ETHICOMP96

(Ethics and Computer)

Ill International Conference

VALUES AND SOCIAL RESPONSIBILITIES OF THE COMPUTER SCIENCE

6-8 November 1996

PROCEEDINGS

Volume 1

Organized by

Pontificial University of Salamanca in Madrid and Foundation Pablo VI, Spain

Luis Joyanes and Porfirio Barroso

In association with

Complutense University of Madrid, Spain

Porfirio Barroso

Centre for Computing and Social Responsibility

De Montfort University, UK

Simon Rogerson

Research Center on Computers Southern Connecticut State University, USA

Terrell Ward Bynum

ETHICOMP96

(Ethics and Computer)

VALUES AND SOCIAL RESPONSIBILITIES OF THE COMPUTER SCIENCE

Venue

Pontifical University of Salamanca in Madrid

Paseo Juan XXIII, 3

28040 MADRID, Spain

6-8 November 1996

PROCEEDINGS

Volume 1

Editors

Chairman

Porfirio Barroso

Director	Director	Director
Terell Ward Bynum	Simon Rogerson	Luis Joyanes

Sponsors

Ministerio de Educaci6n y Cultura

Facultad de Ciencias de la Informaci6n, Universidad Complutense de Madrid

Universidad de San Pablo CEU Comunidad Aut6noma de Madrid

Banco Central Hispano El Corte Inglés

Mapfre IBM

ETHICOMP96

(Ethics and Computer)

Values and Social Responsibilities of the Computer Science

PROCEEDINGS

Volume 1

Venue

Pontificial University of Salamanca in Madrid Paseo Juan xxm, 3

28040 MADRID, spain

Editors

Chairman

PORFIRIO BARROSO

Director	Director	Director
Terell Ward Bynum	Simon Rogerson	Luis Joyanes

Sponsors

Ministerio de Educaci6n y Cultura

Facultad de Ciencias de la Informaci6n,

Universidad Complutense de Madrid

Universidad de San Pablo CEU

Comunidad Aut6noma de Madrid

Banco Central Hispano

El Corte Inglés

Mapfre

IBM

ETHICAL ISSUES ARISNG FROM EXPOSURE TO COMPUTER VIRUSES TROUGH CONTUTER USAGE

AUTHOR: Melius Weideman, Cape Technikon, South Africa

1. ABSTRACT

The ethical issues surrounding computer viruses and the computer user are considered. Two basic types of computer viruses exist: file and boot sector viruses. File viruses attach themselves to executable files, while boot sector viruses hide themselves in the system areas of disks. The names, motives and other detail of three virus authors are discussed, as well as the motives of virus authors in general.

There is a difference in the value program and data files respectively have to the user. Actual results of virus infections, as determined by the research and implications for the computer user are inspected. Research has proven that some viruses can do damage to stored data, while others do no more than annoy the user. A definite level of technical expertise and insight is required to successfully remove a virus from an infected disk.

A very common method of spreading a virus is through the copying of files and disks. The ethical issues surrounding the copying of commercial programs are noted. The future of viruses in the computer world is uncertain: in the absence of DOS most current viruses will probably cease to exist.

2. INTRODUCTION

eth i+cal - in accordance with principles of conduct that are considered correct, esp. those of a given profession or group.

Collins English Dictionary

In this paper some of the ethical issues regarding computer infections as a result of computer usage are investigated.

The basic structure of this paper is as follows:

2.2 VRUSES?

The mere fact that intelligent people spend time, money and effort on computer virus prevention, detection and eradication raises the question: what are the ethical issues involved when considering computer viruses? Why was a computer virus unheard of some years ago, while today every child under 10 knows the name of the latest virus?

A comparison of a computer virus with the Aids virus could shed some light on the topic. Being infected with either one raises eyebrows - “It should not have happened". Both could be dangerous - loss of data or loss of life. You can contract either one by certain morally unacceptable actions - copying software or unnatural relations (and other acceptable, known reasons).

The actual number of viruses known world-wide grows daily, and is currently just over the 8000 mark 8281 according to a well-known antivirus program. (Solomon, 1996)

2.3 RESEARCH

The author has undertaken a research project recently, where the actual damage done by viruses to files stored by computer users was investigated. (Weideman 1994). During the preliminary phases of this project, a Virus Clinic was held where members of the public and users from industry could make use of available expertise on viruses. Results from this Clinic proved that of all the virus infection complaints received, only 44% turned out to be true infections. Of the remaining 56%, 23% were just queries on viruses in general. The other 33% of the complaints were computer problems due to other factors.

A questionnaire was later used (388 sent out, 190 resumed) to find out what users in the industry have experienced with respect to virus infections. Many users gave unacceptable reasons for their claim that their computer had been infected by a virus. A total of 39% of the respondents listed acceptable reasons for their claims. These facts proved that there exists a fair amount of ignorance amongst computer users about viruses in general.

Transparency: Copy of directory showing uninfected file sizes.

