1991

Three Letters on Computer Security and Society

Eugene H. Spafford
Purdue University, spaf@cs.purdue.edu

Report Number:
91-088

THREE LETTERS ON COMPUTER SECURITY AND SOCIETY

Eugene H. Spafford

CSD-TR-91-088
December 1991

Three Letters on Computer Security and Society

Purdue Technical Report CSD-TR-91-088

Eugene H. Spafford
Department of Computer Sciences
Purdue University
West Lafayette, IN 47907–1398
spaf@cs.purdue.edu

December 1991

Over the past few years, I have had occasion to write letters to the editors of various journal in response to publication of others' material. Many of these have focused on the interaction of computer security policy with the interests of the computing profession and society at large. I have had several requests for copies of three of these letters, and I have collected all three in one document for ease of distribution.

The enclosed letters were all published in somewhat abbreviated form. Each is presented here, as I wrote it, and before any editing was done for publication.

The first letter was published in the *ACM Forum* section of COMMUNICATIONS OF THE ACM. The issue was #33(10), and appeared in October of 1990.

The second letter was published in SCIENCE NEWS, #139(20), and appeared in the May 18, 1991 issue.

The third letter will be published in THE SCIENCES in the January/February 1991 issue.

Tel: +1 317 494-7825
Fax: +1 317 494-0739
E-mail: spaf@cs.purdue.edu

Department of Computer Sciences
Purdue University
West Lafayette, IN 47907-1398

9 June 1990

Editor
Communications of the ACM
ACM Publications Office
11 West 42nd. St.
New York, NY 10036

To the editor:

The May issue of *Communications* contained a "News Track" account of some of my remarks on hiring known hackers/crackers. I believe the report was derived from my keynote presentation at the 3rd DPMA Virus Workshop, held March 14 in New York. Unfortunately, the item in question did not report the full context of my remarks, and thus the actual intent was obscured.

It is my contention that we should not do business with companies that hire known computer miscreants **because of their criminal escapades.** There are two reasons for this, one grounded in good business sense, and the other grounded in professional ethics.

From a business standpoint, hiring a known computer criminal because of his criminal past is likely to be a liability. The individual has already shown that he (or she) has not felt constrained to respect legal and ethical boundaries, or that he has exhibited poor judgment in not thinking about adverse consequences. What indication is there that such behavior will not be repeated? Furthermore, there is no indication that someone who breaks into a system knows how to protect the system or make it better — he has only shown that he knows how to break in. This is the origin of my "arsonist" statement, quoted in the article. As a customer of such a firm, it is possible I would never be as confident about the integrity of its products as if the hacker had not been hired.

From a professional standpoint, I view the hiring of computer criminals **because of their notoriety or criminal success** to be insulting and unconscionable. Consider that there are many tens of thousands of people who have worked for years to become knowledgeable and responsible members of the profession, and many thousands more currently studying the discipline. What will it mean to them if a criminal is hired to a position of responsibility because of a violation of professional standards? Should the rest of us seek distinguished appointments by spectacular violations of the law? What would it say to all of us that a business would value unethical behavior above a record of accomplishment and professionalism? To ignore or accept

such behavior is to allow our profession to be besmirched. I view it as an insult, and to acquiesce quietly would appear to be a violation of our Code of Professional Conduct.

Note that I am **not** in any way suggesting that we act to prevent these individuals from being employed in a computing-related profession. If the individual involved has the necessary training and background, and is as qualified as other applicants, then he should be treated as any other individual applying for a position. This is especially true once an individual has served a sentence for his crimes. Robert T. Morris, for instance, has demonstrated a keen interest and more than moderate facility with computers. To protest his taking a computing-related job would be to unfairly embellish the sentence already imposed by the federal court. We should not seek to second-guess our legal system, nor extract revenge above and beyond the punishment already meted out. To do so would be petty and mean-spirited.

In summary, my remarks at the Virus Workshop argued that we should protest if businesses reward these offenders for their actions; I did not mean to suggest that we forbid these individuals from ever working in computing-related jobs. I also did not suggest that we devise any additional punishment for Mr. Morris. He has been sentenced for his crime, and it is not for us to seek to augment his punishment. It is time for all of us to move on and put that whole incident behind us.

Regards,

Eugene H. Spafford
Assistant Professor

Tel: +1 317 494-7825
Fax: +1 317 494-0739
E-mail: spaf@cs.purdue.edu

Department of Computer Sciences
Purdue University
West Lafayette, IN 47907-1398

21 February 1991

Mr. Patrick Young, Editor
Science News
1719 N. St. NW
Washington, DC 20036

Dear Mr. Young:

In the February 9 *Letters* column, Professor Bruce Henricksen made some comments about access to computing systems that are often made by others who do not understand the full scope of what is stored on computers. His letter was printed without a response, and I believe a response is warranted.

