Professor Spafford's involvement with software engineering and security include positions on the editorial boards of the journals *Computing Systems* and the *International Journal of Computer and Software Engineering*. He is coauthor of the books *Practical Unix Security*, published by O'Reilly and Associates (1991), and of *Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats*, ADAPSO (1989). He has contributed chapters to many other books on computer security and professional ethics, and has spoken internationally at conferences, symposia, and colloquia on these issues.

Dr. Spafford is a member of the Association for Computing Machinery (ACM). He is chair of the ACM Self-Assessment Committee, and is a member of the ACM Education Board. He is also a Senior Member of the IEEE and Computer Society of the IEEE, and a member of the Usenix Association.

[11] Bill Landreth. *Out of the Inner Circle: a Hacker's Guide to Computer Security.* Microsoft Press, New York, 1984.

[12] Adelaide, John Perry Barlow, Robert Jacobson Bluefire, Russell Brand, Clifford Stoll, Dave Hughes, Frank Drake, Eddie Joe Homeboy, Emmanuel Goldstein, Hank Roberts, Jim Gasperini JIMG, Jon Carroll JRC, Lee Felsenstein, Tom Mandel, Robert Horvitz RH, Richard Stallman RMS, Glenn Tenney, Acid Phreak, and Phiber Optik. Is computer hacking a crime? *Harper's Magazine*, 280(1678):45–57, March 1990.

[13] Richard Stallman. *GNU EMacs Manual*, chapter The GNU Manifesto, pages 239–248. Free Software Foundation, 1986.

[14] M. Douglas McIlroy. Unsafe at any price. *Information Technology Quarterly*, IX(2):21–23, 1990.

[15] P. J. Denning, D. E. Comer, D. Gries, M. C. Mulder, A. Tucker, A. J. Turner, and P. R. Young. Computing as a discipline. *Communications of the ACM*, 32(1):9–23, January 1989.

[16] Allen B. Tucker, Bruce H. Barnes, Robert M. Aiken, Keith Barker, Kim B. Bruce, J. Thomas Cain, Susan E. Conry, Gerald L. Engel, Richard G. Epstein, Doris K. Lidtke, Michael C. Mulder, Jean B. Rogers, Eugene H. Spafford, and A. Joe Turner. Computing curricula 1991, 1991. Published by the IEEE Society Press.

About the Author

Gene Spafford received a Ph.D. in 1986 from the School of Information and Computer Sciences at Georgia Institute of Technology. In 1987, Professor Spafford joined the faculty of the Department of Computer Sciences at Purdue University. He is an active researcher with the NSF/Purdue/University of Florida Software Engineering Research Center (SERC) there.

Besides a continuing widely-known and respected involvement in the Usenet and other forms of electronic conferencing, Dr. Spafford does research on issues relating to increasing the reliability of computer systems, and the consequences of computer failures. This includes work with computer security, software testing and debugging, and issues of liability and professional ethics.

need to develop and act according to some shared ethical values. The members of society need to be educated so that they understand the importance of respecting the privacy and ownership of data. If locks and laws were all that kept people from robbing houses, there would be many more burglars than there are now; the shared mores about the sanctity of personal property are an important influence in the prevention of burglary. It is our duty as informed professionals to help extend those mores into the realm of computing.

References

[1] Donn Seeley. A tour of the worm. In *Proceedings of the Winter 1989 Usenix Conference*. The Usenix Association, January 1989.

[2] Eugene H. Spafford. The internet worm: Crisis and aftermath. *Communications of the ACM*, 32(6):678–698, June 1989.

[3] Eugene H. Spafford. An analysis of the internet worm. In C. Ghezzi and J. A. McDermid, editors, *Proceedings of the 2nd European Software Engineering Conference*, pages 446–468. Springer-Verlag, September 1989.

[4] Clifford Stoll. *Cuckoo's Egg*. Doubleday, New York, NY, 1989.

[5] John Schwartz. The hacker dragnet. *Newsweek*, 65(18), April 1990.

