December, 2011

Solving Virus Problems by Computer Users- a TRIZ perspective

Umakant Mishra
1. Introduction

A computer virus is a malicious executable code that causes problem to the innocent computer users. Generally viruses cause various problems by infecting files and damaging various components of a computer. The computer virus is a problem not only to the user but also to everybody whoever is associated with computers, including systems administrators, corporate managers and even anti-virus manufacturers. We will start with an assumption that there is a need to address this problem.
1.1 Defining a Problem – the First Step of Problem Solving

Before addressing any problem it is necessary to define the problem by analyzing the problem in its context. Many problems are found to be already solved or cease to exist when properly analyzed. For example, the computer virus is not a problem to everybody, at least not to the people who don’t use computer. Besides, the same situation may be a problem to one person at one time but may not be a problem to another person or at a different time. For example, creation of virus is an undesirable phenomenon for a computer-user but is a desirable phenomenon for an anti-virus manufacturer.

Analyzing the problem is an essential step because the same scenario of virus infection creates different problems to people at different levels, such as, a normal computer user, a system administrator, a corporate manager and an anti-virus developer because of the difference in their goals and requirements.

![Diagram: Different types of people around virus problems]

When we analyze a virus problem in detail, we see that the problem is not the same for every level of user. For example, the virus problem faced by an end user is not the same as the virus problem faced by a network administrator. Besides, the problem faced by a novice user – who does not know how to install an anti-virus, may be different from the problems faced by an advanced user, who might have installed an anti-virus, but is facing the adverse effects of anti-virus or difficulties in updating the virus database.

1.2 Application of Different Solutions in Different Situations

As the problems are different for different people, the solutions are also different. For example, if a user’s computer is infected in office, one of his solutions can be to leave the office and work on his personal computer at home, as his goal is probably to submit the report by a dead line. But the systems administrator...
cannot leave the office and do something similar at home, as his goal is to remove the virus from the computers in the office.

Thus we see that the same root cause (in this case, the computer virus) creates different problems to different people. The problems are narrated in different terms and solved in different methods. No single solution is always the best. A good solution may work for some group of people but may not work for every group of people.

In this article, we will analyze the virus problem from the angle of computer users and will see how best can he solve the problem. We will do the same exercise for a network administrator and an anti-virus manufacturer in separate articles.

2. Analyzing the virus problem of an end user

An end user uses a computer for a purpose, say, word processing or gaming or emailing. When the computer is infected, his work is disturbed. His main objective is not to remove the virus but to do his work. If he can continue his word processing or gaming without removing the virus (may be unusual) he would not mind sheltering the virus in his computer.

2.1 The apparent problems reported by the end users

Although the cause of the problem is computer virus, the problem is reported differently by different computer users. For example the user may say “The computer is behaving erratically, some program is not running, the system is hanging, the system is not booting” and so on. The user may say “Everything was well till I worked in the morning, but I don’t know how suddenly my file became corrupt.” Although the problems are described in very different terms, an experienced System Administrator links all these complaints to just one problem, i.e., virus infection.

It will be interesting to analyze the problems reported by the users before going for a solution. Have a look at the types of complaints reported by the end users.

# The computer is behaving erratically, some executable is not running, pen drive is not reading, system is hanging, system is not booting and so on.
# He is facing (virus like) problems in one particular cyber café or in one of his friend’s computer.
# His file is missing or corrupted. So he cannot produce the output in time or he cannot keep to his target.
# His boss will be angry; his job will be in stake.
# The virus may come out of his computer and infect his body.
2.2 Analysis of the Problems Reported by End Users

Each of the above-described problems appears to be different. Let's analyze them one by one.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The computer is behaving erratically, some executable is not running, pen drive is not reading, system is hanging, and system is not booting etc. The user's personal problem while interacting with the computer. He may not be doing any significant work, may be just gaming, but he expects his computer to behave in an orderly way. He is worried of the erratic behavior of his computer. If his pen drive is not reading, he may be happy to get a new pen drive, or if his system is hanging he may be happy to see it repaired or get a new system.</td>
</tr>
<tr>
<td>2</td>
<td>The user is facing (virus like) problems in one particular cyber café or in one of his friend's computer. This situation is different from the above. The user doubts or knows about the virus infection in some specific computers. But he will not bother to heal those computers. He will try to avoid that cyber café and prefer to visit a different cyber café in future.</td>
</tr>
<tr>
<td>3</td>
<td>The user's file is missing or corrupted. So he cannot produce his output in time. This situation is more of target related. The user faces problem because his targets are affected. He will not bother about the virus if he can produce his result within the target period. The user will be happy to get a copy of his lost file, or to extend his submission deadline than wasting time on the virus.</td>
</tr>
<tr>
<td>4</td>
<td>His boss will be angry, as he has not been able to do his work. This situation is slightly different from the above. The user although has lost his work or file because of virus, his worry is the boss or the job. He can manage the situation if the boss is satisfied by other means.</td>
</tr>
<tr>
<td>5</td>
<td>The virus may come out of his computer and infect his body. This problem is purely psychological based on a false notion. When the user knows that the computer virus cannot work upon human body, his problem will be solved.</td>
</tr>
</tbody>
</table>

