Detecting Boot Sector Viruses- Applying TRIZ to Improve Anti-Virus Programs

Umakant Mishra
Detecting Boot Sector Viruses  
Applying TRIZ to improve anti-virus programs

Umakant Mishra  
Bangalore, India  
http://umakantm.blogspot.in

Contents
1. Introduction to boot sector viruses .................................................................1  
   1.1 What is boot sector virus ........................................................................2  
   1.2 How does it spread ..............................................................................2  
2. Problems in detecting boot sector virus .........................................................3  
   2.1 Boot sector virus remains memory resident ............................................3  
   2.2 Boot sector virus is loaded before loading of OS .................................4  
   2.3 Boot sector virus is loaded on every booting ........................................4  
   2.4 Boot sector virus enters through infected floppies ..................................5  
3. Inventions on preventing/detecting boot sector virus ....................................5  
   3.1 Software anti-virus facility (Patent 5559960) .........................................5  
   3.2 Virus protection in computer systems (Patent 5802277) .......................6  
   3.3 BIOS-level floppy boot-sector virus prevention (Patent 6550007) .........8  
4. Summary ......................................................................................................9  
Reference: ....................................................................................................10

1. Introduction to boot sector viruses

A computer virus is a destructive computer program, which spreads itself from computer to computer and causes unauthorized and unwanted changes to the information stored in those computer systems.

There are various types of viruses, such as, file viruses, boot sector viruses, macro viruses, worms, trojans etc. Different types of viruses cause different types of damages/disturbances in a computer system. Some viruses alter or destroy data on the disk, some scramble characters on video display screen, some display misleading messages to the users, some consume computer/network resources thereby making the computer/network slow.
1.1 What is boot sector virus

The bootstrap code or the boot record is the first piece of code that is loaded into the memory when the computer is booted from a floppy or hard disk. All floppy diskettes and hard disks contain this small program known as boot record or Master Boot Record (MBR) in the boot sector that is typically the first sector of the disk. When a computer is booted, the microprocessor first reads the Master Boot Record from the disk. Thus MBR is quite necessary for the booting operation. The boot sector is typically 512 bytes of data on PC’s. The boot sector occupies exactly one sector and is provided in the first sector of the partition.

![Boot Sector Virus Infection](image)

The boot sector virus is called so as it infects the boot record on the floppy diskettes or hard disks. The boot sector viruses infect floppy disks and hard disks by inserting themselves into the boot sector of the disk. The boot sector virus or Master Boot Record virus (or MBR Virus) replaces the computer’s MBR and partition table with its own code. The MBR virus typically enters the computer through infected floppy disks.

There are also multi-partite viruses that are a combination of file virus and a boot sector virus. Many of the early age viruses were boot sector viruses.

1.2 How does it spread

The boot sector viruses generally transfer through infected floppy disks. When a diskette, infected with a boot sector virus, is placed into a computer system and the system is allowed to boot, the “virus transfer code” in the infected boot record executes. Then the boot sector virus transfers itself to the hard disk by overwriting the disk’s original boot sector with its own code. The worst thing is that the computer need not have to boot from the floppy in order to be infected. Any floppy, infected with a boot sector virus, can infect the computer even if the floppy disk is not bootable.

A typical scenario is for a user to receive a diskette from an innocent source that contains a boot disk virus. The user can read the diskette for normal operations without triggering the boot sector virus. But if the diskette is there in the drive when the computer is turned on, then the computer will look for the boot sector in “A” drive and load the boot sector virus.
When the system reads the infected boot sector, the control of the system is passed to the infected boot sector. At this point, the “virus transfer code” of the infected boot sector executes and hooks the Interrupt 13h vector which controls the harddisk, floppy and other disk R/W access. This hook executes a piece of code during all Int 13h routines and causes the boot record of any device accessed to be updated with the virus code. The hook remains in memory throughout the time that the computer system is powered on and reinstalls itself from the boot record when the system is rebooted. Thus the harddisk becomes permanently infected with the boot sector virus. Even though there is a virus detection utility installed on the system, it fails to detect the presence of the virus and its activities.

