# Are Computer Hacker Break-ins Ethical?*

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

**Abstract**

Recent incidents of unauthorized computer intrusion have brought about discussion of the ethics of breaking into computers. Some individuals have argued that as long as no significant damage results, break-ins may serve a useful purpose. Others counter with the expression that the break-ins are almost always harmful and wrong.

This article lists and refutes many of the reasons given to justify computer intrusions. It is the author's contention that break-ins are ethical only in extreme situations, such as a life-critical emergency. The article also discusses why no break-in is "harmless."

## 1 Introduction

On November 2, 1988, a program was run on the Internet that replicated itself on thousands of machines, often loading them to the point where they were unable to process normal requests. [1, 2, 3] This *Internet Worm* program was stopped in a matter of hours, but the controversy engendered by its release raged for years. Other recent incidents, such as the "wily hackers"[1] tracked by Cliff Stoll [4], the "Legion of Doom" members who are alleged to have stolen telephone company 911 software [5], and the growth of the computer virus problem [6, 7, 8, 9] have added to the discussion. What constitutes improper access to computers? Are some break-ins ethical? Is there such a thing as a "moral hacker"?[10]

It is important that we discuss these issues. The continuing evolution of our technological base and our increasing reliance on computers for critical tasks suggests that future incidents may well



[1] I realize that many law-abiding individuals consider themselves *hackers* — a term formerly used as a compliment. The press and general public have co-opted the term, however, and it is now commonly viewed as a pejorative. Here, I will use the word as the general public now uses it.

have more serious consequences than those we have seen to date. With human nature as varied and extreme as it is, and with the technology as available as it is, we must expect to experience more of these incidents.

In this article, I will introduce a few of the major issues that these incidents have raised, and present some arguments related to them. For clarification, I have separated a few issues that often have been combined when debated; it is possible that most people are in agreement on some of these points once they are viewed as individual issues.

## 2 What is Ethical?

Webster's Collegiate Dictionary defines ethics as: "The discipline dealing with what is good and bad and with moral duty and obligation." More simply, it is the study of what is *right* to do in a given situation—what we *ought* to do. Alternatively, it is sometimes described as the study of what is *good* and how to achieve that good. To suggest whether an act is right or wrong, we need to agree on an ethical system that is easy to understand and apply as we consider the ethics of computer break-ins.

Philosophers have been trying for thousands of years to define right and wrong, and I will not make yet another attempt at such a definition. Instead, I will suggest that we make the simplifying assumption that we can judge the ethical nature of an act by applying a deontological assessment: regardless of the effect, is the act itself ethical? Would we view that act as sensible and proper if **everyone** were to engage in it? Although this may be too simplistic a model (and it can certainly be argued that other ethical philosophies may also be applied), it is a good first approximation for purposes of discussion. If you are unfamiliar with any other formal ethical evaluation method, try applying this assessment to the points I raise later in this paper. If the results are obviously unpleasant or dangerous in the large, then they should be considered unethical as individual acts.

Note that this philosophy assumes that *right* is determined by actions and not by results. Some ethical philosophies assume that the ends justify the means; our current society does not operate by such a philosophy, although many individuals do. As a society, we profess to believe that "it isn't whether you win or lose, it's how you play the game." This is why we are concerned with issues of due process and civil rights, even for those espousing repugnant views and committing heinous acts. The process is important no matter the outcome, although the outcome may help to resolve a choice between two almost equal courses of action.

Philosophies that consider the results of an act as the ultimate measure of good are often impossible to apply because of the difficulty in understanding exactly what results from any arbitrary activity. Consider an extreme example: the government orders a hundred cigarette smokers, chosen at random, to be beheaded on live nationwide television. The result might well be that many hundreds of thousands of other smokers would quit "cold turkey," thus prolonging their lives. It might also prevent hundreds of thousands of people from ever starting to smoke, thus improving the health and longevity of the general populace. The health of millions of other people would improve as they would no longer be subjected to secondary smoke, and the overall impact on the environment would be very favorable as tons of air and ground pollutants would no longer be released by smokers or tobacco companies.

Yet, despite the great good this might hold for society, everyone, except for a few extremists, would condemn such an *act* as immoral. We would likely object even if only one person was executed. It would not matter what the law might be on such a matter; we would not feel that the act was morally correct, nor would we view the ends as justifying the means.