The above are just the examples and not the complete list of various ways a problem is perceived and addressed. One might have experienced many more interesting manifestations of the same basic virus problem. Thus we see that although the main problem is nothing but the virus in all the above cases, the perceptions of the problem are different. When the objectives are different, the approach to solve a problem can be different.
2.3 Analysis of alternative solutions

In the first case the user may be given a new pen drive to replace the old pen drive which was not reading, or given a new joystick to replace the old joystick which was not functioning, or given an additional 1 GB memory as the previous memory was slow. Although all these solutions will work for a short period, unless the virus is cleaned, the user is likely to face similar problems soon because of virus infection.

In the third situation, the problem is solved by given a backup of the file. The user continues working on his file and his problem is solved. But unless the virus is cleaned from his computer, he may loose his file again or face similar other obstacles to progress his work.

The alternative solution in the third instance is to extend the target date. As the target date is extended, the user gets more time to redo his lost work. But again unless the virus is cleaned he might face similar or other obstacles while doing his work.

The fourth situation is again different. The focus is not on the work rather on the goal of the work, i.e., the job or boss or business. If the boss is happy or job is secured then no care for the virus. However, in such cases, although the user is saved for a short period, the loss will burden on somebody else, such as the boss or the business.

Thus we saw that although the same problem is seen from different angles and apparently solved by different methods, the problem is not actually solved unless the root cause of the problem is analyzed, explored and solved, which is “virus” in this case.

3. Ideal Final Result

Ideal Final Result is the ultimate solution of any problem. Although we saw that various people may adopt various methods to solve a virus problem, it is a fact that the problem will occur again and again unless the actual virus is removed. Hence a better solution is to focus on the core issue, i.e., protecting the computer from virus attack.

However, protection from virus is not always easy. One may have to spend money (for buying anti-virus), spend time (for updating virus definitions), upgrade knowledge (to ensure that the virus is no more), spare resources (for running anti-virus) etc. As per TRIZ concepts, the ideality is calculated by the formula:

\[ \text{Ideality} = \frac{\text{Benefits}}{\text{Costs} + \text{Harms}} \]

To present differently, increased ideality means “increase in benefits”, "decrease in costs" and "decrease in harms". Hence, in this case just virus removal is not a
good solution if the user has to break his head and waste all his time in doing so. Ideally, the computer resources should be protected but without spending money, time and effort, irrespective of whether it is possible or not. Let’s frame some Ideal Final Results:

- **Computer virus should not be created or computer virus should not exist at all**—if no virus then no infection and obviously no virus problem.
- **The computer should never become infected by any computer virus**—even if the viruses are created, the computer (of the user) should never be infected (may be by using some kind of protection?).
- **The user should not spend money on buying anti-virus products nor waste time and energy on installing and maintaining those products**—even if an anti-virus is to be used then it should be free and automated.
- **The user should not waste system resources for running anti-virus**—even if the anti-virus is free of cost, the user should not waste valuable system resources which could affect the system performance and user productivity adversely.

However, as we see in many circumstances it is not possible to achieve all the Ideal final goals to the fullest extent. In many cases we can achieve a goal only partially because of various limitations. In some cases the achievement of one desired goal may reduce the achievement of another desired goal, thus creating a contradiction. Let’s first see what a user can probably do to avoid virus problem and then analyze some of the contradictions involved therein.

