are made, the better. However, an exaggerated level of checking may lead to poor acceptance and hence non-compliance among users. DIAGNOSE has extensive command line qualifiers which the data security manager can use to schedule the checks and control DIAGNOSE's reporting. The options include checking only on certain days of the week or randomly with a specified probability, eg. 20% of the times that DIAGNOSE is run.

What action should be taken, and by whom, if an error is discovered during checking using DIAGNOSE?

The action to be taken generally depends upon the nature of the error discovered. The important issue is to establish suitable procedures for handling an event of this sort, so that the user or data security manager who discovers a system integrity error knows what to do, whom to report to, how to document the incident, where to find further information, whether or not use of the affected computer can be permitted to continue, and so on.

What level of reporting should be operated?

At the lowest level, the user may simply run DIAGNOSE as and when scheduled, taking whatever

action seems appropriate to him in the event of DIAGNOSE reporting an error. In most cases this is insufficient and a written record of the results is necessary. DIAGNOSE provides the option of printing a security report which gives the status of all items being checked. The report is formatted ready for signing and filing and allows a system integrity log to be built up. DIAGNOSE can, if desired, suppress its report on all items except those showing errors. In the event of errors being detected, DIAGNOSE includes a checklist of recommended actions within the report. For example, if a dual checking procedure is being operated (i.e. checking by users *and* by the data security department) then it may be appropriate for the data security manager to produce printed security reports, but not the users.

Should the security reports be customised?

DIAGNOSE produces its security reports in a standard format by default. As part of a corporate security strategy, however, it may be necessary for the format and content of the security report to be customised to the requirements laid down by the data security department within a particular organisation. This applies especially to the action checklists in the event of errors, when users may need to be told which telephone number to ring or whom to contact in the data security department. Customisation of the reports and messages is available through Sophos.

Should DIAGNOSE be run from removable or fixed media?

The most secure way of running DIAGNOSE is to keep the module on write-protected removable media also containing the operating system, and to switch on and bootstrap the system from that disk or tape before running the check. This ensures that no virus on the non-removable system media can interfere with the bootstrapping process and thus with the operation of DIAGNOSE. Even if DIAGNOSE is run

from fixed media it will detect most errors, but a stealth virus already active could be able to circumvent it. If, for example in the case of PCs, it has been decided that users will perform regular checks on their own machines, a good balance between acceptance and security can be achieved by running DIAGNOSE from the fixed disk by the user as part of the normal power-up process, while the data security manager makes periodic or random spot checks with his own copy of DIAGNOSE from a write-protected floppy disk.

When should re-fingerprinting be allowed, and by whom?

There should be procedures governing the installation of new software, the replacement of old software with a new release, and so on. It is important that these procedures should dictate when to re-fingerprint the system using VACCINE and who should be responsible.

What documentation should be made available to the users?

Depending upon the answers to some of the above questions, a decision must be made as to the form and content of documentation made available to the users. It may be appropriate to include the VACCINE documentation as part of a wider document covering security or computer operation. To aid the process of producing customised documentation, site licence copies of VACCINE include the user manual in machine-readable form. This also makes possible integration of the manual into an on-line help facility.

What action should be taken to educate users?

It is important for computer users to be aware of the potential dangers of computer viruses and other forms of deliberate or accidental system corruption. They should also be aware of standard preventative measures which minimise the chance of a system being infected, corrupted or damaged. Education of

users can be achieved by means ranging from circulation of memos to organisation of seminars. Sophos' consultants regularly give lectures, seminars and workshops covering all aspects of the subject, including demonstrations of computer viruses. These talks can be tailored to individual customers' requirements and presented on-site in the form of specific product training courses for end-users.

What budget exists or should exist for data security?

The best-planned strategy can grind to a halt if suitable budgetary arrangements are not made. Many companies still improvise by buying data security products and services out of a Data Processing Department 'slush' fund or similar allocation, but this is generally unsatisfactory for any systematic implementation of data security in a large organisation. A budgetary resource must be coupled with a suitable allocation of authority to spend it; this will typically be given either directly to the data security department, or to a procurement department which is advised by the data security managers.

