Computers & Security, 14 (1995) 391-402

Technologically Enabled Crime: Shifting Paradigms for the Year 2000

Sarah Gordon

Command Software Systems Inc, 1061 E.Indiantown Road, Suite 500, Jupiter, FL 33477, USA.

This article will consider the social and ethical factors involved in the transmission of computer viruses and other malicious software. In addition to the people, we will consider the part the systems and technology play in the spread of this sort of data. We will draw parallels with one of the more well known scientific paradigms, the medical one, and note the similarities with the problems we now face. We will describe the evolution of methods of virus distribution: virus exchange bulletin boards, virus exchange networks, distribution sites, robot servers, and books. The article will discuss viruses for sale and make some comparisons between distribution of computer viruses and the distribution methods of 'hacking tools'. Other issues examined in this article include the characteristics of individuals involved in the distribution of these types of programmes, and problems of legal redress, as well as possible solutions based on ethics and ethical theory.

Introduction

We have available today a global system of communication technology. There also exist programs whose purpose is to disrupt the way this system functions. Moreover, the system is the perfect medium to host and transfer the very programs designed to destroy the functionality of the system itself. In this article I will discuss the factors usually neglected in studies concerning computer virus infections.

Traditional Epidemiological Studies

ep-i-de-mi-ol-o-gy \,ep-e-,de^--me^--'a^:l-e-je^-, -,dem-e^--\ n [LL epidemia + ISV -logy] (ca. 1864). 1: a branch of medical science that deals with the incidence, distribution, and control of disease in a population. 2: the sum of the factors controlling the presence or absence of a disease or pathogen (Webster's).

There are various factors commonly considered when estimating the probability of virus infections. We have factors such as the ability of the virus to replicate, the amount of contact any given machine has with the general population of computers, and the presence of any computers currently infected. Elaborate studies have been done to calculate the possibilities of any given population becoming infected. In one such study by Dr. Alan Solomon [Solomon, 1990], one conclusion is that early detection is a very effective way to reduce the incidence of viruses in a population of computers. In fact, early detection is cited as one of the crucial factors in limiting infection. One such model illustrates how finding a virus contributes to its detection and eradication [1].

There are cases however, where a virus being 'found' means it will spread further and further; the same can be said of some hacking tools. These cases are where the malicious programs are 'found' on computing systems, where they have been placed for exchange or distribution. These are programs which will not be detected in their 'current state' by any virus detector or casual search methodologies. When they are found, by people looking

[1] In the Solomon model, the rate of new infections is proportional to the number of infected PCs, to the number of uninfected PCs and to the probability of infection. The rate of infections being eradicated is proportional to the number of infected PCs, and to the probability of detection.

0167-4048/95/$9.50

for them (and in some cases by the casual observer who just happens to see them, download or ftp them, and use them), they spread from user to user and their use becomes widespread; in some cases, epidemic.

Social Aspects

In addition to being concerned with detecting viruses which are active in computing systems, we now find ourselves in the position of needing to detect and identify viruses and other malicious software which are non-active. We are faced today with an entire system of communication technology which is the perfect medium to host and transfer the very programs designed to destroy the functionality of the systems. We suggest that technologies not only tend be created out of human endeavour and the accompanying social values, but to shape the values of the communities from which they arise; that they can take on an ethical/moral dynamic of their own. These values, as we will show, are not always consistent with the values of the communities which create them.

The Causal Connection

In this section, I will examine the sorts of programs which are sometimes used in criminal and/or unethical ways. People which make use of the current technology to distribute the tools and information will be discussed.

Malicious Software

By malicious program, I refer to a program designed to perform a harmful action. This action could range from deliberate destruction of data, as is the case with some viruses, to the interception of confidential information, as is the case with programs such as the recently publicised sunsniffer. For the purposes of this article, the computing technologies referred to are those which are affected, or which have the potential to be affected.

While it is not required for a program to do obvious damage to classify as a virus, for the purpose of this article a virus is stipulated as a program that replicates in some environment, alters executable code and does damage by controlling your computer system without your knowledge or consent; a trojan is stipulated as a program which appears legitimate, but which does deliberate damage to your computer system's files. While viruses have for the most part been confined to personal computers running under MS-DOS, we are beginning to see both more interest and more viruses written for Unix based systems.

The hacking tools discussed are computer programs including trojanized login programs, which capture passwords, shell scripts which exploit operating system bugs and text files which give instructions on how to hack computer systems.

Of course, these programs alone do no damage. They must be installed, executed or read and used as "instruction manuals"; this is accomplished initially by a human. It is interesting to note that many people insist that programs are 'unethical'. Other voices insist the programs are not capable of being ethical or unethical; they are simply code. Traditionally, programs were not seen as capable of being ethical or non-ethical in and of themselves, primarily because they were not autonomous agents. However, viruses have the capability to be exactly this. For this reason, if the viruses we are seeing today are in any way the precursors to full-scale autonomous agents, we should be concerned with which ethical models we will incorporate into them. Will they make their decisions based on the good of all of society; will they make their decision based on unwavering moral principles? Will they be totally self-preservationist? There appears to be little if anything to indicate these programs with which we are concerned in this article bear any relationship to artificial intelligence or artificial life despite claims to the contrary by their producers, and for this reason are not ethical or unethical in and of themselves.

