The Design and Implementation of an Antivirus Software Advising System

Eugene Chamorro, Jianchao Han, Mohsen Beheshti
Department of Computer Science
California State University, Dominguez Hills
1000 E. Victoria Street, Carson, California, 90747, USA
echamorro@toromail.csudh.edu; jhan@csudh.edu; mbeheshti@csudh.edu

Abstract – **People use computers for all kind of activities: online gaming, shopping, entertainment, emails, facebook, study, research, etc. At the same time, the risk of infection by malicious programs in these computers is rising. The main issue is that general users don't understand what a virus is and how computers get infected. On the other hand, many vendors produce antivirus software with different features to prevent or remove these viruses from people's computers. General users don't understand the concept of each feature in these programs, nor is there a tool to advise users about what the features mean and help them select the right software for personal or business needs. The purpose of this paper is to create an advising system to assist general users to study about computer virus and antivirus, understand the various features of antivirus software products, and select right antivirus software to protect their computers.**

Key Words – viruses; security risks; malware; antivirus software; computer protection systems

I. Introduction

We're living in the age of technology and communications. Computers are part of our lives. We use them at home, school and work. Internet has spiked the usage of this technology since it is an open window for knowledge, entertainment, communication, e-business, etc. This technology also expanded to smart phones and tablet computers like iPods. Unfortunately, these devices (computers, smart phones, and iPods) are exposed to viruses and other malware, infecting computers with purpose of stealing personal and financial information, or tracking the users' move for commercial purposes. Antivirus software has been created to protect users from these attacks. Different vendors provide prevention and removal of malicious programs. The problem resides when the general user doesn't have the knowledge or skill to understand what a virus is and how it spreads. They don't know what program to select and buy to protect his or her device (s) or select among different features from these programs. This paper is to create a advising software program that will provide the users with the right knowledge and help them select the right tool to get them protected according to their business or personal needs.

This paper is organized as follows. Section II gives an overview to virus' history, definitions, methods of infections, types, and some algorithms used. Section III presents about what antivirus software is and the type of instruction detection they use. Section IV will be comparing the features of antivirus software provided by different vendors. Section V will describe our design and implementation of an advising software system to help users learn the knowledge about computer virus and antivirus software as well as help non-technical people choose between different antivirus software vendors according to their needs.

II. Computer Viruses Overview

A. Theory of Self-replication

To understand what a virus is and how it works, we need to go back on time and study one of the elements that use this technology, "self-replication". John von Neumann, one of the greatest computer architects who created the model/vision of computers we use today, also was the first to provide the model of self-replication. Neumann introduced the model of Cellular Automata as a formal model of self-reproducing biological systems. Peter Zsor, in his book of "The Art of Computer Virus Research and Defense", describes Neumann's vision on self-building automata. Using the main components such as a universal machine, a universal constructor and information on a tape, any universal machine can read the information on the tape and using the universal constructor replicate its code by creating a new machine [8]. In other words, the machine which has the available hardware (memory) can create a copy of itself by following a sequence of steps. Then it detaches itself to the newly created machine. Other scientist continued his work and this model was taken to other science.

B. How Does It Work?

P. Sarkar describes a model of Self-Reproducing Automata in [7], which can be applied to computer viruses. A virus needs a computer to exist. In other words as an automaton is a self-operating machine, a modern computer composed by BIOS, OS, programs and data is also a self-operating machine. A virus can replicate itself as explained in the self-replication model. Therefore, a computer virus is defined as a computer program that will infect (damage) or destroyed its host system and can copy itself and infect other computers in order to destroy or cause damage to other systems as well.

There are two classes of viruses: viruses that infect a computer deleting operating system file, killing the host computer before replicating or copying themselves to other systems. Other viruses, copy themselves to other programs and files stored in the host computer corrupting programs to perform in a certain way and then replicating themselves through storage devices, internet or email systems to other systems.

Some viruses are mild and causes error message to appear on the screen or opening a different files than the one

978-0-7695-4654-4/12 $26.00 © 2012 IEEE
DOI 10.1109/ITNG.2012.161

you are opening. Other viruses can cause the system to crash, deleting files (operating systems files or data files) or corrupting the data in the host computer. In summary, there are three main components in all viruses: a replication mechanism, a trigger and a task [9]. These components enable the virus to replicate itself and move from computer to computer executing a series of tasks to damage or destroy the system.

