Network Working Group
Request for Comments: 1135

J. Reynolds
ISI

December 1989

The Helminthiasis of the Internet

Status of this Memo

This memo takes a look back at the helminthiasis (infestation with, or disease caused by parasitic worms) of the Internet that was unleashed the evening of 2 November 1988. This RFC provides information about an event that occurred in the life of the Internet. This memo does not specify any standard. Distribution of this memo is unlimited.

Introduction

> ----- "The obscure we see eventually, the completely apparent takes longer." ----- Edward R. Murrow

The helminthiasis of the Internet was a self-replicating program that infected VAX computers and SUN-3 workstations running the 4.2 and 4.3 Berkeley UNIX code. It disrupted the operations of computers by accessing known security loopholes in applications closely associated with the operating system. Despite system administrators efforts to eliminate the program, the infection continued to attack and spread to other sites across the United States.

This RFC provides a glimpse at the infection, its festering, and cure. The impact of the worm on the Internet community, ethics statements, the role of the news media, crime in the computer world, and future prevention will be discussed. A documentation review presents four publications that describe in detail this particular parasitic computer program. Reference and bibliography sections are also included in this memo.

1. The Infection

> ----- "Sandworms, ya hate 'em, right??" ----- Michael Keaton, Beetlejuice

Defining "worm" versus "virus"

A "worm" is a program that can run independently, will consume the resources of its host from within in order to maintain itself, and can propagate a complete working version of itself on to other machines.

A "virus" is a piece of code that inserts itself into a host, including operating systems, to propagate. It cannot run independently. It requires that its host program be run to activate it.

In the early stages of the helminthiasis, the news media popularly cited the Internet worm to be a "virus", which was attributed to an early conclusion of some in the computer community before a specimen of the worm could be extracted and dissected. There are some computer scientists that still argue over what to call the affliction. In this RFC, we use the term, "worm".

1.1 Infection - The Worm Attacks

The worm specifically and only made successful attacks on SUN workstations and VAXes running Berkeley UNIX code.

The Internet worm relied on the several known access loopholes in order to propagate over networks. It relied on implementation errors in two network programs: sendmail and fingerd.

Sendmail is a program that implements the Internet's electronic mail services (routing and delivery) interacting with remote sites [1, 2]. The feature in sendmail that was violated was a non-standard "debug" command. The worm propagated itself via the debug command into remote hosts. As the worm installed itself in a new host the new instance began self-replicating.

Fingerd is a utility program that is intended to help remote Internet users by supplying public information about other Internet users. This can be in the form of identification of the full name of, or login name of any local user, whether or not they are logged in at the time (see the Finger Protocol [3]).

Using fingerd, the worm initiated a memory overflow situation by sending too many characters for fingerd to accommodate (in the gets library routine). Upon overflowing the storage space, the worm was able to execute a small arbitrary program. Only 4.3BSD VAX machines suffered from this attack.

Another of the worm's methods was to exploit the "trusted host features" often used in local networks to propagate (using rexec and rsh).

It also infected machines in /etc/hosts.equiv, machines in /.rhosts, machines in cracked accounts' .forward files, machines cracked accounts' .rhosts files, machines listed as network gateways in routing tables, machines at the far end of point-to-

point interfaces, and other machines at randomly guessed addresses on networks of first hop gateways.

The Internet worm was also able to infect systems using guessed passwords, typically spreading itself within local networks by this method. It tried to guess passwords, and upon gaining access, the worm was able to pose as a legitimate user.

1.2 Festering - Password Cracking

The worm festered by going into a password cracking phase, attempting to access accounts with obvious passwords (using clues readily available in the /etc/passwd file), such as: none at all, the user name, the user name appended to itself, the "nickname", the last name, the last name spelled backwards. It also tried breaking into into accounts with passwords from a personalized 432 word dictionary, and accounts with passwords in /usr/dict/words.

Most users encountered a slowing of their programs, as the systems became overloaded trying to run many copies of the worm program, or a lack of file space if many copies of the worm's temporary files existed concurrently. Actually, the worm was very careful to hide itself and leave little evidence of its passage through a system. The users at the infected sites may have seen strange files that showed up in the /usr/tmp directories of some machines and obscure messages appeared in the log files of sendmail.

1.3 The Cure

Teams of computer science students and staff worked feverishly to understand the worm. The key was seen to get a source (C language) version of the program. Since the only isolated instances of the the worm were binary code, a major effort was made to translate back to source, that is decompile the code, and to study just what damage the worm was capable of. Two specific teams emerged in the battle against the Internet worm: the Berkeley Team and the MIT team. They communicated and exchanged code extensively. Both teams were able to scrutinize it and take immediate action on a cure and prevent reinfection. Just like regular medical Doctors, the teams searched, found and isolated a worm specimen which they could study. Upon analyzing the specimen and the elements of its design, they set about to develop methods to treat and defeat it. Through the use of the "old boy network" of UNIX system wizards (to find out something, one asks an associate or friend if they know the answer or who else they could refer to to find out the answer), email and phone calls were extensively used to alert the computer world of the program patches that could be used at sites to close the sendmail hole and

fingerd holes. Once the information was disseminated to the sites and these holes were patched, the Internet worm was stopped. It could not reinfect the same computers again, unless the worm was still sitting in an infected trusted host computer.

The Internet worm was eliminated from most computers within 48-72 hours after it had appeared, specifically through the efforts of computer science staffs at the University research centers. Government and Commercial agencies apparently were slow in coming around to recognizing the helminthiasis and eradicating it.

2. Impact

> ----- "Off with his head!!!" ----- The Red Queen,
> Alice in Wonderland

Two lines have been drawn in the computer community in the aftermath of the Internet worm of November 1988. One group contends that the release of the worm program was a naive accident, and that the worm "escaped" during testing. Yet, when the worm program was unleashed, it was obvious it was spreading unchecked. Another group argues that the worm was deliberately released to blatantly point out security defects to a community that was aware of the problems, but were complacent about fixing them. Yet, one does not necessarily need to deliberately disrupt the entire world in order to report a problem.

Both groups agree that the community cannot condone worm infestation whether "experimental" or "deliberate" as a means to heighten public awareness, as the consequences of such irresponsible acts can be devastating. Meanwhile, several in the news media stated that the author of the worm did the computer community a favor by exposing the security flaws, and that bugs and security flaws will not get fixed without such drastic measures as the Internet worm program.

In the short term, the worm program did heighten the computer community's awareness of security flaws. Also, the "old boy network" proved it was still alive and well! While networking and computers as a whole have grown by leaps and bounds in the last twenty years, the Internet community still has the "old boys" who trust and communicate well with each other in the face of adversity.

In the long term, all results of the helminthiasis are not complete. Many sites have either placed restrictions on access to their machines, and a few have chosen to remove themselves from the Internet entirely. The legal consequences of the Internet worm program as a computer crime are still pending, and may stay in that condition into the next decade.

Yet, the problem of computer crime is, on a layman's level, a social one. Legal statutes, which notoriously are legislated after the fact, are only one element of the solution. Development of enforceable ethical standards that are universally agreed on in the computer community, coupled with enforceable laws should help eradicate computer crime.

3. Ethics and the Internet

> ----- "If you're going to play the game properly, you'd better know every rule." ----- Barbara Jordan

Ethical behavior is that of conforming to accepted professional standards of conduct; dealing with what is good or bad within a set of moral principles or values. Up until recently, most computer professionals and groups have not been overly concerned with questions of ethics.

