Solving Virus Problems by System Administrators- a TRIZ perspective

Umakant Mishra
Solving Virus Problems by Systems Administrators
- A TRIZ Perspective

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

Contents

1. Introduction ................................................................. 1
2. Analyzing virus problems faced by Systems Administrators ............ 2
   2.1 The problems faced by a systems administrator ........................ 3
   2.2 Typical solutions adopted by a Systems Administrator ............... 3
   2.3 Ideal Final Goal ................................................................ 3
3. Addressing virus problems faced by Systems Administrators ............ 4
   3.1 Preventive Actions ............................................................... 4
   3.2 Curative Actions .................................................................. 5
4. Problems and contradictions faced .................................................. 5
   4.1 Contradiction of scanning time .............................................. 5
   4.2 Contradiction of virus scanning and system performance ......... 6
   4.3 Contradiction of putting anti-virus in network gateway .......... 7
   4.4 Contradiction of repetitive scanning at every client .............. 7
5. Comparing the problems faced by a Corporate Manager ................. 8
   5.1 Ideal Final Result ................................................................. 8
   5.2 Comparing the Goal of the Corporate Manager and Anti-Virus Producer ... 8
6. Summary .............................................................................. 9
Reference: ................................................................................ 10

1. Introduction

A computer virus is a malicious executable code which is generally loaded onto a computer system without the knowledge of a user and causes unauthorized and unwanted changes to the components of the computer or to the information stored on the computer. The viruses can delete the files, format the hard disk and wreak havoc in a computer system.

The computer virus is not only a problem to the end user but also a problem to everybody whoever is associated with computers, including systems administrators, corporate managers and even anti-virus manufacturers. In the previous article we discussed about the virus problems faced by the end users. In this article we will focus on the problems faced by the systems administrators.
(Note: The term “Systems Administrator” may be understood in generic sense that is synonymous to Network Administrator, LAN Manager etc. who takes care of anti-viral measures for a group of computers or networks as one of the job responsibilities.)

2. Analyzing virus problems faced by Systems Administrators

The first and foremost step of solving a problem is to analyze and define the problem. A majority of problems are automatically solved or cease to exist when properly analyzed. Let’s analyze the problem of virus in detail.

The same situations of virus infections may be a problem to one person at one time but may not be a problem to another person or to the same person at a different time. Besides, the same scenario of virus infection creates different problems to people at different levels, such as, a computer user, a systems administrator, a corporate manager and an anti-virus developer because of the difference in their experience, visions, requirements and goals.

![Diagram showing the scale of knowledge on computer virus and relationships between anti-virus developer, system administrator, corporate manager, and computer user.]

The problems faced by the systems administrators are different from that faced by the end users, because of the difference in their responsibilities and goals. When the goals are different, the problems are different; the solutions can also be different. For example, if a user’s computer is virus infected he can leave office and work on his personal computer at home, where his goal is to submit a report by a target date. But a systems administrator cannot leave office to work at home, because his goal is to remove virus from the computers in the office.

Although many users report on virus problems they don’t report alike. For example, the user may report like “The computer is behaving erratically, some files are missing, some executable is not running, the system is hanging, or the system is not booting” and so on. But an experienced systems administrator may understand all those complaints to be one single problem, i.e., virus infection.
2.1 The problems faced by a systems administrator

Let’s analyze the problem faced by a Systems Administrator before going for any solution. The job of a Systems Administrator (or Network Administrator or LAN Manager) is to keep the computers and network safe and free from virus attack. When there is a virus outbreak in the computer systems in a network environment the systems administrator typically faces the following problems.

- His stress level goes up as various users start complaining about virus problems.
- His workload goes up, as he has to scan and remove virus in all the computes. He may have to apply patches or updates or may have to change the anti-virus software.
- His boss will be angry and blame him because he has not been able to tackle the virus problem.