C. *Type of viruses*

Viruses can be classified in many ways. It depends on different variables such as the origin of the virus, technique used to infect, type of files they infect, the damage they cause, etc. Viruses may contain three characteristics: They replicate by making copies of themselves; they have a population growth with the overall change in the number of instances due to self-replication or they many need another executable code in order to exist [10]. The main type of viruses includes:

1. *Boot sector viruses* affect the boot sector of a hard drive. This also includes viruses infecting legacy devices such as the boot sector of floppy disks.
2. *Directory viruses* change the path where a file is located.
3. *Stealth viruses* are created to avoid detection by the antivirus software. Sometimes they hide in memory and keep a clean copy of the files they infect. In that way, when the antivirus search for that file, the virus will change the path to the location where the original file is kept preventing the antivirus software to detect the infected file. Sometimes new viruses are also described as stealth viruses.
4. *Macro Viruses* infects the macros within a document or template.
5. *Program viruses* contaminate files containing program files with a files extension such as .exe, .com, sys, .dll, and .ovl.
6. *Resident viruses* reside in RAM memory. They corrupt files as they are opened, closed, renamed, etc. interrupting all operation executed by the files.
7. *Multipartite viruses* are hybrid viruses of boot sector and program viruses [5]. They usually infect the boot sector in the hard disk with the data containing the instruction how the computer should start up. When the computer boots up, it spreads the virus around infecting all files.
8. *Polymorphic viruses* are capable of mutating themselves when they replicate, keeping the original algorithm. It is the virus that changes in which its code changes, but not its function. Therefore, it is harder to detect.
9. *File deleting viruses:* this type of virus is designed to delete certain type of files such as spreadsheet or word processors [9].
10. *Mass mailers:* This type of virus works within the e-mail programs targeting the user's address book. The virus sends itself to all individuals in the address book. Then it infects each of the individuals address books in the newly infected computer and the cycle starts over again.
11. *Parasitic virus:* This type of virus attaches itself to executable files and replicates, when the infected program is executed [14].

Other type of infections that are not considered as a virus, but they can damage the computer, including worms, Trojan horses, logic bombs, malware, spyware, adware, back doors, zombies, and rootkits [4, 8, 9, 12].

D. *File infection techniques*

There are many techniques that virus writers use in order to attach the virus to files. Here are some techniques:

1. *Overwriting viruses*

This technique is one of the most primitive techniques. It was used by most common viruses. The virus inserts its code into an area of the original file. This allows the virus to be executed whenever files are accessed. The program will work correctly when it is infected because part of its code has been replaced by the malicious code. For this reason, files infected by this virus cannot be disinfected. They have to be deleted. One variation of this technique was the Random Overwriting Viruses in which the code was inserted to a random location of the host program.

2. *Appending viruses*

In this technique the virus add itself at the end of a file. A jump instruction is inserted at the front of the file pointing to the location where the virus code is located. When the file is loaded to the memory, the jump instruction is executed and the virus is loaded to memory. This technique is fast since the virus needs to write its code at the end of the file. It uses a smaller buffer to load the host, operating with less memory. These viruses are known as parasitic viruses and spread very fast without being detected [8] because they maintain the original functionality of their host victim file.

3. *Prepending viruses*

In this technique the virus adds itself to the beginning of the file. This technique is much slower than the Appending technique. It is a more elegant technique and in most of the cases, the virus doesn't destroy the host program. Since different files have their own file structure, the virus must consider what file it will target first to keep its structure intact after it inserts itself. The virus code also stats with a jump instruction to give control to the virus code. High level programming languages such as C or Delphi are used for this technique.

4. *Companion viruses*

This technique is of non-destructive type. In this technique the malicious code replaces the name of the host files in a program with non-standard names and it makes a copy of itself with the standard-name of the original file. For instance, the virus can change the name of a file extension from COM to CON and then rename itself with COM extension. Then it can set its attributes to Hidden, Archive. In this way the control of the host program is transferred to itself when the user executes the program or calls the file.

5. *Interrupt 21H Hook*

This technique is used by non-memory resident parasitic virus copying itself to the interrupt Vectors table, hooking INT 21h and writing itself to the end of the Com files to be executed. There are a number of functions that the virus should do in order to be effective, includes file search functions, handle-based read functions, FCB-based read functions, and move file pointer functions [13].

