The Cornell Commission: On Morris and the Worm

After careful examination of the evidence, the Cornell commission publishes its findings in a detailed report that sheds new light and dispels some myths about Robert T. Morris and the Internet worm.

Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, Thomas Santoro

Robert Tappan Morris, Jr. worked alone in the creation and spread of the Internet worm computer program that infected approximately 6,000 computers nationwide last November. That principal conclusion comes from a report issued last April 3, by an internal investigative commission at Cornell University, Ithaca, NY.

The report labeled Morris' behavior "a juvenile act that ignored the clear potential consequences." Of the graduate student's intentions in releasing the virus, the commission claims: "It may simply have been the unfocused intellectual meandering of a hacker completely absorbed with his creation and unharnessed by considerations of explicit purpose or potential effect."

Morris is currently on leave of absence from Cornell, and the university is prohibited by federal law from commenting further on his academic status. Morris was not interviewed by the commission, a decision he made under advice of his attorney. According to Cornell Provost Robert Barker, both the federal prosecutors and Morris' defense attorney asked that the release of the report be delayed. "We fully understand their reasons for this request," he said. "However, after six months we feel an overriding obligation to our colleagues and to the public to reveal what we know about this profoundly disturbing incident."

The Cornell commission, chaired by M. Stuart Lynn, vice president of information technologies, included professors Theodore Eisenberg, law; David Gries, computer science; Juris Hartmanis, computer science; Don Holcomb, physics; and Thomas Santoro, Associate University Counsel. The objective of the panel was to determine the involvement of Morris or of other members of the Cornell community in the worm attack and the implications of the worm for Cornell policies. They also studied the motivation and ethical issues underlying the worm's development and release.

The following excerpt is the Summary of Findings and Comments section of the commission's 45-page report entitled **The Computer Worm**. To obtain a copy of the full report, which includes detailed accounts of the commission's findings, supportive arguments, and investigative methods, along with copies of news clippings, program comments, and full text versions of the preceding articles by Eugene Spafford and Donn Seeley, contact: The Office of the Vice President for Information Technologies, 308 Day Hall, Cornell University, Ithaca, NY 14853-2801, (607) 255-3324.

SUMMARY OF FINDINGS

Based on the evidence presented, the commission[1] finds that:

- Robert Tappan Morris, a first-year computer science graduate student at Cornell, created the worm and unleashed it on the Internet.
- In the process of creating and unleashing the worm, Morris violated Computer Science Department policy on the use of departmental research computing facilities.

Impact of the Worm

- The performance of computers "infected" by the worm degraded substantially, unless remedial steps were taken. Eventually such infected computers would come to a halt. These symptoms were caused

[1] The commission has chosen not to adopt an express standard of proof for its findings. The findings are only qualified where the Commission cannot reach a definitive conclusion.

by uncontrollable replication of the worm clogging the computer's memory. The worm, however, did not modify or destroy any system or user files or data.
- Based on anecdotal and other information, several thousand computers were *in*fected[2] by the worm. The commission has not systematically attempted to estimate the exact number infected. Many thousands more were *af*fected in the sense that they had to be tested for infection and preventive measures applied even if the computers were not infected. It appears that the operation of most infected and potentially affected computers and of the research done on those computers was brought to a halt in order to apply remedial or preventive measures, all of which required the diversion of considerable staff time from more productive efforts.

Mitigation Attempts

- Morris made only minimal efforts to halt the worm once it had propagated, and did not inform any person in a position of responsibility as to the existence and content of the worm.

Violation of Computer Abuse Policies

- The Cornell Computer Science Department "Policy for the Use of the Research Computing Facility" prohibits "use of its computer facilities for browsing through private computer files, decrypting encrypted material, or obtaining unauthorized user privileges." All three aspects of this policy were violated by Morris.
- Morris was apparently given a copy of this policy but it is not known whether he read it. Probably he did not attend the lecture during orientation when this policy was discussed, even though he was present on campus.

Intent

- Most probably Morris did not intend for the worm to destroy data or other files or to interfere with the normal functioning of any computers that were penetrated.
- Most probably Morris intended for the worm to spread widely through host computers attached to the network in such a manner as to remain undiscovered. Morris took steps in designing the worm to hide it from potential discovery, and yet for it to continue to exist in the event it actually was discovered. It is not known whether he intended to announce the existence of the worm at some future date had it propagated according to this plan.
- There is no direct evidence to suggest that Morris intended for the worm to replicate uncontrollably. However, given Morris' evident knowledge of systems and networks, he knew or clearly should have known that such a consequence was certain, given the design of the worm. As such, it appears that Morris failed to consider the most probable consequences of his actions. At the very least, such failure constitutes reckless disregard of those probable consequences.

