InterCheck client-server virus detection

Dr. Jan Hruska, Tim Twaits, Ronnie Sutherland, Sophos Plc, Oxford, England

Part # tr00007h/960118

Introduction

This document discusses InterCheck client-server virus detection. It describes the InterCheck principle, its advantages and gives technical information on how the system works.

Virus protection of networks

There are two distinct elements of a network which need to be virus checked:

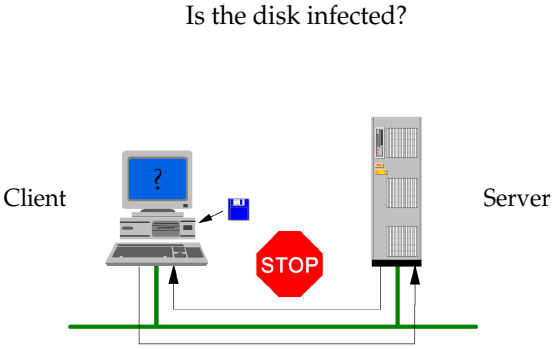
- the files held on the server
- the workstations connected to the server

The files held on the server are best checked by a server-based scanner (an NLM on NetWare, Windows NT scanner on Windows NT etc.). Workstations normally require on-line virus checking of any disks introduced into the system, as well as files being executed. This has traditionally been done by memory-resident (TSR) scanners, but the growth in virus numbers and virus complexity makes such programs increasingly cumbersome and, consequently, impractical. The need to update any scanner with new virus information means that new TSRs are introduced on a regular basis, which can cause clashes with other TSRs and affect system reliability.

As the number of viruses increases, the TSR scanners are getting bigger. As the complexity of viruses increases, the impact of TSR scanners on workstation performance also increases. The servers, on the other hand, do not usually suffer from the same limitations and will continue to be able to run virus-scanning software in the future.

InterCheck

InterCheck extends the power of the server-based virus detection from the server out to the workstations. This provides true client-server operation which is completely automatic and transparent to the end user.



How does InterCheck work?

The InterCheck client software is a program running on the workstation. Unlike scanners, it does not contain any virus-specific information. The virus detection (InterCheck server functionality) is provided by a server-based SWEEP.

The InterCheck client maintains a database of authorised items for each workstation. Any attempt to access an unknown program or disk causes the client to request authorisation from the server. This authorisation is given only after the server has verified that the item is not infected. This process is automatic and does not require any user intervention.

If the program is infected, the authorisation is refused, the user is automatically informed and access to the infected program is denied.

The InterCheck client requires no updating. Installation can be automated across the network. There is no need to configure individual workstations.

Once a program or a disk has been authorised it can be used without further checking, unless it is modified.

If a virus is discovered on a workstation, the server will broadcast a message to designated users, as well as recording details of the workstation and the file where the virus is found.

Working as a pair of communicating processes the InterCheck client and server ensure complete virus protection for the whole network.

Network overheads

The usual initial concern about the client-server virus detection is the overhead in copying the files to the server to be checked. In practice, however, the overheads are minimal due to the following:

- Once an item is authorised, it does not need re-authorisation unless it changes
- SWEEP is run locally when InterCheck is started
- Centralised checksumming is used (if available on the server)

Item authorisation

Once an item has been authorised (a boot sector or an executable file) it does not need re-authorisation unless it is modified. Boot sectors and executable files do not (should not) change, so the need for authorisation is kept to a minimum.

SWEEP is run locally

In order to minimise the network overheads, a local copy of SWEEP is run on the workstation whenever a new copy of workstation SWEEP is installed on the server (this does not apply to Macintosh clients). This causes all local executables to be authorised, limiting the need for server authorisation to any new and changed items.

Centralised checksumming

Centralised checksumming enables all clients to benefit from the server authorising an item either after a client request or by the server SWEEP. For example, a copy of a commonly used program will only have to be authorised by the first user executing it. All other users will benefit from that in not having to re-authorise it.

Centralised checksumming is currently available on NetWare and Windows NT server versions of SWEEP.

InterCheck clients

DOS

The DOS InterCheck TSR client occupies around 10K of RAM and automatically loads into high memory.

