Information Security (TDDC03) Project

Spring 2007

Security and Usability of Anti-Virus Software

Mati-ur-Rehman Khan & Muhammad Hassan Abbas

Supervisor: Almut Herzog

Security and Usability of Anti-Virus Software

Mati-ur-Rehman Khan, Muhammad Hassan Abbas
Dept. of Computer and Information Science
Linköping University
Linköping, Sweden
{matkh777,muhab879}@student.liu.se

Abstract

In this comparison study we have evaluated the security and usability of four types of anti-virus software by installing them on a PC and evaluating them to a security and usability test. We downloaded four different anti-virus software products, two of them are freeware and two are evaluation versions of commercial products. We have tested these with respect to three criteria that we chose ourselves. Our conclusion is that the security and usability of anti-virus software is judged on how it updates its virus databases and program updates.Also how promptly it provides user with clear alerts of what needs to be performed or had performed to ensure the security of system. All of them have some flaws, both in usability and security.

1. Introduction

Security of a computer system is an important consideration. It is a critical issue for home users and companies while deciding which product should be used to prevent systems from Trojans, viruses and malwares. In the market, anti-virus products are available by many vendors, broadly divided into two main categories i.e. freeware anti-virus products or commercial anti-virus products. All anti-virus software almost performs the same functionality, so the decision may be driven by recommendations, particular features, availability, or price [2]. In this project we study four anti-virus products and evaluate them according to usability and security criteria. The four anti-virus products that we evaluate are:

1. Norton Anti-virus 2007 by Symantec Corporation.[3]
2. McAfee Virus Scan Plus 2007 by Network Associates.[4]
3. AVG Anti-virus Free Edition 7.5.467. by Grisoft.[6]
4. Avast Anti-virus Home Edition 4.7.942 by Alwil Software. [5]

2. Methodology

2.1 Selection Criteria

We decided to use these products because the article “Who's Who in Anti-virus Software” by Andy Patrizio dated August 2, 2006 [1] says that Symantec has 54 % market share and its next competitor is McAfee with 19 %. So we decided to evaluate these two commercial top market shareholders and two freeware products.

In our study the first two described products are commercial and the last two are freeware. The reason for choosing products from commercial and free environment will help to judge whether freeware software is more usable or secure then commercial product or not.

3. How we evaluated

The evaluations were performed on a Pentium III 450 MHz PC with 512 MB RAM. The operating system of the test computer was Windows XP Professional, with Service Pack 2. We installed anti-virus software one by one to test our criteria on the system.

4. Evaluation Criteria

The criteria we choose to evaluate these products are:

1. Update Procedure of anti-virus software: For : For anti-virus software it is of utmost importance that virus definitions are up to date and that software vulnerabilities of the anti-virus software

are remedied as soon as possible. Therefore we evaluate the update procedure of anti-virus software

2. Performance of each product while performing system scan and memory usage: For anti-virus software scan time is important after installing the anti-virus the user will always scan the system for virus removal. In that case, usage of memory resources and scanning time is important. If anti-virus consumes a lot of memory then it will create problem for the user to do multiple tasks at the same time.

3. Evaluation of Product response by probing a virus into the system to judge the behavior of anti-virus software. Because it is of utmost importance how anti-virus responds to a virus attack.

We used a test file that has been provided by EICAR (European Institute for Computer Anti-virus Research) [7] for distribution as the [EICAR Standard Anti-Virus Test File]. It is safe to pass around this file because it is not a virus, and does not include any fragments of viral code. Most products react to it as if it was a virus though they typically report it with an obvious name, such as "EICAR-AV-Test". We opened this file using Web Browser to view the results of each anti-virus product.

5. What we evaluated

5.1. Installation

5.1.1. Norton Anti-virus

One can install Norton Anti-virus by double-clicking on the downloaded copy of Norton Anti-virus. It takes about 12-15 minutes to install it. It runs a pre-install scan on the system to check the system condition. At the end of installation process it asks for Live Update of the program and virus definitions. Norton requires a system restart after installation.