Individuals

The sort of people which play a role in the distribution of this malicious information vary. There are malicious, intentional players, as well as non-malicious accidental players. I will begin with the virus writers. It would be an error to place them all in one category. They are as diverse as their viruses; each with his own motivation and each subscribing to his own choice of distribution method. The term 'his' is specifically used because there is no evidence of any female virus writer who participates consistently in distribution of computer viruses. The gender issue is one which is discussed in the paper

"The Generic Virus Writer" [Gordon, 94]; it will not be discussed further at this time except to note there is a gender issue.

Virus writers can come from all walks of life; they are diverse in age, location, academic background, and goal. In some cases, the goal is malicious in nature; in other cases, there appears to be no malicious intent. The same is true of the hacker. The traditional profile of hacker [Swanson, Chamelin and Territo, 92] as young adult male, 19-25, socially inept seems to be somewhat inaccurate. There are women involved in the hacker culture, not just as 'fans' and 'hangers-on', but as contributory entities.

Another similarity between types of the virus-involved individuals and roles of the individuals in their subculture and that of hackers and those involved in their subculture is that both may exhibit 'parasitic' behaviour. Parasite in this context refers to people who have no skills of writing replicating code, nor any abilities related to what is commonly referred to as 'hacking'. These people participate in the culture by helping distribute the programs, and the information in crude, traditional ways; telephone conversations, bulletin board chats, uploading/downloading files on dial-up bulletin boards; use of the Internet in some cases to transfer files, and maintenance of huge repositories of information which they cannot contribute to, but which they can allow others to 'benefit' from. They feed off of the 'work' of others. For this reason, they are often referred to as 'parasite hackers' or 'parasites' by members of their social communities.

These are not the only people involved in the epidemiology of malicious programs. Commercial software companies are involved. At least 64 instances of DOS-based commercial software have been released with infected files or infected boot sectors. There are increasing numbers of reports of infections on commercial and shareware CDs released for DOS based machines[2].

[2]. A list of viruses distributed with commercial software, compiled from VIRUS-L, RISKS-FORUM and other public sources, identifies virus infections transmitted through either commercial or government entities in which the distributor would generally have been considered to be a 'reputable source'. Incidents which were unwilling to fully disclose, or incidents in which the source of the infection was unsure were omitted. This list was obtained from Wallace Hale of the PCVRF. It is noted that any additional information may be requested from, or forwarded to cmcdonal@wsmr-emh34.army.mil.

Innocent users are sometimes carriers. We are all familiar with the sneaker net mode of infection, where an office worker carries a disk to his/her co-worker, and in transferring the files or booting from the shared disk, also sometimes transfers the virus. Users can also transfer viruses by not following proper procedures in their environments; not taking the virus threat seriously. Anti-virus software is often disabled by users because it is too slow or not installed at all because the installation is considered too complex. When this lack of provision for detection exists, the user can play host and distributor to viruses without ever being aware of their existence. Administrators also sometimes play a role in the distribution of viruses and other malicious programs, unknowingly. This will be discussed further under the section on Virus Distribution Sites.

Epidemiology

Having defined some types of programs that are used to cause disruption and criminal activity in our networks, aspects of cyberspace and technological development which can contribute to the problem and the general characteristics of some of the people involved, I will now look at the methods by which the people distribute the programs and information.

How Virus Programs Travel

Viruses are exchanged and distributed via at least six methods. The first, the virus exchange BBS, is perhaps the most well known. I will trace the growth of viruses as a novelty, to the beginnings of their place in commercial ventures. To discuss the motivations of the persons involved in each of these individual steps is beyond the scope of this article. I will address the questions: how are the machines and the technology used as methods of communicating information; what kind of information is being communicated?

Virus exchange BBS

One of the common methods utilized by intentional computer virus distributors is the virus exchange bulletin board. The bulletin boards are similar in most respects to mainstream bulletin board systems. The software used by the individual system operators varies. Many of the systems are accessible via telephone, and

some are accessible through telnet. From a humble beginning in Sofia, Bulgaria (the site of the first known virus exchange system), virus exchange bulletin boards have grown into big operations, and in some cases, big business. The first such system was operated by Todor Todorov in Sofia Bulgaria; it made viruses available initially on an 'exchange' basis, but later offered the viruses to anyone who cared to take them. In its initial stage, it encouraged the creation of new viruses by requiring the upload of a new virus in exchange for access to any and all viruses. The system had a total of 294 users and was used primarily by local callers.