Do existing procurement procedures need to be altered?

At some point following a general installation of VACCINE, it is likely that in the course of the organisation's development, new computer systems will be purchased. It is important for procedures to ensure that new equipment is integrated automatically into the existing strategy for integrity checking. If similar requirements apply to other software products, it may be possible to incorporate VACCINE into an existing procurement structure.

Documentation

The answers to the questions in the previous section form a basis upon which to draw up appropriate rules and procedures for the use of VACCINE.

Typical documents in which information about VACCINE should be included are:

- General corporate policy document.
- Corporate standards specification.
- Detailed data security strategy document.
- General end-user guidelines.
- Detailed end-user instructions and procedures.

Formulating this information appropriately to the relevant documents is an essential aspect of developing and installing a corporate security policy.

Site licences

Site licences are a flexible purchase method for large organisations wishing to make widespread use of a particular software package.

Site licence agreements are available and provide a more flexible and efficient means of purchasing the software than do multiple orders for single units and are designed to meet the needs of large organisations.

A master copy of the software is supplied in each appropriate media format. The customer is then free to duplicate and/or use the software as required, up to the specified maximum number of computers on the agreed site. The site can be defined as required, covering anything up to an entire organisation located in several countries.

Periodic upgrades of software and documentation are included as part of every site licence agreement, as is telephone support to a single contact point designated by the customer - typically the data security department.

An annual fee is charged for site licence agreements.

Treating viral infection

This chapter deals with the problem of dealing with a virus once it has been discovered by SWEEP or DIAGNOSE.

Additional information on PC viruses can be found in the 'Computer Viruses' chapter of Sophos' *Data Security Reference Guide*.

Recovery from a virus attack

Recovery from a virus attack involves two main stages:

1. Elimination of the virus from infected areas.
2. Recovery from any virus side-effects.

Eliminating viruses

SWEEP's automatic disinfection facilities, or DOS commands, can deal with many virus attacks:

- **Infected boot sectors** can be disinfected (in some cases) or neutralised.
- **Infected files** can be deleted.
- **Infected documents** can be disinfected.

The sections below explain how to prepare for disinfection and how to deal with each kind of infected item.

Establishing a clean environment

A clean boot disk, i.e. an uninfected write-protected system floppy disk, is normally an essential part of the manual virus recovery procedure. A separate clean boot disk will be required for each different operating system version, and it is vital that these are created on uninfected machines.

To create a bootable system disk, enter at a DOS prompt **on a DOS machine**:

```
FORMAT A: /S
```

Copy HIMEM.SYS, EMM386.EXE, FDISK.EXE, SYS.COM (not to be used on Windows NT), DEBUG.EXE, SMARTDRV.EXE, SCANDISK.EXE (or CHKDSK.EXE for MS-DOS 5 and before), and FORMAT.COM onto the disk. HIMEM.SYS is an Extended Memory (XMS) driver which allows SWEEP to use all the PC's memory thereby improving performance. SMARTDRV.EXE is a disk caching program which improves SWEEP's performance by minimising the amount of disk access required when traversing the directory structure of a disk.

Create a CONFIG.SYS file with the following lines:

```
DEVICE=A:\HIMEM.SYS
DEVICE=A:\EMM386.EXE
DOS=HIGH,UMB
FILES=15
BUFFERS=40
```

Create an AUTOEXEC.BAT with the following line:

```
A:\SMARTDRV.EXE
```

Make the disk write-protected (to ensure that it cannot become infected with a virus), and label it with the operating system for which it was created.

If a computer becomes infected, use the clean boot disk to boot the computer. This will ensure that

various items on the computer can be examined through a 'clean' operating system, giving the virus no chance to employ hiding techniques.

Dealing with infected boot sectors on the hard disk

Infected boot sectors **on hard disks** can be dealt with in two ways:

1. Disinfection

This is the preferred approach. Before attempting this, it is advisable to backup any important data contained on the hard disk.

Reboot the PC with a clean boot disk. Use SWEEP for DOS to disinfect the virus with the command

```
SWEEP -DI
```

This will also disinfect any infected documents that SWEEP is capable of disinfecting.