### 4. Guidelines to End Users for Solving Virus Problems

- Don’t use external floppies especially for booting because most traditional viruses (such as boot sector viruses) spread through floppies. (Principle-9: Prior Counteraction).
- Don’t use external storage media like floppies, CDs, DVDs, pen drives etc. coming from unknown sources. Carrying information from one computer to another can carry viruses with them (Principle-9: Prior Counteraction).
- If it is so necessary to use floppies, CDs, DVDs, pen drives or other external storage media, then you must first virus-scan that media before using on the computer (Principle-9: Prior Counteraction).
- A malware is generally invited into the machine by web browsing, email and outside storage like pen drive, CD, DVD etc. If we guard these incoming routes we can narrow down the chances of virus infection.
Don’t download programs (such as games, screensavers, freeware etc.) from unreliable websites. Programs from unreliable sources can contain viruses (Principle-9: Prior Counteraction).

If you have to download files for specific need, you must scan the downloaded files through an anti-virus program before running them (Principle-9: Prior Counteraction).

Don’t open emails coming from unknown sources. Don’t automatically open email-attachments. If you are not sure about the attachment, better delete it. Never run attachments from unknown sources (Principle-9: Prior Counteraction).

Use a more secured operating system like UNIX. The robust security feature of UNIX operating system keeps viruses away from the system (Principle-8: Counterweight).

If you are using an unsecured operating system like Windows, install an anti-virus program on your computer (Principle-8: Counterweight).

Users must update their anti-virus software regularly to download the codes for detecting latest threats and the patch security holes. As new viruses, worms and Trojan horses are born on a daily basis, an outdated virus database cannot detect the new viruses (Principle-19: Periodic Action).

Scan the whole computer regularly through the anti-virus program. (Principle-19: Periodic Action).

Configure your anti-virus program to run automatically on system start-up and run at all times as a resident program (Principle-25: Self service, Principle-20: Continuous action).

Enable virus auto-protection - to detect and remove viruses immediately as soon as they are found. Auto protecting and auto healing features of Antivirus software- The residential component remains active in the memory and protects the system from virus attacks at real-time. (Principle-20: Continuous action, Principle-25: Self Service).

Scan the email attachments even if they are from known sources. The attachments might have been infected with malicious code, like Trojan horses, even without knowledge of the sender (Principle-9: Prior Counteraction).

You should enable macro virus protection for Microsoft applications and should never run macros in a document unless you know what they are
supposed to do. There is seldom a good reason to add macros in a document; hence avoiding all macros can be a good policy.

⇒ If a file or email is already infected, then use an anti-virus to disinfect or remove the virus impressions from the file or email (Principle-2: Taking out).

⇒ If it is not possible to disinfect a file or mail then delete that file or mail from the computer so that it does not infect other files (Principle-2: Taking out).

⇒ If a deleted file is important then recover it from the back up. Of course, keep a back up of all your important files so that you can recover in emergency situations (Principle-25: Copying).

⇒ Better keep the backups in optical media like CDs and DVDs, which make it read only and prevent from being infected by any virus.

⇒ One may use different operating systems on different file systems. A virus is not likely to affect both. For example, Windows backups can be put on Linux Platforms and Linux backup can be put on Windows Systems (Reverse application of Principle-33: Homogeneity).

⇒ 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 and attack each other’s activities.

5. Contradictions in solving virus problems

Although an end user is sincere and willing to follow the long list of do’s and don’ts mentioned above, he might fail to follow the same because of various reasons. Moreover, even if he follows them all with sincerity, he may not get a complete relief from the virus problem. There are many more problems that he will still have to face. Let’s analyze some of those complicated situations.

5.1 The classical contradiction

Generally a user never wants his computers to be infected, but the companies selling anti-virus products gain financial incentives for viruses written and spread. The user does not want the virus to be created at all, but the anti-virus companies want some new viruses to be created in order for the survival of their business.
The user neither wants any virus to be created, nor wants to be panic over virus infection, nor wants to pay for the anti-virus software. But the software vendors want some new viruses to be created and want the public to be panic over the threat to pay more for the anti-virus product. In such a case, the loss of one leads to the gain of the other.

5.2 Environmental compulsion

A user may like to adopt all the above precautionary measures in order to prevent virus attacks. But he may be working in an office where his computer is connected to other computers in a LAN. He may have to exchange files with co-workers and connect to Internet for searching reference materials. This working pattern may make his computer a victim of virus attacks unless adequate precautionary measures are taken in the LAN.

5.3 Problem of selection and procurement

Selection and procurement of the right anti-virus product is a problem. One has to consider the price of the product, performance reliability, demand for computer resources etc. A common user may not be sufficiently knowledgeable to evaluate various aspects of anti-virus software in order to choose the right product.