The number of 'regular' files on this system was at least double the number of viruses; according to the system operator, the non-virus files were the most frequently accessed. Following the popularization of this system via negative publicity as well as 'word of mouth advertising' by users, other systems began to emerge. Currently, virus exchange bulletin boards are known to exist in North America, Latin America, Europe (including Switzerland where it has become a crime to offer viruses via a BBS; and Holland, where it is also a criminal offence); Australia, Asia and Africa. The systems sometimes state they are Virus Research Bulletin Boards. Some of the systems are 'private'; others allow access to anyone who wishes to participate. These individual systems have led to a new development; that of the virus exchange network.

Virus exchange networks

These systems were for the most part well-publicized by word of mouth, electronic mail and advertising on other systems of the same type. While hack/phreak systems had been in existence for some time, the virus exchange phenomenon was a relative latecomer to the underground scene. Within roughly a three year period, the operators and users of such systems had formed a relatively small but tightly knit community, and the formation of organized networks followed. The networks provided even faster distribution of new viruses to network members. The majority of these systems operated using regular dial-up modems and a network structure similar to the Fidonet. The networks have names such as vX-Net (Virus Exchange Net), NuKEnet (named after the NuKE virus writing group which founded the network), and MeltNet (an exclusive net which has never been known to release a virus outside of the network).

These networks have been observed to overlap; often systems will participate in more than one of the networks. In some cases, the networks will publicly identify themselves as "Virus Research BBS", while in another network they are known by their virus exchange system or virus distribution affiliated name. One such instance was the Virginia Institute of Virus Research, which was also known as the Black Axis BBS. This system was represented in the Fidonet echomail conference as a virus research centre; it was identified in another network as the world headquarters for the NuKE virus writing group, operating under the name "The Black Axis". This is not an isolated instance, but is perhaps the most well known. The virus exchange systems as exist via regular dial-up access are easily accessible to users. Since they are self-administered, they are not usually subject to any form of external review or assessment.

Virus distribution sites

As interest in viruses grew, the abilities and resources of the virus writers and distributors grew. Some of the young virus writers became college aged; access to Internet facilities became available. Internet virus sites became more commonplace, and information about the ever-changing locations was transferred at the same fast rate as the viruses themselves. It is not uncommon to find university ftp sites used as virus distribution sites. This creates a problem for overworked administrators, who in many cases have no idea what is passing through their systems. How can we detect these viruses? In some cases they are not directly detectable, having been encoded by some standard (or non-standard) utility such as uuencode; in other cases they are archived. Both these methods make their detection by current scanning methodologies difficult if not impossible. They are not active in memory, or existing in any form which a traditional scanner may recognize. In many cases these are MS-DOS viruses, which are transferred using Unix machines. They are often in and out of sites before most administrators know their systems have been used for the purpose of holding or transferring the data.

Virus distribution robots and file servers

Use of automated distribution programs known as 'bots' and 'servers' is a relatively recent addition to the methods used to distribute viruses. By contacting one of the servers via electronic mail, or by asking the 'robot' for the files, a user can relatively anonymously retrieve

viruses via the Internet. The connection can of course be monitored, but they do not appear to be routinely monitored by the administrators or by the users themselves. One recently programmed file server reportedly transferred to users approximately 15 000 to 20 000 files (viruses and text files) per week during its three months of operation. There were approximately 1000 files available for download/transfer from this server. The operator of the server learned to make and use bots during his self-taught experience with the Linux operating system. Following the success of the server, he programmed a bot which was actively distributing viruses on the Internet Relay Chat. He states he put the server online to do something that had never been done before — Internet wide virus distribution. As the server was anonymous, there is no way to know what sort of users accessed the files, their intended purpose, or the result of the accessibility.

According to the server operator, the supplier of Internet service declared a breach of contract following the huge volume of file transfers; he was forced to remove the server. Such servers, and bots, can be used for distribution of any type file, not just viruses; this transfer of information can be accomplished with relative anonymity.

Virus instruction books

Books on how to make viruses have become popular, and contests are sponsored to build the smallest virus; the most politically incorrect virus; the virus best able to defeat anti-virus programs. In 1990, Mark Ludwig copyrighted *The Little Black Book of Computer Viruses*. This book contained general information about types of viruses. It contained computer source code for the viruses as well as an order blank readers could use to order the code on disk; it also contained what the book refers to as "compiled executable programs for all of the viruses and related programs in this book". There was a disclaimer, requiring the purchaser to assume full responsibility for any damage that may be caused by any of the programs. The viruses themselves were not particularly innovative. Several of them have been found in the wild since the publication of the book. This book created some controversy, followed by the release of a second book. The second book was released without much attention in the United States; however, in France, there was considerable controversy surrounding the release of the book. There have been other books published which contain computer virus source code. They have not achieved the notoriety of the Ludwig book. I am not suggesting any books should be banned. However, there are ethical considerations with which computing professionals need to be concerned. I will discuss these further later in this article.