2. Replacing the boot sector

Alternatively, the boot sector can in many cases be overwritten with a clean one.

Reboot the PC with a clean boot disk, and check that the contents of the infected drive are visible (e.g. with `DIR`).

If the directory listing is okay, the **master boot sector** can be overwritten with the command

```
FDISK /MBR
```

and the **DOS boot sector** can be overwritten with the command

```
SYS C:
```

If using the SYS command to overwrite a DOS boot sector virus, it is essential that the clean boot disk was for the same version of DOS as the infected PC.

Also, if the infected PC is not a DOS machine (e.g. it is running Windows NT), the SYS command should not be used because it is operating system specific.

Important! If the contents of the hard disk are not visible after a clean boot, contact Sophos' technical support for advice. Some boot sector viruses do require additional action for full recovery. For example, the *OneHalf* virus encrypts the boot sector so that it is only readable when the virus is in memory.

Dealing with infected boot sectors on floppy disk

Floppy disks with infected boot sectors can either be disinfected with SWEEP or reformatted.

1. Disinfection

Reboot the PC with a clean boot disk. Then use SWEEP for DOS to disinfect the virus, with the command

```
SWEEP -DI
```

This will also disinfect any infected documents SWEEP is capable of disinfecting.

2. Reformatting

Alternatively**, reboot the PC with a clean boot disk**, copy the valuable data from the infected disk to a clean destination (it is safe to copy files if the PC has been booted from a clean boot disk), and reformat the disk using

```
FORMAT A:
```

if the disk is in drive A:.

Dealing with infected executable files

It is generally inadvisable to attempt to disinfect infected executables. This is because it is not possible to ensure that the executable has been properly

restored after disinfection; it may be unstable which may put valuable data at risk.

Reboot the PC with a clean boot disk. Then locate all the infected executables, delete them, and restore clean versions from the original installation disks, from a clean PC, or from sound backups.

Dealing with infected documents

When dealing with infected documents, it is not necessary to reboot from a clean system disk. However, it is important to ensure that the application that created the document is not open when disinfection is attempted.

In some cases it is possible to manually edit the macros from the infected document using the relevant application. However, some macro viruses now operate a form of stealth to prevent users from doing this. For example, *Winword/ShareFun* prevents the use of the Tools / Macro and File / Templates menu option. Please consult Sophos' technical support before attempting to perform manual disinfection of macro viruses.

Recovery from virus side-effects

Recovery from virus side-effects depends on the virus. In the case of innocuous viruses such as *Cascade*, recovery from side-effects is not necessary, while in the case of a virus such as *Michelangelo*, recovery will involve the restoration of a complete hard disk from the most recent backups.

Some viruses, such as *Winword/Wazzu* gradually make minor changes to users' data. This sort of corruption (e.g. the removal of the word 'not' from a sentence in a Word file) can be very hard to detect and highly undesirable.

The most important thing when recovering from virus side-effects is the existence of **sound backups**. Original executables should be kept on write-protected disks, so that any infected programs can easily be replaced by the original clean versions.

Sometimes it is possible to recover data from disks damaged by a virus. Sophos can also supply utilities for repairing the damage caused by some viruses. Contact Sophos' technical support for advice.

Other points

There are a few other things worth bearing in mind after a virus attack:

- Discover and close loopholes which allowed the virus to enter the organisation.
- Inform any possible recipients of infected disks outside the organisation that they may be affected by the virus.
- In the UK, inform the *Computer Crime Unit* of *New Scotland Yard* in London about the attack (Tel 0171 230 1177, Fax 0171 230 1275).

Troubleshooting

This chapter provides answers to some common problems encountered when using VACCINE.

VACCINE / DIAGNOSE run slowly

If you have chosen the long list of items to be fingerprinted, VACCINE and DIAGNOSE will take longer to run than if the medium or short lists have been chosen.

Check the list of items to be fingerprinted.

Network Error: file in use

If a network file is already open when DIAGNOSE tries to examine it, a message similar to the following will be displayed:

```
Network Error: file in use during OPEN A FILE.  File =
F:\ARCHLOG\00000041.REC
Abort, Retry?
```

If a file is to be accessible to several processes at the same time, it must be marked as ‘shareable’ by using the NetWare utility FILER.

