Essay on Computer Virus

> *“A computer virus is a kind of software that infects programs, data or dices and can reproduce itself in the same or another form. Despite all preventive measures, the viruses are becoming an order of the day. Viruses are enemies of computers and destroy whatever is stored in it, innocently, calmly and intelligently.“*

It was Fred Cahen who incidentally coined the expression ‘Computer Virus‘. The term ‘Virus‘ and ‘ worm‘ used in science fiction novels in the early 1970s. Mound the same period, researchers at Xerox Corp., created and demonstrated a self-replicating code, called viruses.

A virus is a program that can modify another program if deemed infected. This can also become an evolved copy of the original virus program. Every program that gets infected may also act as a virus and thus the infection multiplies. The critical property of a virus is its ability to infect other programs. Every general-purpose system currently in use is open to viral attacks in some secure systems, the virus tends to spread further when created by some user of the system. A virus has the potential to spread throughout any system which allows sharing. The virus can be generated and introduced by a hacker. The perpetrator gets the satisfaction of demonstrating human superiority over a cybernetic system.

With the advent of the Internet a haven- has been created for virus mongers. Critical ongoing research involves determining how quickly a virus could spread to a large percentage of computers in the world. Studies through simplified mathematical models of the virus spreading in typical computer networks have been going on. Obviously, virus-like programs have to be written, injected into systems and the effect has to be studied. In a simulated environment, the extent, speed, and effect of infection are studied. Several experiments have been systematically carried out. The anti-virus program writers must be doing similar experiments before eventually bringing out their anti-virus packages.

Virus study indicates a set of undecidable detection problems’. A list could be as follows:

- Detection of a virus by its appearance.
- Detection of a virus by its behavior.
- Detection of the evolution of a known virus.
- Detection of a triggering mechanism by its appearance.
- Detection of a triggering mechanism by its behavior.
- Detection of the evolution of a known triggering mechanism.
- Detection of a viral detector by its behavior.
- Detection of the evolution of a known viral detector.
- Safety of a protection scheme.

With networking becoming the order of the day, a virus may get initiated only through a particular node or through a few nodes and may give an appearance of having originated from some other node. A virus may also get kindled at some stages of a program in an executable file and not necessarily whenever the program is called for.

Experts say that a virus need not be used only for evil purposes. A very interesting theory in compression through virus has been developed. It can be explained that a simple virus can be written to find the uninfected executable files, compress them and insert themselves into them. Upon execution, the infected program decompresses itself and executes normally. Studies indicate that such a virus could save over 50 percent of the space taken up by the executable files in an average system. The performance of infected programs decreases slightly as they are decompressed, and then the ‘compression virus’ implements a particular `time-space trade-off.

Another example could be that a virus program can be written in such a way as to find ‘uninfected’ executable. It will plant itself in its beginning. After a given date and time the virus would cause the executable to ‘refuse service’ by going into an indefinite loop. And in modem networking with the level of sharing that is prevalent, the entire system would become unusable as of that moment. Anti-virus operators might find a great deal of hard work is required to treat/undo the damage caused by such a virus.

Types of Viruses

Non-TSR file virus: This is the simplest form of the virus to write- and the least effective, so one is unlikely to be troubled by them. When an infected program is first to run, the virus code carries out its task checking that an executable file is not infected, then attaching a copy to it. It then runs the original program to which it is attached. In contrast, TSR viruses load themselves into memory when they are executed and are able to infect any executable program they can reach from that point.

Boot sector Virus: This is the other major type ofvin_is. Most of the boot sector consists of a simple, small program that is used to start DOS, or whatever operating system is installed. Boot sector viruses replace this with virus code and typically move the boot sector to another part of the disc. When the PC boot, the virus code is executed first. Then the virus runs the real boot sector. Avery’s slow boot from an infected floppy with an excess of floppy disc activity is a common symptom of an infected machine.

Multipartite Viruses: These combine both techniques. They can infect both boot sectors and files. The file version df' Tequila', for example, infects the Master Boot Record. Once the PC has been booted from an infected MBR, the virus goes memory resident and infects all accessed .EXE files.