Viruses for sale

Viruses are offered for sale by individuals. Several such offers were posted in various Fido and Usenet newsgroups. In addition, some magazines carry advertisements for viruses. Magazines also offer virus source code; the sale of these magazines appears to be legal at this time in the United States. Virus writers and distributors have begun creating and selling new viruses to some anti-virus product developers for inclusion in the 'scanner' programs. Government and industry sources have been said to purchase or obtain viruses from virus exchange systems or virus distributors, to perform testing of the anti-virus software they are considering. The virus phenomenon has become big business.

How Hacking Tools Travel

Hacking tools, such as shell scripts which exploit system holes, buglists, etc. appear to travel via different sorts of paths.

In the case of these tools, and the people who exchange them, the scenario appears to alter slightly. The majority of hacking tools appear to be created after the announcement of a software bug. Hackers then create tools to exploit the bugs. In some cases, the hackers themselves find the bugs. There appears to be more creativity, individual action, and intentional sharing of the information among hackers than among the virus involved individuals; however, the information has tended to be limited to those who are judged (within the subculture) of understanding and contributing to further development of the tools. In some case, individuals obtain one set of tools and use them to obtain others by simply taking them from the filesystems of the tool developers.

Primarily they have been shared amongst individuals in the relatively tightly knit hacking community, until recently. We are now beginning to observe a shift which is cause for concern:

• Hackers sharing programs	• Hackers sharing programs
• shared among small group	• shared among small groups
• not widely distributed	• distributed more widely
	• wide banded
• not generally used maliciously	• used maliciously

This shift can be observed by following the distribution of one hacking tool commonly know as the sunsniffer. Initially the sniffer was distributed only to a very few people. The source code and executable code for this sniffer were later 'widebanded'. Widebanding refers to indiscriminate intentional distribution of a program, through every available method. In some cases this is done to make tracing of the original distributor more difficult.

The sniffer, which compromised the security of large number of systems on the Internet, worked by using a feature of the operating system called /dev/nit. This is the network interface tap, and it can read/write from/to different interfaces. The program was configured to place /dev/nit in promiscuous mode, because it could then read all traffic from any machine on the cable, even routed mail. Administrators who had not properly configured their own /dev/nit helped enable the compromise of their own systems. However, this 'hole' was designed into the system, making this compromise possible. It is not feasible to disable a machine to prevent its compromise.

As people became more aware of the use of this program by a few individuals, the potential for apprehension of the individuals increased, so the tool was distributed a bit more widely. At the same time, other individuals began to find this 'sniffer' on machines which had been compromised; they would then take a copy of it to use elsewhere. Copies of the sunsniffer were placed on publicly available FTP sites, where any user with access to anonymous FTP could obtain the program. The shift we are observing whereby hackers are distributing information such as this on a much wider scale than before is illustrated by the speed and manner of the distribution of this sniffer.

What has brought about this shift? As suggested earlier, technology can bring about an ethic of its own that is not necessarily in keeping with the ethic of the creators of the technology. While this can be said of virtually any technology, it appears to be particularly applicable in the case of computing technologies. This will be further discussed in the section on 'Future Trends', in which I will examine some of the reasons for the shifts we are observing.

Recently, there have been more hacker voices calling for public dissemination of both operating system holes and fixes. There are diversified opinions in both communities regarding whether or not such information distribution would benefit either of the communities in regard to their respective goals. Whether or not this idea gains widespread acceptance in either community remains to be seen.

Private BBS

While private BBS are set up, offering some tools, these tools tend to be of relatively minor significance: war-dialers, phreaking information, information easily available about operating systems. Some BBS do contain more technically advanced materials, but access to them appears to be more exclusive than is the case with virus exchange bulletin board systems. Most of the information on h/p/a/v (hacking, phreaking, anarchy and virus) systems is of lower quality; most of the tools found are said to be trivial.

Networked BBS

Networked systems seem to be much less frequent, and those that do exist do not appear to offer the more exclusive tools.

Usenet

An interesting aspect of hacking tools is the use of Usenet news for their distribution. Source code for hacking tools appears on various Usenet groups, but usually this is after hackers have had access to them for some time. Such source code can be saved by readers, and compiled to create tools such as shell scripts to install port hoppers, and so on. It has been my experience in talking with a number of persons who have arrived relatively recently into the 'hacking scene' that they are not capable of using these tools. The problem usually appears to be the necessity to modify the programs for different platforms; these people simply do not possess the ability to do it. Another problem is the a priori

technical knowledge required. It does little good for a hacker to have a device that exploits a bug in kmem, for instance, if he does not know what to do once he has access to kmem. Simple programs for altering utmp files require modification as simple as directory paths; frequently, people do not have even the skills to do this. Commonly, such persons will access a Unix system and enter DOS commands such as DIR, or type HELP.