2. Problems in detecting boot sector virus

There are several methods of detecting viruses, such as, signature scanning, heuristic scanning, integrity checking etc. As the characteristics of different viruses are different their detection methods are also different. All methods of detection do not work for all types of viruses.

Boot sector viruses are often more dangerous than file viruses. The boot sector viruses are directed at the boot sector of a bootable medium e.g., hard disk or floppy diskette. Since the master boot record executes every time the computer is started, the boot sector virus is loaded from the beginning and remains resident in the memory till the computer is shut down. It hooks the interrupt vectors to control Read/Write operations and becomes very dangerous to the integrity of the computer system. Besides it remains permanently in a computer until the system is totally damaged and fails to boot.

2.1 Boot sector virus remains memory resident

The first thing the boot sector virus does is that it loads itself into the memory before anything else. The virus hooks the Interrupt 13h vector which controls the hard disk, floppy and other media access. This hook inserts a piece of code which is executed during all Int 13h routines and infects the boot record of any device accessed. The hook remains in memory throughout the time that the computer system is powered on and reinstalls itself from the boot record when the system is rebooted (either by powering up or by means of ALT-CTRL-DEL). By this mechanism, the system hard disk remains permanently infected with that boot sector virus and even if there is a virus detection facility installed on the system hard disk, it will be powerless to prevent the infection. In addition, no knowledge of the virus transfer will be flagged and the infected diskette may well be inadvertently used on further computer systems.

Ideal Final result:

- The memory of a computer should not allow a virus to be resident
- The master boot record should check itself for genuineness before loading into system memory.
Possible Solution:

⇒ The boot sector data should be compared with the original / genuine boot sector code before loading into the memory.

2.2 Boot sector virus is loaded before loading of OS

Since the boot sector is the first item of data accessed during the boot up of a computer system, a virus in that location is virtually without defense. The boot sector viruses overwrite the disk’s original boot sector with its own code so that the virus is loaded into the memory before anything else.

Ideal Final result:

• The boot sector of a disk should be resistant to virus infection.
• The boot sector should check its genuineness before loading.

Possible Solution:

⇒ Loading an anti-virus before the boot sector virus is loaded, i.e., before the Operating System is loaded.
⇒ Comparing the checksum of the boot sector with the checksum of the original uninfected boot sector before every booting.
⇒ Keeping a copy of the boot sector in a secured place and replace the code when the original boot sector is infected.

2.3 Boot sector virus is loaded on every booting

The boot sector virus replaces the content of the original boot record in the hard disk. As the boot record is loaded every time when the system is turned on, the infected boot record is loaded every time the system boots.

Ideal Final result:

• The master boot record should be uninfectable.
• The system should boot from an uninfected media

Possible Solution:

⇒ One solution to control boot sector viruses was provided by McAfee ROMSHIELD. ROMSHIELD is an IC chip that is designed to fit into the boot ROM socket found on most Ethernet LAN adapters. The ROMSHIELD chip automatically scans every diskette inserted into the computer for boot sector viruses before the diskette is accessed.
⇒ Using an EFI (Extensible Firmware Interface) based operating system where the boot sector of the hard disk is copied to the non-volatile memory and read from the non-volatile memory on each boot. This method bypasses the boot sector access of the hard disk during system initialization and protects the computer system from potential boot sector viruses (Patent 6907524, invented by Huntington, et al., assignee Phoenix Technologies Ltd., June 2005).
2.4 Boot sector virus enters through infected floppies

The boot sector virus typically enters the computer through infected floppy disks. If an infected floppy is there in the drive when the system is booting the system reads the infected boot record from the floppy even if the floppy is not bootable. Thus the problem can occur just because of failing the human memory of removing the floppy disk from the drive after its usage is over.

Ideal Final result:
- The system should not seek to read a floppy while booting
- The system should know and avoid an infected disk to boot from

Possible Solution:
- Disable floppy seek during booting in the CMOS setup.
- If there is a floppy in the drive while the computer is booting then the system may ask the user whether he wants to boot from the floppy (US Patent 6550007, described later).
- The system should boot without reading data from the boot sector, e.g., non-disk-based Operating Systems, or a BTOS (described below).