The local checksums are stored in the file INTERCHK.CHK in the root directory of the workstation hard drive, or in the \SWEEP\LISTS directory on the file server for diskless workstations. If centralised checksumming is provided by the server, the client will consult the central checksum database held on the server in addition to its own.

The DOS system functions intercepted by the DOS client can be selected by the CheckOn configuration file option (please consult the appropriate InterCheck manual for details on using this). There are 3 options:

Program Execution (CheckOn=EXEC)

InterCheck checks all programs and overlays which are loaded using the standard DOS 'load and execute' function (interrupt 21 function 4B). The program files are checked before the program starts running and infected programs are not allowed to run.

Access to Programs (CheckOn=ACCESS)

In this mode, InterCheck considers any file with the following extensions to be a program: COM, EXE, SYS and OV?. InterCheck intercepts the DOS open file functions (interrupt 21 functions 0F, 3D & 6C) and the rename file functions (interrupt 21 functions 17 & 56). Infected programs cannot be opened or renamed. For example, the following operations would fail if the file `VIRUS.SYS` was infected:

```
COPY VIRUS.SYS A:\
RENAME VIRUS.SYS NEWVIRUS.SYS
RENAME OLDVIRUS.SYS VIRUS.SYS
```

InterCheck also intercepts the DOS close file functions (interrupt 21h functions 10h & 3Eh). New and modified program files are checked at this point. InterCheck does not check the file until after it has been created, so although a warning will be generated when a file is infected, the file will still exist on the disk. However, InterCheck will not allow the file to be copied or executed.

Note that using CheckOn=ACCESS will cause programs packed inside compressed files (ZIP, ARC etc.) to be checked as they are unpacked.

Floppy disks (CheckOn=FLOPPY)

InterCheck will check the boot sector of any removable disk the first time a new disk is accessed by DOS. Access to clean files on an infected disk is not prevented, but InterCheck will continue to warn the user that the disk is infected.

InterCheck intercepts the use of Ctrl-Alt-Del to reset the PC. The PC cannot be restarted in this manner if InterCheck detects an infected floppy disk in drive A.