This is not to say that the tools are not useful in helping them to learn; however, it is clear that these tools require more than a casual knowledge of the systems they are intended for use on. As the toolkits become more developed, less skill is required on the part of the users. However, some basic knowledge is still required.

FTP sites

The use of Usenet for distribution of such tools is not the only way the Internet is used to facilitate the travel of hacking tools. FTP sites are routinely used for drop sites. These in many cases require special accesses or passwords, but in some cases tools are left on public sites, either through oversight on the part of the individuals involved, or intentionally.

Social Factors

The connection between certain aspects of current computing technology and the crimes/activities being facilitated will be examined, with emphasis on the paradigm shifts which have been proven to improve the overall health of other forms of scientific research.

Cyberspace As Facilitator

I will now consider the aspect of this cyberspace environment known as dehumanization. Not all computing technologies are heavily influenced by the dehumanization and other psychological aspects of cyberspace which are seen in the environment surrounding the 'malicious computer program', but it should not surprise us that people who have little contact with other human beings due to their intense immersion in the electronic communities we have designed have lost sight of their humanity. It follows that the impact of their actions is often seen, at least by them, as impacting machines, not other human beings.

We should also consider the aspects of cyberspace which facilitate inequality, and the possible results of these inequalities. This environment is no different than in any other aspect of society; it is normal for people to be unequal. For example, we do not all have access to the same quality of health care; not everyone has even a house in which to put a terminal. Cyberspace however, introduces a unique form of inequality in that the sort of information which is becoming available will provide what could be a very extreme advantage to those who 'have' versus those who 'have not' — indeed, this advantage/disadvantage could impact the electronic community in such a way that the community could become unable to maintain itself entirely. Unequal access to information puts those who do not have the access at the distinct disadvantage of ever being able to fulfil their potential in the electronic society. While this is inherent in most societies, we are in a position now which could enable us to minimize some aspects of social inequality by careful planning and policy making. Unlike other areas, in cyberspace this structure is not yet intact; there is still time to integrate equalizing factors. Most importantly, we need to consider what sorts of information belong in cyberspace; what sort of access policies should governments envision; is the idea of access for everyone feasible or even desirable.

At this time, cyberspace does tend to facilitate some inequality; this inequality is manifested in the number of 'victims'. It can be argued that there is a great equalization, due to lack of real world visual biases or clues inherent in net communication and interaction; however, it is important to consider that along with the lack of the visual 'bias' triggers comes a lack of contextual clues. Without these clues, often people do not realise their behaviour is unacceptable. If it is alright to do one little thing, another little thing is added to it. Eventually, you can end up with a very anti-social behaviour, which was totally acceptable every step of the way by one's peer group. This is not to suggest that we should find a way to take real-time, real-space clues and integrate them into net societies. As users are given more and more power, the potential for trickery, lies, deceit and abuse increases right along with the potential for 'good'. It may be wise to consider the nature of cyber-societies and the processes of social influence within them. [Sproull, 93]

Technology As Enabler

In addition to the people, we must consider the part the systems and technology play in the spread of this sort of data. We can best do this by drawing a parallel with one of the more well known scientific paradigms, noting the similarities with the problem we now face:

Medical Science in the early 1960s	Communication Technology Today
• We can do it	• We can do it
• We should do it	• We should do it
• We must do it	• We must do it

The "it" in the first case refers to advances in medicine relating to health care, and research; in particular fields such as genetic engineering. What occurred during this time was a remarkable advancement of technology which left scientists and researchers in somewhat of a quandary over exactly what, and how much, of this research and development should be put into common usage or pursued at all. We find a similar situation today, with computing technologies not only surpassing the abilities of administrators and users to understand them, but of the technologies themselves at times enabling their own destruction. It is perhaps wise to consider at some point what safeguards we should require. In the 60's, science turned to the field of ethics — a field which was dying according to some — and asked the question "Just what exactly should we do? What is *right* to do?". From this introspection, the field of bio-ethics emerged. [Bartels, Smith, 93] [Gustafson, 70].

When we look at medical science, and medical research today, we find questions being asked:

The Medical Science Paradigm today:

- We can do it
- Should we do it?
- How should we do it?

We can observe the shifts resulting from the interaction with ethical concerns. This shift has meant perhaps less scientific 'advancement', but perhaps has placed medical science more in line with its true goals. The same could be said for integration of ethics with other scientific disciplines. As the technologies of computing today advance, they tend to focus on what the machines can do. In this assumption, we could be neglecting what we really need and want them to do. [USPGO, 93]

Future Trends

The technologies described to this point which have enabled the sorts of crimes we are now seeing in our global computing environments were surely not created or designed to facilitate these sorts of behaviours. We must, however, take a serious look at contributory factors.