Organizations and computer professional groups have recently, in the aftermath of the Internet worm, issued their own "Statement of Ethics". Ethics statements published by the Internet Activities Board (IAB), the National Science Foundation (NSF), the Massachusetts Institute of Technology (MIT), and the Computer Professionals for Social Responsibility (CPSR) are discussed below.

3.1 The IAB

The IAB issued a statement of policy concerning the proper use of the resources of the Internet in January, 1989 [4] (and reprinted in the Communications of the ACM, June 1989). An excerpt:

The Internet is a national facility whose utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community.

The U.S. Government sponsors of this system have a fiduciary responsibility to the public to allocate government resources wisely and effectively. Justification for the support of this system suffers when highly disruptive abuses occur. Access to and use of the Internet is a privilege and should be treated as such by all users of this system.

The IAB strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

(a) seeks to gain unauthorized access to the resources of the Internet,

(b) disrupts the intended use of the Internet,

(c) wastes resources (people, capacity, computer) through such actions,

(d) destroys the integrity of computer-based information, and/or

(e) compromises the privacy of users.

The Internet exists in the general research milieu. Portions of it continue to be used to support research and experimentation on networking. Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise great caution in the conduct of their work. Negligence in the conduct of Internet-wide experiments is both irresponsible and unacceptable.

The IAB plans to take whatever actions it can, in concert with Federal agencies and other interested parties, to identify and to set up technical and procedural mechanisms to make the Internet more resistant to disruption. Such security, however, may be extremely expensive and may be counterproductive if it inhibits the free flow of information which makes the Internet so valuable. In the final analysis, the health and well-being of the Internet is the responsibility of its users who must, uniformly, guard against abuses which disrupt the system and threaten its long-term viability.

3.2 NSF

The NSF issued an ethical network use statement on 30 November 1988, during the regular meeting of the Division Advisory Panel for Networking and Communications Research and Infrastructure (and reprinted in the Communications of the ACM (June of 1989) [5]), that stated, in part:

The Division Advisory Panel (DAP) of the NSF Division of Networking and Communication Research and Infrastructure (DNCRI) deplores lapses of ethical behavior which cause disruption to our national network resources. Industry, government, and academe have established computer networks in support of research and scholarship. Recent events have accentuated the importance of establishing community standards for the ethical use of networks. In this regard, the DNCRI DAP defines as unethical any activity which purposefully or through negligence:

a. disrupts the intended use of the networks,

b. wastes resources through such actions (people, bandwidth or computer),

c. destroys the integrity of computer-based information,

d. compromises the privacy of users,

e. consumes unplanned resources for control and eradication.

We encourage organizations managing and operating networks to adopt and publicize policies and standards for ethical behavior. We also encourage these organizations to adopt administrative procedures to enforce appropriate disciplinary responses to violations and to work with appropriate bodies on drafting legislation in this area.

3.3 MIT

MIT issued a statement of ethics entitled, "Teaching Students About Responsible Use of Computers" in 1985-1986 (and reprinted in the Communications of the ACM (June 1989) [6]). The official statement of ethics specifically outlined MIT's position on the intended use, privacy and security, system integrity, and intellectual property rights.

Those standards, outlined in the MIT Bulletin under academic procedures, call for all members of the community to act in a responsible, ethical, and professional way. The members of the MIT community also carry the responsibility to use the system in accordance with MIT's standards of honesty and personal conduct.

3.4 CPSR

The CPSR issued a statement on the Computer Virus in November 1988 (and reprinted in the Communications of the ACM (June 1989) [7]). The CPSR believes:

The incident should prompt critical review of our dependence on complex computer networks, particularly for military and defense-related function. The flaws that permitted the recent virus to spread will eventually be fixed, but other flaws will remain. Security loopholes are inevitable in any computer network and are prevalent in those that support general-purpose computing and are widely accessible.

An effective way to correct known security flaws is to publish

descriptions of the flaws so that they can be corrected. We therefore view the effort to conceal technical descriptions of the recent virus as short-sighted.

CPSR believes that innovation, creativity, and the open exchange of ideas are the ingredients of scientific advancement and technological achievement. Computer networks, such as the Internet, facilitate this exchange. We cannot afford policies that might restrict the ability of computer researchers to exchange their ideas with one another. More secure networks, such as military and financial networks, sharply restrict access and offer limited functionality. Government, industry, and the university community should support the continued development of network technology that provides open access to many users.

The computer virus has sent a clear warning to the computing community and to society at large. We hope it will provoke a long overdue public discussion about the vulnerabilities of computer networks, and the technological, ethical, and legal choices we must address.

4. The Role of the Media

> ----- "You don't worry about whether or not they've written it, you worry whether or not they've read it before they go on the air." ----- Linda Ellerbee, the Pat Sajak Show.

Airplane accidents, Pit Bulldog attacks, drought, disease...the media is there...whether you want them there or not. Predictably, some members of the press grabbed on to the worm invasion of the Internet and sensationalized the outbreak. Sites were named (including sites like NASA Ames and Lawrence Livermore) and pointed to as being "violated". Questions of computer security were rampant. Questions of national security appropriately followed. The alleged perpetrator of the worm tended to be thought of by the press as a "genius" or a "hero".

During the helminthiasis of the Internet, handling this news media "invasion", was critical. It's akin to trying to extinguish a major brush fire with a news reporter and a microphone in your way. Time is of the essence. The U.C. Berkeley group, among others, reported that it was a problem to get work accomplished with the press hounding them incessantly. At MIT, their news office was commended in doing their job of keeping the press informed and satisfied, yet out of the way of the students and staff working on the a cure.

What is an appropriate response?? At MIT, even a carefully worded

"technical" statement to the press resulted in very few coherent press releases on the Internet worm. Extrapolation and "flavoring" by the press were common. According to Eichin and Rochlis, "We were unable to show the T.V. crew anything "visual" caused by the virus, something which eventually become a common media request and disappointment. Instead, they settled for people looking at workstations talking 'computer talk'." [10]

Cornell University was very critical of the press in their report to the Provost: "The Commission suggests that media exaggeration of the value and technical sophistication of this kind of activity obscures the far more accomplished work of those students who complete their graduate studies without public fanfare; who make constructive contributions to computer sciences and the advancement of knowledge through their patiently constructed dissertation; and who subject their work to the close scrutiny and evaluation of their peers, and not to the interpretations of the popular press." [9]

5. Crime in the Computer World

> ----- "A recent survey by the American Bar Association found that almost one-half of those companies and Government agencies that responded had been victimized by some form of computer crime. The known financial loss from those crimes was estimated as high as $730 million, and the report concluded that computer crime is among the worst white-collar offenses." ----- The Computer Fraud and Abuse Act of 1986

The term White Collar crime was first used by Edwin Sutherland, a noted American criminologist, in 1939. Sutherland contended that the popular view of crime as primarily a lower class (Blue Collar) activity was based on the failure to consider the activities of the robber barons and captains of industry who violated the law with virtual impunity.

In this day and age, White Collar crime refers to violations of the law committed by salaried or professional persons in conjunction with their work. Computer crimes are identified and included in this classification. Yet, law enforcement agencies have historically paid little attention to this new phenomenon. When a trial and conviction does occur, it's resulted more often in a fine and probation, than a prison term. A shift became apparent in the late 1970s, when the FBI's ABSCAM investigation (1978-80) resulted in the conviction of several U.S. legislators for bribery and related charges.