III. ANTI-VIRUS SOFTWARE

Anti-virus software programs are programs created to prevent, detect and remove virus from computers. Most antivirus software programs include prevention and removal of malicious programs such as adware, spyware, worms, and Trojan horses to name a few. Antivirus software vendors include MacAfee, Norton, TrendMicro and others. They offer the same core features (for virus) and added features to remove other malicious programs. Antivirus software includes many strategies for detection, prevention and removal.

The main task done by ant-virus software is detection, to detect if a code is a virus code or not. This includes checking the codes of incoming emails from user's computer. This is the most important tasks; it may prevent the computer to get infected. Once the virus is detected, the next process is to identify what kind of virus it is and then cleaning or removing the detected virus.

A. Viruses Detection Techniques

There are different detection techniques used by antivirus software to detect viruses [6], which can be categorized into two main methods; static methods and dynamic methods. With static methods, the program tries to find viruses without running any code; while dynamic methods decide if the code is infected by running code or observing its behavior [11].

Static methods include scanners, heuristics and integrity checkers [11].

- *Scanners:* The basic idea is to look for string that is known to be part of virus [8]. Scanners technique can be divided in first, second, third and fourth-generation scanners [14]. Scanners can also be classified by the way they are invoked. This includes on-demand scanners when run by the users or on-access scanners when an on-access scanners runs continuously, scanning every file when it is accessed.
- Integrity checkers generate checkcodes and check the checksum of each program. Since a virus infects a program without changing its checksum, the integrity checkers will catch the change. If the comparison fails, something may have occurred and it will trigger more investigation.
- Heuristic analysis identify new and variants of known malware using heuristics.

Dynamic methods include behavior blockers, emulation, and rootkit detection.

- *Behavior blocking* (also known as script blocking or behavior monitor blocking) is a tool that monitors real time program's behavior in order to find any suspicious activity. It starts when the OS of the computer starts. If any suspicious activity is found, it then warns the user and blocks the activity.
- *Emulation:* In this technique the code is analyzed using an emulated environment in order to protect the computer if the virus runs itself [11]. The CPU is emulated first. The memory is emulated second keeping track of the memory used. Then the emulator copies parts of operating system to be emulated as well as certain part of hardware such as timers. The emulator controller decides when to stop the emulation and finally, the emulator can get extra data to be analyzed.
- *Rootkit* detection watching for any changes in the PC file system.

Other methods include ***cloud antivirus*** which involves the uses of multiple scan engine when documents are sent to a network cloud [3].

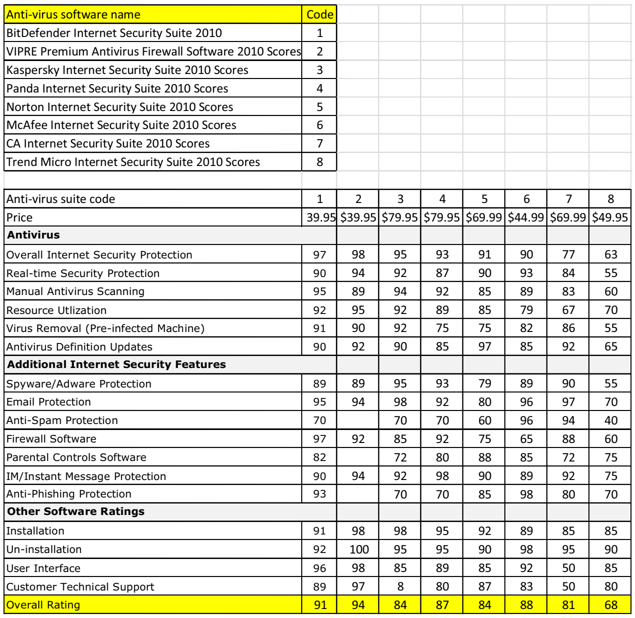
B. Anti-virus Software and utilities

Many anti-virus products are on the markets. Some of them offer other tools such as network firewall and specialty tools. *Network firewalls* are not antivirus software, but they protect computers from outsiders limiting or blocking some activities that may result in virus propagation on remote access. *Specialty tools* protect computers from adware, spyware, or any malicious programs.