3 VIRUS BASICS

3.1 VIRUS TYPES

We cannot talk about computer viruses without clarifying at least some of the apparently technical jargon dumped on us by the virus revolution.

Every computer virus can be classified as either a file or a boot sector virus. A file virus is a program which attaches itself to a normal executable program file, and loads itself into memory when that file is run from disk.

A boot sector virus Writes its code into one of the system areas (i.e. a non-user area) on a magnetic disk, and loads itself into memory when an attempt is made to boot from that disk. (Weidemam 1994)

As an example, we can look at one of each of the two types.

Transparency: Copy of directory showing infected file sizes.

After loading the Jerusalem virus into memory first, then running the files as listed, these files became infected with the virus. The size increase in the file is apparent, where the increase is the sue of the virus program.

Transparency: Copy of directory showing infected file sizes

Similarly, a copy of a healthy boot sector shows some recognisable disk areas of a DOS-formulated disk.

Transparency: Healthy Boot Sector

Comparing this with a copy of the b90t sector of the same disk after having been infected by the Exebug virus, shows totally unintelligible information. What you are seeing here is of course the code of the Exebug virus, and not the normal boot sector information.

Transparency: Exebug Infected Boot Sector

3.2 RESEARCH

The results of the author's research proved that certain viruses cause more infections than others.

Transparency: List of most common Viruses in SA

From this list, a selection of 15 viruses were chosen for the rest of the research project.

Transparency: List of 15 viruses used in research.

These viruses were then used, one at a time, to infect a range of disks containing a variety of application programs and data files. The resultant infected disks were then inspected to ascertain the data loss, if any. After recording all results, the memory and disks were disinfected, and the process repeated for the next virus. Results of this research are discussed later.

4 VIRUS AUTHORS

4.1 AUTHORS

Is it ethically correct to write, release or knowingly propagate a computer virus? If the motives of all virus authors were known, this question would be easy to answer.

Virus authors do not have any intentions of making money from their endeavours, and therefore do not advertise. Hence not a great many virus authors are known, and it is difficult to establish who the authors were of certain viruses. Their motives are even more difficult to determine. A few authors, however, are known, and a brief look at these authors and there apparent motives might answer some of the questions on ethics posed earlier.

4.2 INTERNET WORM

The much publicised case of the Internet worm is worth inspecting. On 2 November 1988, a rogue program (later called the Internet worm) was released onto the net by a young graduate, Robert Morris. An interesting point to note is that his father was a computer security expert at the USA National Security Agency! This program contained a programming error, which caused it to replicate far faster than

planned. As a result, many thousands of computer systems ground to a halt because of the large number of (otherwise harmless) programs running in their memories. (Spafford, 1989)

Apparently Morris's motivation was to prove to these superiors that the security on their Unix system was inadequate. Whatever the real reason was, computer users argued for years (some still do!) about the ethical correctness of young Morris's actions. On the one hand, the worm incident certainly woke up many network administrators to evaluate the security on their own systems - a positive result. However, it was also felt that an invasion of many user's privacy took place, not to mention the thousands of expensive man-hours wasted in the ensuing attempt to recti& the situation.

Transparency: Worm dictionary

Test your own feelings on the ethical correctness of this incident by imagining your department's computer system being brought down in this way.

4.3 BRAIN VIRUS

The story behind the famous Brain virus reads like a paperback. During the late eighties, two brothers ran a small computer shop in Lahore, Pakistan. They sold copies of well-known commercial software, mostly to tourists (Lotus 1-2-3 for $1.50). A loophole in their laws did not make this practise illegal.

The one brother wrote his own software, and found (to his surprise?) that many people would rather copy somebody else's original programs than buy their own. In the process, he reasoned, they took money from his pocket. As a result, he wrote a clever piece of code which was put on some of the disks sold in their store. This program became known as the Brain virus, and was designed to destroy data on the disk it used as a host. Whenever a local came in, he would get a clean copy of whatever he bought. Foreigners (particularly Americans, because they pirate programs, according to the brothers), received contaminated copies of the software of their choice (Elmer De Witt, 1988)

The only reason why the author of this virus is known, is because he put his details into the coding!

Transparency: Brain infected Boot Sector

Most of us will probably agree that copying commercial software is not ethically correct. However, how would you feel if you lose a lot of data as a result of your illegal copying, especially if you know that a certain programmer out there is responsible for it?

Ironically, the story about the Brain virus was published a few months before the release of the Internet worm..

4.4 ADS VRUS

During 1989, a disk was sent to 20699 computer users, claiming to contain a program which will test your likelihood of contracting the Aids virus (the real not the computer type!). The program refused to install if the computer does not have a hard drive, and insisted to install on the hard drive when present.

After loading, it uses an expert system type interface to determine from the user's answers the chances of the user being infected with Aids. However, after running a certain number of times, the program would do software damage to the information on the hard drive.

The alleged author of this virus, Joseph Popp, has been certified as mentally unable to stand trial. Apparently he is currently dressing himself with weird materials like cardboard boxes and empty bottles, and we probably will not have to be concerned about any future viruses from him (Gibbs, 199t)

Some interesting points are being made on the covering slip that accompanied the disk containing the original Aids virus. A large amount of money has to be deposited in a Panama bank account by the recipient, and a strange guarantee is given.