[6] Eugene H. Spafford, Kathleen A. Heaphy, and David J. Ferbrache. *Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats*. ADAPSO, Arlington, VA, 1989.

[7] Lance Hoffman, editor. *Rogue Programs: Viruses, Worms, and Trojan Horses*. Van Nostrand Reinhold, 1990.

[8] David J. Stang. *Computer Viruses*. National Computer Security Association, Washington, DC, 2nd edition edition, March 1990.

[9] Peter J. Denning, editor. *Computers Under Attack: Intruders, Worms, and Viruses*. ACM Books/Addison-Wesley, 1991.

[10] Bruce J. Baird, Lindsay L. Baird Jr., and Ronald P. Ranauro. The moral cracker? *Computers and Security*, 6(6):471–478, December 1987.

all the effects resulting from such an act.

Of course, I have not discussed every possible reason for a break-in. There might well be an instance where a break-in might be necessary to save a life or to preserve national security. In such cases, to perform one wrong act to prevent a greater wrong may be the right thing to do. It is beyond the scope or intent of this paper to discuss such cases, especially as no known hacker break-ins have been motivated by such instances.

Historically, computer professionals as a group have not been overly concerned with questions of ethics and propriety as they relate to computers. Individuals and some organizations have tried to address these issues, but the whole computing community needs to be involved to address the problems in any comprehensive manner. Too often, we view computers simply as machines and algorithms, and we do not perceive the serious ethical questions inherent in their use.

When we consider, however, that these machines influence the quality of life of millions of individuals, both directly and indirectly, we understand that there are broader issues. Computers are used to design, analyze, support, and control applications that protect and guide the lives and finances of people. Our use (and misuse) of computing systems may have effects beyond our wildest imagining. Thus, we must reconsider our attitudes about acts demonstrating a lack of respect for the rights and privacy of other people's computers and data.

We must also consider what our attitudes will be towards future security problems. In particular, we should consider the effect of **widely** publishing the source code for worms, viruses, and other threats to security. Although we need a process for rapidly disseminating corrections and security information as they become known, we should realize that widespread publication of details will imperil sites where users are unwilling or unable to install updates and fixes.[3] Publication should serve a useful purpose; endangering the security of other people's machines or attempting to force them into making changes they are unable to make or afford is not ethical.

Finally, we must decide these issues of ethics as a community of professionals and then present them to society as a whole. No matter what laws are passed, and no matter how good security measures might become, they will not be enough for us to have completely secure systems. We also

[3] To anticipate the oft-used comment that the "bad guys" already have such information: not every computer burglar knows or will know *every* system weakness — unless we provide them with detailed analyses.

3.5 The Social Protector Argument

One last argument, more often heard in Europe than the U.S. is that hackers break into systems to watch for instances of data abuse and to help keep "Big Brother" at bay. In this sense, the hackers are protectors rather than criminals. Again, this assumes that the ends justify the means. It also assumes that the hackers are actually able to achieve some good end.

Undeniably, there is some misuse of personal data by corporations and by the government. The increasing use of computer-based record systems and networks may lead to further abuses. However, it is not clear that breaking into these systems will aid in righting the wrongs. If anything, it will cause those agencies to become even more secretive and use the break-ins as an excuse for more restricted access. Break-ins and vandalism have not resulted in new open-records laws, but they have resulted in the introduction and passage of new criminal statutes. Not only has such activity failed to deter "Big Brother," but it has also resulted in significant segments of the public urging more laws and more aggressive law enforcement — the direct opposite of the supposed goal.

It is also not clear that these are the individuals we want "protecting" us. We need to have the designers and users of the systems — trained computer professionals — concerned about our rights and aware of the dangers involved with the inappropriate use of computer monitoring and recordkeeping. The threat is a relatively new one, as computers and networks have become widely used only in the last few decades. It will take some time for awareness of the dangers to spread throughout the profession. Clandestine efforts to breach the security of computer systems do nothing to raise the consciousness of the appropriate individuals. Worse, they associate that commendable goal (heightened concern) with criminal activity (computer break-ins), discouraging proactive behavior by the individuals in the best positions to act in our favor. Perhaps it is in this sense that computer break-ins and vandalism are most unethical and damaging.

