CHECKVIR ANTI-VIRUS TESTING AND CERTIFICATION

Dr Ferenc Leitold
Veszprém University, Hungary

Certification programmes provide a useful independent assessment of the capabilities of software products. Anti-virus products present a unique challenge for testers – the nature of viruses and anti-virus products being such that, even were a product to remain static the viruses it must detect will not, thus making regular re-testing essential. In this article Ferenc Leitold introduces the CheckVir anti-virus testing service and certification programme, and in the following article Matt Ham provides an overview of Virus Bulletin's own VB 100% testing procedures.

It is important for all software testers and quality engineers to test their programs in as many different environments as possible, with numerous input combinations. In the case of anti-virus products this task is more difficult because the products change very rapidly. Anti-virus software usually includes several tens of thousands of detection and disinfection algorithms, which should be tested regularly on a large number of virus samples and, of course, on non-virus objects as well.

The *CheckVir* project has provided a regular anti-virus testing service since April 2002, and in January 2004 a monthly anti-virus certification process was started.

AIMS OF THE PROJECT

The *CheckVir* project aims to provide clear, accurate and reliable testing of anti-virus products. A number of rules were set out at the beginning of the project. Some of them are as follows:

- Infected objects must be made by replicating the virus – which proves the 'viral property' of infected objects.
- No application other than the anti-virus software will be installed on the test platform.
- All available service packs and updates of both the operating system and the anti-virus product must be installed.
- Every test must be repeatable.

The main goals of the testing and certification procedures are to decrease the number of bugs in the products, as well as minimise the number of problems related to anti-virus products. Problems and bugs are distinguished as follows: a problem is when a new feature needs to be developed into the product – for example, if an anti-virus product cannot detect a virus or disinfect it. The presence of a bug means that the product does not behave correctly – for example, if an anti-virus product informs the user that a particular virus has been removed, but the cleaned program file is unable to run.

REGULAR TESTING

As part of the *CheckVir* project's regular anti-virus testing service tests are executed monthly on different platforms. Regular tests are based on virus detection and disinfection. Scanning is tested both on demand and on access, and email scanning of both incoming and outgoing traffic is also put to the test. Other tests include speed tests, heuristic tests, testing of packed objects and testing of the storage area of email clients.

CheckVir's regular testing is a powerful aid for developers in indentifying the following problems that may be found in anti-virus products:

- The anti-virus software is able to detect a virus, but does not deal with unusual cases (e.g. the infected file is too small or too big where there is an error in the virus).
- The behaviour of at least two versions of an anti-virus product developed by the same company and working with the same engine are different (e.g. the *Windows Me* version of an anti-virus product can detect a virus, but the *Windows XP* version of the same product is unable to detect the same virus in the same sample).
- The behaviour of at least two scanning methods of an anti-virus product using the same engine and database are different (e.g. the on-demand scanner can detect a virus, but the on-access scanner of the same product is unable to detect the same virus in the same sample).
- The behaviour of the product's disinfection capability is different when using two different versions of the same anti-virus product (e.g. versions for different platforms).
- The behaviour of the product's disinfection capability is different when using different scanning methods (on demand and on access).
- The anti-virus software is able to detect a particular virus, but only in some samples (e.g. in the case of polymorphic and macro viruses).
- The anti-virus product does not wipe all virus-related macros correctly from a document.
- The anti-virus program is unable to distinguish between similar viruses. In some instances, the program makes mistakes during the disinfection procedure.

- The anti-virus program is able to disinfect a particular virus correctly, but the disinfected file may not be able to be executed from some samples.
- Other functional problems (e.g. the anti-virus software hangs during the disinfection procedure for a particular virus).

CHECKVIR AV CERTIFICATION PROGRAMME

The *CheckVir* anti-virus certification program includes all products that are submitted for the regular *CheckVir* testing service. Currently there are three levels of certification:

- *Standard level*. Here, the products' virus detection capability (alone) is examined. The anti-virus products must find all of the virus samples in the test set. The products must provide on-demand and on-access scanning facilities, and the results of the tests of these must be the same.
- *Advanced level*. Here the products' virus detection and killing capabilities are examined using on-demand and on-access scanning. Products must meet all the conditions required for the Standard level and they must repair all of the infected objects, with the following conditions:
  - If, theoretically, it is possible to repair the whole original object correctly (bit by bit), then the repaired object must be identical to how it was prior to infection.
  - If it is not possible to repair the whole original object correctly (bit by bit), but it is (theoretically) possible to repair the object with minor changes and with the functionality of the repaired object restored to the same as it was prior to infection, then anti-virus products must repair the object in this way: the functionality of the repaired object must be the same as it was before infection.
  - In the case of macro viruses, the macros in a repaired document and the macros that were stored in the document prior to infection must be the same (in both name and content). After a notification to the user the anti-virus product may delete all of the macros from the infected document.
  - In the case of boot viruses, infected sectors must be the same after the killing procedure as they were before infection. Data stored in the boot sector (e.g. partition information) or in the master boot record may not be changed during the killing procedure. If it is not possible to restore the original master boot record then, after notifying the user, the anti-virus product may generate a standard master boot record.
- *Mailscanner*. In this case anti-virus products must provide an email scanning service. Both incoming and outgoing infected messages must be identified and anti-virus products must disinfect the email or block the corresponding traffic. This means that a user cannot send or receive infected email. The Mailscanner certification is independent of the Standard and Advanced levels of certification.

The virus test set used for certification is based on viruses published on the WildList prior to the test. At least 80 per cent of the set includes viruses that are published in the last three issues of the WildList. A maximum of 20 per cent of the set may include any virus published on any WildList. The list of viruses that will be included in the test set is published at the beginning of the month on the *CheckVir* website. The anti-virus developers then have about 10 days to upgrade their products before the deadline for product submission. This means that the certification procedure does not deal with the latest viruses.

CERTIFICATION RESULTS

In the first half of 2004 six certification procedures were carried out. Each month the certification process was executed on two platforms (client and server). In this case anti-virus developers submitted two products. The following table show the summary of the certification results:

AV developer	No. of products submitted	No. of Standard certifications	No. of Advanced certifications
Grisoft	7	7	-
Softwin SRL	7	6	-
ID Anti-Virus Lab	5	5	-
Computer Associates	7	2	5
F-Secure Ltd.	7	7	-
Kaspersky Lab.	7	7	-
Network Associates	7	7	-
Eset Software	7	7	-
Norman ASA	7	5	-
Panda Software	7	7	-
Trend Micro	7	1	6
VirusBuster Ltd	7	5	2
MicroWorld Technologies	2	-	2

The results of each certification procedure are published on the *CheckVir* website, http://www.checkvir.com/, in the month following the testing process.

The CheckVir anti-virus testing service is free for the first test of any AV company. More information can be found at http://www.checkvir.com/.