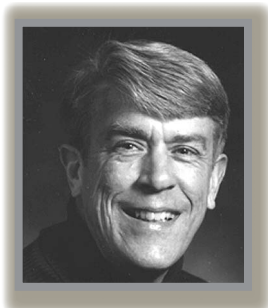


## Viruses Are Beginning to Get to Me!

**Robert L. Glass**

*... in which I oppose the increasing frequency of virus attacks*

I'm not at all sure whether the topic I'm writing about is valid for this column. Loyal Opposition is intended to cover topics where I'm loyal to the field of software engineering but where I oppose some kind of old wives' or husbands' tales that I believe are leading the field in wrong directions.



So what am I opposing in this column? I want to come down firmly against viruses and their increasing frequency. Viruses, I hear you asking? Isn't everybody against viruses?

### **Why write about that?**

Well, yes, I have to admit. But there are a couple of reasons why I want to write about viruses even though no sane person really favors them. Reason 1 is that the news on viruses is disturbing. Their number is dramatically increasing, in spite of all efforts to curb them. I'll return to this reason later.

Reason 2 is related to Reason 1. In recent months, I've been deluged by viruses. You know how statistical realities, such as Reason 1, don't really hit you until your own ox is gored? Well, my own ox is getting gored so frequently that there's virtual blood all over my computer. I'll elaborate on that thought later, also.

But first, there's that loyal opposition thing to deal with. I've been a contrarian for so long

that I still remember a colleague, 50-something years ago, calling me "Zag-Nuts, the Rabble Rouser" (in those days I was inordinately addicted to the Zag-Nuts candy bar). And I persist in contrariness to this day. It wasn't all that long ago that a conference where I was speaking presented me with an honest-to-goodness certificate proclaiming me the "Premier Curmudgeon of Software Practice." (I display that plaque proudly on my office wall!) I delight in questioning the unquestionable, standing in front of steamrollers.

Given all that, why should I waste my time questioning the frequently questioned, standing in front of a parked steamroller? Because, to be honest, "I'm mad as hell, and I'm not going to take this any more." Those virus attacks I spoke of have just plain been getting to me.

### **Let me count the ways**

Getting to me how? Let me explain (this is my discussion of Reason 2). Back in May 2004, my ISP instituted a new virus- and spam-suppressing tool. That, of course, is a very good thing. But, when this tool suppresses a virus or some spam, it sends me a message telling me it did so. Suddenly, I was made very aware of the number of viruses and spam I was getting. And that number was truly ugly. I decided, as a sometime researcher, to gather a little data on them. Here's what I learned.

*Continued on p. 102*

## Classified Advertising

**SUBMISSION:** Rates are \$110.00/column inch. Eight lines per column inch. Send copy one month prior to publication date to: Marian Anderson, *IEEE Software*, Email: [manderson@computer.org](mailto:manderson@computer.org).

**HIGH-PERFORMANCE COMPUTING ENGINEER.** Must have M.S. in Physics or related, 3 yrs exp in job offered or 3 yrs exp in large system administration using UNIX OS, and authorization to work in the U.S. on a permanent basis. Perform installation and assist users with science, engineering, and statistical applications, including parallel compilers and schedulers, optimizing and parallelizing compilers and parallel implementations in clustered and symmetric multi processing environments on multiple architectures. Qualified applicants send resumes to C. Fitch, Notre Dame, Office of Info. Tech, 371 IT Center, Notre Dame, IN 46556. Employment references verified.

**OREGON GRADUATE INSTITUTE, Faculty Openings in Computer Science and Electrical Engineering.** Following an institutional merger in 2001, the Oregon Graduate Institute of Science and Technology (OGI) became one of the four schools of Oregon Health & Science University (OHSU). This merger was based on the vision that computer science and electrical engineering will make major inroads in the life sciences during the coming decade, and that a uniquely close interdisciplinary relationship between a school of medicine and a school of engineering presents opportunities for playing a major role in this revolution. The CSEE Department is looking for individuals who understand not only how computer science and electrical engineering can be applied to the life sciences, but also how this new space of applications presents new and exciting fundamental computational research questions. The Department invites applications for faculty positions at all ranks. Specific areas of interest include, but are not limited to: Image Analysis, Information Retrieval for Heterogeneous Data, Medical Robotics, Computational models of physiology, 3D Visualization, Speech and Language Technologies, Reliable Software for Medical Devices and Systems, Privacy and Security. The typical teaching load in CSE is two quarter courses per year. OGI offers a generous startup package. OGI is located 12 miles west of Portland, Oregon, in the heart of the Silicon Forest. Portland's extensive high-tech community, diverse cultural amenities and spectacular natural surroundings combine to make the quality of life here extraordinary. To learn more about the department, OGI, OHSU and Portland, please visit <http://cse.ogi.edu>. To apply, send a brief description of your research interests, the names of at least three references, and a curriculum vitae with a list of publications to: Chair, Recruiting Committee, Department of Computer Science and Electrical

