Some Musings on Ethics and Computer Break-Ins

Eugene H. Spafford

Department of Computer Sciences
Purdue University
W. Lafayette, IN 47907-2004

spaf@cs.purdue.edu

ABSTRACT

In November and December, the computing community experienced the release of the Internet Worm, computer break-ins at Lawrence Livermore National Labs, and the temporary disconnection of the Milnet because of computer break-ins on a machine belonging to the Mitre Corporation. These incidents have led to many discussions about responsibility and ethics. Many of these discussions, particularly in forums such as the Usenet, have become heated without leading to any commonly-accepted conclusions.

This paper addresses some of these points. The intent is to summarize a few of the principal arguments supporting various positions and to argue some points of particular merit. At the end, references are given to material that may help provide background material for readers seeking further information.

Included in this discussion are the questions of whether individuals breaking into our machines are doing us a favor, and whether those individuals should in any way be encouraged. The paper concludes with some observations about the importance of the discussion, and the need to reach a consensus in the computer profession, if not in society as a whole.

Introduction

On November 2, 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. This *Internet Worm* program was stopped in a matter of hours, but the controversy engendered by its release has raged for weeks. The occurrence of other machine break-ins, possibly as ‘‘copycat’’ acts, has only served to fuel these discussions.

It is important that we discuss these issues. The continuing evolution of our technological base and our increasing reliance on computers for critical tasks implies that future incidents may well be more serious in their consequences. We must also admit that there will be more such incidents, with human nature as varied and extreme as it is, and with the technology as available as it is.

This paper presents a brief introduction to a few of the major issues that have been raised by the Worm incident. My intent is to present some of the arguments on each of these topics as a basis for further thought and discussion. References are provided at the end of the paper to enable the interested reader to explore particular aspects of the problem in greater depth.

In the following discussion, I have separated issues that often have been combined when debated. This, by itself, may help to clarify some of the issues; it is possible that most people are in agreement on some of these points once they are viewed as individual issues.

A Comment on Ethics

Ethics is the study of what is *right* to do. Alternatively, it is sometimes described as the study of what is *good* and how to achieve that good. To enable me to suggest whether an act is right or wrong, it is necessary for me to describe an ethical system that you, the reader, can understand and apply. I have made the simplifying assumption that we can judge the ethical nature of an act by applying a Kantian assessment: would we view that act as proper if **everyone** were to engage in it on a regular basis? Although I am aware that this may be too simplistic a model (and it could be argued that other ethical philosophies can also be applied), I will use this as a first approximation for purposes of argument. Kant's work has considerably influenced our contemporary ethical thought, and using this approach provides an understandable, initial point of reference; the reader unfamiliar with the philosophy and science of ethics may wish to consult some of the cited references for further information.

Note that this philosophy assumes that *right* is determined at least as much by actions as 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 individuals espousing repugnant views.

In summary, to judge the ethical good of an activity by the results rather than the means to achieve those results is not in keeping with our current social mores. Also, it is important to note that philosophies that consider the results as the measure of good are often impossible to apply because of the difficulty of understanding exactly what results from any arbitrary activity.

Consider an (extreme) example: if the government were to behead, on live TV, 1000 people chosen at random because they smoke, then the result might well be that many hundreds of thousands of 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. Despite the great good this would hold for society, everyone except for a few extremists would condemn such an idea as immoral. We would likely object even if only one person were involved. It would not matter what the law might be on such a matter; we would not feel that it was morally correct.

Note that we would be unable to judge the morality of such an act by evaluating the results, because we would not know the full scope of those results. Such an act might have effects on issues of law, public health, tobacco use, and daytime TV shows for decades or centuries to follow. Such a system of ethics would not allow us to evaluate our current activities at the time we would need such guidance.

Issues and Discussion

One of the first issues to be discussed after the release of the Internet Worm dealt with the intent of the author. A common topic of speculation was exactly why the Worm program had been written and released to the Internet. Suggested explanations put forth by the community have ranged from ''simple accident'' to ''the actions of a hostile sociopath.''

The problem with any speculation on this topic is that we do not **know** the real intent. Although an author has been alleged, he has not made any public statement about his reasons; because of pending legal actions, it is unlikely that such a statement will be made anytime soon.