In order to have the computer protected, antivirus software definition files needs to be updated daily since new viruses are unfortunately created every day. Live update is one of the features on all antivirus software. Anti-virus software products have some drawbacks. They might degrade computer performance since it is always running in the background to protect the computer. The degrade computer performance varies on the product and tools used by that product. Some products are more efficient and user friendly than others. Antivirus software alone is not the only means of protection for a computer. The computer needs to have the system patches up-to-date, especially if the user is using operating systems and products from Microsoft.

C. Anti-virus Software Comparison

The two charts illustrated in Figures 1 and 2 show two different ways of comparing different antivirus software vendors and the features that the antivirus software provides. Figure 1 shows eight internet security suites with antivirus software from different vendors, including BitDefender, VIPRE, Kaspersky, Panda, Norton, McAFee, CA, and Trend Micro. The data is excerpted from the PC Antivirus review [1]. These software are tested, evaluated, and rated against the following features in three categories. The first category of features is "core" features, including "*Overall Internet Security Protection*", "*Real-time Security Protection*", "*Manual Antivirus Scanning*", "*Resource Utilization*", “*Virus Removal (Pre-infected Machine)*”, and “*Antivirus Definition Updates*”. The second category is a set of internet security features, including “*Spyware/Adware Protection*”, “*Email Protection*”, “*Anti-spam Protection”*, “*Firewall Software*”, *“Parental Controls Software”, “IM/Instant Message Protection”,* and *“Anti-phishinig Protection”.* The third category of features includes *“time installation”, “uninstallation”, “User Interface”* and *“Customer Technical Support”.* The overall rating is listed at the bottom row.



Anti-virus software name	Code
BitDefender Internet Security Suite 2010	1
VIPRE Premium Antivirus Firewall Software 2010 Scores	2
Kaspersky Internet Security Suite 2010 Scores	3
Panda Internet Security Suite 2010 Scores	4
Norton Internet Security Suite 2010 Scores	5
McAfee Internet Security Suite 2010 Scores	6
CA Internet Security Suite 2010 Scores	7
Trend Micro Internet Security Suite 2010 Scores	8

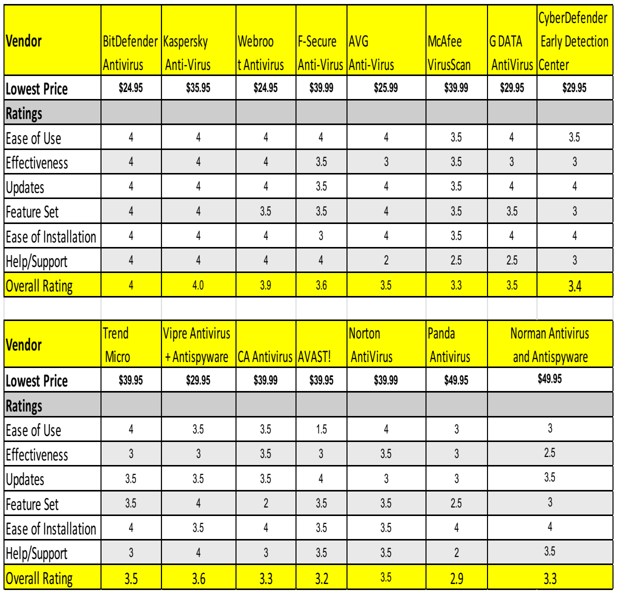
Anti-virus suite code	1	2	3	4	5	6	7	8
Price	39.95	$39.95	$79.95	$79.95	$69.99	$44.99	$69.99	$49.95
Antivirus								
Overall Internet Security Protection	97	98	95	93	91	90	77	63
Real-time Security Protection	90	94	92	87	90	93	84	55
Manual Antivirus Scanning	95	89	94	92	85	89	83	60
Resource Utlization	92	95	92	89	85	79	67	70
Virus Removal (Pre-infected Machine)	91	90	92	75	75	82	86	55
Antivirus Definition Updates	90	92	90	85	97	85	92	65
Additional Internet Security Features								
Spyware/Adware Protection	89	89	95	93	79	89	90	55
Email Protection	95	94	98	92	80	96	97	70
Anti-Spam Protection	70		70	70	60	96	94	40
Firewall Software	97	92	85	92	75	65	88	60
Parental Controls Software	82		72	80	88	85	72	75
IM/Instant Message Protection	90	94	92	98	90	89	92	75
Anti-Phishing Protection	93		70	70	85	98	80	70
Other Software Ratings								
Installation	91	98	98	95	92	89	85	85
Un-installation	92	100	95	95	90	98	95	90
User Interface	96	98	85	89	85	92	50	85
Customer Technical Support	89	97	8	80	87	83	50	80
Overall Rating	91	94	84	87	84	88	81	68