The legal implication of the Internet worm program as a computer crime is still pending, as there are few cases to rely on. On the

Federal level, HR-6061, "The Computer Virus Eradication Act of 1988" (Herger & Carr) was introduced in the U.S. House of Representatives. On the State level, several states are considering their own statutes. Time will tell.

Meanwhile, computer network security is still allegedly being compromised, as described in a recent DDN Security Bulletin [12].

6. Future Prevention

> ----- "This is a pretty kettle of fish." ----- Queen Mary to Stanley Baldwin at the time of Edward VII's abdication

What roles can the computer community as a whole, play in preventing such outbreaks? Why were many people aware of the debug problem in the sendmail program and the overflow problem in fingerd, yet, appropriate fixes were not installed in existing systems?

Various opinions have emerged:

1) Computer ethics must be taken seriously. A standard for computer ethics is extremely important for the new groups of computer professionals graduating out of Universities. The "old" professionals and "new" professionals who use computers are ALL responsible for their applications.

2) The "powers that be" of the Internet (IAB, DARPA, NSF, etc.) should pursue the current problems in network security, and cause the flaws to be fixed.

3) The openness and free flow of information of networking should be rightfully preserved, as it demonstrated its worth during the helminthiasis by expediting the analysis and cure of the infestation.

4) Promote and coordinate the establishment of committees or agency "police" panels that would handle, judge, and enforce violations based on a universally set standard of computer ethics.

5) The continued incidences of "computer crime" show a lack of professionalism and ethical standards in the computer community. Ethics statements like those discussed in this RFC, not only need to be published, but enforced as well. There is a continuing need to instill a professional code of ethics and responsibilities in order to preserve the computer community.

7. Documentation Review

> ----- "Everybody wants to get into the act!" ----- Jimmy Durante.

Quite a number of articles and papers were published very soon after the worm invasion. Books, articles, and other documents are continuing to be written and published on the subject (see Section 9, Bibliography). In this RFC, we have chosen four to review: The Cornell University Report on "The Computer Worm" [8], presented to the Provost of the University, Eichin and Rochlis' "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988" [9], Donn Seeley's "A Tour of the Worm" [10], and Gene Spafford's, "The Internet Worm Program: An Analysis" [11].

7.1 The Cornell University Report

The Cornell University Report on "The Computer Worm", was presented to the Provost of the University on 6 February 1989, by the Commission of Preliminary Enquiry, consisting of: Ted Eisenberg, Law, David Gries, Computer Science, Juris Hartmanis, Computer Science, Don Holcomb, Physics, M. Stuart Lynn, Office of Information Technologies (Chair), and Thomas Santoro, Office of the University Counsel.

An introduction set the stage of the intent and purpose of the Commission:

1) Accumulate all evidence concerning the involvement of the alleged Cornell University Computer Science graduate student in the worm infestation of the Internet, and to assess the gathered evidence to determine the alleged graduate student was the perpetrator.

2) Accumulate all evidence concerning the potential involvement of any other members of the Cornell University community, and to assess such evidence to determine whether or not any other members of the Cornell University community was involved in unleashing the worm on to the Internet, or knew of the potential worm infestation ahead of time.

3) Evaluate relevant computer policies and procedures to determine which, if any, were violated and to make preliminary recommendations to the Provost as to whether any of such policies and procedures should be modified to inhibit potential future security violations of this general type.

In the summary of findings and comments, the Commission named the Cornell University first year Computer Science graduate student that allegedly created the worm and unleashed it on to the Internet. The findings section also discussed:

1) the impact of the invasion of the worm,
2) the mitigation attempts to stop the worm,
3) the violation of computer abuse policies,
4) the intent,
5) security attitudes and knowledge,
6) technical sophistication,
7) Cornell's involvement,
8) ethical considerations,
9) community sentiment,
10) and Cornell University's policies on computer abuse.

The report concluded that the worm program's gathering of unauthorized passwords and the dissemination of the worm over a national network were wrong. The Commission also disclaimed that contrary to media reports, Cornell University DID NOT condone the worm infection, nor heralded the unleashing of the worm program as a heroic event. The Commission did continue to encourage the free flow of scholarly research and reasonable trust within the University/Research communities.

A background on the worm program, methods of investigation, an introduction to the evidence, an interpretation and findings, acknowledgements, and an extensive appendices were also included in the Commission's report.

7.2 "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988"

Eichin and Rochlis' "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988", provides a detailed dissection of the worm program. The paper discusses the major points of the worm program then reviews strategies, chronology, lessons and open issues, acknowledgements; also included are a detailed appendix on the worm program subroutine by subroutine, an appendix on the cast of characters, and a reference section.

A discussion of the terms "worm" versus "virus" is presented. These authors concluded that it was a "virus" infection, not worm infection. Thus they use the term "virus" in their document. In Section 1, goals and targets by the teams of computer scientists were defined. There were three steps taken to find out the inner workings of the virus:

- isolating a specimen of the virus in a form which could be analyzed.

- "decompiling" the virus, into a form that could be shown to reduce to the executable of the real things, so that the higher level version could be interpreted.

- analyzing the strategies used by the virus, and the elements of its design, in order to find weaknesses and methods of defeating it.

Major points were outlined of how the virus attacked and who it attacked:

How it entered.

Who it attacked.

What it attacked.

What it did NOT do.

In Section 2, the target of the attacks by the virus were discussed. This included the sendmail debug mode, the finger daemon bug, rexec and passwords, rsh, trusted host features, and information flow. A description of the virus' self protection included how it covered its tracks, and what camouflage it used to go undetected to the machines and system administrators. Flaws were analyzed in three subjects: reinfection prevention, heuristics, and vulnerabilities not used.

Many defenses were launched to stop the virus. Some were convenient or inconvenient for end users of the infected systems. Those mentioned in this document included:

- full isolation from the network

- turning off mail service

- patching out the "debug" command in sendmail

- shutting down the finger daemon

- fixing the finger daemon

- mkdir /usr/tmp/sh (a simple way to keep the virus from propagating)

- defining pleasequit (did not stop the virus)

- renaming the UNIX C compiler and linker

- requiring new passwords for all users

After the virus was diagnosed, a tool was created which duplicated the password attack (including the virus' internal directory) and was posted to the Internet. System administrators were able to analyze the passwords in use on their system.

Section 3 chronicles the events that took place between Wednesday, 2 November 1988 through Friday, 11 November 1988 (EST). In Section 4, lessons and open issues are viewed and discussed:

- Connectivity was important.

- The "old boy network" worked.

- Late night authentication is an interesting problem. (How did you know that it really is MIT on the phone??)

- Whom do you call (if you need to talk to the manager of the Ohio State University network at 3 o'clock in the morning)?

- Speaker phones and conference calling proved very useful.

- The "teams" that were formed and how they reacted to the virus is a topic for future study.

- Misinformation and illusions ran rampant.

- Tools were not as important as one would have anticipated.

- Source availability was important.

- The academic sites performed the best, better than government and commercial sites.

- Managing the press was critical.

General points for the future:

- "We have met the enemy and he is us." (Alleged author of the virus was an insider.)

- Diversity is good.

- "The cure shouldn't be worse than the disease." (It may be more expensive to prevent such attacks than is is to clean up after them.)

- Defenses must be at the host level, not the network level. (The network performed its function perfectly and should not be faulted; the flaws were in several application programs.)

- Logging information is important.

- Denial of service attacks are easy.

- A central security fix repository may be a good idea.

- Knee-jerk reactions should be avoided.

Appendix A describes the virus program subroutine by subroutine. A flow of information among the subroutines is pictured on page 19. Appendix B presents the 432 words built in the worm's dictionary. Appendix C lists the "cast of characters" in defeating the virus.