Professor Henricksen implies that access to "nonmilitary, unclassified" systems should be unrestricted; he cites the models of the library and the university for the sharing of ideas. Unfortunately, such open access is something most people would *not* want — open access to their medical records, their bank records, their credit histories, their income tax histories, or their police records would not be something the average person would appreciate. At universities, student grades and faculty personnel files are not open records, nor are results of prepublication research — all of which are often kept on computers. At the library, librarians closely guard records of what items individuals have checked out for personal use. In industry, trade secrets, customer mailing lists, accounting and purchasing records, and personnel evaluations are all kept confidential. The list can be extended. The list can be extended to include many more "nonmilitary, unclassified" records that have a legitimate privacy requirement.

Another problem with unrestricted access to arbitrary systems is the difficulty of knowing when access is merely to browse, and when it is a prelude (or attempt) at something less benign. As someone who works in computer security research, I can assure you that access is the first step in most cases of theft, sabotage, and other forms of computer security threat. Restricting access is the best way to prevent malicious individuals from slipping into a system under the guise of innocent curiousity.

In an ideal world, Professor Henricksen's view of open access to computers might well be the ideal. Unfortunately, we do not have an ideal world. The need for (and rights to) privacy, and the need to keep systems secure from tampering mean that we must continue to restrict access

to a significant number of our computer systems.

Regards,

Eugene H. Spafford
Assistant Professor

Tel: +1 317 494-7825
Fax: +1 317 494-0739
E-mail: spaf@cs.purdue.edu

Department of Computer Sciences
Purdue University
West Lafayette, IN 47907-1398

30 September 1991

Mr. Peter G. Brown, Editor
The Sciences
622 Broadway
New York, NY 10012

Dear Mr. Brown:

Although you invited me to respond in 500 words or less, I find that I cannot make an adequate response within that constraint. I believe you have done a grave disservice to your readers and to the community with the publication of Fred Cohen's article, and this letter expresses the reasons why I believe that.

I began to read the recent article by Dr. Fred Cohen [1] with considerable interest. Dr. Cohen is a pioneer in the field of computer virus research, and I have found many of his writings quite thought-provoking. Unfortunately, by the time I finished his article, I was quite dismayed. I believe that Dr. Cohen has failed to adequately consider both the practicality and the ethics of his proposal.

First of all, I believe that there is an obvious conflict of interest involved when the vendor of a computer virus prevention product sponsors a contest soliciting the development of new viruses. I am further troubled by the lack of a list of the judges of the contest and the criteria for winning. I will not discuss these points further, however, as they are minor matters compared with my main concern: I believe that the writing of computer viruses is unethical, [2–3] and to encourage their development in an unsupervised manner is likewise unethical.

Computer viruses spread without the informed consent of the owner of the software ("host") they "infect," and they are usually not limited in their spread, in time or space. If scientists were to experiment with organic viruses capable of infecting humans and possessing these same properties, we would likely be taking vigilante action against them, contest or no. Encouraging the general populace to develop organic viruses would bring about widespread condemnation; yet, oddly, encouraging the development of computer viruses leads to publication in a journal.

To his credit, Dr. Cohen explicitly prohibits viruses that exhibit the above two dangerous properties from being eligible for his contest. However, many viruses cause damage because of flaws within the code, or unexpected properties of their target computing environment; examples include the "Stoned" virus for IBM PCs, and the "WDEF" virus for Apple Macintoshes (cf., [3–

5]). What will be the attitude of the community as a whole if a new destructive virus appears on the scene because of a bug in the software meant to contain it? What if something similar to Robert T. Morris's Internet Worm were to be discovered and explained as a buggy test version intended for Cohen's contest?

This brings me to another argument with Dr. Cohen's article: we disagree about the definition of the term "computer virus." Cohen describes Morris's Internet program as a "virus," while I (and others) would define it as a "worm." [6–7] Morris's program did not alter existing software to include a copy of itself as do viruses. His program was no more a virus than is a compiler (suggesting an interesting class of potential submissions to the contest). In fact, if we intuit a definition of "contest-acceptable virus" from Cohen's article to be something that spreads from system to system, that requires permission to install itself, and has limited potential for spread (like the Worm), it is no longer clear we are speaking about viruses at all!

Harold Thimbleby of Stirling University, Scotland and Ian Witten of Calgary University, Canada have done extensive work on software that would meet the above intuited definition of a computer virus. They have developed some very sophisticated self-propagating applications, including self-updating databases with window-based interfaces. [8–9] It is not at all clear that the community recognizes these as viruses. Professor Thimbleby himself has chosen to call them "liveware" to make the distinction clear. I am surprised that Dr. Cohen is unfamiliar with their work and did not cite it in his *Sciences* article; it would be a clear favorite if it were to be entered in the ASP contest. However, it also serves to illustrate how something that might win the contest is not likely to be viewed as a "virus" by the community of researchers.

This brings me to the second of my two major objections to Cohen's article and contest. I believe that his underlying thesis is flawed: I do not believe that there are any *practical* "good" viruses. During the Second Conference on Artificial Life, held in Santa Fe in 1990 (cf. [10]), I was on a panel discussing computer viruses. Russell Brand, another panelist, made the observation that there is nothing that can be done by a computer virus that cannot be done more efficiently and generally by other means. This observation was debated by the panel, and discussed extensively by others since that time. To my knowledge, everyone involved in these discussions now believes that is a true statement.