Transparency: Aids virus covering slip

5 MOTIVES FOR WRITING VIRUSES

The author is not aware of any company who would be willing to pay a programmer to write computer viruses. The question then is: if financial gain is not the motive, why would anybody spend precious time to produce an item which nobody asked for, nobody will buy, and many computer users will pay to get rid OP There must be some motivation involved.

5.1 MOTIVES

Some possible motivations are:

- To point out the need for tighter security on a computer system - the apparent motive for the Internet worm.
- To punish buyers of pirated software - Brain virus.
- Financial gain - to be able to collect the rewards, the author stands a chance of becoming known?
- Get back an employer - once again the chances of being traced are reasonably high.
- Challenge - can I do it? This is a common motive for hackers and students - only students have the time to spend on something that they will not be paid for!
- Boredom. Once again, this is a fairly unlikely situation for any serious computer expert.

Do you think these motivations are valid reasons for producing any viruses program?

6 RESULTS OF VIRUS INFECTIONS

6.1 MISCONCEPTIONS

It was clear from many of the answers received via the questionnaires mentioned earlier that the average user in industry labours under many misconceptions concerning viruses. Some of the answers to the questions posed are listed as an example.

6.2 RESEARCH

The next stage of the research was to determine exactly what damage, if any, was caused to the 4 areas of a variety of magnetic disks by each one of the 15 viruses identified earlier. The issue here was not how the viruses operate, or what their (sometimes rather interesting) symptoms are. It was considered important to determine the effect on user’s data and files.

6.3 VALUE OF FLES

It is imperative to understand the difference in value program files and data files have to a user. Loss of program files does normally not pose a major threat - the user or support personnel can easily restore them from master disks or from backup media. However, lost or damaged data files are virtually impossible to restore in fill, since even a recent backup is unlikely to include all data files created by the user.

Have you ever had the experience of entering your house or car after it has been robbed - did you also experience that uneasy feeling that your privacy has been invaded? The result of a virus infection is similar - the user feels that something (rather unethical!) has happened to his data, without his consent.

6 4 CONCLUSION

The author's conclusion was that the damage done by computer viruses to stored information are generally limited to one file or disk area. Where damage to stored information did occur, it was often reversible. However, a thorough understanding of computer disk areas, architecture, and memory layout and of programs like Debug, Norton Utilities, etc. is required to remove virus infections. (Weideman, 1994)

7. IMPLICATIONS FOR COMPUTER USERS

During 1994, the average-sized corporation (1000 PC's) lost $300 000 in productivity and costs (IBM, 1996). Nobody can argue the ethical correctness of copying commercial software and thereby taking money out of the pocket of the author, distributors, etc. (Microsoft, 1996)

Transparency: Microsoft Piracy Alert

Transparency: Software Licence Agreement

Copying of software and virus spreading go hand in hand. If a user claims that he has suffered a computer virus infection, he should not hesitate to explain how the virus managed to invade his system (if possible!). There is a strong possibility that software has been copied illegally somewhere in the chain of events that lead up to the infection taking place.

8 THE FUTURE

All viruses mentioned in this presentation, and indeed 99% of known viruses, are DOS-based programs. DOS is an operating system which runs in real mode, implying that programs have full access to memory and disks, and can violate many basic rules regarding the inner workings of computers. Other operating systems, including Windows 95, OS/2, Windows NT and Unix run in protected mode where this sort of violation is not possible.

It is saved to predict that the writing of new viruses and spreading them under these operating systems will require a new approach by virus authors. These viruses will be much more complex pieces of code, and they will have to be "tested" well before operating successfully. The actual programs will therefore be much bigger, and will be noticed easier.

9 CONCLUSION

It is clear that the computer virus issue is shrouded in a veil of uncertainty. Current virus programs vary from the innocuous which do little more than annoy the user, to the really destructive ones that corrupt files and disk areas. Regardless of their actions, computer viruses are unwanted programs running on computers without their operator's consent, and as such is a phenomenon which can only harm the IT industry-

One can only hope that the new generation of operating systems available to the PC market will curb the creation and spreading of the traditional DOS virus as we have come to know it.

Transparency: How to be totally safe from all Virus Infections.

10. REFERENCES

- De Witt, P.E. (1988), Time Magazine, sept 26, 62.
- Gibbs, C (1991), Computer Weekly, November 12, l.
- IBM, (1996), Combating computer viruses: BM's new computer immune system, EEE Parallel and Distributed Technology 4 , Summer.
- Microsoft, (1996), Microsoft Piracy Alert, February l.
- Solomon, A (1996), Dr Solomon's Antivirus Toolkit, Version 7.58
- Spafford, E (1989), The Internet Worm Program: An analysis, Purdue Technical Report CSD-TR-823
- Weideman, M (1994), A critical evaluation of the destructive impact of computer viruses on files stored by personal computer users.