*International Journal For Technological Research In Engineering* *ISSN (Online): 2347 - 4718*
*National Conference on Importance of Inter-disciplinary Studies in Higher Education in the areas of Engineering, Science, Management and Humanities*
*(February – 2018)*

# A COMPUTER VIRUS PROBLEM: USEFUL TECHNOLOGICAL ACHIEVEMENTS

Teena Hadpawat[1], Dipesh Vaya[2]
Department of Computer Science & Engineering, SS College of Engineering, Udaipur, Rajasthan, India

***Abstract: Technology has been developed to help us estimate the safety and effectiveness of anti-virus technology before it is organized. Technology for dealing with known viruses has been very successful and is being extended to deal with previously unknown viruses automatically. There are still important research problem for the solution to any significantly improve ability to deal with the virus problems of the near future. The purpose of this paper is giving the outline the problems, to suggest approaches, and to encourage those interested in research in this field to pursue them. I also observe a number of open research problems in the area of protection from computer viruses. For each problem, I review the work that has been done and suggest possible approaches. There will plenty of important and interesting new problems that must be solved in this field.***
***Keywords: Heuristic detection, HTML and Pro-active approach.***

## I. INTRODUCTION

Some people believe that "virus research" means "analyzing the viruses." But I discuss several important research problems in the area, reviewing what is known on each problem and what remains open. Over the last decade, a single method of detecting computer viruses has nearly covered each others. In this method, a string of bytes was selected from some known virus and the virus scanner looked for that string in files as a way of determining if that file was infected with that virus. After that, more complex techniques were developed which involved looking for various substrings in various parts of the file [1].

All of these techniques have one thing in common; they look for static characteristics of viruses that are already known. In that time, around twenty thousand different viruses were created. Then a question comes up that how a method could deal with already know viruses be effective in an environment with so many new viruses? The reason is simple: over the past ten years, only a few hundred of viruses have actually been seen in real customer events. Even those spread quite slowly on a global scale, typically requiring months or years to become prevalent around the world. This provided the anti-virus industry plenty of time to discover a new virus, derive a cure and make it available for all before many PCs had been infected.

## II. VIRUS DETECTION APPROACHES

Analyzing Heuristic Detection Methods, Distributed Approaches to an Immune System, Pro-Active Approaches to Controlling Viruses and Limited-Function Environments.

A). ANALYZING HEURISTIC DETECTION METHODS: The anti-virus industry also developed Heuristic Detection methods for detecting previously unknown viruses. Heuristics are on the horns of the same problem as any other virus detection method, detecting as many viruses as possible while having as few false positives as possible. But the virus background is changing [2]. No longer are we dealing with simple DOS file and boot viruses. Excel and Word macro viruses are currently the most widespread viruses and Windows NT viruses are starting to be written. We have seen the first attempt at a Java application virus and on the possibility are entirely new kinds of viruses that will take advantage of the Internet to spread it selves. Future kinds of viruses will arise and become widespread much more quickly than in the past. It is important that we have ways to find new instances of these viruses before they spread globally [3]. We may not have the luxury of long-lasting beta periods to help tune our heuristics to eliminate false positives. We certainly can't expect users to be sophisticated enough to tune dozens of different, complex heuristics if the authors of the heuristics are unable to do so. The difficulty is that very small work has been done in this area. Apart from experience with individual heuristics as they are used in individual products, we don't know how they will work or how many problems they will cause. In fact, since few heuristics have been described in the open literature, it is hard to know how good even current heuristics are. To further complicate matters; virtually all heuristics have been developed without regard to the ability to estimate their false positive and false negative rates before they are in wide-scale use. So the challenge is to develop classes of broadly useful heuristics that can be understood analytically before they are deployed and preferably, updated as the threat evolves without requiring entirely new methods [4]. One possible starting point is a heuristic based on traditional signatures but signatures that are common to large classes of already known viruses. Combinations of these signatures can detect variants of viruses in these classes. Probabilities that individual string signatures will cause false positives in non-infected files can be estimated with techniques that have already been developed [5].