Thus, any suppositions about his intent must be viewed as little better than guesswork.

One speculation can be addressed, however. Some individuals contend that the release of the program was an accident—that it somehow ‘‘escaped’’ during test. There is one compelling reason that suggests that this is not the case: the program had no way of being stopped, as would be be the case if it were being tested. The code contained no check that would allow someone to halt the program, nor was there any mechanism to limit the spread off the machine. The code did not check for any file or other condition that would signal it should stop. Rather, it contained code to evaluate with caution and sometimes ignore the one condition that was to limit its growth—the presence of another Worm on the same machine. Once started, the program would spread unchecked. For these reasons, it seems implausible that the code was under test. Thus, the conclusion must be that the Worm was started on purpose—it was a deliberate act.

It has been argued that the Worm was released to illustrate security defects to a community that would not otherwise pay attention. This seems unlikely. The alleged author was well-known to personnel at many 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. If we consider the immediate response he obtained in October when he revealed the bug in *ftp*, there appears to be little merit in the arguments that he did not know how to report a bug or that no one would listen to him.

In the more general case, this argument is also without merit. Although some system administrators might have been complacent about the security of their systems before this incident, personnel at Berkeley, most computer vendors, managers of government computer installations, and system admininstrators at major universities and colleges have always been attentive to reports of security problems. Someone wishing to report a problem with the security of a system need not exploit it to report it. It is incumbent on someone concerned about a problem to report it to a proper authority. (One does not set fire to the neighborhood shopping center to bring attention to a fire hazard inherent in the parking lot, then try to justify the act by claiming that the firemen never listen when anyone calls.)

It is worth noting that some people have advanced the related argument that bugs and security flaws will not get fixed without drastic measures. The claim is that the people who break into systems are performing a service by illustrating these problems, and they should be 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 engaging 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. When considered from this perspective, coupled with our working definition of *right*, we can see that it would be immoral to reward computer burglars and vandals.

Another flaw with this argument is that it completely ignores the technical and economic causes 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[1] systems—employed as tools, and maintained by the vendor. The

[1] So named because the users expect to purchase the systems, plug them in, ‘‘turn the key,’’ and use them. This is common in business environments where the employees are using a fixed set of applications.

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 to trespass into their places of business; to do so in a vigilante effort to somehow force them to upgrade their security structure is presumptuous and reprehensible.

A related contention is that the users themselves are somehow responsible for such break-ins if they are not running the latest security enhancements and corrections. Again, this assumes that there is some moral or legal responsibility to make such patches, and that every user has the capability to make such patches. *Computer burglars* break into systems by choice, not because of the presence or absence of some particular software. A burglary is not justified, morally or legally, by an argument that the victim has poor locks and was therefore ''asking for it.''

A further argument has been made that vendors are responsible for the on-going maintenance of their software, and that such security breaches should immediately require vendors to issue corrections to their customers, past and present. This is not economically feasible, nor is it technically workable. Many sites customize their software or otherwise run systems incompatible with the latest vendor releases. For a vendor to be able to provide instant 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, but the increased cost of such ''instant'' fix distribution would add to the price of any such system—increasing the cost borne by the customer. It is unreasonable to expect the user community[2] to sacrifice flexibility **and** pay a higher cost per unit just for faster corrections to the occasional security breach.

Vendors do bear some responsibility for security, however. They supply a product to their customers that should meet some minimum expected standards of fitness. For the average user, this includes an expectation that the data on the system will be secure. Vendors should therefore be sure to test the software with security in mind. Further, the vendors should always educate their customers about the extent to which they can trust the security of their systems, and to understand the support (if any) the vendor will provide for security-related problems.

Favor?

An oft-quoted comment was that the author of the Internet Worm did us a favor by exposing the security flaws. A favor is defined as doing someone a kindness. In a sense, the Worm as constructed was a kindness—it could have been written to be destructive instead of just contagious. As it was, the worm only exposed some serious security flaws, and it heightened our awareness of security concerns. It was in this sense a kindness, although it is not something for which we should thank its author. The result does not make the activity morally correct; as has already been explained, if everyone were to write and run such programs, it would clearly be wrong.