Engineering, OGI School of Science and Engineering at OHSU, 20000 NW Walker Road, Beaverton, Oregon 97006. Applications sent in before February 15, 2005 will be given preference. All applications will be reviewed. The email address for inquiries is: [csedept@cse.ogi.edu](mailto:csedept@cse.ogi.edu). CSEE has close ties with the recently-formed Department of Biomedical Engineering (BME), including research and teaching collaborations, and jointly appointed faculty. We encourage applicants with active interests in biomedical engineering applications to visit the BME website at <http://bme.ogi.edu>. OGI/OHSU is an Equal Opportunity/Affirmative Action employer. We particularly welcome applications from women, minorities, and individuals with disabilities.

**INDIANA UNIVERSITY SOUTH BEND, Department of Computer and Information Sciences, Assistant Professor of Computer Science/ Informatics.** The Department of Computer and Information Sciences invites applications for one or more tenure track positions for the 2005-2006 academic year. A Ph.D. in computer science or informatics or closely related area is required. Candidates with expertise in areas such as software engineering, computer security, computer networks, or areas within informatics will be given preference. Successful candidates will be expected to teach both undergraduate and graduate courses. Duties include research and teaching eighteen semester hours per year (usually 5 courses). Salary will be competitive. The position comes with an excellent fringe benefit package. Applicants should submit by February 1, 2005, a letter of application, a curriculum vitae, transcripts, and letters from three references to: Dr. Hossein Hakimzadeh, Chair, Department of Computer and Information Sciences, Indiana University South Bend, South Bend, IN 46634. At least one of the letters should address teaching qualifications. These materials may also be faxed to (574) 520-5589, or transmitted by email to [hhakimza@iusb.edu](mailto:hhakimza@iusb.edu). Applications received after the deadline will be considered only if a suitable candidate cannot be found in the initial applicant pool. As an AA/EEO/ADA employer, IUSB encourages women, minorities and the disabled to apply. Additional information about the department may be obtained by visiting our web site at [www.cs.iusb.edu](http://www.cs.iusb.edu) or [www.informatics.iusb.edu](http://www.informatics.iusb.edu).

**DRESDEN UNIVERSITY OF TECHNOLOGY, Master of Computer Science (MCS), Dresden, Germany.** The computer science department of TU Dresden is a top-tier department in Germany. We offer two International Master Programs in computational engineering and computational logic. As a state supported institution, the tuition for these programs is free! The focus of the computational engineering program is on building software-intensive systems. For more information please see <http://www.computational-engineering.de>

## LOYAL OPPOSITION

*Continued from p. 104*

In early fall 2004 I took a one-day sample of my messages. Of the 71 messages I received, 38 (53 percent) were viruses. Another 17 percent were spam. Except, of course, that each virus notification message was a sort of spam, because it was of no other use to me, resulting in a total of 70 percent spam.

What viruses was I receiving? Seventeen of them were a MIME-type message. Thirteen were of the Netsky variety. Four were something called "Kriz." Two more were Mydoom, and another two were Fun Love.

What were the subjects of these viruses? (The subject, of course, is supposed to entice you into opening the message's attachment—in a very real sense, opening Pandora's Box). There was a fascinating variety of subjects, some of them quite clever—"approved," "important," "old times," "corrected," and even one that announced itself as "garbage." But one subject dominated. There were several minor variations on the wording, but the essence was "delivery status notification." The virus claimed to be providing me with information on some prior email that it wanted me to think I had sent.

And where did these viruses come from? Here, I must admit I'm on shaky ground. I suspect that the "sender" identified in these messages is as fictional as the subjects were, or at least that the "sender" tells us nothing useful about who actually sent them. Once again, there was a variety of senders, with names such as "consultants" and "venus" and even "misterbeverlyhills." But, as with subjects, one sender dominated. Almost half the viruses came from some variant of yahoo.com. (Remember that I said I was on shaky ground here? I tend to think that this was a one-day phenomenon, because since that day I haven't noticed such a dominance of yahoo messages.)