Figure 1. Chart comparing different versions

The PC magazine compares 16 antivirus software according to 6 features [2]: *Ease of Use, Effectiveness, Updates, Feature Set, Ease of Installation* and *Help/Support*. The 16 antivirus software include BitDefender Antivirus, Kaspersky Antivirus, Webroo Antivirus, F-Secure Antivirus, AVG Antivirus, McAfee VirusScan, GData Antivirus, CyberDefender Early Detection Center, Trend Micro, Vipre Antivirus+Antispyware, CA Antivirus, AVASTI, Norton Antivirus, Panda Antivirus, and Noman Antivirus and Antispyware. Each of these software is tested and scored against above 6 features, as shown in Figure 2.

IV. DESIGN AND IMPLEMENTATION

Given various antivirus software with different features and prices on the market, most computer users don’t know how to select and buy to protect his or her device (s) or select among different features from these software products. In order to provide the non-technical users with the right knowledge and help them select the right tool to get them protected according to their business or personal needs, we have created an antivirus software advising system to assist them to make decisions. This section will introduce the design and implementation of the advising system.



Vendor	BitDefender Antivirus	Kaspersky Anti-Virus	Webroo t Antivirus	F-Secure Anti-Virus	AVG Anti-Virus	McAfee VirusScan	G DATA AntiVirus	CyberDefender Early Detection Center
Lowest Price	$24.95	$35.95	$24.95	$39.99	$25.99	$39.99	$29.95	$29.95
Ratings								
Ease of Use	4	4	4	4	4	3.5	4	3.5
Effectiveness	4	4	4	3.5	3	3.5	3	3
Updates	4	4	4	3.5	4	3.5	4	4
Feature Set	4	4	3.5	3.5	4	3.5	3.5	3
Ease of Installation	4	4	4	3	4	3.5	4	4
Help/Support	4	4	4	4	2	2.5	2.5	3
Overall Rating	4	4.0	3.9	3.6	3.5	3.3	3.5	3.4

Vendor	Trend Micro	Vipre Antivirus + Antispyware	CA Antivirus	AVAST!	Norton AntiVirus	Panda Antivirus	Norman Antivirus and Antispyware
Lowest Price	$39.95	$29.95	$39.99	$39.95	$39.99	$49.95	$49.95
Ratings							
Ease of Use	4	3.5	3.5	1.5	4	3	3
Effectiveness	3	3	3.5	3	3.5	3	2.5
Updates	3.5	3.5	3.5	4	3	3	3.5
Feature Set	3.5	4	2	3.5	3.5	2.5	3
Ease of Installation	4	3.5	4	3.5	3.5	4	4
Help/Support	3	4	3	3.5	3.5	2	3.5
Overall Rating	3.5	3.6	3.3	3.2	3.5	2.9	3.3

Figure 2. Chart comparing different versions

A. *The Advising System Description*

The advising system is targeted to the audience without knowledge in antivirus software terminology and products. It can be used as a tool for personal use and business use by providing information on both domains. The system is to educate users about virus, antivirus, and antivirus software features. It helps users decide on what software vendor and product to choose in terms of their business or personal needs.

The system consists of three parts, which are represented as three use cases. The use case diagram about this advising system is shown in Figure 3.

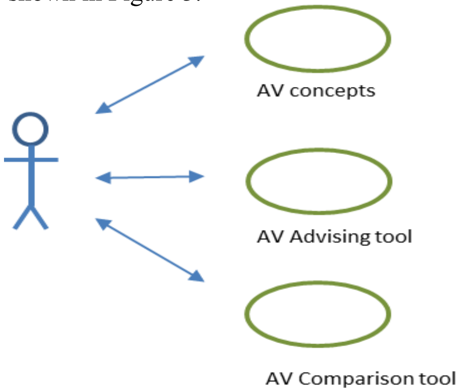


Figure 3. The use case diagram

The first use case “AV concepts” will display a web page describing all terms used by antivirus vendors. This will be used to show the general users about the meaning of these terms so he or she can get familiar with these concepts. The second use case “AV advising tool” represents the advising tool. This tool will let the user select from a series of question, the type of antivirus software he or she is looking for. It provides a list of vendors and the web links to these products according to the questions he or she answered. The third use case "AV Comparison tool" provides an interaction tool with which the user can select different vendors and compare the rating of all the antivirus software in the system according to some specific features. This helps the user understand what is the best product according to the rates provided by this tool. These rates are the results of tests performed by different third parties.