Security Attitudes and Knowledge

- This appears to have been an uncharacteristic act for Morris to have committed, according to those who knew him well. In the past, particularly while an undergraduate at Harvard University, Morris appears to have been more concerned about protecting against abuse of computers rather than in violating computer security.
- Harvard's policy on misuse of computer systems contained in the Harvard Student Handbook clearly prohibited actions of the type inherent to the creation and propagation of the worm. For this and other reasons, the commission believes that Morris knew that the acts he committed were regarded as wrongful acts by the professional community.
- At least one of the security flaws exploited by the worm was previously known by a number of individuals, as was the methodology exploited by other flaws. Morris may have discovered the flaws independently.
- Many members of the UNIX® community are ambivalent about reporting security flaws in UNIX out of concern that knowledge of such flaws could be exploited before the flaws are fixed in all affected versions of UNIX. There is no clear security policy among UNIX developers, including in the commercial sector. Morris explored UNIX security issues in such an ambivalent atmosphere and received no clear guidance about reporting security flaws from his peers or mentors at Harvard or elsewhere.

Technical Sophistication

- Although the worm was technically sophisticated, its creation required dedication and perseverance rather than technical brilliance. The worm could have been created by many students, graduate or undergraduate, at Cornell or at other institutions, particularly if forearmed with knowledge of the security flaws exploited or of similar flaws.

Cornell Involvement

- There is no evidence that anyone from the Cornell community aided Morris or otherwise knew of the worm prior to its launch. Morris did inform one student earlier that he had discovered certain security weaknesses in UNIX. The first that anyone at Cornell learned that any member of the Cornell community might have been involved came at approximately 9:30 p.m. on November 4, 1988 when the Cornell News Service was contacted by the *Washington Post*.

Ethical Considerations

- Prevailing ethical beliefs of students towards acts of this kind vary considerably from admiration to tolerance to condemnation. The computer science profession as a whole seems far less tolerant, but

[2] We use the term "infect" to signify that at least one copy of the worm was left on the penetrated computer.

® UNIX is a registered trademark of AT&T.

BONNER & O'CONNELL
A PARTNERSHIP INCLUDING A
PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
900 17TH STREET, N.W., SUITE 600
WASHINGTON, D.C. 20006
(202) 462-1300 CABLE: BONOCS
TELECOPIER (202) 833-2021

WALTER J. BONNER*
EDWARD C. O'CONNELL*
STEPHEN C. GLASSMAN, P.C.**
THOMAS A. GUIDOBONI*
JOHN C. HAYES, JR.*
JOHN T. BRENNAN, JR
DAVID W. O'BRIEN*
THOMAS B. SHULL
KATHLEEN M. STRATTON

PAUL R. DEAN
OF COUNSEL

401 BROADWAY
SUITE 308
NEW YORK, NEW YORK 10013

5615 RIGGS ROAD
GAITHERSBURG, MARYLAND 20879
(301) 670-8200

600 CAMERON STREET
2ND FLOOR
ALEXANDRIA, VIRGINIA 22314

ADMITTED ALSO IN * MD ** NY

January 4, 1989

SENT VIA TELECOPY

Thomas Mead Santoro, Esquire
Associate General Counsel
Cornell University
500 Day Hall
Ithaca, New York 14853

Re: Robert T. Morris

Dear Mr. Santoro:

This letter is intended to confirm in writing our earlier telephone discussions. You have advised me that the Provost of Cornell University has initiated an investigation into the so-called "computer virus" incident, and that the results of this investigation are to be made available to the general public. You further stated that this inquiry is neither a disciplinary proceeding nor part of the academic grievance process at Cornell, but rather is sui generis. Finally, you requested that Mr. Morris make himself available for an interview by the Cornell investigators.

As you are well aware, the United States Attorney for the Northern District of New York has been pursing a grand jury investigation into the same computer virus incident and Mr. Morris' possible involvement therein. The eventual outcome of this process could be a multiple count federal felony indictment against Mr. Morris, and thereafter a trial on this indictment. Under these circumstances, I have advised Mr. Morris to rely on his constitutional right to remain silent, and he has chosen to follow this advice. Therefore, regretfully, we must decline Cornell's request for an interview at this time.

Mr. Morris does wish me to convey to you his willingness and, indeed, strong desire to cooperate fully with the inquiry by Cornell, once the criminal proceedings are concluded.

I hope you will make this letter available to the persons undertaking the inquiry on behalf of Cornell and explain to them, if necessary, the reasons for this decision.

If you have any questions, or if I can be of further assistance, please contact me.

Sincerely,

BONNER & O'CONNELL

By _____
Thomas A. Guidoboni

TAG/ps

cc: Robert T. Morris

Letter from Morris' attorney

the attitudes of the profession may not be well communicated to students.