Alternatively, VACCINE can be instructed to exclude these files from fingerprinting. See ‘Installing VACCINE onto a file server’ in the ‘Installing VACCINE’ chapter.

Text unclear on a black/white monitor

Some black / white monitors appear to the PC as colour, resulting in an unclear output in SW. This is especially apparent on some LCD (Liquid Crystal Displays). To force INSTALL or VACCINE to output black / white text use the -BW command line qualifier:

```
INSTALL -BW
```

Could not open file F:\PUBLIC\VACCINE.EXE

This error message appears if VACCINE is run from a NetWare file server after being set as an execute-only attribute.

To remedy the problem, delete VACCINE.EXE on the network and reinstall it from the distribution floppy disk.

False positives

A change reported by DIAGNOSE may not have been caused by a virus. Consult the ‘What can cause changes’ section in the ‘About VACCINE’ chapter.

If you are ever in doubt, contact Sophos’ Technical Support for advice.

Fingerprinting memory increases the chance of false positives and is unnecessary if the PC has been bootstrapped securely.

False negatives

A false negative is the opposite of a false positive, i.e. the event in which DIAGNOSE fails to report a virus in an infected file or sector.

Stealth viruses

Stealth viruses such as *4K* and *Joshi* actively hide themselves from anti-virus software. If the virus is memory-resident, DIAGNOSE will not discover its presence on a PC. To avoid this problem, prevent the virus from becoming memory-resident in the first place, by performing a secure bootstrap as described in the ‘VACCINE installation’ chapter.

Glossary

ANSI: American National Standards Institute is the organisation which issues standards in the US.

ASCII: American Standard Code for Information Interchange is the standard system for representing letters and symbols. Each letter or symbol is assigned a unique number between 0 and 127.

Background Operation: The name applied to a program running in a multitasking environment over which the user has no direct control.

Backup: A copy of computer data that is used to recreate data that has been lost, mislaid, corrupted or erased.

BAT: The extension given to 'batch' file names in MS-DOS. A batch file contains a series of MS-DOS commands, which can be executed by using the name of the file as a command. AUTOEXEC.BAT is a special batch file which is executed whenever a PC is switched on, and can be used to configure the PC to a user's requirements.

Binary: A number system with base 2. The binary digits (bits) are 0 and 1. Binary arithmetic is used by today's computers since the two digits can be represented with two electrical or magnetic states, for example the presence and absence of a current.

BIOS: The Basic Input/Output System of MS-DOS which constitutes the lowest level of software which interfaces directly with the hardware of the microcomputer. The BIOS is usually stored in a ROM chip.

Bit: The smallest unit of information. It can only have the value 0 or 1. The word 'bit' is derived from the initial and final letters of the phrase 'Binary Digit'.

Boot Sector Virus: A type of computer virus which subverts the initial stages of the bootstrapping process. A boot sector virus attacks either the master bootstrap sector or the DOS bootstrap sector.

Booting-up: A process carried out when a computer is first switched on or reset, where the operating system software is loaded from disk (either hard disk or floppy disk).

Bootstrap Sector: Part of the operating system which is first read into memory from disk when a PC is switched on (booted). The program stored in the bootstrap sector is then executed, which in turn loads the rest of the operating system into memory from the system files on disk.

Bootstrapping: The same as Booting-up.

Byte: A set of 8 bits which is the amount of information sufficient to store one character. It is usually the smallest individual unit that can be read from or written to memory.

Checksum: A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered. Usually 32 or 64 bits long.

COM: The extension given to a type of executable files in MS-DOS. They are similar to EXE files, but can only contain up to 64K of code and data. In operating systems other than DOS, the extension .COM can have a different significance.

Companion Virus: A virus which 'infects' EXE files by creating a COM file with the same name and containing the virus code. They exploit the PC-DOS property that if two programs with the same name exist, the operating system will execute a COM file in preference to an EXE file.

