Literature review: methods of virus protection essay

Computer viruses are most critical area in computer science. All computer users in the world are suffering from this threat. Viruses reproduce themselves and spread through computer to computer as well as network to network. There are some antivirus software and some best practices to prevent from computer viruses. As well as this literature review contains the present situation of computer viruses, protection from computer viruses and how new antivirus software performs on computer viruses.

end{abstract}

section{Introduction}

“ The only secure computer is one that’s unplugged, locked in a safe and buried 20 feet under the ground in a secret locationA? A? A, A? A, A?”

Dennis Huges, FBI

begin{sloppypar}

end{sloppypar}

The above statement shows the current security situation of computers and the role computer viruses play in computer world.

begin{sloppypar}

end{sloppypar}

Computer virus is a program that can execute itself with the help of another infected executable program without knowledge of computer user and infect to computer. Viruses usually copy itself in current host and another new host

also. So generally viruses are infecting to executable files. Some kinds of viruses only reproduce itself within the current host and from the current host to another host and spread in the host. Those are harmless than viruses that damage to the computer program, activities and data in the computer.

begin{sloppypar}

end{sloppypar}

But there are some other malicious software other than the viruses. Those are called malware. These malicious software can spread without help of executable program.

begin{sloppypar}

end{sloppypar}

Computer viruses are also computer programs. So anyone who has a personal computer can create a virus program with few lines of codes. This means birth places of viruses are widely available. Also a virus is activated in host computer; the infection can spread through network (LAN or Internet) to other computers.

begin{sloppypar}

end{sloppypar}

Virus attaches itself to other program and spreads with them. Most of the time virus attaches to executable program, when the infected executable program is running then virus is also executing behind that process. Also

computer viruses can infiltrate to operating system. So all operating systems like MS Windows, PC Dos, Unix and Macintosh OS have probability to infect with viruses.

begin{sloppypar}

end{sloppypar}

Some viruses do some destruction as soon as they enter a system. But some of others are programmed to lie dormant until activate by some signal. The signal may be mouse click, specific date, time or specific common sequence of keystrokes. As an example the famous Michelangelo virus, it is set to activate his birthday March 6.

begin{sloppypar}

end{sloppypar}

Protecting the computers from the malicious software is the most challenging thing. But there are many ways to protect the computers from computer viruses. Although there are lots of methods to protect the computers from viruses, the computer users also have a responsibility to protect the computers from computer viruses. From the next section of review is considered about different types of Malware. cite{1}

newpage

section{Different types of Malware}

There are different types of Malware spread in computer world. But it can mainly identified as follow.

begin{itemize}

item Viruses

item Worms

item Trojan Horses

item Logic Bomb

end{itemize}

begin{figure}[h]

par

includegraphics[bb = 0 0 100 325]{virus. png}

caption{Malware Growth by Year} cite{10}

par

end{figure}

newpage

subsection{Viruses}

Virus is block of executable code that is attached itself to another executable program by attaching external code, overwriting or replacing of the

executable program code. When the computer user execute the infected program the automatically activate virus also by executing the hide block of code. This is the way how virus is infected to computer without knowing of user. But viruses get help from computer user to propagate in his machine.

begin{sloppypar}

end{sloppypar}

There are several types of viruses; they are categorized into various categories according to the way how they infect to system and what part of system is. Figure1 shows how Malware growth with year. It clearly show increase of Malware in year by year. cite{1, 5}

begin{itemize}

item Boot sector viruses

item Macro viruses

item File infecting viruses

item Polymorphic viruses

item Stealth viruses

item Multi-partite viruses

item Resident viruses

item Companion viruses

item FAT viruses

end{itemize}

subsubsection{Boot sector viruses}

Boot sector viruses are infected to the boot sector of computer otherwise master boot record of computer. Boot sector viruses are very difficult to detect because the master boot sector is the first thing loaded when computer started. So if this virus effect to computer, the virus get fully control of the machine.