## What did I think about all of this?

My first thought was kind of paranoid. I thought that, because I write a

contrarian column, I was being virus-attacked by those who disagree with my stances. In recent months I have, after all, probably offended some people on such subjects as

- The validity of open source approaches (Open source zealots, to be honest, scare me.)
- Whether software project schedule pressure is a good thing (I came down hard against those who think so.)
- Whether traditional software engineering is entirely a good thing (I noted that the agile approaches, some industry approaches, and an increased focus on maintenance could or would be improvements over the “norm.”)
- Whether the theoretician’s view of modeling is worthwhile (I questioned the validity of some fundamental theoretical concepts.)

That’s a lot of potential enemies.

But *IEEE Software*’s editors asked me to rethink that paranoid stance, and it’s just as well they did. Three different virus experts said that my problems are very unlikely to be payback. Most virus attackers, they said, don’t read technical publications such as this one. (One expert even said that he doubts that most virus attackers read anything at all, but I think there was some bitterness there.) If anything is happening here at all, the experts said, it’s simply that my email address is being published with my columns. And given that I like hearing from you readers, that’s a problem I’ll just have to live with!


Recall Reason 1, which says that viruses are increasing in spite of efforts to curb them? Well, I base that statement on a bit of additional research I’ve done since beginning this whole quest. First, there was the feature article in the September 2004 *Consumer Reports*. It was largely about spam, not viruses, but what was depressing was that it reported that the “Can-Spam” law, which went into effect in January 2004, has had no effect whatsoever. (CR says that 47 percent of those surveyed said they were actually getting

more spam since the law was passed.) CR said this was because the law was “flawed.” The law requires consumers to opt out of spam intake, rather than putting the onus on spam senders. (CR pointed out that the approaches to suppressing obnoxious phone calls and peddlers is just the opposite, and that those approaches work just fine.) CR did also deal with the subject of viruses, noting that “virus attacks have flared up again” and suggesting “8 ways to foil viruses and hackers.”

But the really depressing news on viruses came from the Sept. 20 *Wall Street Journal* article “Money Increas-

ingly Is Motive for Computer-Virus Attacks.” More and more often, the article reported, “on-line attackers are ... professional criminals bent on making money.” The article noted a “fourfold increase in the number of new viruses,” the largest increase the tracking company has ever documented. How do they make money? Infecting computers such that they can be used for launching massive spam attacks. Collecting sensitive financial information. Stealing identities and credit card numbers for more immediate financial theft.

**S**o there you have it. I’m mad as hell, I don’t want to take this anymore, and I suppose the truth of the matter is that I can’t do anything about it!

I am curious about something. Has the number of viruses (especially) and spam (less so) that you’re getting increased recently? And what, if anything, are you doing about it? 

**Three virus experts said that my problems are very unlikely to be payback. Most attackers, they said, don’t read technical publications such as this one.**

**Copyright and reprint permission:** Copyright © 2005 by the Institute of Electrical and Electronics Engineers, Inc. All rights reserved. Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limits of US copyright law for private use of patrons those post-1977 articles that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Dr., Danvers, MA 01923. For copying, reprint, or republication permission, write to Copyright and Permissions Dept., IEEE Publications Admin., 445 Hoes Ln., Piscataway, NJ 08855-1331.

**IEEE Software** (ISSN 0740-7459) is published bimonthly by the IEEE Computer Society. IEEE headquarters: Three Park Ave., 17th Floor, New York, NY 10016-5997. IEEE Computer Society Publications Office: 10662 Los Vaqueros Cir., PO Box 3014, Los Alamitos, CA 90720-1314; +1 714 821 8380; fax +1 714 821 4010. IEEE Computer Society headquarters: 1730 Massachusetts Ave. NW, Washington, DC 20036-1903. Subscription rates: IEEE Computer Society members get the lowest rates and choice of media option—\$44/35/57 US print/electronic/combination; go to [www.computer.org/subscribe](http://www.computer.org/subscribe) to order and for more information on other subscription prices. Back issues: \$20 for members, \$121 for nonmembers (plus shipping and handling). This magazine is available on microfiche.

**Postmaster:** Send undelivered copies and address changes to IEEE, Membership Processing Dept., IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855-1331. Periodicals Postage Paid at New York, NY, and at additional mailing offices. Canadian GST #125634188. Canada Post Publications Mail Agreement Number 40013885. Return undeliverable Canadian addresses to PO Box 122, Niagara Falls, ON L2E 6S8, Canada. Printed in the USA.

**Robert L. Glass** is editor emeritus of Elsevier’s *Journal of Systems and Software*, the publisher and editor of the *Software Practitioner* newsletter, and someone “whose head is in the theory of software engineering but whose heart is in its practice.” Contact him at [rglass@indiana.edu](mailto:rglass@indiana.edu) (promise not to tell anyone his email address); he’ll be pleased to hear from you.