Consider that a computer virus is nothing other than a program coupled with code to transport and install itself as part of existing software. It will be more difficult (or impossible) than a stand-alone program to update for new releases, customize, and maintain. A virus will also be more difficult to write and test for correctness than will a stand-alone program because of its interaction with its environment. Viruses are simply not the most practical or efficient approach to any particular task. His example in the article of the billing system demonstrates an inadequacy in the data model used and tools available, and not the superiority of using a quasi-virus. Even the example Cohen gave in his PhD dissertation of a compression virus would be better served by a well-written stand-alone program over which the user has more control. I believe that any attempt made to promote "useful" viruses involves a contradiction of the word "useful," assuming that "useful" does not also imply "malicious."

To return to my first fundamental objection (and the one I feel most strongly about) – the impropriety of encouraging virus authorship. We have been battling computer viruses for five years now, and the indications are that the problem is growing exponentially (cf. [11–12]). Computer viruses — even those intended to be harmless, and limited in scope and duration — continue to cause untold amounts of damage to computer systems. For someone of Dr. Cohen's reputation within the field to actually *promote* the uncontrolled writing of any kind of virus, even with his stated stipulations, is to act irresponsibly and immorally. To act in such a manner is likely to encourage the development of yet more viruses "in the wild" by muddling the ethics and dangers involved. It will reinforce the attitude that there may be some benefit to be gained from writing viruses (when there is as yet absolutely no clear indication that such is the case), and may encourage people to begin uncontrolled experiments with viruses they might not otherwise have undertaken. We have seen cases already where well-trained virus researchers have accidentally released experimental computer viruses into the population; to encourage amateurs to also engage in risky behavior that may lead to similar or worse results is quite appalling. It is my fond hope that no one attempts to enter Dr. Cohen's contest, and that he quickly recognizes the dangers and cancels it.

A few decades ago, physicists talked about peaceful uses of atomic weapons, such as blasting out canals and destroying threatening icebergs. They were attempting, in good faith, to put a better moral cast on their research. Thankfully, none of them offered money in a contest for the best demonstration of such an application! Alfred Nobel, horrified at the use to which his invention of stabilized explosives were being put, did not establish a contest for the best peaceful use of dynamite. Instead, he established world-reknowned awards for research in peaceful pursuits, funded by the income from his discovery. It is quite unfortunate that ASP and Dr. Cohen could not have taken a similar approach with their $1000 prize. They could have made a powerful statement about responsible behavior, but instead have increased the danger to the community and generated doubts about their own motivations.

Eugene H. Spafford
Assistant Professor

References

[1] *Friendly Contagion: Harnessing the Subtle Power of Computer Viruses*, by Fred Cohen, THE SCIENCES, Sep/Oct 1991, pp. 22–28.

[2] *Computer Viruses and Ethics*, by Eugene H. Spafford, in COLLEGIATE MICROCOMPUTER, special issue on the Rose-Hullman/GTE Computing and Ethics Seminars, *to appear*, 1992.

[3] COMPUTER VIRUSES: DEALING WITH ELECTRONIC VANDALISM AND PROGRAMMED THREATS, by Eugene H. Spafford, Kathleen A. Heaphy and David J. Ferbrache, ADAPSO, 1989.

[4] ROGUE PROGRAMS: VIRUSES, WORMS, AND TROJAN HORSES, edited by Lance J. Hoffman, Van Nostrand Reinhold, 1990.

[5] COMPUTERS UNDER ATTACK: INTRUDERS, WORMS AND VIRUSES, edited by Peter J. Denning, ACM Press/Addison-Wesley, 1990.

[6] *What is A Computer Virus?*, by Eugene H. Spafford, Kathleen A. Heaphy and David J. Ferbrache, Chapter 2 in [4].

[7] *An Analysis of the Internet Worm*, by Eugene H. Spafford, in LECTURE NOTES IN COMPUTER SCIENCE #387, Springer-Verlag, 1989.

[8] *Bugs, Viruses and Liveware: Collected Papers* by Harold Thimbleby, technical report of the Department of Computer Science, Stirling University, Scotland, 1990.

[9] *Liveware: A New Approach to Sharing Data in Social Networks*, by I. H. Witten, H. W. Thimbleby, G. F. Coulouris, and S. Greenberg, in INTERNATIONAL JOURNAL OF MAN-MACHINE STUDIES, 1990.

[10] ARTIFICIAL LIFE II, STUDIES IN THE SCIENCES OF COMPLEXITY, VOLUME XII, edited by D. Farmer, C. Langton, S. Rasmussen, and C. Taylor, Addison-Wesley, 1992.

[11] *Virus Trends: Up, Up, Up* by David Stang in NATIONAL COMPUTER SECURITY ASSOCIATION NEWS, 2(2), March/April 1991.

[12] *The Kinetics of Computer Virus Replication* by Peter S. Tippet in PROCEEDINGS OF THE FOURTH ANNUAL DPMA COMPUTER VIRUS & SECURITY CONFERENCE, New York, March 1991.