It could be the case that we have simply allowed technology to progress too quickly, with insufficient planning. This is not to suggest that we should stifle technology, but that we may need to begin now to pay particular attention to the ethical model that the technological model is generating. As an example, consider FSP and FTP applications. We have seen how FTP (File Transfer Protocol via connection state protocol) can in some cases allow files to be transferred anonymously. This is a good and necessary thing, and its potential for abuse or misuse could be minimized by correct configuration policies. FSP, or File Server Protocol (Transfers via Connection list) in which you have a connection only during pings, requests, etc. are an improvement in that you do not tie up resources during inactivity; however, use of FSP usually requires no special privileges to set up and no special ports; it doesn't require separate file systems, and anyone can set up this sort of 'server'. We are seeing the same sorts of problems with these FSP servers as we are seeing with the DCC (Direct Client to Client transfer services) applications and Bots that are being used to transfer viruses and other programs on IRC (Internet Relay Chat).

The anonymity of both of these applications plays a role in the ethical models of behaviour that have developed around their uses. While FTP sites are used to transfer the sorts of programs and information with which we are concerned, there appears to be a much higher incidence of FSP sites being used on a regular basis to transfer this information and data. The controversy surrounding anonymity and pseudo-anonymity is one which will probably continue for a long time as we learn the effects of such freedoms. However, what we can see

now is that these sorts of anonymous applications do provide almost a 'Use Me for Your Own Purposes' sign.

Other technologies which have had huge influence on society have developed relatively slowly, enabling us to at least somewhat predict future trends; however, in the case of computing technology, not only do we have few precedents on which to build our analysis, the technology by nature is rather esoteric. This creates an environment perfectly adapted to the development of pseudo-revolutionary counter culture and the exploitation of those who have, or are perceived to have, power. Additionally, the trends which we are able to predict would seem to indicate that legal methods of redress are inadequate at best. A proactive approach to the problems facing us as relating to hacking, virus writing distribution and dissemination of information which has the deliberate design of being used in a harmful or malicious way, would have to include ethics and education. The types of ethics and education will be discussed briefly in the next section.

Solutions

Both legal and ethical solutions to some of the problems discussed in this article are worth considering. However, both have limitations, and need to be used in a cooperative, multidisciplinary approach. I will look now at some of the methods that can be used to address the problems.

Laws

Laws are one method. There are however, problems with laws addressing computer viruses, virus source code, and hacking 'tools'. As evidenced by cases involving members of a well known 'hacker' group, jurisdiction can be a problem. In one particular case, the alleged perpetrator physically resided in the United States; the system he reportedly attacked was located in Australia. The question of jurisdiction has, to this point, made prosecution impossible. [Cook, 93]

Laws concerning viruses have problems due to their lack of enforceability, jurisdiction and the matter of recovery. As I have shown, the nature of the methods of exchanging computer viruses and hacking tools tend to hamper any real assessment of exactly how much information is being exchanged and by whom. While of course there are ample mechanisms for monitoring information exchanges, we need to be concerned with various policies (both legal and ethical) when we consider monitoring communications to ensure their 'acceptability'. The vast majority of known virus writers are not capable of providing recovery should they actually be convicted of a crime, successfully prosecuted, and found guilty. Finally, there is the international nature of virus distribution, which adds to the already complicated situation.

While courts have usually found that information distributors are not strictly liable for damage caused by distribution of misinformation, some decisions have held that distributors of products can be held strictly liable for the results of reliance on misinformation contained in the product [Cook, 93]. The United States Commerce Department, in January 1990, found that international system administrators have an affirmative obligation to review the contents of their systems to locate improper or illegal traffic, specifically traffic in programs which have controlled export under the Export Administration Act or the Arms Export Control Act.

While laws are still evolving and no one knows for sure what the end result will be, it seems safe to assume that administrators and commercial system owners will eventually face possible liabilities for actions of their users, such as virus infected products, viruses distributed via networks, stolen credit card information transferred via their networks, users businesses disrupted because adequate safeguards were not in place. This however does not solve the problem. The administrators may have a responsibility ethically and perhaps eventually legally to know what is going on on their systems; however, we cannot ignore the obvious gap between what a system should enforce and what it is actually expected to enforce. We must also be cognizant of the gap between what we can expect will be enforced and the social policies and mores that exist in any given environment [Neumann, 93].

The concept of Free Speech as a Constitutional Right is invoked by many proponents of unrestricted virus 'exchange' in the United States. There are forms of speech that are not protected by the First Amendment to the United States Constitution; additionally, there are precedents which bring serious questions to the First Amendment defence. The virus problem is not confined

to the United States alone, and any laws specific to any individual country may not be applicable in another country. The discussion of free speech and/or First Amendment rights is beyond the scope of this article; it is mentioned due to its large role in the defence of virus writing in the United States.