3. Inventions on preventing/ detecting boot sector virus

3.1 Software anti-virus facility (Patent 5559960)

| Problem | There are various anti-virus programs in the market which are all loaded after the computer is booted. But a bootstrap-time virus can take hold of the computer system before the anti-virus software is loaded and interfere with the operation of anti-virus software. In such cases the anti-virus program may not function as desired. |

| Invention | Software anti-virus facility (Patent 5559960) |

Patent 5559960 (invented by Jonathan Lettvin, Sept 1996) provides a virus resistant disk to store the anti-virus program. The invention stores the anti-virus in a hidden partition and loads it at the time of booting before any bootstrap-time virus is executed.

The objective of the invention is to provide a startup disk (diskette or hard disk) that can execute anti-virus program before the bootstrap-time viruses are executed (Principle-13: Other way round, Principle-9: Prior Counteraction).

The invention also creates a “hidden partition” to store the anti-virus software (Principle-32: Color Change). The hidden-partition shields the anti-virus software from viruses. Besides the hidden partition is created in the boot block (BIOS parameter block) hence it does not reduce the disk’s formatted or advertised capacity.
Alternatively, the disk may contain a bootstrap-time operating system (BTOS) which executes an anti-virus program and disk-maintenance program stored in the hidden partition. The BTOS then loads the normal bootstrap program which loads the normal operating system like MS DOS (Principle-24: Intermediary).

3.2 Virus protection in computer systems (Patent 5802277)

| Problem | The boot sector is the first item of data to be loaded in a computer system. Since the boot sector viruses are loaded before the OS is loaded and take control of the OS functions, the conventional anti-virus programs do not work effectively for these viruses. Although a checksum approach is useful while booting from a hard disk, it does not help while booting from a floppy drive. There is a need for an improved technique in order to provide protection against infection by a boot sector virus. |
The conventional anti-virus programs can function only after the computer is successfully booted with an operating system. Hence, these methods cannot protect the computer from boot sector viruses that attack when a computer system boots, i.e., before installation of the operating system.

**Invention**  
**Virus protection in computer systems (Patent 5802277)**

Patent 5802277 (invented by Cowlard, Sep 1998) discloses a method to protect a system against infection by boot sector viruses carried by floppy diskettes.

The invention stores the virus signatures and virus detection code in a Flash ROM. The virus detection code is executed after POST (Power On Self Test) and before passing control to a bootable media, whether a hard disk or floppy.

The virus signatures and virus detection program in the Flash ROM checks for the presence of any boot sector virus in the boot media and passes control to the boot code only if it does not find any virus. If a virus is found, the boot operation is halted and a warning is conveyed to the user about the virus. Thus the invention detects the virus in between the steps of POST and loading the boot sector (Principle-24: Intermediary).

The invention stores the virus detection code in a ROM (or preferably in Programmable ROM to allow updates). The invention proposes various methods of virus detection, such as; applying non-signature based heuristic analysis wherein “fuzzy logic” is employed, using virus signatures that is stored in the system memory along with the virus detection code etc.

This method is effective against boot sector viruses from all types of bootable media, even including floppies, which are generally not susceptible to the checksum method. The invention stores the virus detection code and virus signatures in the same ROM in which the system stores BIOS and POST. Hence it does not require an additional ROM chip.
3.3 BIOS-level floppy boot-sector virus prevention (Patent 6550007)