begin{sloppypar}

end{sloppypar}

When boot sector virus infect to computer, they first move or replace the original boot code with infected boot code. Then the original boot code move to another sector of on disk and labeled that part as bad sector. So it will not use in future. The important thing is 75 per cent of viruses attacks are reported from boot sector viruses. The main and only way computer can infected with this virus is boot computer using infected disk. So some modern anti-virus software is designed to check infected disk, when boot using disk and before boot strap is loaded. cite{1, 2}

subsubsection{Macro viruses}

In computing macro virus is virus that is crated using macro language. Macro language built into software such as word processor. So macro viruses

propagate with applications which are used macros. In most of the time macro viruses infected with MS Office Word,

MS Office Excel. However many of windows applications have to potential infected macro viruses too.

begin{sloppypar}

end{sloppypar}

Because some applications allow macro program to be embedded in documents. So when the document is opening the macro run automatically. Also macro viruses spread rapidly because of peoples share data, documents and also use internet to get data and email document. Therefore Microsoft suggests opening file without macros or user can verify there is no damage macro with the document. But these methods are also not worked at all macro viruses. cite{2, 3}

subsubsection{File infecting viruses }

File infecting viruses are infected to flies, and sometime they are allocated memory of computer. Files infecting viruses are infected with executable files, but most of the time it infect to executable files with extensions . COM, . EXE and . OVL.

begin{sloppypar}

end{sloppypar}

Consider with boot sector viruses these are easy to detect. If the file infecting virus infects to some document, usually it increases the size of the file. Therefore Anti-virus software can detect those viruses using that feature. cite{1}

subsubsection{Polymorphic viruses}

Polymorphic viruses are change there appearance in each time when it infect to computer. So it is very difficult to detect theses type of viruses.

begin{sloppypar}

end{sloppypar}

Polymorphic viruses also block of programming code, so they are encrypting there code using different algorithms every time they attack to system. Some polymorphic viruses can assume over two billion different guises. Therefore anti-virus software should make with good algorithmic scanning techniques instead of simple string based scanning techniques. cite{1, 4}

subsubsection{Stealth viruses}

Stealth virus is a virus that hides its track after infecting to system. These types of viruses also try to hide from operating system and Anti-virus software. Therefore stealth viruses always stay in memory then they can intercept all attempts to use the operating system.

Therefore these viruses waste memory available for user and hide it form both user and Anti-virus software. It hides changes it creates to files, directory structure and operating system also.

begin{sloppypar}

end{sloppypar}

When detected theses type of viruses using Anti-viruses software, then first it should disable the virus before correct the memory location in memory because stealth viruses also stay in memory. cite{1, 6}

subsubsection{Multi-partite viruses}

Multi-partite viruses infect both boot sector and executable program. Therefore this type of virus very difficulty detected. cite{1}

subsubsection{Resident viruses}

Permanent viruses reside in the RAM. cite{7}

subsubsection{Companion viruses}

These are working like resident viruses or direct action viruses.

subsubsection{FAT viruses}

These infect to the file allocation table.

subsection{Worms}

Worms is a self-replicating computer malware type. It spread copy of itself to other host using computer network. Worms different than viruses how the reproduce and spread. It was known viruses want host program or boot sector to activate it need file transfer (infected file) to another computer to spread to it. But worms did not want any host files to execute and they can execute independently and spread using network. Therefore they normally find addresses to propagate and they pick addresses in three ways,

begin{itemize}

item Randomly generate addresses

item Find addresses in system tables

item Find addresses in a program

end{itemize}

begin{sloppypar}

end{sloppypar}

The threat of worms is equivalent to that of viruses. Computer worms can damage and destroyed some important files and it can crash critical programs to stop working sometime. The very prominent examples of worms are the MS-Blaster and Sasser worms. cite{1, 2, 8}

subsection{Trojan horses}

Trojan horses are distractive programs that hide in some valuable and useful software in internet. Some time worms and viruses hide within Trojan horses. The different between virus an Trojan hours is Trojan did not spread itself.