2.2 Typical solutions adopted by a Systems Administrator

The systems administrator may take a regular course of action – taking data backup, downloading anti-virus updates, scanning all the computers etc. If the situation is beyond his control he may seek help from experts from outside.

Alternatively the person may adhere to an unprofessional solution - may start blaming users saying that they don’t know how to handle the computers; or create a bigger problem to divert everybody’s attention from the virus problem; or apply for sick leave and go home.

2.3 Ideal Final Goal

But what the systems administrator ultimately wants in such a scenario? It is interesting to note that unlike the end user he does not want all the computer viruses to vanish completely from the world, as in such a case he will loose part of his job and salary. Unlike the end user he does not mind procuring an anti-virus product, as his company will pay for the procurement. His ultimate objectives may be as below:

⇒ The anti-virus software, that he has selected and deployed in the network, should protect the computers and the network from virus infection.
⇒ The anti-virus software should be easy to install, easy to update and easy to maintain so that his workload is well within his control.
⇒ The methods and policies he adopts for virus protection should work perfectly and no virus should be able to attack any computer system in his network environment.
3. Addressing virus problems faced by Systems Administrators

Let’s now list down a few of actions usually undertaken by the systems administrators and LAN managers to solve virus problems.

3.1 Preventive Actions

⇒ Selection, procurement and deployment of a suitable anti-virus product. The parameters of selection may include price of the product, reliability of the product, product features, OS compatibility etc.

⇒ Implementing anti-virus policy – the network administrator may include an anti-virus policy into the network security policy in order to ensure that the anti-virus measures are properly implemented. The anti-virus policy may include a minimum version of an anti-virus product, minimum update of signature database, a minimum scanning at system startup, specific configurations for automatic scanning of files etc.

⇒ A malware generally invited into the machine by web browsing, email downloading and copying from outside storage media like pen drives, CD, DVD etc. There is a need to guard these incoming routes in order to narrow down the chances of virus infection.

⇒ Implementing anti-virus in the gateway or the proxy server – this would help a lot of infected materials to be filtered before entering into user computers (Principle-8: Counterweight).

⇒ Enabling virus auto-protection– to detect and remove viruses immediately as soon as they are found. (Principle-20: Continuous action). The auto protection and auto healing modules of Antivirus software remain active in the computer memory and protect the system from virus attacks at real-time. (Principle-25: Self Service).

⇒ Restricting users to run the computer in user mode having limited rights and not as administrators. This would prevent some viruses that require an administrator or equivalent rights to infect.

⇒ Educating users to ensure that users update their anti-virus software regularly and follow virus prevention guidelines.

⇒ Keeping regular backup of the systems and servers. One may use different operating systems on different file systems for online backup. A virus is not likely to affect both. For example, Linux backup may be kept in a Windows system and Windows backup may be kept in a Linux system.
3.2 Curative Actions

⇛ When there is an outbreak of ferocious virus the LAN manager may physically unplug the network cables (Principle-2: Taking Out). However, such drastic measures can negatively affect the uninfected sectors of the corporate LAN and cause inconvenience for the end users.

⇛ In case of some memory resident viruses - it may be necessary to (1) disconnect all power supplies including auxiliary power supplies to remove all memory contents from the physical memory, (2) the computer is started up from an external disk with clean OS, (3) a virus extermination program is executed to remove a memory resident virus, (4) the original environment is restored wherein the computer is not infected with a virus.

⇛ If there is a need to turn off anti-virus temporarily in order to restore a computer, the systems administrator may disconnect the computer from the network before disabling the anti-virus program. He may enable the anti-virus program again after the restoration is complete.

⇛ One should not run multiple antivirus software on the same system. As the anti-virus programs do strange activities like a virus, they are likely to suspect each other's activities.

4. Problems and contradictions faced

# There are a large number of memory resident viruses, which do not go even after being detected and cleaned through an anti-virus program. Such viruses remain active in the main memory and do not go even after powering down.