B. The Architectual Design

The advising system is designed as a web-based system with the three-tier architecture. The client tier is the user interface, which translates commands from the computer to the system and displays the results. The middle tier manages business logic and execution. Its main function is to process the commands using the business logic and coordinate the function between the other two layers. The database tier handles database management. Its main function is to store the data and retrieve the results of the query from the user. This architecture is illustrated in Figure 4.

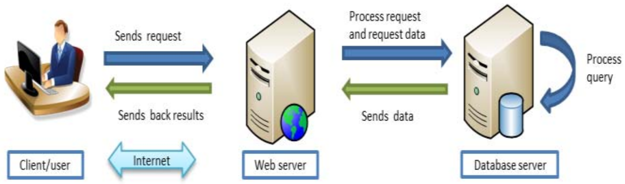
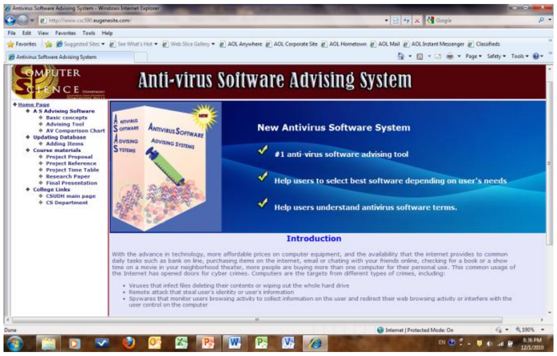


Figure 4. The advising system architecture

A web browser running on a client will send requests to a web server over the Internet. The web server will store web applications designed to run a web server, which contains business classes. The web serve processes the request, passes the request for data to the database server, and then responds the user's requests with the database retrieval.

C. The Interface Design

The system interface includes four parts. The main interface, shown in Figure 5, is the master page to display an index webpage giving general information on the system, describing the problem and solution that the system will solve.



Anti-virus Software Advising System

New Antivirus Software System

✓ #1 anti-virus software advising tool

✓ Help users to select best software depending on user's needs

✓ Help users understand antivirus software terms.

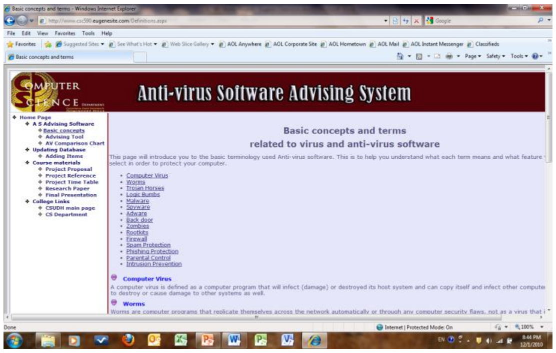
Introduction

With the advance in technology, more affordable prices on computer equipment, and the availability that the internet provides to common daily tasks such as bank on line, purchasing items on the internet, email or chating with your friends online, checking for a book or a show time on a movie in your neighborhood theater, more people are buying more than one computer for their personal use. This common usage of the Internet has opened doors for cyber crimes. Computers are the targets from different types of crimes, including:

- Viruses that infect files deleting their contents or wiping out the whole hard drive
- Remote attack that steal user's identity or user's information
- Spywares that monitor users browsing activity to collect information on the user and redirect their web browsing activity or interfere with the user control on the computer

Figure 5. The advising system main page

The basic concept web page will browse through the different terminology used by antivirus vendors. This page is corresponding to the "AV Concepts" use case and is shown in Figure 6.



Anti-virus Software Advising System

Basic concepts and terms
related to virus and anti-virus software

This page will introduce you to the basic terminology used Anti-virus software. This is to help you understand what each term means and what feature select in order to protect your computer.