begin{sloppypar}

end{sloppypar}

Normally Trojan hours spread into two parts those are client side and server side. When the client Trojan executes in computer the server the attacker otherwise server can get high level control of the client computer.

begin{sloppypar}

end{sloppypar}

The Trojan hours spread in several ways, most of the time with infected e-mail attachment. Also virus developers use some chat program like Yahoo messenger, Skype to spread these Trojans.

begin{sloppypar}

end{sloppypar}

Commonly there are several types of Trojan horses like remote access Trojan, password sending Trojan, key loggers, destructive Trojan, FTP Trojan and proxy Trojan. cite{1, 9}

subsection{Logic bomb}

The logic bomb virus is a piece of code that are inputted into a software system. When a certain and specific condition is met, such as clicking on an internet browser or opening a particular file, the logic bomb virus is set off. Many programmers set the malicious virus off during days such as April Fools Day or Friday the 13th. When the virus is activated, then various activities will take place. For example, files are permanently deleted. cite{1, 10}

newpage

section{How viruses spread}

Virus is one kind of malicious software which does some kind of harm to the activities of the computer. They always need a host program or any executable program to be executed its code. As viruses cannot execute its code by itself, the virus has to get the help of another file. Because of this reason, the viruses can effect only to several kinds of files such as html files with JavaScript, word documents and spread sheets. As the files with the extension ‘. gif’, ‘. jpg’,’. wav’,’. mp3? files considered as pure data files, a virus cannot do a harm to these files.

begin{sloppypar}

end{sloppypar}

What the viruses do to spread is copying its code to another executable file. Then when that executable file is executed by another person the code of the virus is also executing and it then starts to search for files it can reside in the same computer or in the other computer which has been connected to the computer. Then the newly attacked programs are also trying to search

for files which it can attack. If the infected file sends to another computer by a removable media, the computer virus infects to that computer too.

begin{sloppypar}

end{sloppypar}

There are number of ways which a virus can enter into a computer. Most of the time viruses are spreading through the internet. As creation of viruses is rapidly increasing and internet is everywhere available, spread of the computer viruses has increase more and more. Computer viruses are coming to the computer with e-mails in e-mail attachments. When the user opens the e-mail, the computer virus enters into the computer and grows in the computer. Another way of entering a virus into a user’s computer is by downloading something from some web sites. Through floppy disks or another removable media, it is possible for a virus to enter into a computer. cite{1}

section{What the computer viruses and other malicious software can and cannot do}

begin{itemize}

item Use disk space by the computer viruses in vain.

item Delete or modify the content of the infected files.

item Interrupt to some operations of the infected computer.

item Display some messages or images.

item Decrease the performance of the computer.

item Block the computer networks.

item Do not do any harm to the hardware components that are connected to the computer.

end{itemize}

section{Protection from computer viruses}

Once a computer infects with some computer viruses, the computer users cannot identify whether a computer virus has entered into the computer or computer system as some computer viruses are in idle mode for some period of time. The computer users can know that a computer virus has entered into the computer only by looking at the evidence of the destruction they have done. So the computer users must always consider about the safety of their computer before a virus do some destruction to the computer.

begin{sloppypar}

end{sloppypar}

As most of the computer users are now aware of the computer viruses, they specially pay their attention to limit the chance for a computer virus to enter into their computer. By just installing an anti virus software the users cannot give the responsibility of protecting the computer from computer viruses only to the anti virus software programs. The computer users also have the responsibility of protecting the computer from computer viruses. Although

most of the computer users trust and use an anti virus software to protect their computers from computer viruses, there are best practices which should be followed by the computer users.

begin{itemize}

item When downloading software or any other thing from web sites the users should always be careful to download them from reliable web sites.

item As viruses can come with e-mail attachments when the computer user checks the e-mails, messages from unknown contacts should not be opened.

item If the user is logging into the computer with admin privileges, the chance to be infected by some computer viruses or malware is greater than the user log into the computer with user privileges. As some viruses cannot enter into the computer when the user logged as a user, log into the computer with user privileges is safer.

item Restrict the other users from “ write” privilege is another option.