Note that we would be unable to judge the morality of such an action by evaluating the results, because we would not know the full scope of those results. Such an act might have effects favorable or otherwise, on issues of law, public health, tobacco use, and daytime TV shows for decades or centuries to follow. A system of ethics that considered primarily only the results of our actions would not allow us to evaluate our current activities at the time when we would need such guidance; if we are unable to discern the appropriate course of action prior to its commission, then our system of ethics is of little or no value to us. To obtain ethical guidance, we must base our actions primarily on evaluations of the actions and not on the possible results.

More to the point of this paper, if we attempt to judge the morality of a computer break-in based on the sum total of all future effect, we would be unable to make such a judgement, either for a specific incident or for the general class of acts. In part, this is because it is so difficult to determine the long-term effects of various actions, and to discern their causes. We cannot know, for instance, if increased security awareness and restrictions are better for society in the long-term, or whether these additional restrictions will result in greater costs and annoyance when using computer systems. We also do not know how many of these changes are directly traceable to incidents of computer break-ins.

One other point should be made here: it is undoubtedly possible to imagine scenarios where a computer break-in would be considered to be the preferable course of action. For instance, if vital medical data were on a computer and necessary to save someone's life in an emergency, but the authorized users of the system cannot be located, breaking into the system might well be considered the right thing to do. However, that action does not make the break-in ethical. Rather, such situations occur when a greater wrong would undoubtedly occur if the unethical act were not committed. Similar reasoning applies to situations such as killing in self-defense. In the following discussion, I will assume that such conflicts are not the root cause of the break-ins; such situations should very rarely present themselves.

## 3 Motivations

Individuals who break into computer systems or who write *vandalware* usually use one of a few rationalizations for their actions. (See, for example, [11] and the discussion in [12].) Most of these individuals would never think to walk down a street, trying every door to find one unlocked, then search through the drawers of the furniture inside. Yet, these same people seem to give no second thought to making repeated attempts at guessing passwords to accounts they do not own, and once on to a system, browsing through the files on disk.

These computer burglars often present the same reasons for their actions in an attempt to rationalize their activities as morally justified. I present and refute some of the most commonly used ones in what follows; motives involving theft and revenge are not uncommon, and their moral nature is simple to discern, so I shall not include them here.

### 3.1 The Hacker Ethic

Many hackers argue that they follow an ethic that both guides their behavior and justifies their break-ins. This hacker ethic states, in part, that all information should be free.[10] This view holds that information belongs to everyone, and there should be no boundaries or restraints to prevent anyone from examining information. Richard Stallman states much the same thing in his GNU Manifesto.[13] He and others have further stated in various forums that if information is free, it logically follows that there should be no such thing as intellectual property, and no need for security.

What are the implications and consequences of such a philosophy? First and foremost, it raises some disturbing questions of privacy. If all information is (or should be) free, then privacy is no longer a possibility. For information to be free to everyone, and for individuals to no longer be able to claim it as property, means that anyone may access the information if they please. Furthermore, as it is no longer property of any individual, that means that anyone can alter the information. Items such as bank balances, medical records, credit histories, employment records, and defense information all cease to be controlled. If someone controls information and controls who may access it, the information is obviously not free. But without that control, we would no longer be able to trust the accuracy of the information.

In a perfect world, this lack of privacy and control might not be a cause for concern. However, if all information were to be freely available and modifiable, imagine how much damage and chaos would be caused in our real world by such a philosophy! Our whole society is based on information whose accuracy must be assured. This includes information held by banks and other financial institutions, credit bureaus, medical agencies and professionals, government agencies such as the IRS, law enforcement agencies, and educational institutions. Clearly, treating all their information as "free" would be unethical in any world where there might be careless and unethical individuals.

Economic arguments can be made against this philosophy, too, in addition to the overwhelming need for privacy and control of information accuracy. Information is not universally free. It is held as property because of privacy concerns, and because it is often collected and developed at great expense. Development of a new algorithm or program, or collection of a specialized database, may involve the expenditure of vast sums of time and effort. To claim that it is free or should be free is to express a naive and unrealistic view of the world. To use this as a justification for computer break-ins is clearly unethical. Although not all information currently treated as private or controlled as proprietary needs such protection, that does not justify unauthorized access to it or to any other data.