5.1.2. McAfee Anti-virus

One can install McAfee Anti-virus by double-clicking on the downloaded copy of McAfee Anti-virus Product. It takes about 14-16 minutes to install it. It runs a pre-install scan on the system to check the system condition. At the end of installation process it checks for product and virus updates to update the product. It needs a system restart after installing the product.

5.1.3. AVG Anti-virus

One can install AVG Anti-virus by double-clicking on the downloaded copy of AVG Free Anti-virus Product. It takes about 5-6 minutes to install it. It has the option of doing scanning whole system, with the option of low memory or high memory usage selection. At the end of installation process it checks for updates to update the product. It does not need a system restart after installing the product.

5.1.4. Avast Anti-virus

One can install Avast Anti-virus by double-clicking on the downloaded copy of Avast Anti-virus Product. It takes about 4-6 minutes to install it. It asks for setting up a boot time scan on the system to check the system condition. It needs a system restart after installing the product.

5.2. Program and Virus Definitions Updates

5.2.1. Norton Anti-virus

The first definition update is done right after the installation. After that Norton has the option to allow Automatic Live Update. By default it is turned on. One can configure Live Update in the settings. System needs to be restarted after the updates.

5.2.2. McAfee Anti-virus

Virus definition update is done after the installation. In the later run you can right click on the system try icon of McAfee Anti-virus and click on the updates or you can go to Security center and click on the update option. It automatically checks for available updates about virus definitions and program updates. An icon is shown in the system tray about the progress. Updates requires a system restart.

5.2.3. AVG Anti-virus

First update of virus definitions is done at the end of installation. In the later run you can right click on the system try icon of AVG Anti-virus and click on the check for updates or you can go to control center and click on the check for update option. It automatically checks for available updates about virus definitions and program updates. A window is opened showing the information about the updates. System does not needs to be restarted after the updates.

5.2.4. Avast Anti-virus

Avast does all the program and virus updates automatically. One can also configure updates manually. One can right click on the system try icon of Avast Anti-virus and in the updating section one can perform program updates or virus definition updates. A popup is shown with sound option when an update is done and system restart is required.

5.3. Performance of System Scan and Memory Usage

The performance of a virus scan was evaluated on the same size of data for each product. The data size according to Windows XP Folder Properties was 3.00 GB, consisting of 7,146 files and 622 folders.

5.3.1. Norton Anti-virus

The results we got after the Norton anti-virus performs custom scan on the system shows that it has performed scan in 17 minutes on 19336 files and folders. It does not show any clock measurements, so we estimate it using the system clock. We can choose any folder or drive for custom scanning purpose.

The results for memory usage, taken from the Windows task manager during the above scanning process, show that Norton anti-virus consumes around 12,000 K to 13,832 K memory. It also has the option to run the scan in background. In that case memory usage is extremely low i.e. 3,428 K.

5.3.2. McAfee Anti-virus

To perform a custom scan using McAfee anti-virus is a difficult task. It only allows system created folders like My Documents etc. to have the option of custom scan or particulate drives like C:/ or D:/. It took 25 minutes to perform scan on the data. It automatically scanned 30 processes and 252 cookies also. And the scan results show that it scanned 7179 files in all. It does not show any duration measurements, so we have to calculate it manually checking the starting time and subtracting it by using the last scan time shown by McAfee.

The results for memory usage, from task manager during the above scanning process show that McAfee anti-virus consumes between 30,000 K to 35,000 K memory. It has different spikes of memory usage between these two limits. It is experienced that McAfee has many ups and downs between these memory limits during the whole process.

	Norton	McAfee	AVG	Avast
Time for Scan (Minutes: seconds)	17	25	9:33	24:43

Table1: Time for Scan by Anti-virus

5.3.3. AVG Anti-virus

You can perform a custom scan easily even on a single directory. It took 9 minutes and 33 seconds to perform scan on the data. And the results show that it scanned 15759 objects in all. Scan summary shows duration measurements.