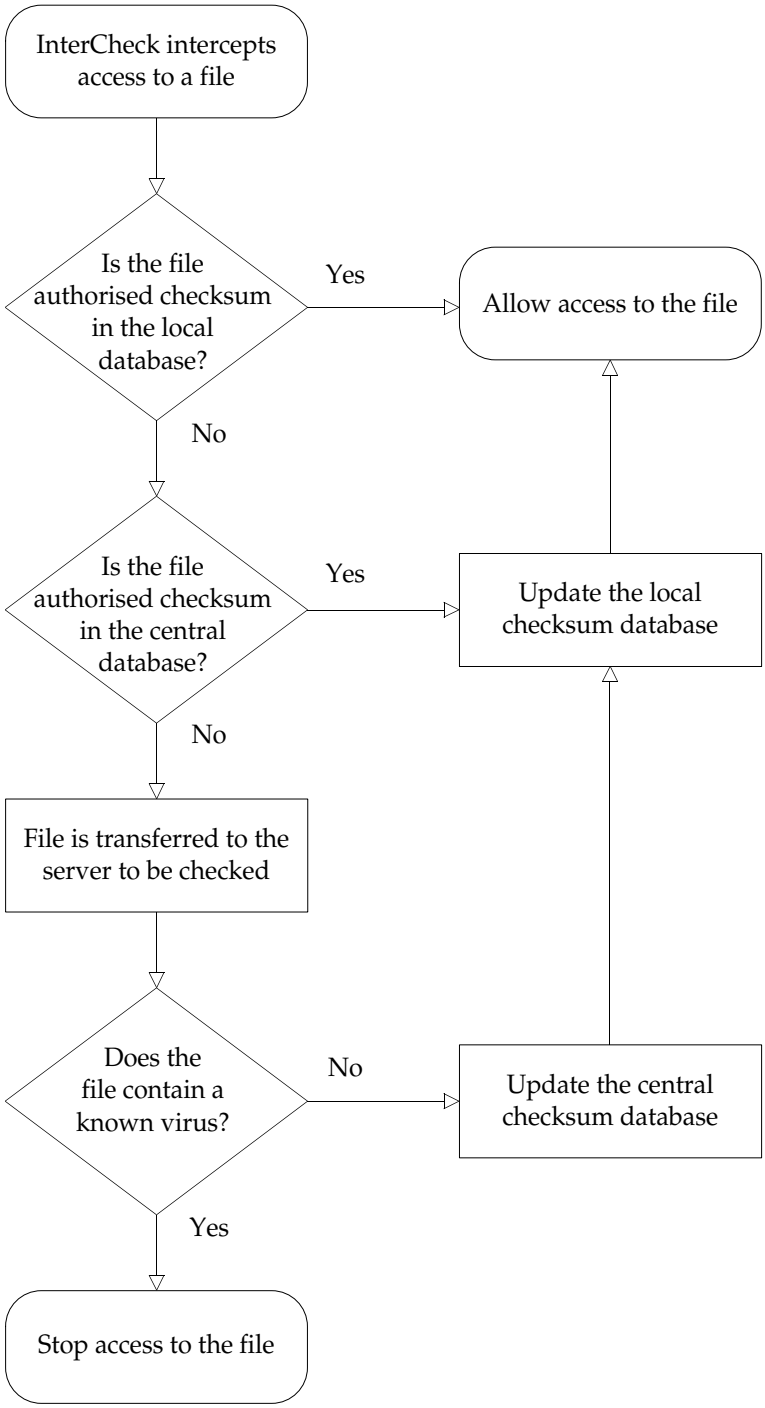


Figure 2: Flow diagram showing the use of the checksum database by InterCheck

Windows Client

The Windows client is an extension of the DOS client. Two additional components required to support Windows are loaded automatically as Windows starts if the DOS InterCheck client is already active:

1. A virtual device driver (interchk.386) intercepts file I/O operations that would otherwise bypass the hooks installed by the DOS client.

2. A background application (icpopup.exe) handles the display of messages, such as virus alerts, to the user.

The detection of program files is extended in Windows. When the CheckOn=EXEC option has been selected, InterCheck will examine the contents of all files which are opened. Any file which contains a valid Windows program header is checked for viruses.

Windows 95 Client

The Windows 95 client is implemented as a dynamically loadable virtual device driver (VxD). There are 3 major components:

- The loader (icwin95.exe)
- The virtual device driver (icdriv95.vxd)
- The support application (icsupp95.exe)

The VxD intercepts file operations performed by the IFS (Installable File System) manager.

Macintosh

The InterCheck client can be used on any Macintosh with System 7.0 or later with either 68k or PPC architecture. It occupies around 25k of memory. It has been designed to run as a System Extension and will capture application launches and either allow the application to execute or send it to the server for virus scanning (Fig. 2).

Cryptographic checksums of applications are held in an invisible file (ICChecksum) on the startup disk.