### 3.2 The Security Arguments

These arguments are the most common ones within the computer community. One common argument was the same one used most often by people attempting to defend the author of the Internet Worm program in 1988: break-ins illustrate security problems to a community that will otherwise not note the problems.

In the Worm case, one of the first issues to be discussed widely in Internet mailing lists dealt with the intent of the perpetrator — exactly why the worm program had been written and released. Explanations put forth by members of the community ranged from simple accident to the actions of a sociopath. A common explanation was that the Worm was designed to illustrate security defects to a community that would not otherwise pay attention. This was not supported by the testimony during the author's trial, nor is it supported by past experience of system administrators.

The Worm author, Robert T. Morris, appears to have been well-known at some universities and major companies, and his talents were generally respected. Had he merely explained the problems or offered a demonstration to these people, he would have been listened to with considerable attention. The month before he released the Worm program on the Internet, he discovered and disclosed a bug in the file transfer program *ftp*; news of the flaw spread rapidly, and an official fix was announced and available within a matter of weeks. The argument that no one would listen to his report of security weaknesses is clearly fallacious.

In the more general case, this security argument is also without merit. Although some system administrators might have been complacent about the security of their systems before the Worm incident, most computer vendors, managers of government computer installations, and system administrators at major colleges and universities have been attentive to reports of security problems. People wishing to report a problem with the security of a system need not exploit it to report it. By way of analogy, one does not set fire to the neighborhood shopping center to bring attention to a fire hazard in one of the stores, and then try to justify the act by claiming that firemen would otherwise never listen to reports of hazards.

The most general argument that some people make is that the individuals who break into systems are performing a service by exposing security flaws, and thus should be encouraged or even rewarded. This argument is severely flawed in several ways. First, it assumes that there is some compelling need to force users to install security fixes on their systems, and thus *computer burglars* are justified in "breaking and entering" activities. Taken to extremes, it suggests that it would be perfectly acceptable to engage in such activities on a continuing basis, so long as they might expose security flaws. This completely loses sight of the purpose of the computers in the first place — to serve as tools and resources, not as exercises in security. The same reasoning would imply that vigilantes have the right to attempt to break into the homes in my neighborhood on a continuing basis to demonstrate that they are susceptible to burglars.

Another flaw with this argument is that it completely ignores the technical and economic factors that prevent many sites from upgrading or correcting their software. Not every site has the resources to install new system software or to correct existing software. At many sites, the systems are run as turnkey systems — employed as tools and maintained by the vendor. The owners and users of these machines simply do not have the ability to correct or maintain their systems independently, and they are unable to afford custom software support from their vendors. To break into such systems, with or without damage, is effectively to trespass into places of business; to do so in a vigilante effort to force the owners to upgrade their security structure is presumptuous and reprehensible. A burglary is not justified, morally or legally, by an argument that the victim has poor locks and was therefore "asking for it."

A related argument has been made that vendors are responsible for the maintenance of their software, and that such security breaches should immediately require vendors to issue corrections to their customers, past and present. The claim is made that without highly-visible break-ins, vendors will not produce or distribute necessary fixes to software. This attitude is naive, and is neither economically feasible nor technically workable. Certainly, vendors should bear some responsibility for the adequacy of their software,[14] but they should not be responsible for fixing every possible flaw in every possible configuration.

Many sites customize their software or otherwise run systems incompatible with the latest vendor releases. For a vendor to be able to provide quick response to security problems, it would be necessary for each customer to run completely standardized software and hardware mixes to ensure the correctness of vendor-supplied updates. Not only would this be considerably less attractive for many customers and contrary to their usual practice, but the increased cost of such "instant" fix distribution would add to the price of such a system — greatly increasing the cost borne by the customer. It is unreasonable to expect the user community to sacrifice flexibility **and** pay a much higher cost per unit simply for faster corrections to the occasional security breach. That assumes it was even possible for the manufacturer to find those customers and supply them with fixes in a timely manner, something unlikely in a market where machines and software are often repackaged, traded, and resold.

The case of the Internet Worm is a good example of the security argument and its flaws. It further stands as a good example of the conflict between ends and means valuation of ethics. Various people have argued that the Worm's author did us a favor by exposing security flaws. At Mr. Morris's trial on Federal charges stemming from the incident, the defense attorneys also argued that their client should not be punished because of the good the Worm did in exposing those flaws. Others, including the prosecuting attorneys for the government, argued that the act itself was wrong no matter what the outcome. Their contention has been that the result does not justify the act itself, nor does the defense's argument encompass all the consequences of the incident.