# Although the systems administrator informs the users about the do's and don'ts, he has practically no control over any user to prevent him accessing any infected site on the Internet or using any infected storage media from outside.

# New viruses are created almost on every day. Even if the administrator updates the antivirus on a regular basis there is still a possibility of seeing a new virus.

4.1 Contradiction of scanning time

As the population of viruses increases, the size of signature database also increases accordingly which in turn increases the scanning time. With thousands of possible virus types and hundreds of gigabytes of file storage a complete virus scan can easily take several hours. But generally we cannot afford so much of time for this purpose.
If a scanner includes less number of signatures or less number of algorithms then there is possibility of some viruses being escaped. On the other hand if a scanner includes all available signatures and all possible algorithms then the scanning process will become unbearably slow. We need to apply more scanning algorithms to detect all types of viruses, but at the same time we need to apply less scanning algorithms to scan fast.

⇒ One of the solutions to the above problem is to spread over the scanning process in several sessions. The scanning ends as we stop it and resumes again in future from the point where it left at the previous session (Principle-1: Segmentation).

⇒ Another solution is to do a partial virus scanning of the core elements like main memory, boot sector, file system etc. A partial virus scanning is done every time the computer boots (Principle-16: Partial or Excessive Action).

⇒ Speed scanning or fast mode virus scanning- which scans the memory, system files and critical areas of the disk. The fast mode does not scan the individual files on the disk (Principle-21: Skipping).

⇒ While a fast scanning is done during system boot up or once in a day, a complete virus scanning can be done once in a week or so (Principle-19: Periodic Action).

4.2 Contradiction of virus scanning and system performance
Executing an anti-virus program often consumes significant amount of system resources (like memory and processor) and makes other programs run slow. That’s one of the main reasons why most people don’t like running an anti-virus.

⇒ We want to run an anti-virus to keep the computer safe and free from virus. But we don’t want our computer to run slow when we are working on our important jobs. In other words let the anti-virus scan the computer, but let it not affect our work.

⇒ The solution is to schedule virus scanning during nights or on holidays when people are not working. The self-running feature of the anti-virus program can run automatically at the pre-scheduled day and/or time (Principle-25: Self Service).
Problems involved
However, this idea may work in an office environment. But it has no meaning for a personal computer which is used anytime irrespective of any day of the week or any hour of the day.

Possible solution
⇒ Let the anti-virus run when the system is running but we are not working. Some anti virus programs can be scheduled to run when the system is left idle for certain time (Principle-25: Self Service).

4.3 Contradiction of putting anti-virus in network gateway
There are two methods of administering anti-virus software in a network. One is to install on each individual computer and the other is to install directly into the firewall. But both the methods have several disadvantages. Having a single point protection makes the scanning slow. On the other hand putting on individual computers increases administrative workload.

| Contradiction | Implementing anti-virus directly into the firewall prevents viruses from entering from the Internet but fails to provide protection from viruses spreading within the LAN. Implementing anti-virus on every computer within a LAN protects individual computers from virus, but increases administration work for installation and configuration of anti-virus on each computer. We want to protect the computers from both external (Internet) and internal (within the LAN) infections but we don’t want to increase administration load. |

4.4 Contradiction of repetitive scanning at every client
In a corporate shared environment, many files are shared by users just by copying them from computer to computer. Although the files were already scanned in their previous location they are usually scanned again and again in every computer they are copied to.

| Contradiction | While sharing files on a network, we want to ensure that the files we share are free from viruses but we don’t want to waste time and resources to scan the shared files. |
5. Comparing the problems faced by a Corporate Manager

In the above pages we saw some problems faced by the Systems Administrators (or LAN Managers). But a corporate manager does not face the problems that are faced by the Systems Administrators. They see the same virus scenario differently and they face a different set of challenges.

# Budget allocation and financial provision for virus prevention in the corporate environment.

# Employing right people as the network administrators and network security managers. Ensuring that the network administrators work according to the conventions in the industry.