7.3 "A Tour of the Worm"

In Donn Seeley's "A Tour of the Worm", specific details were presented as a "walk thru" of this particular worm program. The paper opened with an abstract, introduction, detailed chronology of events upon the discovery of the worm, an overview, the internals of the worm, personal opinions, and conclusion.

The chronology section presented a partial list representing the current known dates and times (in PST). In the descriptive overview, the worm is defined as a 99-line bootstrap program written in the C language, plus a large relocatable object file that was available in VAX and various Sun-3 versions. Seeley classified activities of the worm into two categories of attack and defense. Attack consisted of locating hosts (and accounts) to penetrate, then exploiting security holes on remote systems to pass across a copy of the worm and run it. The defense tactics fell into three categories: preventing the detection of intrusion, inhibiting the analysis of the program, and authenticating other worms. When analyzing this particular program, Seeley stated that it is just as important to establish what the program DOES NOT do, as what it does do:

This worm did not delete a system's files,

This worm did not modify existing files,

This worm did not install trojan horses,

This worm did not record or transmit decrypted passwords,

This worm did not try to capture superuser privileges,

This worm did not propagate over UUCP, X.25, DECNET, or BITNET,

This worm specifically draws upon TCP/IP,

and

This worm did not infect System V systems, unless they had been modified to use Berkeley network programs like sendmail, fingerd, and rexec.

In section 4, the "internals" of the worm were examined and charted. The main thread of control in the worm was analyzed, then an examination of the worm's data structure was presented. Population growth of the worm, security holes, the worms' use of rsh and rexec network services, the use of the TCP finger service to gain entry to a system, and the sendmail attack are discussed. Password cracking and faster password encryption algorithms are discussed.

In the opinions section, certain questions that a "mythical ordinary system administrator" might ask were discussed:

Did the worm cause damage?

Was the worm malicious?

Will publication or worm details further harm security?

7.4 "The Internet Worm Program: An Analysis"

Gene Spafford's "The Internet Worm Program: An Analysis", described the infection of the Internet as a worm program that exploited flaws in utility programs in UNIX based systems. His report gives a detailed description of the components of the worm program: data and functions. He focuses his study on two completely independent reverse-compilations of the worm and a version disassembled to VAX assembly language.

In Section 4, Spafford provided a high-level example of how the worm program functioned. The worm consisted of two parts: a main program, and a bootstrap (or vector) program. A description from the point of view of a host that was infected was presented.

Section 5 describes the data structures and organization of the routines of the program:

1) The worm had few global data structures.

2) The worm constructed a linked list of host records.

3) The worm constructed a simple array of gateway IP addresses through the use of the system "netstat" command.

4) An array of records was filled in with information about each network interface active on the current host.

5) A linked list of records was built to hold user information.

6) The program maintained an array of "object" that held the files that composed the worm.

7) A mini-dictionary of words was present in the worm to use in password guessing.

8) Every text string used by the program, except for the words in the mini-dictionary, was masked (XOR) with the bit pattern 0x81.

9) The worm used the following routines:

```
 setup and utility:
         main, doit, crypt, h_addaddr,
         h_addname, h_addr2host, h_clean,
         h_name2host, if_init, loadobject,
         makemagic, netmastfor, permute,
         rt_init, supports_rsh, and supports_telnet

 network and password attacks:
         attack_network, attack_user, crack_0,
         crack_1, crack_2, crack_3, cracksome,
         ha, hg, hi, hl, hul, infect, scan_gateways,
         sendWorm, try_fingerd, try_password,
         try_rsh, try_sendmail, and waithit
```

Camouflage:
checkother, other_sleep, send_message,
and xorbuf

In Section 6, Spafford provides an analysis of the code of the worm. He discusses the structure and style, the problems of functionality, camouflage, specific comments, the sendmail attack, the machines involved, and the portability considerations.

Finally, appendices supply the "mini-dictionary" of words contained in the worm, the bootstrap (vector) program that the worm traversed over to each machine, a corrected fingerd program, and the patches developed and invoked to sendmail to rectify the infection.

8. References

[1] Allman, E., "Sendmail - An Internetwork Mail Router", University of California, Berkeley, Issued with the BSD UNIX documentation set, 1983.

[2] Postel, J., "Simple Mail Transfer Protocol", RFC 821, USC/Information Sciences Institute, August 1982.

[3] Harrenstien, K., "NAME/FINGER", RFC 742, SRI, December 1977.

[4] Internet Activities Board, "Ethics and the Internet", RFC 1087, IAB, January 1989. Also appears in the Communications of the ACM, Vol. 32, No. 6, Pg. 710, June 1989.

[5] National Science Foundation, "NSF Poses Code of Networking Ethics", Communications of the ACM, Vol. 32, No. 6, Pg. 688, June 1989. Also appears in the minutes of the regular meeting of the Division Advisory Panel for Networking and Communications Research and Infrastructure, Dave Farber, Chair, November 29-30 1988.

[6] Massachusetts Institute of Technology, "Teaching Students About Responsible Use of Computers", MIT, 1985-1986. Also reprinted in the Communications of the ACM, Vol. 32, No. 6, Pg. 704, Athena Project, MIT, June 1989.

[7] Computer Professionals for Social Responsibility, "CPSR Statement on the Computer Virus", CPSR, Communications of the ACM, Vol. 32, No. 6, Pg. 699, June 1989.

[8] Eisenberg, T., D. Gries, J. Hartmanis, D. Holcomb, M. Lynn, and T. Santoro, "The Computer Worm", Cornell University, 6 February 1989.

[9] Eichin, M., and J. Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988", Massachusetts Institute of Technology, February 1989.

[10] Seeley, D., "A Tour of the Worm", Proceedings of 1989 Winter USENIX Conference, Usenix Association, San Diego, CA, February 1989.

[11] Spafford, E., "The Internet Worm Program: An Analysis", Computer Communication Review, Vol. 19, No. 1, ACM SIGCOM, January 1989. Also issued as Purdue CS Technical Report CSD-TR-823, 28 November 1988.

[12] DCA DDN Defense Communications System, "DDN Security Bulletin 03", DDN Security Coordination Center, 17 October 1989.

9. Bibliography

Alexander, M., "A Year Later, Internet Still Under Attack", Computerworld, Vol. 23, No. 45, Pg. 1, 6 November 1989.

Alexander, M., "It's Ba-a-ack: 'No Nukes Worm' Haunts Internet", Vol. 23, No. 45, Pg. 6, 6 November 1989.

Aucoin, R., "Computer Viruses: Checklist for Recovery", Computers in Libraries, Vol. 9, No. 2, Pg. 4, 1 February 1989.

Aviation Week & Space Technology, "Rapid Spread of Virus Confirms Fears About Danger to Computers", Aviation Week & Space Technology, Vol. 129, No. 20, Pg. 44, 14 November 1988.

Barnes, J., "Drawing the Lines: Changes in Computer Technology and Law Guarantee that Resdistricting in ther 1990s will be Different and a More Difficult Game", National Journal, Vol. 21, No. 13, Pg. 787, 1 April 1989.

Bellovin, S., "Security Problems in the TCP/IP Protocol Suite", Computer Communication Review, Vol. 19, No. 2, Pg. 32, 1 April 1989.

Bellovin, S., "The Worm and the Debug Option", Forum Risks to the Publics in Computer and Related Systems, Vol. 7, No. 74, ACM Committee on Computers and Public Policy, 10 November 1988.