- Computer Virus
- Worms
- Trojan Horses
- Logic Bumbs
- Malware
- Spyware
- Adware
- Back door
- Zombies
- Rootkits
- Firewall
- Spam Protection
- Phishing Protection
- Parental Control
- Intrusion Prevention

Computer Virus

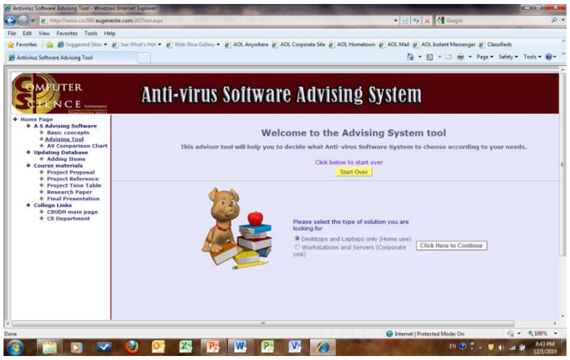
A computer virus is defined as a computer program that will infect (damage) or destroyed its host system and can copy itself and infect other compute to destroy or cause damage to other systems as well.

Worms

Worms are computer programs that replicate themselves across the network automatically or through any computer security flaws, not as a virus that i

Figure 6. The basic concept web page

The "AV Advising tool" use case is implemented as a sequence of interactions, which will be discussed next subsection. The enterance page to advising is shown in Figure 7.



Anti-virus Software Advising System

Welcome to the Advising System tool

This advisor tool will help you to decide what Anti-virus Software System to choose according to your needs.

Click below to start over

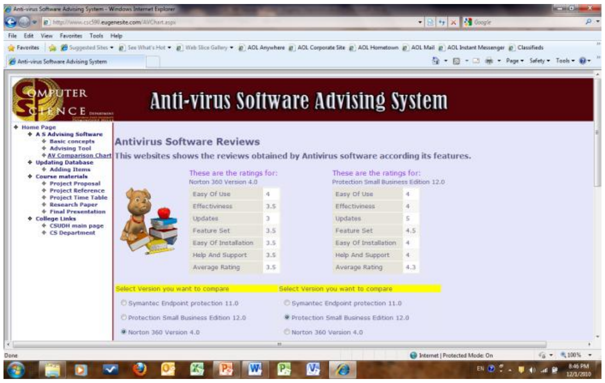
Please select the type of solution you are looking for

● Desktops and Laptops only (Home use)

○ Workstations and Servers (Corporate use)

Figure 7. The advising page

The antivirus software comparison chart webpage is comparing the features of various antivirus software products in terms of the users' requests, which is shown in Figure 8.



Anti-virus Software Advising System

Antivirus Software Reviews

This websites shows the reviews obtained by Antivirus software according its features.

These are the ratings for:
Norton 360 Version 4.0

Easy Of Use	4
Effectiviness	3.5
Updates	3
Feature Set	3.5
Easy Of Installation	3.5
Help And Support	3.5
Average Rating	3.5

These are the ratings for:
Protection Small Business Edition 12.0

Easy Of Use	4
Effectiviness	4
Updates	5
Feature Set	4.5
Easy Of Installation	4
Help And Support	4
Average Rating	4.3

Select Version you want to compare

○ Symantec Endpoint protection 11.0

○ Protection Small Business Edition 12.0

● Norton 360 Version 4.0

Select Version you want to compare

○ Symantec Endpoint protection 11.0

● Protection Small Business Edition 12.0

○ Norton 360 Version 4.0

Figure 8. The antivirus comparison

D. Advising Process

The advising process is a decision-making process, where the user will have to go through a series of questions in order for the system to understand the user's needs and provide for a solution. The questions include "free or non-free software", "business or personal use", "which operating systems", and various "features". The decision tree in Figure 9 depicts of a part of this interaction process.