Finally, we may wish to examine ways in which laws can be used to create positive ethical models in individuals and groups. First, quoting a release from the Technical and General Assemblies of the International Federation for Information Processing[3]. "In view of the potentially serious and even fatal consequences of the introduction of 'virus' programs into computer systems, the Technical and General Assemblies of IFIP urge:

1. All computer professionals to recognize the disastrous potential of computer viruses.

2. All computer educators to impress upon their students the dangers of virus programs.

3. All publishers to refrain from publication of the details of actual virus programs."

We see a very good suggestion as to how we may begin to positively influence students and young people. We can observe how this has been seen to work in the past by looking at the issue of drinking and driving. At one point in time, drinking and driving was a personal issue. As we as a society began to see some of the consequences of this interaction, we began to pass laws which restricted such behaviour. There was some resistance to this type of law initially, which people saw as an infringement on their right to drink alcohol and drive their vehicles. However, as the law became more widely accepted, people began to refuse to drink and drive on the principle that it is 'wrong' to do. Policymakers and lawmakers are very aware of this form of societal control. However, they are often not very aware of the societal structure of 'cyberspace', and for this reason there is the danger that laws they make will not create the desired ethical model, but will instead create a backlash or revolutionary movement against the society. By continuing to take time to develop realistic policies and effective laws, it is possible we can avoid such a backlash.

Ethical Considerations

The ethical approach to addressing these concerns is one worth further consideration. What role does ethics currently play in our computing environments? What role, if any, should it play? Ethics is quite the 'in' word, and is often promoted as the be-all and end-all solution to all the problems we face dealing with virus and malicious software distribution. Ethics, however, cannot and should not be seen as a 'behaviour regulator'. It is not a drug one can force down someone's throat, and cure them of their 'disease'. If we are to use ethics to help us to solve some of the problems discussed in this article, where and how should we begin? There are several areas of immediate concern.

Commonly, ethics is promoted, if at all, in our computing environments as something related to individual action. While ethics certainly can be important in matters of our interpersonal actions and subsequently on our actions as they impact the society, we seem to ignore the issues of ethical evaluation of institutions [Ladd, 93].

Questions related to distributive justice (here, I refer to rights in the sense of both negative and positive rights; specifically, what can I expect to do free from any infringement from government or individuals, and what duty does my society have to provide me with access, freedoms, security, development and distribution of resources), and other ethics of management are worthy of consideration.

There have been voices calling for more clearly defined professional ethics and more involvement of professional societies in defining and promoting 'professional ethics'. Considering ethics is by nature a reflective, critical field, it would seem that while ethical norms may be documented, to assume we can arrive at some 'ethical statement of principle' is somewhat unrealistic. Ethics are not laws, rules, policies or agreements. It is not something one can put on from the outside. Of course, ethics can and should play a role in creation of codes of conduct. Such codes of conduct are necessary and important tools in imparting behavioural guidelines to others [Forrester, Morrison 94]. We must be careful not

[3]. "The resolution was formulated by the then chairman of IFIPs Technical Committee TC-11 'Computer Security', Professor William J. Caelli, of Queensland University, Brisbane/Australia, and the then chairman-elect of IFIPs TC-9 'Computer and Society', Prof. Klaus Brunnstein of Hamburg University. IFIP General assembly asked the then president, Ashley Goldsworthy, to inform all member societies and to ask the governments to take proper actions." (Used with permission).

to confuse codes of conduct, which are based on ethical principles, with ethics themselves. If we do not take care, we are subject to a slippery slope where we may believe that we are somehow 'above' the ethical principles we apply to others. This can create a hypocrisy which only exacerbates the problems that are created by other factors, as outlined in this article. The development of codes of behaviour is often looked to as one ethical solution. This may be a factor in showing individuals what is acceptable, but cannot be viewed as a method for instilling ethical behaviour in any group.

Another concern is what type of 'ethics' should we look to for help in understanding and solving the problems of malicious program distribution. Is it the ethical theory itself that we must reintegrate into the educational system? According to the ACM/IEEE-CS Curriculum Task Force, undergraduate programmes need to "prepare students to understand the field of computing both as an academic discipline and as a profession within the context of a larger society". One of the main goals is cited as exposing students to the "ethical and societal issues that are associated with the computing field." The question of whether this instruction should consist of ethical theory or application is prominent. One school of thought is that we need to teach ethical applications now, before the problem gets any worse. Another view is that teaching ethical theory will allow us to develop ethical applications which will continue to develop as the technology develops.

Conclusion

When a new technology emerges, a paradigm associated with that technology appears or is borrowed from an associated technology. As the technology develops towards maturity, the paradigm shapes its development. At certain points, it becomes apparent that the paradigm is no longer appropriate, and a paradigm shift occurs. Typically this is first seen as an outlandish if not heretical move by some maverick individual. But if the shift is appropriate, it becomes adopted by the scientific community, and then serves to shape or even control the further development of the technology. Without such paradigm shifts, the technology may become stagnated, or even dangerously out of touch with its aims and the society around it. Computer science is no exception.