Bender, D., "Computer Law: Evidence and Procedure", (Kept up to date with supplements.), M. Bender, New York, NY, 1978-present.

Bidgoli, H., and R. Azarmsa, "Computer Security: New Managerial Concern for the 1990's and Beyond", Journal of Systems Management,

Vol. 40, No. 10, Pg. 21, 1 October 1989.

Bloombecker, J., "Short-Circuiting Computer Crime", Datamation, Vol. 35, No. 19, Pg. 71, 1 October 1989.

Bloombecker, J., and J. Buck, "Computer Ethics for Cynics", Computers and Society, Vol. 18, No. 3, Pgs. 30-32, ACM Special Interest Group on Computers and Society, New York, NY, July 1988.

Bologna, J. "Computer Insecurities: An Analysis of Recent Surveys on Computer Related Crime and Computer Security", Data Processing & Communications Security, Vol. 12, No. 4, Fall 1988.

Bologna, J. "The One Minute Fraud Auditor", Computers & Security, Vol. 8, No. 1, Pg. 29, 1 February 1989.

Boston Herald, "Computer Whiz Puts Virus in Computers", Pg. 1, Boston Herald, 5 November 1988.

Brand, R., "Attack of the Tiger Teams: Inside America's Computer Security Crisis", Tempus Books, August 1989.

Brenner, A., "LAN Security", LAN Magazine, August 1989.

Brunner, J., "The Shockwave Rider", Harper & Row, 1975.

Burger, R., "Computer Viruses: A High-Tech Disease", 2nd Edition, Abacus, Grand Rapids, Michigan, 1988.

Campbell, B., and C. Jackson, "The Internet Worm: Rethinking the Security Threat", Unisphere, Vol. 9, No. 1, Pgs. 44, 46, 48, April 1989.

Campell, D., "Computer Contagion", Security Management, Vol. 32, No. 10, Pg. 83, 1 October 1988.

Chain Store Age Executive, "Retail Technology: Computer 'Viruses'", Chain Store Age Executive, Vol. 64, No. 12, Pg. 67, 1 December 1989.

Chess, D., "Computer Viruses and Related Threats to Computer and Network Integrity", Computer Networks and ISDN Systems, Vol. 17, No. 2, 1989.

Christiansen, D., "A Matter of Ethics", IEEE Spectrum, Vol. 25, Pg. 15, August 1988.

Cohen, F., "Computational Aspects of Computer Viruses", Computers & Security, Vol. 8, No. 4., Pg. 325, 1 June 1989.

Cohen, F., "Models of Practical Defenses Against Computer Viruses", Computers & Security, Vol. 8, No. 2, Pg. 149, 1 April 1989.

Colyer, J., "Risks of Unchecked Input in C Programs", Forum Risks to the Publics in Computer and Related Systems, Vol. 7, No. 74, ACM Committee on Computers and Public Policy, 10 November 1988.

Commerce Clearing House, "Guide to Computer Law", (Topical Law Reports), Chicago, Ill., 1989.

Communications of the ACM, "Letters", ACM Forum, Vol. 32, No. 6, Pgs. 672-673, June 1989.

Communications of the ACM, "Letters", ACM Forum, Vol. 32, No. 9, Pgs. 1044-1045, September 1989.

Computers & Security, "Random Bits & Bytes", Computers & Security, Vol. 8, No. 3, Pg. 178, 1 May 1989.

Computer Law and Tax Report, "Difficult to Prosecute Virus Authors", Computer Law and Tax Report, Vol. 15, No. 5, Pg. 7, 1 December 1988.

Computer Law and Tax Report, "Virus Bill Introduced", Computer Law and Tax Report, Vol. 15, No. 4, Pg. 13, 1 November 1988.

Computerworld, "MIS Reacts", Pg. 157, 7 November 1988.

Cornell Computer Science Department, "Policy for the Use of the Research Computing Facility", Cornell University, 21 August, 1987.

Data Communications, "Internet Virus Aftermath: Is Tighter Security Coming?", Data Communications, Vol. 17, No. 14, Pg. 52, 1 December 1988.

Dean, P., "Was Science-fiction Novel Germ of a Computer Virus?", Los Angeles Times, San Diego County Edition, Part V, Pgs. 1, 2, & 3, 9 November 1988.

DeBow, Y., "Bankers Review Security Procedures After Virus Attack", Computer Banking, Vol. 6, No. 1, Pg. 8, January 1989.

Defense Data Network, "BSD 4.2 and 4.3 Software Problem Resolution", DDN MGT Bulletin #43, DDN Network Information Center, 3 November 1988.

Demaio, H., "Viruses - A Management Issue", Computers & Security, Vol. 8, No. 5, Pg. 381, 1 August 1989.

Denning, P., "The Science of Computing: The Internet Worm", American Scientist, Vol. 77, No. 2, Pgs. 126-128, March 1989.

Devoy, J., Gilssmann, R., and K. Miklofsky, "Media, File Management Schemes Facilitate WORM Utilization", Computer Technology Review, Vol. 8, No. 13, Fall 1988.

Dewdney, A., "Computer Recreations; Of Worms, Viruses and Core War", Scientific American, March 1989

Discover, "Technology: Communicable Computer Disease", Discover, Vol. 10, No. 1, Pg. 64, 1 January 1989.

El-Baghdadi, M., "The Pivotal Role in Computer Security", Security Management, Vol. 33, No. 7, Pg. 63, 1 July 1989.

Electronic Learning, "Computer Viruses: An Epidemic Real or Imagined?", Electronic Learning, Vol. 8, No. 6, April 1989.

Eloff, J., "Computer Security Policy: Important Issues", Computers & Security, Vol. 7, No. 6, Pg. 559, 1 December 1988.

Ellerbee, L., "And So It Goes", G.P. Putnam's Sons, Berkley Edition, June 1987.

Ellis, A., "Underwriting Update-Computer Viruses: Working Out the Bugs", Best's Review, Vol. 90, No. 1, Pg. 84, 1 May 1989.

Elmer-DeWitt, P., "Invasion of the Data Snatchers! - A 'Virus' Epidemic Strikes TERROR in the Computer World", Time Magazine, Technology Section, Pgs. 62-67, 26 September 1988.

Elmer-DeWitt, P., "The Kid Put Us Out of Action", Time Magazine, Pg. 76, 14 November 1988.

Elmer-DeWitt, P., "You Must Be Punished", Time Magazine, Technology Section, Pg. 66, 26 September 1988.

Fainberg, T., "The Night the Network Failed", New Scientist, Vol. 121, No. 1654, Pg. 38, 4 March 1989.

Fenwick, W., Chair, "Computer Litigation, 1985: Trial Tactics and Techniques", Litigation Course Handbook Series No. 280, Prepared for distribution at the Computer Litigation, 1985: Trial Tactics and Techniques Program, February-March 1985.

Fifield, K., "Smartcards Outsmart Computer Crime", Computers & Security, Vol. 8, No. 3, May 1989.

Fisher, L., "On the Front Lines in Battling Electronic Invader", The New York Times, November 1988.

Fites, P., Johnston, P., and M. Kratz, "The Computer Virus Crisis", Van Nostrand Reinhold, New York, NY., 1989

Forcht, K., Thomas, D., and K. Wigginton, "Computer Crime: Assessing the Lawyer's Perspective", Journal of Business Ethics, Vol. 8, No. 4 April 1989.

Friis, W., "Is Your PC Infected?", ABA Banking Journal, Vol. 81, No. 5, Pg. 49, 1 May 1989.