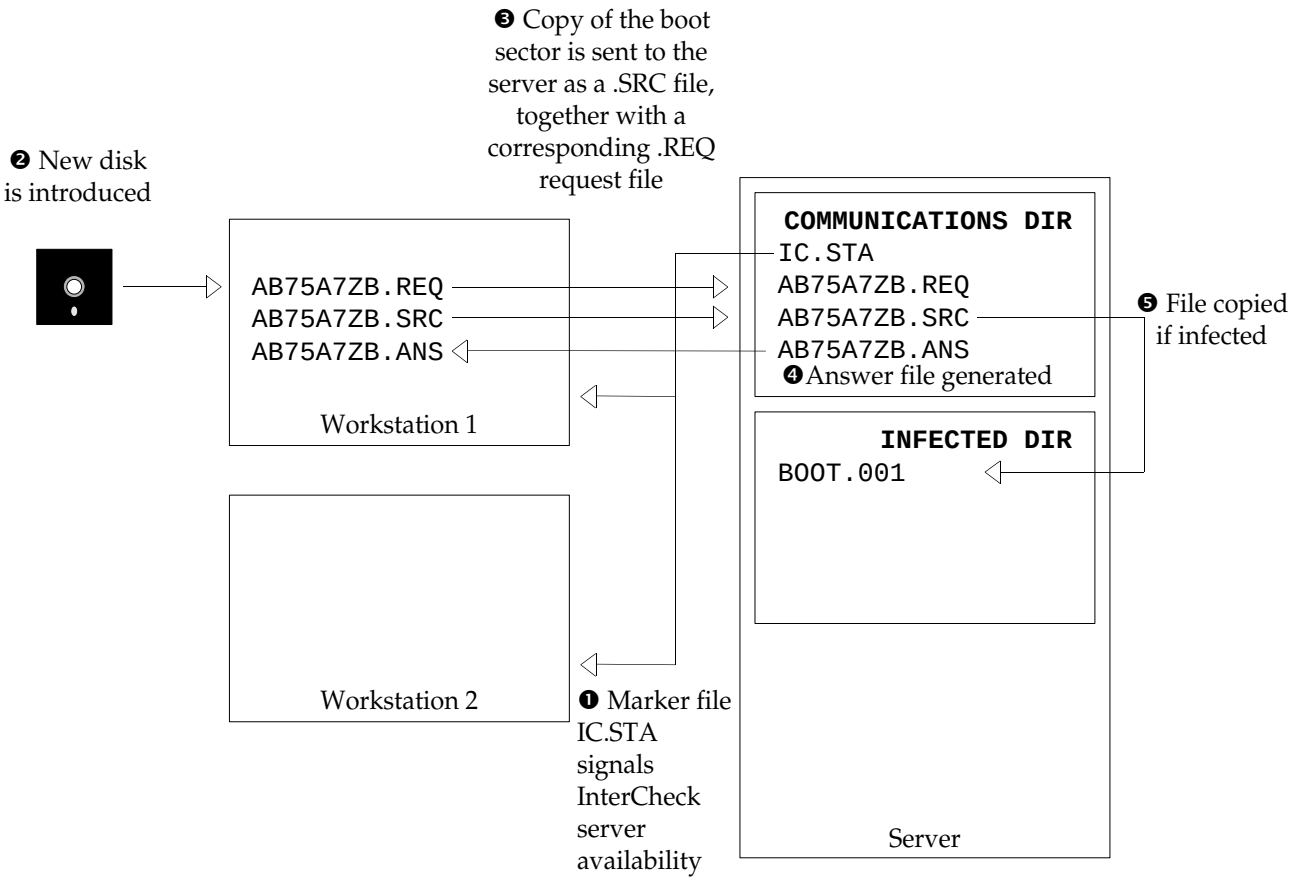


Figure 3: InterCheck request generation and processing

Communication between clients and the server

All communications are done at file level, which makes the InterCheck client independent of the server operating system and network transport protocol.

A communications directory is required for which all clients have read/write permission. This is normally a subdirectory of the area used to hold the client (e.g. \SWEEP\COMMS on a NetWare server).

When the server starts providing InterCheck services, it creates and keeps open the marker file IC.STA in the communications directory (Fig. 3). This is a signal to the clients that the server is active and that their requests will be processed.

A client initiates the request by copying the item to be checked into the communications directory using a random file name and the extension .SRC. It also creates the request file in the communications directory with the same name and the extension .REQ. This creates the description of the request, original file name etc. The client then waits for an answer.

The server process monitors the communications directory and when a .REQ file appears, it virus-checks the corresponding .SRC file. When the .SRC file has been checked, it is either deleted (if not infected) or moved to the infected directory (if infected). The answer file has the same name as the .REQ file but the extension .ANS is then create in the communications directory.

The client waits for the appearance of the corresponding .ANS file which should appear within 60 seconds (this is a default timeout which can be changed). If it does not appear, the client will time out, indicating the error on the screen. Otherwise, the client examines the answer and if the item is clean, allows its execution and if not, prevents it. If the item is clean, its checksum is also added to the local checksum database resident on the hard drive of the client.

If the server supports centralised checksumming, the client will examine the centralised checksum database on the server as well as its own, before making a request to the server.