The results for memory usage, from task manager during the above scanning process show that AVG anti-virus consumes around 10,000 K to 29,000 K memory. It has different spikes of memory usage between these two limits. It is experienced that AVG has noticeable ups and downs spikes between these memory limits. In the start it was rather low like 10,000 K to 13,000 K. Then in the middle and end of the scanning process it was 25,000-27,000 K. Also at the end it was stable to 29,000 K.

	Norton	McAfee	AVG	Avast
Memory Usage (K)	12,000K - 13,832K	30,000K - 35000K	10,000K - 29,000K	35,000K - 40,000K

Table2: Memory Usage by Anti-virus

5.3.4. Avast Anti-virus

You can perform a custom scan easily even on a single directory. It took 24 minutes and 43 seconds to perform scan on the data. And the results show that it scanned 21642 files and 623 folders which is 3.7 GB of data. Scan summary shows duration measurements.

The results for memory usage, from task manager during the above scanning process show that Avast anti-virus consumes around 35,000 K to 37,000 K memory. It has different spikes of memory usage to 40,000 K. But mostly

it usage was shown between 35,000 K to 37,000 K.

5.4. Virus Probe Test

The virus probe was avalaible in four different file formats i.e. as a DOS exe file, as text file, a zip file containing that DOS exe file, and a zip file containing another zip file with DOS exe file.

5.4.1. Norton Anti-virus

Norton blocks the DOS file in exe and text format and quarantines them, but for the zip files Norton did not respond at its access. We were able to download and open the zip file. But as we run this DOS file, it prompts for action and automatically blocks the content and quarantines this file.

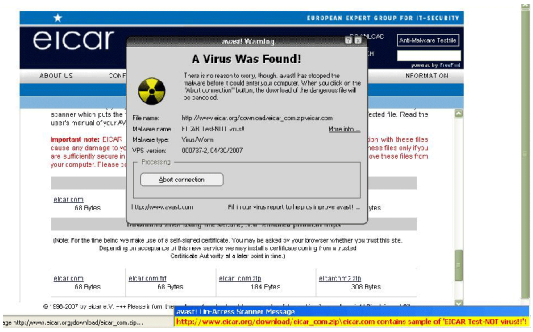

Figure1: Avast Anti-virus alert for virus

5.4.2. McAfee Anti-virus

McAfee did not allow the DOS file access in exe and text format. It blocks it and quarantine it in the Temporary Internet files.

For the zip files McAfee didn't respond at its access. We were able to download and open the zip file. But as we run this DOS file, it prompts for action and automatically blocks the content and quarantines this file.

5.4.3. AVG Anti-virus

For the first format AVG stops the user from downloading this file and prompts for action to abort the connection.

For the second format AVG anti-virus didn't detect this file as a virus at all.

For the zip files AVG didn't show alert at its access. We were able to download and open the zip file. But as we run this DOS file, it gives you a warning and gives you options to deal with the file.

5.4.4. Avast Anti-virus

For the DOS exe and text format Avast On-access Scanner automatically detects the contents as virus and ask you to abort the connection as shown in figure 1.

In case of zip files when we click it we were not able to download it. As soon as the browser tries to store it in the Temporary Internet files Avast On-access Scanner automatically detects the contents as virus and ask you to abort the connection.

6. Conclusions

Anti-virus software shows different results in different scenarios. Some performed better in memory usage, some outclassed others in time to scan system and some gave good results in founding the viruses.

6.1. Program and Virus Definition Updates

In these criteria every anti-virus performed same. Each of the four selected anti-viruses updated their virus definitions and program updates after the installation of the anti-virus. So there wasn't much difference in this regard. With the increasing virus threats on freshly installed systems it's becoming a routine for almost all anti-viruses to update their virus definitions and program updates. A positive surprise was AVG which does not require a restart after updating.

6.2. Performance of System Scan

The products' performance during a system scan was divided in two categories.

a. How much time does each product take to run a full scan on the same amount of data?