Community Sentiment

- Sentiment among the computer science professional community appears to favor strong disciplinary measures for perpetrators of acts of this kind. Such disciplinary measures, however, should not be so stern as to damage permanently the perpetrator's career.

University Policies on Computer Abuse

- The policies and practices of the Cornell Computer Science Department regarding computer abuse and security are comparable with those of other computer science and many other academic departments around the nation.
- Cornell has policies on computer abuse and security that apply to its central facilities, but not to departmental facilities.
- In view of the pervasive use of computers throughout the campus, there is a need for *university-wide* policy on computer abuse. The commission recommends that the Provost establish a committee to develop such policy, and that such policy appear in all legislative and policy manuals that govern conduct by members of the Cornell community.
- In view of the distributed nature of computing at Cornell, there is also a need for a university-wide committee to provide advice and appropriate standards on security matters to departmental computer and network facility managers. The commission recommends that the Vice President for Information Technologies be asked to establish such a committee.

COMMISSION COMMENTS

The commission believes that the acts committed in obtaining unauthorized passwords and in disseminating the worm on the national network were wrong and contrary to the standards of the computer science profession. They have little if any redeeming technical, social or other value. The act of propagating the worm was fundamentally a juvenile act that ignored the clear potential consequences. The act was selfish and inconsiderate of the obvious effect it would have on countless individuals who had to devote substantial time to cleaning up the effects of the worm, as well as on those whose research and other work was interrupted or delayed.

Contrary to the impression given in many media reports, the commission does not regard this act as an heroic event that pointed up the weaknesses of operating systems. The fact that UNIX, in particular BSD UNIX, has many security flaws has been generally well known, as indeed are the potential dangers of viruses and worms in general. Although such security flaws may not be known to the public at large, their existence is accepted by those who make use of UNIX. It is no act of genius or heroism to exploit such weaknesses.

A community of scholars should not have to build walls as high as the sky to protect a reasonable expectation of privacy, particularly when such walls will equally impede the free flow of information. Besides, attempting to build such walls is likely to be futile in a community of individuals possessed of all the knowledge and skills required to scale the highest barriers.

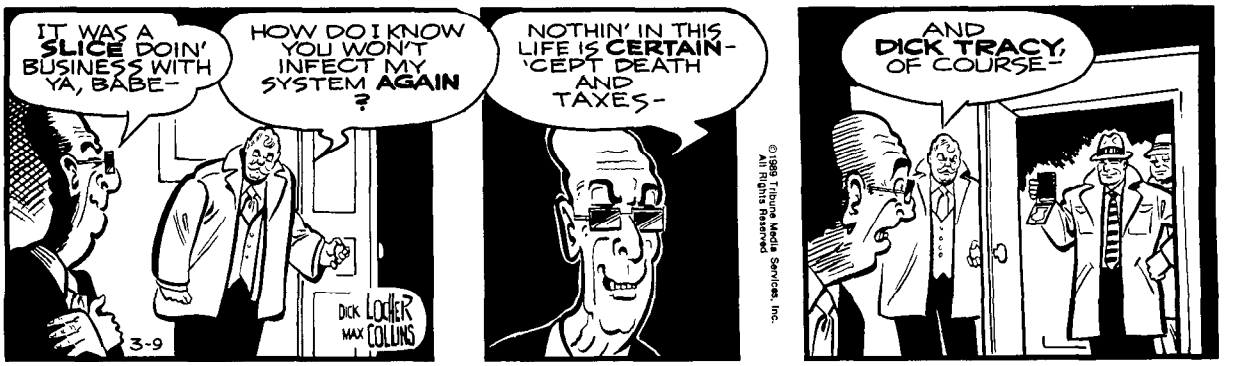
There is a reasonable trust between scholars in the pursuit of knowledge, a trust upon which the users of the Internet have relied for many years. This policy of trust has yielded significant benefits to the computer science community and, through the contributions of that community, to the world at large. Violations of such a trust cannot be condoned. Even if there are unintended side benefits, which is arguable, there is a greater loss to the community as a whole.

This was not a simple act of trespass analogous to wandering through someone's unlocked house without permission but with no intent to cause damage. A more apt analogy would be the driving of a golf cart on a rainy day through most houses in a neighborhood. The driver may have navigated carefully and broken no china, but it should have been obvious to the driver that the mud on the tires would soil the carpets and that the owners would later have to clean up the mess.

Experiments of this kind should be carried out under controlled conditions in an isolated environment. Cornell Computer Science Department faculty would certainly have cooperated in properly establishing such an experiment had they been consulted beforehand.

The commission suggests that media exaggerations 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 science and the advancement of knowledge through their patiently constructed dissertations; and who subject their work to the close scrutiny and evaluation of their peers, and not to the interpretations of the popular press.

DICK TRACY®



Reprinted with permission: Tribune Media Services.