# Provisioning alternative arrangements to provide working environments in case of virus outbreaks. Ensuring backup of critical data and protection of sensitive data by the security managers according to the industry standard.

5.1 Ideal Final Goal or Ideal Final Result

⇒ There should be no computer virus
(or none of the computers in his office should get infected by any computer virus.)

⇒ There should be no expenditure on buying anti-virus products, no administrators (/human resources) required for installing and maintaining those products and no wasting of time by anybody for this purpose.

Note that the Ideal Final Goal of the corporate manager is very similar to that of the end user. But the mechanics of the corporate manager to achieve the IFR is very different.

5.2 Comparing the Goal of the Corporate Manager and Anti-Virus Producer

Although everybody wants to remove the viruses from computer, the exact goals of different people are different. Let’s compare the goals of the user/corporate manager with that of the anti-virus vender:

<table>
<thead>
<tr>
<th>From users’ perspective</th>
<th>From anti-virus venders’ perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td># The computer should never get infected (no need of purchasing, installing or maintaining any anti-virus software)</td>
<td># The computer should never get infected after installing the intended anti-virus product.</td>
</tr>
</tbody>
</table>
# The computer and the files inside the computer should have immunity to any kind of viruses

# The computers using their anti-virus product should have immunity to protect from any kind of virus at any circumstance.

# Ideally no anti-virus software should be required to keep the computer healthy

# People should use their anti-virus product, however, their anti-virus should be fast, effective and capable of detecting all types of viruses.

As we see above, although everybody wants to solve the problem of virus, the goals and objectives are different for different groups, such as, end users, systems administrators and anti-virus developers. Although the IFR is “No Virus” for a larger group of end users, the IFR is not so for a smaller group of virus and anti-virus producers.

As we see above, although everybody wants to solve the problem of virus, the goals and objectives are different for different groups, such as, end users, systems administrators and anti-virus developers. Although the IFR is “No Virus” for a larger group of end users, the IFR is not so for a smaller group of virus and anti-virus producers.

According to TRIZ theories, every system is moving towards an Ideal Final Goal to achieve an Ideal Final Result. Here, although the Ideal Final Goal is “No virus”, it is not easy to achieve that state because of the fundamental contradiction illustrated above.

### 6. Summary

Computer virus is not only a problem for the end users, it is also a problem for systems administrators, corporate managers and anti-virus producers. However, the nature of problem is different for different groups. While analyzing the problem of computer virus we see that different people involved in this
phenomenon have different objectives and conflicts of interests. For example, although everybody in the chain (including the user, systems administrator, corporate manager, software vendor and anti-virus developer) wants something in common (i.e., to keep the computer free from virus), everybody’s perception of the problem is different, goal is different and method of solving the problem is different. This situation leads to a complex physical contradiction.

Under the circumstance there are various questions to be answered.

- Can a computer be fully immune to viruses?
- Is it possible to have a virus neutral environment?
- Can there be an effective method of scanning computers remotely?
- Can macro viruses be prevented without any anti-virus software if Microsoft will fix security flaws in Microsoft Office suite?
- Can using Linux desktops provide protection from majority of viruses?
- Can there be an effective utilization of anti-viral viruses?

Every stage of an evolution is an output of a combination of innumerable factors. While analyzing various aspects of a virus control mechanism, we find that it is not possible to arrive at a “No virus” situation, unless there is a paradigm change that creates alternative jobs and goals for the virus makers as well as anti-virus makers. Unless such a revolutionary change takes place, the only predictable future at this point of time is a virus environment that is “better controlled”.

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 has authored the books "TRIZ Principles for Information Technology", "Improving Graphical User Interface using TRIZ", "Using TRIZ for Anti-Virus Development" etc. and working on a book on "Management Information Systems". Many of his articles are available in SSRN eLibrary, bepress, Arxiv etc. More about Umakant is available at http://umakantm.blogspot.in.