I have argued above that we are now at the point where a significant paradigm shift is necessary in this area. The speed with which global electronic communication is developing has brought with it an enormous benefit to all those fortunate enough to be able to exploit it. It has also brought opportunities to those who are willing to abuse it. The way in which it has introduced relative and absolute anonymity to its users itself may encourage acts which would otherwise have appeared to be too risky to the perpetrator. That is, its very nature may encourage various kinds of antisocial activities, ranging from innocent pranks through serious malicious damage to data and individuals to downright criminal fraud. The speed and power of the technology itself enables these activities to take place, and encourages them. Since its principle users are relatively young, and may be impressionable or unprincipled, an ethos has developed in which it is 'cool' to be an outlaw. Moreover, the inherent power embodied in being able to control the 'system' is itself potentially irresistibly attractive.

It is natural, given the way that societies tend to develop, that antisocial or otherwise undesirable activities lead to legislation against them, designed to contain or eradicate them. This is the point we have reached with such excesses on the Internet. This is the current paradigm of control, and the one that is influencing the development of the technology. However, legislation is notorious for not solving the problems it is designed to deal with. A paradigm shift is now necessary, both in the way the technology develops further and in the way that malicious activities associated with it are combatted. The problem of Internet abuse cannot be solved by trying to legislate it out of existence. It is necessary to promote an ethical approach to computing. This itself requires there to be an ethical model of developing computer science. The paradigm for this technology can no longer be determined purely along scientific lines. Introducing ethics into the way the technology is used will help to instill appropriate ethics in the users of the technology, and thus to reduce the numbers of abusers. If this programme is successful, it will soon sound outdated and even 'lame' to say "it's ok to do it if it isn't illegal", just as it has become 'uncool' to drink and drive; not merely illegal, but unethical, and not the sort of thing that enhances the image and status of a potential role model.

We cannot eliminate the social aspects of malicious computer program development and distribution through solely legal means, or through solely technical

means. We can look to technology for detection in some cases, and to law for prosecution or relief in some cases. In all cases, resources to enable us to emphasise and integrate ethical computing behaviours in all areas — not just in areas relating to viruses and hacking — may provide a stabilizing influence. Our computing environments are very vulnerable regarding distribution of information — after all, it is what they were designed to do. I suggest that we need to focus somewhat more on what we were designed to do: to behave as rational self-policing beings and to impart this ethical model to people learning the technology. Without the proper interaction of laws, education and ethical development, there is a very real risk that this technology will soon become unusable and ultimately self-destructive.

Bibliography

Bartels, Smith, 93, "New Frontiers in Genetic Testing and Screening: The Human Genome Project", Bartels, Dianne M. and Truesdell-Smith, Elizabeth, Centre for Biomedical Ethics, University of Minnesota, August 1993.

Cook, 93, "Network Traffic Liability: 1993", Cook, William J., op-ed for AMS Invitational Conference on Technical, Ethical and Legal Aspects of Computer and Network Use and Abuse. Report forthcoming.

Forrester, Morrison 94, "Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing", MIT Press, 1994.

Gordon, 94, "The Generic Virus Writer", Gordon, Sara; Virus Bulletin Conference.

Gustafson, 1970, "Basic Issues in the Biomedical Fields", Soundings 53, Summer 1970 151ff.

Ladd, 93, "Critical Reflections on Ethical Issues Relating to Computer and Network Use and Abuse", Ladd, John, Dept. of Philosophy, Brown University. AAAS Invitational Conference on Technical, Ethical and Legal Aspects of Computer and Network Use and Abuse. Report forthcoming.

Neumann, 93, "Limitations of Computer-Communications Technology, MAS Invitational Conference on Legal, Ethical and Technological Aspects of Computer and Network Use and Abuse. Report forthcoming.

President's Commission for the Study of Ethical Problems in Medicine and Biomedical and Behavioural Research, "Splicing Life". US Government Printing Office.

Solomon, 90, Epidemiology and Computer Viruses, Solomon, Alan, 1990, S&S International.

Sproull, 93, "Social Influence in Electronic Groups", Sproull, Lee, December 1993 from "Atheism, Sex, and Databases", Sproull, Lee and Faraj, Samer, in progress — Presented at AAAS Invitational Conference on Technical, Ethical and Legal Aspects of Computer and Network Use and Abuse. Report forthcoming.

Swanson, Chamelin and Tenito, 92, "Criminal Investigation", Swanson, Charles, Chamelin, Neil and Territo, Leonard, ed. Butcher, Phillip A. and Rosenberg, Elaine. pp. 53.

Acknowledgements

I am grateful to Tom Wachtel, Tim Martin, Jon David, and Harold Highland for their comments on an earlier draft. They are not responsible for any errors or omissions.

Sarah Gordon is a security analyst with Command Software Systems Inc. This article was originally presented at the Tenth International Information Security Conference IFIP SEC'94, organized by Technical Committee 11 of the International Federation of Information Processing.