CRC: Cyclic Redundancy Check, a mathematical method for verifying the integrity of data. It is a form of checksum, based on the theory of maximum length polynomials. While more secure than a simple checksum, CRCs don't offer true cryptographic security. See cryptographic checksum.

Cryptographic Checksum: A checksum calculated by using a cryptographically based algorithm. It is impossible to 'engineer' changes to data in such a way as to leave a cryptographic checksum unchanged.

Device Driver: A program used to 'handle' a hardware device such as a screen, disk, keyboard etc. This allows the operating system to use the device without knowing specifically how the device performs a particular task.

DOS: Disk Operating System. See MS-DOS.

DOS Bootstrap Sector: The bootstrap sector which loads the BIOS and DOS into PC RAM and starts their execution. Common point of attack by boot sector viruses.

Downloading: A process where data is transferred electronically from a 'host' computer to an intelligent terminal or PC.

EXE: The extension given to executable files in MS-DOS. These are similar to .COM files, but can contain more than 64K of code and data.

False Negative: An existent event reported as non-existent, e.g. the absence of a virus when the virus is present.

False Positive: A non-existent event reported as existent, e.g. the presence of a virus when no virus is present.

FAT: File Allocation Table, a mnemonic term used by the MS-DOS operating system (and others) to describe the part of a disk which contains information describing the physical location on the disk of the chains of clusters forming the files stored on that disk.

Hexadecimal: A system of counting using number base 16. The numbers 10 to 15 are represented by the characters 'A' through 'F' respectively. Hexadecimal is often abbreviated to hex. Each hex digit is equivalent to four bits (half a byte) of information.

Interrupt: A mechanism by which a process can attract the immediate attention of the CPU, usually in order to serve an urgent request from an external device. Interrupt table on 8086 microprocessors occupies the bottom 1K of RAM.

ISO: International Organisation for Standardisation, the worldwide federation of international standards bodies.

Link Virus: A virus which subverts directory entries to point to the virus code.

MAC: Message Authentication Code, a cryptographic checksum for a message. Unlike a digital signature, a MAC requires knowledge of a secret key for verification.

Master Bootstrap Sector: The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the PC is bootstrapped. It contains the partition table as well as the code to load and execute the bootstrap sector of the 'active' partition. Common point of attack by boot sector viruses.

MS-DOS: The Disk Operating System sold by Microsoft. It is the most common microcomputer system in the world, and operates on the IBM PC.

Multi-partite Virus: A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector viruses and parasitic viruses.

Nibble: A set of 4 bits.

Operating System: The computer program which performs basic housekeeping functions such as maintaining lists of files, running programs etc. PC operating systems include MS-DOS and OS/2, while minicomputer and mainframe operating systems include Unix, VMS and MVS.

OVL: The extension commonly given to overlay files in MS-DOS. Overlay files are used with large programs which cannot fit into RAM: parts of the program are loaded as and when needed. Overlay files can have any extension, not just .OVL.

Parasitic Virus: A computer virus which attaches itself to another computer program, and is activated when that program is executed. A parasitic virus can append itself to either the beginning or the end of a program, or it can overwrite part of the program.

Polymorphic Virus: Self-modifying encrypting virus.

Stealth Virus: A virus which hides its presence from the PC user and anti-virus programs, usually by trapping interrupt services.

SYS: The extension given to system file names in MS-DOS. An example is the file CONFIG.SYS which sets up various configuration parameters for the operating system on power-up.

Trojan Horse: A computer program whose execution would result in undesired side effects, generally unanticipated by the user. The Trojan horse program may otherwise give the appearance of providing normal functionality.

TSR: Terminate and Stay Resident, a term used to describe an MS-DOS programs which remains in memory after being executed. A TSR can be re-activated either by a specific sequence of keystrokes, or at some specific time, or by some specific signal from an I/O port.

Index

S

T

U

V

W

User comment form

We welcome your comments and suggestions on our software and documentation. They help us to provide you with better products. Please fax this form to +44 1235 559935. Comments about this manual can also be emailed to <publications@sophos.com>.

