Antivirus Antiperformance

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Nothing is free – that observation is sometimes known as the second law of thermodynamics and sometimes referred to as TANSTAAFL (or TINSTAAFL) for "There ain't (is) no such thing as a free lunch."

As some readers know, I have a very inclusive sense of the scope of "information security." Using the Parkerian Hexad, security specialists say that we are concerned with protecting six fundamental attributes of information: confidentiality, possession or control, integrity, authenticity, availability and utility (for details, see "What's Important for Information Security: A Manager's Guide" on my Web site in HTML or PDF on page < http://www.mekabay.com/infosecmgmt/index.htm >. Today I want to point out a quirk about using antivirus programs when you need high performance from your computer.

From 1980 to 1990, I earned my living in operations management; I was a performance specialist for Hewlett-Packard and specialized in operating-systems internals, database design and internals, and performance optimization. One of the principles of computer performance analysis is that there are only four contributions to program performance beyond application program design: access to and speed of the
1) processor
2) memory
3) disk operations;
4) network operations.

Now, I run an excellent antivirus on my main system and on my portable, which I keep synchronized so I can work either at my home office or away at the University or on trips. The operation, using LapLink, takes only a few minutes to synchronize over 18,000 files. A friend of mine was watching as I started the operation and asked me why I disabled my antivirus (AV) on both systems while synchronizing. I explained that the AV, although immensely useful when handling files coming in from outside the systems, is not necessary when transferring between two computers both of which are protected by the same program. "But what difference does it make?" asked my friend. Well, it turns out that the AV is consulted on every file-open operation; even if the file-type is not scanned, there's a momentary pause in the input-output (I/O) that does not matter if you're only doing a few operations – e.g., opening a file and then working on it with your word processor. But if you intend to check thousands of file, each additional fraction of a second can add up to cause significant differences in the time required to complete the job. The difference in the file synchronization is about three-fold faster without the AV.

Similarly, if a process opens the same file(s) over and over, using an AV can contribute enough delay that you can see the results yourself. For example, I have an e-mail client that can rebuild its database to clean out purged items or correct bad pointers and index values. While it is doing so, it repeatedly opens and closes the same files. While preparing this article, I timed the rebuild operation on a small database and found that with the AV operational, the build took 25 seconds;

without the AV, the same operation took 7 seconds. Does it matter for such a small database? No. Could it matter with a larger one? Quite likely. Nobody minds 25 seconds instead of 7 seconds, but one might get offended at 25 minutes instead of 7 minutes. And anyway – the definition of "availability" is a function of habit. I like 7 seconds and become impatient with 25 for this operation; for other operations, I might be happy with 25 and impatient with 75 seconds.

On that topic, I recall that when programmers used to put their new database programs into production with a test group of half a dozen data-input clerks, I urged them to insert a timer in the program to ensure that response time was not _faster_ than the service-level agreement stipulated. The point was that clerks who got used to quarter-second response time might be offended at 2.5 second response, even though the contract stipulated that acceptable performance under load was to be quicker than 5 seconds per transaction. Setting reasonable expectations was much simpler than trying to recover from disappointment.

So let's remember TANSTAAFL: running an AV is necessary and useful, but there may be times when a skilled user will choose to disable the AV while doing I/O-intensive operations.

Just remember to re-enable the AV before you leave your computer.

* * *

Look for the _Computer Security Handbook, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon at: < http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e >

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@compuserve.com >; Web site at < http://www.mekabay.com/index.htm >.