Gardner, E., Samuels, L., and B. Render, "Computer Security", The Journal of Information Systems Management, Vol. 6, No. 4, Pg. 42, Fall 1989.

Gardner, P., "The Internet Worm: What Was Said and When", Computers & Security, Vol. 8, No. 4, June 1989.

Gemignani, M., "Viruses and Criminal Law", Communications of the ACM, Vol. 32, No. 6, Pgs. 669-671, June 1989.

Gerlth, J., "Intruders Into Computer Systems Still Hard to Prosecute", The New York Times, 5 November 1988.

Gerrold, D., "When Harlie Was One", Ballentine Books, 1st Edition, 1972.

Gleissner, W., "A Mathematical Theory for the Spread of Computer Viruses", Computers & Security, Vol. 8, No. 1, Pg. 35, 1 February 1989.

Greenberg, R., "Know thy Viral Enemy: It's More Important Than Ever to Guard Your Data and Your System Against Infection by Computer Viruses", Byte, Vol. 14, No. 6, Pg. 275, 1 June 1989.

Greenia, M., "Computer Security Information Sourcebook", Lexikon Services, Sacramento, CA, 1989.

Harvard College, "Misuse of Computer Systems", Handbook for Students", Pg. 85, Harvard College, 1987-1988.

Hawkins, C., "What Users Should Know About Computer Viruses", Telecommunications, North American Edition, Vol. 23, No. 7, 1 July 1989.

Herrick, G., "Computer Viruses: Prevention is Better than Cure", The

Accountant's Magazine, Vol. 93, No. 992, Pg. 24, 1 March 1989.

Hertzoff, I., "Layer Your LAN", Security Management, Vol. 33, No. 9, Pg. 201, 1 September 1989.

Highland, H., "Reports from the Victims", Computers & Security, Vol. 8, No. 2, Pg. 101, 1 April 1989.

Hispanic Business, "Consumer Showcase: Bits & Bytes: From Thunderstorms to Disgruntled Employees to Computer Viruses, a Data System's Vulnerability is Often Overlooked until Disaster Strikes", Hispanic Business, Vol. 11, No. 8, Pg. 36, 1 August 1989.

Hoffer, J., and D. Straub, "The 9 to 5 Underground: Are You Policing Computer Crimes?", Sloan Management Review, Vol. 30, No. 4, Pg. 35, Summer 1989.

Hoffman, L., "Risk Analysis and Computer Security: Towards a Theory at Last", Computers & Security, Vol. 8, No. 1, Pg 23, 1 February 1989.

Hospitals, "Information Management: Electronic Computer Viruses are not Running Rampant in Hospital Information Systems, but Health Care Executives are Entirely Too Lax About Computer System Security", Vol. 63, No. 11, Pg. 64, 5 June 1989.

Huband, F., and R. Shelton, Editors, "Protection of Computer Systems and Software: New Approaches for Combating Theft of Software and Unauthorized Intrusion", Papers presented at a workshop sponsored by the National Science Foundation, 1986.

Hughes, W., "The Computer Fraud and Abuse Act of 1986, Congressional Record (30 April 1986)", Washington, D.C., 30 April 1986.

Industry Week, "Computer Flu Is After You", Industry Week, Vol. 238, No. 2, Pg. 39, 16 January 1989.

Information Executive, "Promoting Computer Ethics: The Next Generation", Information Executive, Vol., 2, No. 4, Pg. 42, Fall 1989.

Information Hotline, "Plan to Combat Computer Viruses", Vol. 21, No. 8, Pg. 10, 1 October 1989.

Jamieson, R., and L. Graham, "Security and Control Issues in Local Area Network Design, Computers & Security, Vol. 8, No. 4, Pg. 305, 1 June 1989.

Jander, M., "The Naked Network", Computer Decisions, Vol. 21, No. 4, Pg. 39, 1 April 1989.

Joyce, E., "Time Bomb: Inside The Texas Virus Trial", Computer Decisions, Vol. 20, No. 12, Pg. 38, 1 December 1988.

Keenan, T., "Emerging Vulnerabilities in Office Automation Security", Computers & Security, Vol. 8, No. 3, Pg. 223, 1 May 1989.

Kellam-Scott, B., "Profile: Bellcore Computer and Network Security Symposium", Bellcore Exchange, Vol. 5, No. 1, Pg. 24, 1 January 1989.

King, K., "Overreaction to External Attacks on Computer Systems Could be More Harmful Than the Viruses Themselves", Chronicle of Higher Education, Pg. A36, 23 November 1988. Also in: Educom Bulletin, Vol. 23, No. 4, Pg. 5, Winter 1988

Kluepfel, H., "Computer Use and Abuse: Computer Systems and Their Data are Vulnerable to Error, Omission, and Abuse", Security Management, Vol. 33, No. 2, Pg. 72, 1 February 1989.

Kocher, B., "A Hygiene Lesson", Communications of the ACM, Vol. 32, No. 6, Pg. 3, January 1989.

Kosko, J., "Computer Security Experts Advise Steps to Reduce the Risk of Virus Attacks", Virus Discussion List, 22 September 1989.

Kruys, J., "Security of Open Systems", Computers & Security, Vol. 8, No. 2, Pg. 139, 1 April 1989.

Lapsley, P., "'We are Under Attack. . .' (The Internet 'Worm': a Chronology)", UNIX Review, Vol. 7, No. 1, Pgs. 69-70, 72-73, January 1989.

Lerner, E., "Computer Virus Threatens to Become Epidemic", Aerospace America, Vol. 27, No. 2, Pg. 14, 1 February 1989.

Lewyn, M., and D. Carroll, "'Scary' Virus Clogs Top Computers", USA Today, Section A, Col. 2, Pg. 1, 4 November 1988.

Lim, B., "Protection of Computer Programs Under the Computer Program Protection Law of the Republic of Korea", Harvard International Law Journal, Vol. 30, No. 1, Pg. 171, Winter 1989.

Lu, W., and M. Sundareshan, "Secure Communication in Internet Environments: A Hierachical Key Management Scheme for End-to-End Encryption", IEEE Transactions on Communications, Vol. 37, No. 10, Pg. 1014, 1 October 1989.

Lunt, T., "Access Control Policies: Some Unanswered Questions", Computers & Security, Vol. 8, No. 1, Pg. 43, 1 February 1989.

Lynn, M., "Ethical Responsibility Key to Computer Security", The Educational Record, Vol. 70, No. 2, Pg. 36, Spring 1989.

Machalow, R., "Security for Lotus Files", Computers in Libraries, Vol. 9, No. 2, Pg. 19, 1 February 1989.

Maher, J., and J. Hicks, "Computer Viruses: Controller's Nightmare", Management Accounting, Vol. 71, No. 4, Pg. 44, 1 October 1989.

Markoff, J., "Author of Computer 'Virus' is Son of U.S. Electronic Security Expert", Pgs. A1, A7, The New York Times, 5 November 1988.

Markoff, J., "Computer Experts Say Virus Carried No Hidden Dangers", The New York Times, 9 November 1988.

Markoff, J., "Computer Snarl: A 'Back Door' Ajar", Pg. B10, The New York Times, 7 November 1988.

Markoff, J., "Learning to Love the Computer Whiz", The New York Times, 8 November 1988.

Markoff, J., "The Computer Jam: How It Came About", The New York Times, 9 November 1988.

Markoff, J., "U.S. is Moving to Restrict Access to Facts About Computer Virus", Pg. A28, The New York Times, 11 November 1988.