5.4 Problem of updating virus database

Installing an anti-virus product is not enough to prevent viruses. One has to update the virus definition database on a regular basis. But updating the virus database is a boring job and we forget to do this until the virus affects us again.

Possible solutions

⇒ Almost all modern anti-virus programs implement automatic reminders to inform the user that the virus definition database has gone out of date (Principle-25: Self Service).

⇒ Almost all modern anti-virus programs implement self-updating features to connect the user’s computer to the anti-virus developer’s site and download the updated virus definitions from the developer’s website (Principle-25: Self Service).
5.5 Problem of scanning time

As the population of virus increases, the size of the virus definition databases increases and so also 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 a typical user does not like to afford so much of time for this purpose.

If a virus scanner includes less number of virus signatures or less number of detection algorithms then there is a 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 detection algorithms to detect all types of viruses, but at the same we don’t want to afford more time for the scanning operation.

Possible solutions

⇛ One of the solutions 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).

⇛ A complete virus scanning can be done less frequently such as once in a week (Principle-19: Periodic Action).

5.6 Contradiction of virus scanning and system performance

Running an anti-virus consumes significant amount of system resources and affects the system performance negatively. An anti-virus loaded system takes more time to boot, more time to shutdown and runs slow while executing other programs. That’s why many users 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 to sacrifice our valuable system resources to the anti-virus program and make the computer run slow. In other words, we want the anti-virus to scan the computer, but we don't want it to affect our work.

**Possible solutions**

⇒ One solution is to schedule virus scanning during nights or on holidays when we are not working. The self-running feature of the program will automatically run at the pre-scheduled day and/or time (Principle-25: Self Service). (However, this idea may not work for a personal computer which is used anytime irrespective of any day of the week or any hour of the day.)

⇒ Another option is to run the anti-virus when the system is running but we are not working. For example some anti virus programs can be scheduled to run when the system is left idle for certain time (Principle-25: Self Service).

**6. Trends of evolution**

While analyzing the problem of viruses we find certain interesting trends in the method of virus prevention and nature of anti-virus products. These trends can help in predicting more about the situations in future.

1. **Reduced usage of floppies:**
   Booting through floppies -> Developing mechanisms to avoid floppy booting -> CMOS control to avoid floppy seek during booting -> remove floppy drives
   ⇒ From extensive usage of floppy drives to no usage- Reduced usage of floppies prevented viruses which were spreading through floppies

2. **Increasing size of applications:**
   Small size executables to be carried by floppies -> large applications not fitting inside floppies thus needing CDs (Principle-37: Expansion)
   ⇒ As per the above trends, the floppies have gone outdated and most modern computers allow disabling floppy while booting. As the size of applications are becoming larger people can no more carry applications in floppies as they did in 1980’s. As the CDs are used for software distribution and installation, most executable and boot sector viruses are controlled in recent days.
3. Increasing number of viruses -> increasing size of virus definitions.
⇒ The size of virus definition files keeps increasing. A standard virus
definition file is about 100mb during the current time and is supposed to
increase gradually in future.

4. Increasing automation in software application
Automatic reminder-> automatic connection -> automatic downloading and self
configuration.
⇒ The anti-virus softwares are incorporating more and more automations
thereby reducing user intervention.

5. Increasing capacity of the computer hardware
x86 -> Pentium processors -> Pentium dual processors with GHz speed and GBs
of memory
⇒ The increased capacity of the computer hardware reduces the negative
effect of anti-virus software on system performance.

7. Summary
The knowledge on TRIZ helps us analyzing a problem, which is the most
important step in the process of solving the problem. Analysis is important
because the same event may be causing different problems (or benefits) to
different people under different conditions. Some solutions may address the
problem in a short term or narrow perspective but give rise to other problems and
disadvantages. A good solution should be holistic in approach and should lead to
no negative consequences.

When we analyze the problem of computer virus we find that different types of
computer users face different types of problems and seek to different types of
solutions. However, every solution is not ideal. Knowledge of TRIZ helps us
finding an Ideal Solution – that means, while solving the problem of one group
(say e.g., end users) we must ensure that we are not creating problem for
another group (say e.g., administrators) or vice-versa. We will discuss on using
TRIZ for solving virus problems for system administrators and anti-virus
developers in separate articles.

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 Novel 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.