Companion Viruses: Companion viruses create a .COM companion to an .EXE file. Because DOS files . the virus is run before the .EXE file of the same name. The virus then runs the original .EXE.

Polymorphic viruses: These aim to foil anti-virus packages that search for a specific strain by looking for a known sequence of bytes. No two copies of a true polymorphic virus are alike. When polymorphic viruses run they first decrypt themselves and then behave like any other virus. Programs such as the 'Nuke Encryption Device' (NED) and the 'Trident Polymorphic Engine' have been written that turn a standard virus into a polymorphic virus. Fortunately, once measures have been taken by an anti-virus company to defeat each `engine', all viruses processed by it are detectable.

Stealth: Stealth covers a variety of techniques that viruses use to disguise their presence from anything as simple as hiding the increase in file size of executable to full-blown detection of the tools used to detect the virus and the taking of appropriate action to fool them.

Trojans: Trojans are not viruses at all. They are programs that hide a malevolent code within a seemingly innocuous program but they do not replicate. For this reason, the chances of being caught out accidentally by Trojans are low.

Macro viruses: Macro viruses have been predicted for a while. It recently appeared when it was sent out accidentally by Microsoft on a

CD-ROM to OEMs. They called it a `Prank Macro’. It is the first virus that will run on both PCs and Macs. It replicates using an auto-executing Word Basic macro embedded in a document. When the document is loaded, it copies the macro to Word’s settings file . and replaces the File Save command with a routine that also saves a copy of the macro in each document.

Prevention from A Virus Attack

The most fundamental precaution against virus attacks is to limit access to a machine to avoid tamper with the system. In the case of floppy discs, the simplest form of protection is to place write-protect tabs on all discs so that any attempt by a virus to write to the disc would result in an error message. The write-protect tab should be °removed only when data has to be expressly written to the floppy.

It should be remembered that even the simple act of inserting a floppy disc and getting a directory listing can be enough to infect a machine. Though write-protect facilities are generally not available for hard discs, hardware products have started appearing in the market offering users the ability to write-protect hard discs. But being expensive, these are not likely to be used widely.

Software products to write-protect hard discs are also available. But these render themselves vulnerable to virus attack also. In network environments, the use of diskless or hard-disc-only systems is becoming popular. Control of software is then restricted to the file server and network administrators only.

Tips for Prevention of Virus

Infection Even if one buys and uses several anti-virus applications, the best defense is to avoid infection in the first place. There is no absolute guarantee against infection. But the risk can be minimized by following the guidelines listed below:

Boot the system with a write-protected and already scanned floppy disc, which has the boot and system files and set of files of a qualified virus-scanned program.

Even if there is a hard disc and the PC normally boots from that disc, start by first booting the system with the uninfected and write-protected disc boot floppy in the ‘A’ drive.

All floppies should be scanned individually and periodically by using a qualified and uninfected virus scanning (or detection) program.

Discourage the use of floppies of other users unless these are individually scanned and checked for any virus.

Do not use previously formatted floppies brought by others even if these are apparently empty. Reformat all empty floppies with your uninfected system before further use.

Avoid lending floppies.

The most popular carriers of dangerous viruses are floppies containing different popular computer games, horoscopes, astrological predictions, etc. These should be avoided.

The use of pirated software should be completely avoided as most of them are virus carriers.

Take back-ups regularly. A full back-up once a week, with incremental back-ups daily, if necessary, is advisable. Uninfected back-ups allow overwriting infected files. Even infected back-ups permit recovery from logic bombs. Disinfect restored files right away.

Write-protect and back-up the installation discs before installing any new software. If it is not done and the system already has a virus infection, the original program discs could be permanently infected during installation.

Scan network drives used regularly. The files attached to e-mail messages may be infected.

Use the memory-resident, virus spotting portion of the anti-virus application at all times. If an infection is suspected, turn off the system immediately. Reboot from a clean floppy (one without an or a file). Then disinfect the system using a disc-based copy of the anti-virus program.

User should also have some basic knowledge about viruses, their prevention, and cure. The use of good anti-virus software for scanning files regularly should invariably be used by each and every user.

But a single software cannot be depended upon to eliminate the infection from all strains of viruses. The battle against virus infection will be long and perhaps, lasting.