Markoff, J., "'Virus' in Military Computers Disrupts Systems Nationwide", The New York Times, 4 November 1988.

Marshall, E., "The Worm's Aftermath", Science, Vol. 242, Pg. 1121, 25 November 1988.

Martin, M., and R. Schinzinger, "Ethics in Engineering", McGraw Hill, 2nd Edition, 1989.

Martin, N., "Revenge of the Nerds", The Washington Monthly, Vol. 20, No. 12, Pg. 21, 1 January 1989.

McAfee, J., "The Virus Cure", Datamation, Vol. 35, No. 4, Pg. 29, 15 February 1989.

McEwen, J., "Dedicated Computer Crime Units", Report Contributors: D. Fester and H. Nugent, Prepared for the National Institute of Justice, U.S. Department of Justice, by Institute for Law and Justice, Inc.

under contract number OJP-85-C-006, Washington, D.C., 1989.

Menkus, B., "It's Time to Rethink Data Processing Fire Protection", Computers & Security, Vol. 8, No. 5, Pg. 389, 1 August 1989.

Menkus, B., "The Computer Virus Situation is not Encouraging", Computers & Security, Vol. 8, No. 2, Pg. 115, 1 April 1989.

Menkus, B., "The Employee's Role in Protecting Information Assets", Computers & Security, Vol. 8, No. 6, Pg. 487, 1 October 1989.

Menkus, B., "Understanding Password Compromise", Computers & Security, Vol. 7, No. 6, Pg. 549, 1 December 1989.

Menkus, B., "U.S. Government Agencies Belatedly Address Information System Security Issues", Computers & Security, Vol. 7, No. 4, Pg. 361, 1 August 1988.

Meredith, D., "Cornell Panel Concludes Morris Responsible for Computer Worm", Cornell Chronicle, April 1989.

Miller, Jr., K., "Computer Viruses", Business and Economic Review, Vol. 35, No. 4, Pg. 36, 1 June 1989.

Mizock, M., "Ethics--The Guiding Light of Professionalism", Data Management, Vol. 24, No. 8, August 1986.

Modern Railroads, "How to Outwit Computer 'Hackers'", Modern Railroads, Vol. 44, No. 3, Pg. 40, 1 February 1989.

Moir, D., "Maintaining System Security", Dr. Dobb's Journal of Software Tools for the Pro, Vol. 14, No. 6, Pg. 75, 1 June 1989.

Munro, N., "Big Guns Take Aim at Virus", Government Computer News, Vol. 7, No. 24, Pgs. 1, 100, November 1988.

National Computer Security Center, "Proceedings of the Virus Post-Mortem Meeting", NCSC, St. George Meade, MD, 8 November 1988.

National Institute of Standards and Technology, "Computer Viruses and Related Threats: A Management Guide", NIST Special Publication 500-166, August 1989.

Neumann, P., Editor, "Forum of Risks to the Public in Computers and Related Systems", Vol. 7, No. 69, ACM Committee on Computers and Public Policy, 3 November 1988.

Newhouse News Service, "Congressmen Plan Hearings on Virus", The

Seattle Times, Pg. B2, 27 November 1988.

NSF Network Service Center (NNSC), "Internet Computer Virus Update", NSFNET, Cambridge, MA, 4 November 1988.

Ostapik, F., "The Effect of the Internet Worm on Network and Computer Security", Connextions, Vol. 3, No. 9, Pgs. 16-17, September 1989.

Ostrow, R., and T. Maugh II, "Legal Doubts Rise in Computer Virus Case", Los Angeles Times, Part I, Col. 1, Pg. 4, 9 November 1988.

Page, B., "A Report on the Internet Worm", University of Lowell, Computer Science Department, 7 November 1988.

Palmore, T., "Computer Bytes: Viruses and Vaccines", TechTrends, Vol. 34, No. 2, Pg. 26, 1 March 1989.

Parker, D., "Fighting Computer Crime", Scribner, New York, 1983.

PC Week, "'Worm' Attacks National Network", Pg. 8, 7 November 1988.

Perry, W., "Why Software Defects So Often Go Undiscovered", Government Computer News, Vol. 7, No. 24, Pg. 85, 21 November 1988.

Peterson, I., "Worming into a Computer's Vulnerable Core", Science News, Volume #134, 12 November 1988.

Phelps, E., "Bug Bytes", Security Management, Vol. 33, No. 9, Pg. 85, 1 September 1989.

Presstime, "Contagious Communication", Presstime, Vol. 11, No. 3, March 1989.

Radai, Y., "The Israeli PC Virus", Computers & Security, Vol. 8, No. 2, Pg. 111, 1 April 1989.

Reese, L., "Of MICE and Men", Security Management, Vol. 33, No. 9, Pg. 89, 1 September 1989.

Resource Management, "Computer Viruses: Background and Recommendations for Keeping Software Healthy are Detailed", Resource Management, Pg. 8, 1 July 1989.

Richards, T., and R. Knotts, "Top Management's View of Computer Related Fraud", Sig Security, Audit & Control Review, Vol. 6, No. 4, Pg. 34, Winter 1989.

Rivera, A., "Computer Viruses: A Different Perspective", Data

Processing & Communications Security, Vol. 13, No. 1, Winter 1989.

Rowe, J., Shelton, C., and M. Krohn, "Avoiding Computer Viruses", Business Education Forum, Vol. 44, No. 2, Pg. 17, 1 November 1989.

Royko, M., "Here's How to Stop Computer Vandals", Chicago Tribune, 6 November 1988.

Rubin, H., and A. Paliotta, "Perimeter Security for Telecommunication with External Entities", The Internal Auditor, Vol. 46, No. 2, Pg. 40, March-April 1989.

Rubin, M., "Private Rights, Public Wrongs: the Computer and Personal Privacy", Ablex Publishing 1988.

Sampson, K., "Computer Viruses: Not Fads, Not Funny", The Office, Vol. 110. No. 4, Pg. 56, 1 October 1989.

Samuelson, P., "Can Hackers be Sued for Damages Caused by Computer Viruses?", Communications of the ACM, Vol. 32, No. 6, Pgs. 666-669, June 1989.

Schneider, W., "Computer Viruses: What They Are, How They Work, How They Might Get You, and How to Control Them in Academic Institutions", Behavior Research Methods, Instruments, & Computers, Vol. 21, No. 2, Pg. 334, 1 April 1989.

Schultz, J., "Low Cost Security Solutions for Personal Computers", Signal, Vol. 44, No. 3, Pg. 71, 1 November 1989.

Schweitzer, J., "Protecting Information on Local Area Networks", Butterworths, Boston, 1988.

Seeley, D., "Password Cracking: A Game of Wits", Communications of the ACM, Vol. 32, No. 6, Pgs. 700-703, June 1989.

Shadabuddin, S., "Computer Security Problems and Control Techniques", American Business Review, Vol. 7, No., 1, Pg. 14, 1 January 1989.

Shaw, E., Jr., "Computer Fraud and Abuse Act of 1986, Congressional Record (3 June 1986), Washington, D.C., 3 June 1986.

Sheiman, D., "Legal Affairs: Coming Soon...To A Personal Computer Near You", The Amicus Journal, Vol. 11, No. 3, Pg. 38, Summer 1989.

Siegel, L. and J. Markoff, "The High Cost of High Tech, the Dark Side of the Chip", Harper & Row, New York, 1985.

Sims, C., "Researchers Fear Computer 'Virus' Will Slow Use of National Network", The New York Times, 14 November 1988.