The complete results of this incident are not yet clear. There have been other break-ins since the release of the Worm, perhaps inspired by the media coverage of the Worm. More attempts may yet be made. Some sites on the Internet have restricted access to their machines, and others may be removed from the network (or already have been). Combined with the many decades of person-hours devoted to cleaning up after the Worm, this seems to be a high price to pay for a ''favor.''

---

[2] Especially the UNIX community.

The legal consequences of this act are also not yet known. For instance, a bill has been introduced into the House of Representatives, most likely in response to this incident. HR-5061, entitled ''The Computer Virus Eradication Act of 1988,'' introduced in the House by Wally Herger (R-CA) and Robert Carr (D-MI), may be only the first in a series of legislative actions that have the potential to significantly affect the computer profession. In particular, HR-5061 is notable since its wording prevents it from being applied to true computer viruses[3], and its provisions might be interpreted in such a way that almost any distributed software would violate the act. The passage of this bill or similar well-intentioned but misinformed legislation could have a negative effect on the computing profession as a whole.

Conclusions

The principal argument made in this paper is 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, since the activity itself is disruptive and immoral. The results of the act should be considered separately from the act itself. This is especially true when we consider how difficult it is to understand all the effects resulting from such an act.

Historically, computer professionals as a group have not been overly concerned with questions of ethics and propriety. Individuals and some organizations have tried to address these issues, but they cannot be resolved in any comprehensive way without the participation of the whole computing community. Too often, we view computers simply as machines and algorithms, and we do not perceive the ethical questions inherent in their use. When we stop to consider, however, that these machines influence the quality of life of millions of individuals, both directly and indirectly, we come to 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. It is with this in mind that 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 for worms, viruses and other threats to security. We know there are sites where users will be unable or unwilling to install updates and corrections. Widespread publication of detailed code will only serve to aid computer burglars to break into systems such as those.[4] 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. At the same time, we need to develop a method of rapidly developing and disseminating corrections and enhancements as they become known.

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 social mores about the sanctity of

---

[3] It provides penalties only in cases where **programs** are introduced into computer systems, not sections of code or subroutines.

[4] 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.

personal property are a major and important influence in the prevention of burglary. It is our duty as informed professionals to help extend those mores into the computer age.

Suggested Readings

Background information on the *Internet Worm* incident may be found in [Seel89]. and [Spaf89] An introduction to personal and professional ethics can be found in [John85]. [Tayl75] is a good general introduction to various systems of ethics. [Winc68] relates the philosophy of ethics to the development of personal morals. [Lyon84] relates ethics to law. Immanuel Kant's *Foundations of the Metaphysics of Morals* has been translated numerous times, but is probably not a good reference for any but the most serious inquiries.

There are many fine works relating to computer ethics and professional ethics. I would recommend the books [Hoff82], [John85], and [Mart89] as initial references. Other references worth reading include: [Absh81], [Absh82], [Bloo88], [Chri88], [Mitc86], and [Weiz86].

Many works have been published dealing with computer burglars and hackers. Interesting references include [Bair87], [Good83], and especially [Lee86]. The articles [Reid86] and [Stol88] may also provide some insight.

The social consequences of tampering with computers can be inferred from works such as [Hoff86] and the continuing feature ''Risks to the Public'' present in all recent issues of *ACM SIGSOFT Software Engineering News*. Issues of *ACM SIGCAS Computers and Society* usually contain interesting articles about the effects of computers on society, too.

I believe **everyone** involved with computer systems, especially individuals concerned with issues of trust and security, should read [Thom84].

References

Absh81.

Abshire, Gary M., ''Ethics Apply to Computer Specialists, Too,'' *COMPUTERS AND SOCIETY*, vol. 11, no. 2, p. 22, University of Wisconsin, Madison, Wisconsin, Spring 1981.

Absh82.

Abshire, Gary M., ''The ethical insensitivity of computer specialists and what you can do about it,'' *COMPUTERS AND SOCIETY*, vol. 12, pp. 10-11, ACM Special Interest Group on Computers and Society, Winter 1982.

Bair87.