item Put passwords that cannot be easily guessed by another person.

item Backup data.

item Use only trusted software.

end{itemize}

begin{sloppypar}

end{sloppypar}

How much the company or person has to pay for an anti virus software, today most of the computer users are used to get the service of an anti virus software as the data are worth than the amount they pay to protect their computer or computer system. So installing an anti virus software program has become the most popular and reliable method of protecting from computer viruses. cite{14}

newpage

subsection{Computer virus protection with anti virus software programs}

As computer viruses are available everywhere in the world, the better way to protect the systems is installing an anti virus software in them. Because of that reason, there are lots of anti virus software providers to provide their services to the customers. Various anti virus software providers are providing their service to the customers in various ways. They are ‘ client pull method’, ‘ provider push with consent method’, ‘ subscription method’ and ‘ care taking method’.

begin{sloppypar}

end{sloppypar}

Client pull method – After a request from the client or customer for the service of an anti virus software, the service provider provides their service to the client. In this method as its name said, client should take the initiative to get the service.

begin{sloppypar}

end{sloppypar}

Provider push with consent method – The service providers sends email notification about their product and then the customers download the anti virus software and install it on the computer.

begin{sloppypar}

end{sloppypar}

Subscription method – The client agree to an agreement with the service provider. In this method when the vendor updates the anti virus software, the updates will automatically downloaded into the customer’s computer.

begin{sloppypar}

end{sloppypar}

Care taking method – In this method none of the individual computer user should not do anything to protect the computer from viruses. The service provider provides the service as a whole.

begin{sloppypar}

end{sloppypar}

The mechanisms used by various kinds of anti virus programs to detect a computer virus is not able to catch all the viruses or not able to not to catch the non virus things. Traditional anti virus software used two methods to detect a computer virus. cite{15, 16}

subsubsection{String matching technique}

Some anti virus providers stored the codes of the computer viruses in a virus dictionary and when performing a scan, the anti virus software searches the scanning file for a piece of code from the virus dictionary. If a matching character is met, then the anti virus software detects that file as a suspicious file and alerts the user saying there is a suspicious file in the computer.

begin{sloppypar}

end{sloppypar}

But if a virus creator creates and release a new computer virus, as the code of that virus is not available in the virus dictionary, the anti virus program is not able to detect that virus. So the anti virus software which use this technique cannot guarantee that all the computer viruses can be detected by itself. cite{17}

subsubsection{Detecting a virus by monitoring the behavior of the program}

The anti virus programs which use this technique is monitoring the behavior of the scanned program and if there is an unusual behavior, the anti virus program detect it as an infected program and report it to the user.

begin{sloppypar}

end{sloppypar}

But if the anti virus software detect a non infected program as an infected program and after reporting it to the user if the user deletes it from the computer, a problem arise.

begin{sloppypar}

end{sloppypar}

Although the anti virus software can be trusted, there are some fake anti virus software which do not provide a protection against computer viruses. They have created only with the objective of earning money from the computer users by intruding them. Because of this reason, the computer users also have the ability to download and install only the trusted anti virus software. cite{17}

subsection{Antivirus software rating}

The latest antivirus software rates in the world. cite{11}

begin{itemize}

item BitDefender Antivirus 2010 – This provides a great security, simple usability, effective use of resources, and a valuable pricetag and provides up to date technologies to combat viruses and other malware. Active virus control is the latest technology they are looking for to give a great security by always observing the behavior of a file. cite{19}

item Kaspersky Anti-Virus 2010 – All around protection from number of threats like viruses, Trojans, bots, worms, and spyware. This is more easy to use as it has created with user friendly navigations. cite{20}

item Webroot AntiVirus with SpySweeper 2010 – A comprehensive desktop anti virus package which is used a multi-layered approach. Webroot AntiVirus with Spy Sweeper also features proactive technology to find malware before it does any harm to the computer. cite{21}

item Norton AntiVirus 2010 – Great protection level against malware but a problem arises when uninstalling the software as its partial ninstallation. This uses traditional signature based detection mechanism to detect malware. cite{22}