Product: _____ Version: ❒.❒❒

Documentation:	Excellent	Good	Fair	Poor
Accuracy	❒	❒	❒	❒
Completeness	❒	❒	❒	❒
Clarity	❒	❒	❒	❒
Page layout	❒	❒	❒	❒

Software:	Excellent	Good	Fair	Poor
Ease of use:	❒	❒	❒	❒
Ease of installation:	❒	❒	❒	❒
Overall assessment:	❒	❒	❒	❒

Please indicate any errors found in this software or documentation:

_____

_____

_____

Please give any suggestions for improving the software or documentation:

_____

_____

_____

Name: _____

Position: _____

Organisation: _____

Address: _____

_____

Telephone: _____ Fax: _____

Signed: _____ Date: _____

Australia:

Doctor Disk
Level 7
418A Elizabeth Street
Surry Hills NSW 2010
Australia
Email sales@drdisk.com.au
http://www.drdisk.com.au/
Tel 02 9281 2099 · Fax 02 9281 9740 · Code +61

Bahrain:

International Information Systems
PO Box 3086
Flat 31, Building 123 Block 320
Exhibition Road
Manama
Bahrain
Tel 293821, 292040 · Fax 293408 · Code +973

Belgium:

Software Marketing Group
rue E. Van Ophemstraat 40
B-1180 Brussels
Belgium
Email pbuysse@netdirect.be
Tel 02 376 57 42 · Fax 02 376 09 85 · Code +32

Brazil:

Datasafe Produtos de Informática e Serviços Ltda
Rua Santa Justina, 336 Gr. 108
Itaim
04545-041 Sao Paolo SP
Brazil
Email datasafe@originet.com.br
Tel 011 822 1129 · Fax 011 822 1129 · Code +55

Channel Islands:

Softek Services Ltd
20 Peter Street
St Helier
Jersey
JE2 4SP
Email sales@softek.co.uk
http://www.softek.co.uk/
Tel 01534 811182 · Fax 01534 811183 · Code +44

Croatia:

Qubis d.o.o.
Nova Cesta 1
10000 Zagreb
Croatia
Email qubis@zg.tel.hr
Tel 01 391461 · Fax 01 391294 · Code +385

Denmark:

Lamb Soft & Hardware
Lille Strandstraede 14
1254 Copenhagen K
Denmark
Email info@lamb-soft.dk
Tel 3393 4793 · Fax 3393 4793 · Code +45

Finland:

Oy Protect Data Ab
P.O. Box 48
00931 Helsinki
Finland
Email antti.laaja@dlc.fi
Tel 09 752 521 · Fax 09 7525 2210 · Code +358

France:

Racal-Datacom S.A.
18 Rue Jules Saulnier
93206 Saint-Denis Cedex
France
Email plemounier@racal-datacom.fr
Tel (1) 49 33 58 00 · Fax (1) 49 33 58 33 · Code +33

Germany:

NoVIR DATA
Hochofenstrasse 19-21
23569 Lübeck
Germany
Email 100141.2044@compuserve.com
Tel 0451 306 066 · Fax 0451 309 600 · Code +49

Hong Kong:

Racal-Datacom Limited
Sun House
181 Des Voeux Road
Central Hong Kong
Email w_chu@racal.com.hk
Tel 28158633 · Fax 28158141 · Code +852

Ireland:

Renaissance Contingency Services Ltd.
The Mews
15 Adelaide Street
Dun Laoghaire
Co Dublin
Ireland
Tel 01 280 9410 · Fax 01 280 8302 · Code +353

Italy:

Telvox s.a.s.
Via F.lli Cairoli 4-6
40121 Bologna
Italy
Email telvox.teleinf@bologna.nettuno.it
http://www.nettuno.it/fiera/telvox/telvox.htm
Tel 051 252 784 · Fax 051 252 748 · Code +39

Japan:

Computer Systems Engineering Co. Ltd.
23-2 Maruyamacho
Aletsusa Bldg.
Shibuya-ku
Tokyo 150
Japan
Tel 03 3463 5633 · Fax 03 3496 7477 · Code +81

Malta:

Shireburn Co. Ltd.
Carolina Court
Guze Cali Street
Ta'Xbiex, Msd 14
Malta
Email info@shireburn.com
http://www.shireburn.com/
Tel 319977 · Fax 319528 · Code +356