This is certainly true; the complete results of the incident are still not known. There have been many other break-ins and network worms since November 1988, perhaps inspired by the media coverage of that incident. More attempts will possibly be made, in part inspired by Mr. Morris's act. Some sites on the Internet have restricted access to their machines, and others were removed from the network; I have heard of sites where a decision has been made not to pursue a connection, even though this will hinder research and operations. Combined with the many decades of person-hours devoted to cleaning up afterwards, this seems to be a high price to pay for a claimed "favor."

The legal consequences of this act are also not yet known. For instance, many bills were introduced into Congress and state legislatures in subsequent years as a (partial) result of these incidents. One piece of legislation introduced into the House of Representatives, HR-5061, entitled "The Computer Virus Eradication Act of 1988," was the first in a series of legislative actions that had the potential to affect significantly the computer profession. In particular, HR-5061 was notable because its wording would 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 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.

[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 programs to include a copy of itself.[6]

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.

### 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 record-keeping. 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 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 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.


[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.

[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.

[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.

[17] Eugene H. Spafford. Is a computer break-in ever ethical? *Information Technology Quarterly*, IX(2):9–14, 1990.

[18] Eugene H. Spafford. Are computer hacker break-ins ethical? *Journal of Systems and Software*, 17(1):41–48, January 1992.

## 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.

Professor Spafford's involvement with software engineering and security include positions on the editorial boards of the journals *International Journal of Computer and Software Engineering*, *Computers & Security*, the *Virus Bulletin*, the *Journal of Artificial Life*, *Network Security*, and the *Journal of Information Systems Security*. He is coauthor (with S. Garfinkel) of the books *Practical Unix and Internet Security*, published by O'Reilly and Associates (1991, 1996), and of *Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats*, ADAPSO (now ITAA) (1989); and was contributing editor on *Computer Crime: A Crime-fighter's Handbook* (1995) and *Web Security and Commerce* (1997), both also published by O'Reilly. He has written over 100 papers and reports on his research, and contributed chapters to many other books on computer security and professional ethics, and has spoken internationally at conferences, symposia, and colloquia on these and related issues.

Among many other activities, Dr. Spafford is a member of the Association for Computing Machinery (ACM), where he has served as chair of the ACM Self-Assessment Committee, and as a member of the Technical Standards Committee. He is currently a member of the ACM's U.S. Public Policy Committee. He is also a Senior Member of the IEEE and Computer Society of the IEEE, and a charter recipient of the IEEE Computer Society's *Golden Core* award for service to the profession.

## Publication History

This paper originally began as parts of two invited talks: A panel presentation on ethics and security at the Winter 1989 Usenix Conference following the Morris Internet Worm incident, and a presentation by the Harvard Office of Information Technology in November of 1989 on computer rights and responsibilities.

The first written version of these comments appeared in the Harvard INFORMATION TECHNOLOGY QUARTERLY as *Is a Computer Break-in Ever Ethical?*[17]. An expanded version of the paper was then solicited for a special issue of the JOURNAL OF SYSTEMS AND SOFTWARE, where it was published in 1992.[18]

Since then, the article has been widely reprinted in works on computing ethics:

- Reprinted (pp. 125–134) in COMPUERS, ETHICS, & SOCIAL VALUES; D. G. Johnson and

H. Nissenbaum, editors; Prentice-Hall; 1995.

- Reprinted in THE MORAL FOUNDATIONS OF INTELLECTUAL PROPERTY; Adam D. Moore, editor; 1997.
- Reprinted in COMPUTERS, ETHICS AND SOCIETY; M. David Ermann, Mary B. Williams, and Michele S. Shauf, eds.; Oxford University Press; 1997.
- Reprinted in THE ENCYCLOPEDIA OF APPLIED ETHICS; Ruth Chadwick, editor; Academic Press; 1997.
- Reprinted in INTERNET BESEIGED: COUNTERING CYBERSPACE SCOFFLAWS; Dorothy and Peter Denning, editors; Addison-Wesley, 1997.

Copies have been translated into Czech, Russian, German, and Spanish (that I know about) and used in computing group newsletters and university classes that I have not bothered to record.