item ESET Nod32 Antivirus 4 – Kind of desktop anti virus software. But this doesn’t provide a complete security and misses some protection. This is not in the competition with other anti virus software. cite{23}

item AVG Anti-Virus 9 – Includes antivirus and antispyware protection. provides complette protection from harmful downloads and web cites. cite{24}

item F-Secure Anti-Virus 2010 – Great desktop anti virus. Has one of the most effective scan procedure and test results are shown to prove that. When installing this anti virus software, it has been automatically configured to remove the other anti virus software installed to the computer. cite{25}

item G DATA AntiVirus 2011 – Uses two distinct antivirus scanning engines, behavioral/heuristic protection, and even self-learning fingerprinting. This

provides protection against malware spreading via emails and IM. The types of malware which are detected by this anti virus software are, phishing scams, dialers, adware, malicious scripts, Trojans, rootkits and worms. cite{26}

item Avira AntiVir Premium

item Trend Micro AntiVirus + AntiSpyware

end{itemize}

section{Cryptography and viruses}

Cryptography is technique use to safe some data from other unauthorized people. Most of the time this is used when transfers data from computer to another one. But the problem is virus programmers also use this technique to their viruses.

begin{sloppypar}

end{sloppypar}

In cryptography there are different kind of cryptography methods available but most of the time the programmer who create viruses use symmetric single key cryptography. Actually what happen in cryptography is data encrypt using key and send that encrypted data to recipient then recipient decrypt and get original data using the key. This method is so safe because the encrypted data can not anyone understand.

begin{sloppypar}

end{sloppypar}

Normally anti-virus program detect virus using the code of the virus. If there any virus with encrypted code then anti virus software can not identify those viruses.

begin{sloppypar}

end{sloppypar}

Virus creators using cryptography, they encrypt the code of the virus. So some viruses change their aspects moment to moment and system to system but the key is same but is encrypted with virus code. So the virus is safe from anti-virus software, till the code is encrypted.

begin{sloppypar}

end{sloppypar}

But some cryptography viruses keep their key in separate places instead of keep with the same file. So good anti virus software can detect the places which keys are stored. Then it can decrypt the virus code and delete it.

begin{sloppypar}

end{sloppypar}

Therefore computer system is protected some operating system developers keep the system fies as encrypted. So even though, there are some advantages and the facilities in using cryptography systems to be it

prctically applicapable in virus preventation more advanced features of cryptography should be applied. cite{13}

newpage

section{Conclusion}

As computer usage and internet usage is increasing in the modern world, the computer virus creation and the computer virus infection has become a common thing. Computer viruses can destroy a whole computer system or computer network within few seconds. But for any kind of company, the data they have should have confidentiality, integrity and availability. But sometimes those three things will be lost by the computer viruses. So most of the computers users are now try to avoid from the computer viruses.

begin{sloppypar}

end{sloppypar}

But computer virus infection has become so common thing because of the unawareness and the careless of the computer users about computer viruses. If the computer is attacked by a computer virus, the computer users do not do the correct thing to avoid spreading the virus to the other computers. That is why the computer viruses are spreading all over the world quickly. If a new computer virus is found from a user’s computer, the anti virus software providers are unable to provide a solution to the problem before it spread everywhere. The computer user has great responsibility to not to let a computer virus enter into the computer. To mitigate the destruction, this can happen to the computer from computer viruses,

begin{itemize}

item Aware the computer users about computer viruses.

item Backup the data.

item Put passwords which cannot easily guess by the outsiders.

item Not to give write permission to the other persons.

item Do not open suspicious e-mails from unknown contacts.

item Download and use only the recommended software.

item Install an anti virus software.

item Always keep the anti virus database up to date.

item Use only the recommended anti virus software.

end{itemize}

begin{sloppypar}

end{sloppypar}

As computer users are now searching for the best anti virus software which can give the best protection to their computers from computer malware, the anti virus market has grown and saturated with various kinds of anti virus software. But the problem is that though there are more anti virus software with the target of providing a better protection; virus creators are more powerful than anti virus program creators. They encrypt the code of the

computer virus so that any of the anti viruses cannot detect that computer virus.