B). DISTRIBUTED APPROACHES TO AN IMMUNE SYSTEM: As the Internet becomes the common vehicle for communication in the world and mostly people use it. Digital

  

communication will increase vastly in scope and speed. The new kinds of viruses will take advantage of this increase to spread broadly and much more quickly, than present-day viruses. The viruses will spread to thousands of systems in a matter of minutes and around the world in a matter of hours. When this happens, a digital immune system will be flooded with thousands of instances of an in fact new virus within the first hour and all of these will have come from worried customers who want a solution as quickly as possible.

C). PRO-ACTIVE APPROACHES TO CONTROLLING VIRUSES: Current anti-virus technology relies almost entirely on finding a particular virus before being able to deal with it well. As such, it is largely a reactive technology. Customers are required to update their anti-virus software periodically to deal with new threats. Anti-virus vendors have long desired anti-virus solutions that did not require constant updates. Some anti-virus vendors have gone so far as to claim that their products could detect all possible viruses, never make mistakes, and never need updates, a claim that can be easily shown to be mathematically impossible [6]. In these situations, it would be useful to have pro-active technology that could eliminate, or at least limit, the threat.

D). LIMITED-FUNCTION ENVIRONMENTS: In a given programming environment, it can be verified to be impossible to create or modify programs, then that programming environment is incapable of spreading viruses. The Java "sandbox" model is a good example of this kind of limited function as is the Web markup language HTML. We expect that most major programming environments will remain functional enough to support viruses. There will be limited-function environments are useful and acceptable. It will be very interesting to examine problem areas in which environments can be useful, but limited so as not to support viruses. This is particularly important in the area of mobile code on the Internet, in which programs can move from system to system. A way of preventing these programs from creating the obvious virus threat is vital.

## III. CONCLUSION

We have examined a few open problems in computer virus research. This field is not complete and easily expected problems in the relatively near future will require significant new invention to avoid widespread problems with new viruses. Current anti-virus technology is largely reactive, relying on finding a particular virus before being able to deal with it well. Modern programming environments can give rise to viruses that spread increasingly rapidly, and for which a reactive approach becomes ever more difficult. We conclude that in the near future simple programs will evolve into complex interrelated processes. Computer viruses are extremely dangerous programs that will adapt themselves to the ever changing environment of memory by making copies of it selves. Cloning viruses create exact copies of it selves and attach to other files on the hard drive in an attempt to survive detection.

## REFERENCES

[1] Jeffrey O. Kephart and William C. Arnold, "Automatic Extraction of Computer Virus Signatures," Proceedings of the Fourth Virus Bulletin International Conference, R. Ford (ed.), Jersey, UK, Sept. 7-8, 1994, pp. 179-194.

[2] Gerald Tesauro, Jeffrey O. Kephart and Gregory B. Sorkin, "Neural Networks for Computer Virus Recognition," IEEE Expert, Vol. 11, No. 4, Aug. 1996, pp. 5-6.

[3] J.O. Kephart and S.R. White, "Directed-GraphEpidemiological Models of Computer Viruses," Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California, May 20-22, 1991, pp. 343-359.

[4] Jeffrey O. Kephart, Gregory B. Sorkin, Morton Swimmer and Steve R. White, "Blueprint for a Computer Immune System," Proceedings of the Virus Bulletin International Conference, San Francisco, California, October 1-3, 1997.

[5] E.H. Spafford, "The Internet Worm Program: An Analysis," ACM Computer Communication Review, Vol. 19 No. 1, pp. 17-57, Jan 1989.

[6] Fred Cohen, "Computer Viruses: Theory and Experiment," Computers & Security, Vol. 6, pp. 22-35, 1987.

[7] John F. Morar and David M. Chess, "Web Browsers – Threat or Menace", Proceedings of the Virus Bulletin International Conference; Munich, Germany; October 1998.

  