4 Concluding Remarks

I have argued here that computer break-ins, even when no obvious damage results, are unethical. This must be the considered conclusion even if the result is an improvement in security, because the activity itself is disruptive and immoral. The results of the act should be considered separately from the act itself, especially when we consider how difficult it is to understand

education in a cost-effective manner. Some authors of computer viruses claim that their creations are intended to be harmless, and that they are simply learning how to write complex programs.

There are many problems with these arguments. First, as an educator, I claim that writing vandalware or breaking into a computer and looking at the files has almost nothing to do with computer education. Proper education in computer science and engineering involves intensive exposure to fundamental aspects of theory, abstraction, and design techniques. Browsing through a system does not expose someone to the broad scope of theory and practice in computing, nor does it provide the critical feedback so important to a good education (cf. [15, 16]). Neither does writing a virus or worm program and releasing it into an unsupervised environment provide any proper educational experience. By analogy, stealing cars and joyriding does not provide one with an education in mechanical engineering, nor does pouring sugar in the gas tank.

Furthermore, individuals "learning" about a system cannot know how everything operates and what results from their activities. Many systems have been damaged accidentally by ignorant (or careless) intruders; most of the damage from computer viruses (and the Internet Worm) appear to be caused by unexpected interactions and program faults. Damage to medical systems, factory control, financial information, and other computer systems could have drastic and far-ranging effects that have nothing to do with education, and could certainly not be considered harmless.

A related refutation of the claim has to do with knowledge of the extent of the intrusion. If I am the person responsible for the security of a critical computer system, I cannot assume that *any* intrusion is motivated solely by curiosity and that nothing has been harmed. If I know that the system has been compromised, I must fear the worst and perform a complete system check for damages and changes. I cannot take the word of the intruder, for any intruder who actually caused damage would seek to hide it by claiming that he or she was "just looking." In order to regain confidence in the correct behavior of my system, I must expend considerable energy to examine and verify every aspect of it.

Apply our universal approach to this situation and imagine if this "educational" behavior was widespread and commonplace. The result would be that we would spend all our time verifying our systems and never be able to trust the results fully. Clearly, this is not good, and thus we must conclude that these "educational" motivations are also unethical.

have prevented it from being applied to true computer viruses, [2] The passage of similar well-intentioned but poorly-defined legislation could have a major negative effect on the computing profession as a whole.

3.3 The Idle System Argument

Another argument put forth by system hackers is that they are simply making use of idle machines. They argue that because some systems are not used at any level near their capacity, the hacker is somehow entitled to use them.

This argument is also flawed. First of all, these systems are usually not in service to provide a general-purpose user environment. Instead, they are in use in commerce, medicine, public safety, research, and government functions. Unused capacity is present for future needs and sudden surges of activity, not for the support of outside individuals. Imagine if large numbers of people without a computer were to take advantage of a system with idle processor capacity: the system would quickly be overloaded and severely degraded or unavailable for the rightful owners. Once on the system, it would be difficult (or impossible) to oust these individuals if sudden extra capacity was needed by the rightful owners. Even the largest machines available today would not provide sufficient capacity to accommodate such activity on any large scale.

I am unable to think of any other item that someone may buy and maintain, only to have others claim a right to use it when it is idle. For instance, the thought of someone walking up to my expensive car and driving off in it simply because it is not currently being used is ludicrous. Likewise, because I am away at work, it is not proper to hold a party at my house because it is otherwise not being used. The related positions that unused computing capacity is a shared resource, and that my privately-developed software belongs to everyone, are equally silly (and unethical) positions.

3.4 The Student Hacker Argument

Some trespassers claim that they are doing no harm and changing nothing — they are simply learning about how computer systems operate. They argue that computers are expensive, and that they are merely furthering their

[2] It provided penalties only in cases where **programs** were introduced into computer systems; a computer virus is a segment of code attached to an existing program that modifies other programso