Baird, Bruce J., Lindsay L. Baird Jr., and Ronald P. Ranauro, ''The Moral Cracker?,'' *COMPUTERS AND SECURITY*, vol. 6, no. 6, pp. 471-478, North-Holland, December 1987.

Bloo88.

Bloombecker, J. J. Buck, ''Computer Ethics for Cynics,'' *COMPUTERS AND SOCIETY*, vol. 18, no. 3, pp. 30-32, ACM Special Interest Group on Computers and Society, New York, NY, July 1988.

Chri88.

Christiansen, Donald, ''A Matter Of Ethics,'' *IEEE SPECTRUM*, vol. 25, p. 15, August, 1988.

Good83.

Goodfellow, Geoffrey S., ''Testimony by Geoffrey S. Goodfellow,'' *SOFTWARE ENGINEERING NOTES*, vol. 8, pp. 18-23, 1983.

Hoff86.

Hoffman, Lance J. and Lucy M. Moran, ''Societal Vulnerability to Computer System Failures,'' *COMPUTERS AND SECURITY*, vol. 5, no. 3, Elsevier Science Publishers B.V., North-Holland, 1986.

Hoff82.
Hoffman, W. Michael and Jennifer Mills Moore (eds.), *Ethics and the Management of Computer Technology,* Oelgeschlager, Gunn & Hain, Cambridge, Mass., 1982.

John85.
Johnson, Deborah G. and John W. Snapper, *Ethical Issues in the Use of Computers,* Wadsworth Publishing Co., Belmont, CA, 1985. out of print

Lee86.Lee, John A. N., Gerald Segal, and Rosalie Steier, ‘‘Positive Alternatives: A Report on an ACM Panel on Hacking,’’ *COMMUNICATIONS OF THE ACM*, vol. 29, no. 4, pp. 297-299, ACM, New York, NY, April, 1986.

Lyon84.
Lyons, David, in *ETHICS AND THE RULE OF LAW*, Cambridge University Press, Bath, Great Britain, 1984.

Mart89.
Martin, Mike W. and Roland Schinzinger, *Ethics in Engineering,* McGraw Hill, 1989. 2nd. Edition

Mitc86.
Mitcham, Carl, ‘‘Computers: From Ethos and Ethics to Mythos and Religion, Notes on the New Frontier Between Computers and Philosophy,’’ *TECHNOLOGY IN SOCIETY, AN INTERNATIONAL JOURNAL*, vol. 8, no. 3, Pergamon Press, New York, 1986.

Reid86.
Reid, Brian, ‘‘Lessons from the UNIX Breakins at Stanford,’’ *SOFTWARE ENGINEERING NOTES*, vol. 11, no. 5, pp. 29-35, ACM, October 1986.

Seel89.
Seeley, Donn, ‘‘A Tour of the Worm,’’ *PROCEEDINGS OF 1989 WINTER USENIX CONFERENCE*, Usenix Association, San Diego, CA, February 1989.

Spaf89.
Spafford, Eugene H., ‘‘The Internet Worm Program: An Analysis,’’ *COMPUTER COMMUNICATION REVIEW*, vol. 19, no. 1, ACM SIGCOM, January 1989. Also issued as Purdue CS technical report TR-CSD-823

Stol88.
Stoll, Clifford, ‘‘Stalking the Wily Hacker,’’ *COMMUNICATIONS OF THE ACM,* vol. 31, no. 5, pp. 484-497, ACM, New York, NY, May 1988.

Tayl75.
Taylor, Paul W., *Principles of Ethics,* Dickenson Publishing Company, Inc., Encino, CA, 1975.

Thom84.
Thompson, Ken, ‘‘Reflections on Trusting Trust,’’ *COMMUNICATIONS OF THE ACM*, vol. 27, no. 8, pp. 761-763, ACM, New York, NY, August 1984.

Weiz86.
Weizenbaum, Joseph, ‘‘Not Without Us,’’ *ACM SIGCAS: COMPUTERS & SOCIETY*, vol. 16, no. 2,3, pp. 2-7, Association for Computing Machinery, Inc., New York, NY, Summer/Fall 1986.

Winc68.
Winch, Peter, *Moral Integrity,* Oxford, England, 1968.