Sitomer, C., "Crooks Find Computers Useful: Terrorists See Vulnerable Targets", The Christian Science Monitor, Vol. 79, No. 8, Sec. A, Pg. 6, December 1986.

Slayden, P. II, "Computer Flu Blues: Computer Managers Must be Ready to Provide Vaccines Against Infectious Computer Viruses", Security Management, Vol. 33, No. 8, Pg. 108, 1 August 1989.

Spafford, E., "Some Musing on Ethics and Computer Break-Ins", Proceedings of the Winter USENIX Conference, USENIX Association, San Diego, CA, February 1989.

Spafford, E., "The Internet Worm: Crisis and Aftermath", Communications of the ACM, Vol. 32, No. 6, Pgs. 689-698, June 1989.

Spafford, G., "A Cure!!!!!", Forum Risks to the Publics in Computer and Related Systems, Vol. 7, No. 70, ACM Committee on Computers and Public Policy, 3 November 1988.

Spafford, G., "A Worm 'condom'", Forum Risks to the Publics in Computer and Related Systems, Vol. 7, No. 70, ACM Committee on Computers and Public Policy, 3 November 1988.

State of Wisconsin, "Computer Law - State of Wisconsin Statute", Chapter 293, Laws of 1981, Section 943.70, Computer Crimes.

Steinberg, T., "Developing a Computer Security Charter", Sig Security, Audit & Control Review, Vol. 6, No. 4, Pg. 12, Winter 1989.

Stipp, D., and B. Davis, "New Computer Break-Ins Suggest 'Virus' May Have Spurred Hackers", The Wall Street Journal, 2 December 1988.

Stoll, C., "How Secure are Computers in the U.S.A.?", Computers & Security, Vol. 7, No. 6, Pg. 543, 1 December 1988.

Stoll, C., "Stalking the Wily Hacker", Communications of the ACM, Vol. 31, No. 5, Pgs. 484-497, ACM, New York, NY, May 1988.

Stoll, C., "The Cuckoo's Egg", ISBN 00385-24946-2, Doubleday, 1989.

Stuller, J., "Computer Cops and Robbers", Across the Board, Vol. 26, No. 6, June 1989.

Tester, D., "The Key to Data Security", Security Management, Vol. 33, No., 9, Pg. 206, 1 September 1989.

The Accountant, "Computer Viruses", No. 5829, Pg. 25, 1 September 1989.

The Economist, "Halting Computer Hackers", The Economist, Vol. 313, No. 7626, Pg. 18, 28 October 1989.

The Engineer, "Computer Security, Moves to Outlaw Computer Hackers are being Complicated by Computer Viruses", The Engineer, Vol. 268, No. 6935, 23 February 1989.

The Engineer, "Disk Diseases", The Engineer, Vol. 267, No. 6921, Pg. 28, 17 November 1988.

The New York Times, "Forgetfulness and the 'Virus'", The New York Times, 7 November 1988.

The New York Times, "Letter Bomb of the Computer Age", The New York Times, 5 November 1988.

The Wall Street Journal, "Spreading a Virus", A Wall Street Journal News Roundup, 7 November 1988.

Time Magazine, Letters Section, "Poison Program", Pg. 6, 5 December 1988.

Tinto, M., "Computer Viruses: Prevention, Detection, and Treatment", National Computer Security Center C1 Technical Report C1-001-89, June 1989.

Trible, P., "The Computer Fraud and Abuse Act of 1986", U.S. Senate Committee on the Judiciary, 1986.

United States, "Computer Fraud and Abuse Act of 1986, An Act to Amend Title 18, United States Code, to Provide Additional Penalties for Fraud and Related Activities in Connection with Access Devices and Computers, and for Other Purposes", Washington, D.C., G.P.O., Distributor, 1986.

United States Congress House Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, "Implementation of the Computer Security Act: Hearing Before the Subcommittee on Transportation, Aviation, and Materials of the Committee on Science, Space, and Technology", U.S. House of Representatives, One Hundredth Congress, Second Session, Washington, D.C., 22 September 1988.

United States Congress House Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials,

"Implementation of the Computer Security Act: Hearing Before the Subcommittee on Transportation, Aviation, and Materials and the Subcommittee on Science, Research, and Technology of the Committee on Science, Space, and Technology", U.S. House of Representatives, One Hundred First Congress, First Session, Washington, D.C., 21 March 1989.

United States Congress Senate Committee on the Judiciary, "The Computer Fraud and Abuse Act of 1986, Hearing before the Committee on the Judiciary", United States Senate, Ninety-ninth Congress, Second Session, Washington, D.C., 16 April 1986.

United States Congress Senate Committee on the Judiciary, "The Computer Fraud and Abuse Act of 1986, Report (to accompany H.R. 4712)", Washington, D.C., 22 May 1986.

United States Congress Senate Committee on the Judiciary, "The Computer Fraud and Abuse Act of 1986, Report Together with Additional Views", Ninety-ninth Congress, Second Session, Washington, D.C., 3 September 1986.

United States General Accounting Office, "Computer Security", GAO/IMTEC-89-57, June 1989.

United States of America, "Computer Security Act of 1987", G.P.O. Distributor, Washington D.C., 1988.

UNIX Today!, "Uncle Sam’s Anti-Virus Corps", UNIX Today!, Pg. 10, 23 January 1989.

Vance, M., "Computer Crime", Vance Bibliographies, Monticello, Ill., February 1988.

Vasilyev, D., and Y. Novikov, "Technology: Computer Viruses", Soviet Life, No. 394, Pg. 37, 1 July 1989.

Wasik, M., "Law Reform Proposals on Computer Misuse", The Crimminal Law Review, Pg. 257, 1 April 1989.

White, C. Jr., "Viruses and Worms: A Campus Under Attack", Computers & Security, Vol. 8, No. 4, Pg. 283, 1 June 1989.

White, S., and D. Chess, "Coping with Computer Viruses and Related Problems", IBM Research Report RC 14405 (#64367), January 1989.

Wines, M., "A Family’s Passion for Computers, Gone Sour", Pg. 1, The New York Times, 11 November 1988.

Wines, M., "'Virus' Eliminated, Defense Aides Say", The New York Times, 5 November 1988.

Winter, C.," Virus Infects Huge Computer Network", Chicago Tribune, Section I, Col. 2, Pg. 1, 4 November 1988.

Wiseman, S., "Preventing Viruses in Computer Systems", Computers and Security, Vol. 8, No. 5, Pg. 427, 1 August 1989.

Wood, C., "Planning: A Means to Achieve Data Communications Security", Computers & Security, Vol. 8, No. 3, Pg. 189, 1 May 1989.

Yovel, S., "Conquering Computer Viruses", Security Management, Vol. 33, No. 2, Pg. 64, 1 February 1989.

Zajac, B., "Disaster Recovery - Are You Really Ready?", Computers & Security, Vol. 8, No. 4, Pg. 297, 1 June 1989.

Zajac, B., "Legal Options to Computer Viruses", Computers & Security, Vol. 8, No. 1, Pg. 25, 1 February 1989.

Zajac, B., "Viruses: Should We Quit Talking About Them", Computers & Security, Vol. 7, No. 5, Pg. 471, 1 October 1989.

10. Security Considerations

If security considerations had not been so widely ignored in the Internet, this memo would not have been possible.

Author's Address

Joyce K. Reynolds
University of Southern California
Information Sciences Institute
4676 Admiralty Way
Marina del Rey, CA 90292

Phone: (213) 822-1511

EMail: JKREY@ISI.EDU