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Often the floppy disks are just left in the floppy drives of the computer systems. In such cases if the floppy is infected the computer gets infected when it attempts to boot from the floppy. There is a need to solve this problem.</td>
</tr>
<tr>
<td>One solution to the above-described problem is that, the user should check the drive for the presence of any disk every time he or she boots the computer system. <strong>Limitations:</strong> the user may not be present or may be unmindful at the time of booting.</td>
</tr>
<tr>
<td>Another solution is to remove the option of booting from the floppy disk drive in the CMOS setup or to bring it down to the bottom of the list of bootable devices. <strong>Limitations:</strong> in that case it will be difficult again to boot from the floppy by changing all the options in CMOS.</td>
</tr>
<tr>
<td>Yet another solution is to wait until the computer system is actually infected with a virus and then use some type of clean up software to remove it. However, preventing the virus is definitely better than curing it after the infection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Invention</th>
<th>BIOS-level floppy boot-sector virus prevention (Patent 6550007)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent 6550007 (invented by Baxter, et al., assignee Dell USA, April 2003) discloses a simple method of preventing boot sector virus by displaying an alert to the user before trying to boot from a floppy.</td>
<td></td>
</tr>
<tr>
<td>According to the invented protection system when the computer finds a floppy in the drive it alerts a user that the computer system is about to boot from the floppy disk before actually doing so. This option reminds the user about the presence of the floppy in the drive and enables him to remove the floppy disk if he does not intend the computer system to boot from the floppy (Principle-9: Prior Counteraction).</td>
<td></td>
</tr>
<tr>
<td>If the user responds in the affirmative, then the computer system is booted from the floppy disk and the operation proceeds as usual. If the user responds in the negative, the floppy disk boot is skipped and the computer system attempts to boot from the next device listed in its boot table. If the user fails to respond to the query within a predetermined amount of time, the boot protection system skips the floppy disk and boots from the hard disk or other device listed in the boot table.</td>
<td></td>
</tr>
</tbody>
</table>
The assumption behind the invention is that the boot sector virus problem is because of unwanted floppy seek during boot process, which is again mainly because of failing the human memory to remove the floppy disk from the drive after the use of floppy is over. The invention solves this problem just by asking the user whether he wants to boot from the floppy (Principle-23: Feedback) and skipping the floppy boot unless responded positively.

4. Summary

The boot sector virus infects the boot record of the hard disk or floppy disks. It gets loaded onto the memory every time the computer is booted and remains resident in the memory till the computer is shut down. Once entered it alters the boot sector of the hard disk and remains in the hard disk permanently. The boot sector virus enters into a computer mainly by booting from infected floppies.

As the boot sector viruses mainly enter through infected floppies one of the methods of avoiding boot sector virus is by avoiding booting from floppies. This can be achieved by editing the boot device preference in the CMOS setup. But there are situations when we really need to boot from a floppy. In such cases we need to ensure that the floppy is free from viruses.

Sometimes the system may get infected because we forget to remove an infected floppy from the drive while the computer is booting. These situations of unmindfulness can be avoided by asking a confirmation message to the user before booting from the floppy.
While analyzing the problem from TRIZ prospective we try different possibilities to avoid boot sector viruses, such as,

⇒ Can we do away with boot record?
⇒ Can we avoid booting from floppies?
⇒ Can we make the boot record virus resistant?
⇒ Can we keep the boot record in a place which virus cannot access?
⇒ Can the boot record checks itself for virus?
⇒ Can we load the anti virus before loading boot sector?
⇒ Can we remind the user to remove unwanted floppies from the drive?

One method to avoid boot sector virus is by loading some kind of anti-virus before the computer is booted. One possibility may be to load such an anti-virus from a ROM chip. Another possibility may be to load such an anti-virus from a hidden partition that is not accessible to viruses or other programs.

Another method to avoid boot sector virus is to store the boot sector in a separate ROM chip, which is protected from any kind of infection. Although this method works satisfactorily to provide protection against boot sector viruses, it requires an additional ROM to be bought that adds to the cost of the system.

Boot sector viruses can be detected by comparing the checksum of the boot program with that of the original boot program. If there is a difference in the two checksums the boot program is deemed as infected. But this approach is not effective when the system is booting from a diskette, for which there may be no checksum value stored in the computer system.

**Reference:**

About the author

After working for more than 18 years in various fields of Information Technology Umakant is currently doing independent research on TRIZ and IT since 2004. He last worked as Director and Chief Technology Officer (2000-2004) in CREAX Information Technologies (Bangalore). Before that he worked as IS/IT manager (1996-2000) for ActionAid India (Bangalore).

Umakant is a Master in Philosophy (MA), Master in Business Administration (MBA), Bachelor in Law and Logic (LLB), Microsoft Certified Systems Engineer (MCSE+I), Certified Novell Engineer (CNE), Master Certified Novell Engineer (MCNE), Certified Intranet Manager (CIM), Certified Internet Professional (CIP), Certified Software Test Manager (CSTM) and holds many other global IT certifications.