The data size according to Windows XP Folder Properties was 3.00 GB, which contains 7,146 files and 622 folders. Here AVG performed best

by scanning the system in 9 minutes and 33 seconds and the Norton scanned the system in 17 minutes. McAfee and Avast took almost the same time to scan i.e. 25 minutes. Apart from this Norton showed a very interesting result, that it displayed different number of files and folders scanned. It showed 19336 where as total files or folders were 7768. Also, Avast showed in its system scan screen, that it scanned 3.7GB of data where as data on the disk by Windows Folder Properties was 3 GB.

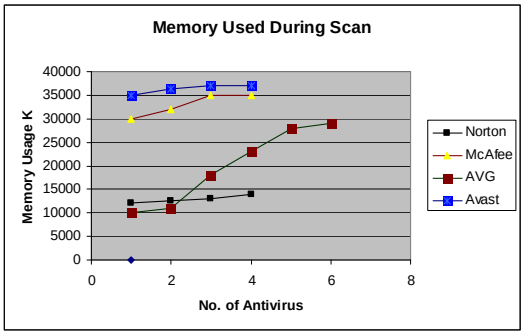

Figure2: Memory Used by Anti-virus

In one of the good point of the free-ware anti-viruses (AVG and Avast) is that they have a system clock built in which tells the time taken to scan the system while this feature was absent in McAfee and Norton.

b. How much RAM (Read only Memory) is used during scanning process.

Norton performed best in this case by utilizing minimum amount memory and then there were only minor differences in the rest of the anti-viruses. One of the important or a positive aspect of Norton was that it allows anti-virus to run in the background and thus giving user freedom to do other work at the same time.

So by observing the time consumed and memory usage Norton performed better then other and then AVG showed us good results also. There wasn't much difference in McAfee and Avast.

6.3. Virus Probe Test

Norton, McAfee, AVG and Avast were able to find virus activity on the first file formats described above. Norton, McAfee and Avast were able to find the virus activity on the second mentioned test virus format, but AVG didn't considered it as a virus and allowed simple execution of the file. For the third and fourth zip format of the test virus, Norton, McAfee and AVG were not able to identify it until it is downloaded and executed on the system. But Avast on the other hand discovered it as a virus and didn't allow the connection to move forward. These results show that Avast was the most useful anti-virus to successfully able to identify test virus in all four formats. Norton and McAfee are at the same level as they both identify the first two file format viruses, but they don't do a deep on-access file scan. AVG was the worst as it was unable to identify one of the file formats test virus file.

6.4. Results

The main purpose of anti-virus is to find viruses at the right time; if it does not provide required results then the purpose of the anti-virus software is not fulfilled. So according to our finding we give the following results. Norton performed better in scanning system and in terms of memory usage and was also able to finding the viruses. Then Avast showed good results in finding the viruses but was bit lacking behind in terms of scanning and memory usage. McAfee gave average results in every aspect where as AVG performed poorly against the other anti-viruses. AVG was good in scanning the system but other than that it showed memory leaks and performed badly in finding the viruses.

6.5. Commercial vs. Freeware

Commercial software (Norton) performed better in less memory usage and finding viruses then Freeware (Avast and AVG) but the difference were surprisingly small. The decision of selecting a particular anti-virus lies in the hand of user.

7. References

[1] Andy Patrizio, Who's Who in Anti-virus Software?, August 2, 2006. http://www.internetnews.com/security/article.php/3623881

Accessed on March 12, 2007

[2] Mindi McDowell, Allen Householder; Copyright 2004 Carnegie Mellon University http://www.us-cert.gov/cas/tips/ST04-005.html

Accessed on March 20, 2007.

[3] Norton Anti-virus Webpage http://www.norton.com

[4] McAfee Anti-virus Webpage http://www.mcafee.com

[5] Avast Anti-virus Webpage http.//www.avast.com

[6] AVG Anti-virus http://www.grisoft.com

[7] European Institute for Computer Anti-virus Research. http://www.eicar.org/anti_virus_test_file.htm

Accessed on April 30, 2007.