begin{sloppypar}

end{sloppypar}

Considering all the fact we can come to a conclusion that any of the computer in the world cannot be there with no virus attack and any of the computer virus protection methods cannot eradicate the computer viruses from the computer forever.

newpage

begin{thebibliography}{widest entry}

bibitem{1} McAfee, emph{An Introduction to Computer Viruses and other Destructive Programs}, Available at: http://www. mcafee. com/common/media/vil/pdf/av_white. pdf

bibitem{2} Markus Hanhisalo, emph{computer Viruses}, Available at: http://www. tml. tkk. fi/Opinnot/Tik-110. 501/1997/viruses. html# 1. Introduction% 20to% 20Computer% 20Viruses

bibitem{3} Top Bits, 2010, {http://www. topbits. com/types-of-computer-viruses. html}

bibitem{4} Spamlaws, 2009, emph{Understanding the Polymorphic Virus}, Available at: http://www. spamlaws. com/polymorphic-virus. html

bibitem{5} Ward Takamiya, Jocelyn Kasamoto, emph{An Introduction to Computer Viruses}

bibitem{6} Spamlaws, 2009, emph{Spotting the Stealth Virus}, Available at: http://www. spamlaws. com/stealth-virus. html

bibitem{7}Spamlaws, 2009, emph{Understanding the Resident Virus}, Available at: http://www. spamlaws. com/resident-virus. html

bibitem{8} Top Bits, 2010{http://www. topbits. com/computer-worm. html}

bibitem{9} Top Bits, 2010{http://www. topbits. com/trojan-virus. html}

bibitem{10} Top Bits, 2010,{http://www. topbits. com/logic-bomb. html}

bibitem{11} emph{AntiVirus Software Review }, http://anti-virus-software-review. toptenreviews. com/

bibitem{12} emph{Computer knowledge virus tutorial}, Available at: www. cknow. com

bibitem{13} Charles P. Pfleeger, Shari Lawrence Pfleeger emph{Security in Computing (4th Edition) }

bibitem{14} Stanley A. Kurzban, emph{Defending against viruses and worms}, Available at: http://portal. acm. org/citation. cfm? id= 68697

bibitem{15} emph{How does anti-virus software work?}, Available at: http://www. antivirusworld. com/articles/antivirus. php

bibitem{16} emph{How Antivirus Software Detect Computer Viruses}, Available at: http://security-antivirus-software. suite101. com/article. cfm/how-antivirus-software-detect-computer-viruses

bibitem{17} emph{How AntiVirus Works}, Available at: http://www. antivirusware. com/articles/how-anti-virus-works. htm

bibitem{18} http://www. darkgovernment. com/news/tag/hacking

bibitem{19} emph{BitDefender Antivirus 2010} http://anti-virus-software-review. toptenreviews. com/bitdefender-review. html

bibitem{20} emph{Kaspersky Anti-Virus 2010}http://anti-virus-software-review. toptenreviews. com/kaspersky-review. html

bibitem{21} emph{Webroot AntiVirus with SpySweeper Review}http://anti-virus-software-review. toptenreviews. com/webroot-antivirus-review. html

bibitem{22} emph{Norton AntiVirus 2010}http://anti-virus-software-review. toptenreviews. com/norton-review. html

bibitem{23} emph{ESET Nod32 Antivirus 4}http://anti-virus-software-review. toptenreviews. com/eset-nod32-review. html

bibitem{24} emph{AVG Anti-Virus 9}http://anti-virus-software-review. toptenreviews. com/avg-review. html

bibitem{25} emph{F-Secure Anti-Virus 2010}http://anti-virus-software-review. toptenreviews. com/f-secure-review. html

bibitem{26} emph {GDATA AntiVirus 2011}http://anti-virus-software-review.

toptenreviews. com/antiviruskit-review. html

end{thebibliography}

end{document}