Netherlands:

CRYPSYS Data Security
P.O. Box 542
4200 AM Gorinchem
The Netherlands
Email crypsys@pi.net
http://www.pi.net/~crypsys/
Tel 0183 62 44 44 · Fax 0183 62 28 48 · Code +31

Forum Data Security
WG Plein 202
1054 SE Amsterdam
The Netherlands
Email forum_data_security@pi.net
Tel 20 685 3486 · Fax 20 612 9702 · Code +31

New Zealand:

Wang New Zealand Ltd
P O Box 6648
Wellington
New Zealand
Email sophos@wang.co.nz
Tel 04 382 0100 · Fax 04 385 6067 · Code +64

Norway:

Protect Data Norge AS
Brobekkveien 80
0583 Oslo
Norway
Email protect_data@oslonett.no
Tel 022 65 64 50 · Fax 022 65 64 58 · Code +47

Poland:

Safe Computing Ltd.
ul. Targowa 34
03-733 Warszawa
Poland
Email info@safecomp.com
http://www.safecomp.com/
Tel 022 6198956 · Fax 022 6700756 · Code +48

Portugal:

Década Informática s.a.
Apt. 7558
Estr. Lisboa/Sintra, Km 2,2
2720 Alfragide
Portugal
Email amandio.sousa@decada.mailpac.pt
Tel 01 471 2045 · Fax 01 471 2191 · Code +351

Singapore:

Racal Electronics (S) Pte. Ltd.
26 Ayer Rajah Crescent #04-06/07
Singapore 139944
Email sales@racal.com.sg
http://www.racal.com.sg/
Tel 779 2200 · Fax 778 5400 · Code +65

Slovakia:

Protect Data Slovakia
Kukolova 1
831 07 Bratislava
Slovak Republic
Email protectd@ba.sanet.sk
Tel 07 541 1527 · Fax 07 541 2210 · Code +421

Slovenia:

Sophos d.o.o.
Zwittrova 20
8000 Novo mesto
Slovenia
Email slovenia@sophos.com
Tel 068 322977 · Fax 068 322975 · Code +386

Spain:

Sinutec Data Security Consulting S.L.
Traversera de Gracia 54-56 Entlo. 3 y 4
08006 Barcelona
NIF B-60062502
Spain
Email sinutec@ysi.es
http://www.sinutec.com/
Tel 93 490 70 52 · Fax 93 490 76 04 · Code +34

Sweden:

Protect Datasäkerhet AB
Humlegardsgatan 20, 2tr
Box 5376
102 49 Stockholm
Sweden
Email info@protect-data.se
http://www.protect-data.se/
Tel 08 459 54 00 · Fax 08 459 54 10 · Code +46

Switzerland:

Performance System Software SA
Rue Jean-Pelletier 6
1225 Chene-Bourg
Geneva
Switzerland
Email jlt@pss.ch
http://www.pss.ch/
Tel 022 860 1030 · Fax 022 349 4775 · Code +41

Turkey:

Logic Bilgisayer Ltd
Esentepe Cad. Techno Centre 10/2
Mecidiyekoy
Istanbul
Turkey
Tel 0212 212 3664 · Fax 0212 212 3669 · Code +90

United States of America:

ACT
7908 Cin-Day Rd, Suite W
West Chester
Ohio 45069
USA
Email farrell@altcomp.com
http://www.altcomp.com/
Tel 513 755 1957 · Fax 513 755 1958 · Code +1

Uruguay:

Datasec
Patria 716
Montevideo 11300
Uruguay
Tel 02 715878 · Fax 02 715894 · Code +598

Sophos Plc • The Pentagon • Abingdon Science Park • Abingdon • OX14 3YP • England • Tel 01235 559933 • Fax 01235 559935
Sophos Inc • 18 Commerce Way • Woburn • MA 01801 • USA • Tel 781 932 0222 • Fax 781 932 0251
Sophos GmbH • Am Hahnenbusch 21 • D-55268 Nieder-Olm • Germany • Tel 06136 91193 • Fax 06136 911940

Email sales@sophos.com • http://www.sophos.com/