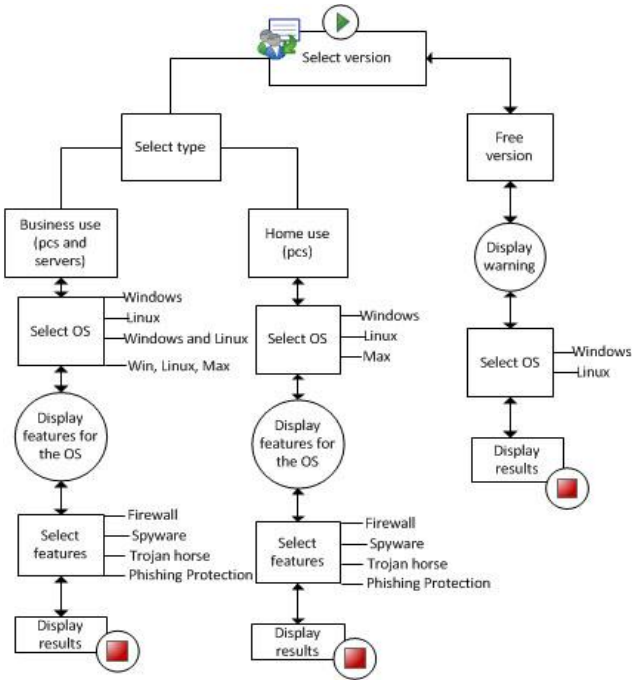


Figure 9. The advising process

V. Conclusion and Future Work

The theory of self-replications is a good start to understand how the virus replication works. A machine with available memory can create a copy of itself by following a sequence of steps. This is the principle a virus infects computers after computers. Nowadays viruses can infect a cell phone, a blackberry or any system that has hardware (memory) and files (set of instructions). New viruses are also created for operating systems that were virus free such as Linux and Apple OS X. On the other hand, antivirus software has also been developed. Many companies specialize in developing software to protect computers from infections for a specific domain such as virus only. Other vendors offer more protection by adding more features to the core protection. The problem resides when people don't understand the concepts behind viruses and antivirus software. They might get lost trying to figure out what is best for their computers in order to protect their assets.

This paper overviewed the virus replication automaton, virus generation techniques, and various types of viruses. The antivirus techniques are surveyed, the antivirus software features are discussed, and the antivirus software products are compared according to different features. In order to help people understand the concepts of virus and antivirus and assist them to make a right decision when selecting the best choice of antivirus software vendor and product in terms of their needs, an antivirus software advising system was developed. The system requirement is described, the system architecture is presented, the user interface is illustrated, and the advising process is also shown.

The more antivirus software products and more features of these products will be added to the advising database of the system presented in this paper. The advising process will be enhanced by integrating knowledge base and inference rules into the advising system. The interpretation of advising process to the user will be also introduced. These will be our future work.

Acknowledgment

This paper is based on work supported by the Department of Homeland Security under the auspices of the Southeastern Regional Visualization and Analytics Center, Cooperative Agreement No. 2009-ST-061-CI0001, and National Science Foundation (NSF) through grant CNS-05040538, and CNS-1104278. Any opinions, findings, and conclusions or recommendations expressed in the paper are those of the authors only.

References

[1] Antivirus Software Reviews http://www.anti-virus-software-review.com/

[2] Antivirus Software http://www.antivirus-software.com/

[3] Anti-virus software: http://en.wikipedia.org/wiki/Antivirus_software#cite_note-zsecurity.com-18

[4] Different type of computer viruses http://www.buzzle.com/articles/different-types-of-computer-viruses.html

[5] Computer Viruses: The type of viruses out there http://www.spamlaws.com/virus-types.html

[6] Computer Virus Detection Techniques http://www.ehow.com/list_7258284_computer-virus-detection-techniques.html

[7] Palash Sarkar, A Brief History of Cellular Automata, ACM Computing Surveys 22(1):81-107, March, 2000.

[8] Peter Zsor, The art of computer virus research and defense, Addison-Wesley, Maryland, USA, 2005.

[9] Michael Erbschloe., Trojams, Worms, and Spyware, Butterworth–Heinemann publications. Oxford, UK, 2005

[10] Roger Grimes, O'Reilly Malicious Mobil Code Virus Protection for Windows, O'Reily and Associates, California, USA, 2001.

[11] John Aycock, Computer Virus and Malware, Springer Science+Business Media, LLC. Calgary, Canada, 2006.

[12] Cameron H. Malin, Eoghan Casey, James M. Aquilina, Malware Forensics: Investigating and Analyzing Malicious Code, Spi Publishing Services, Burlington, USA, 2008.

[13] Mark A Ludwig, The Giant Black Book of Computer Viruses, American Eagle Publication, Arizona, USA, 1995.

[14] William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Inc., New Jersey, USA, 1999.