PROTECTION OF COMPUTER SYSTEMS FROM COMPUTER VIRUSES: ETHICAL AND PRACTICAL ISSUES[*]

Bruce J. Neubauer
Computer Science and Information Systems Department
Pittsburg State University
Pittsburg, KS
bneubaue@pittstate.edu

James D. Harris
Computer Science and Information Systems Department
Pittsburg State University
Pittsburg, KS
jdharris@pittstate.edu

ABSTRACT

Computer viruses, worms, and Trojan horse programs cost individuals, companies and government agencies millions of dollars every year. Traditional responses have involved use of antiviral software which remove infections or which restrict the transmission of infected communications, and firewalls. The need to rapidly respond to new or threatened attacks has increased the popularity of subscription services which allow users to quickly obtain the most up-to-date antiviral protection. However, unprotected systems can become infected and can rapidly propagate that infection to many other systems. In response, more invasive antiviral agents can be imagined. This paper addresses ethical issues related to the protection of computer systems and delivery of that protection. Five categories in a "Protection Mechanism Grid" are proposed. The categories are based upon possible protection delivery mechanisms and the options available to system owners. The practical and ethical implications of each category are addressed.

BACKGROUND

Computer viruses, Trojan horse programs, and worms are of increasing concern to all computer users. A computer virus is a self-replicating piece of code that is designed with malicious intent. When activated, viruses cause unexpected and undesired behavior on the infected computer or on the network to which the computer is attached. Computer viruses are spread from machine to machine by the sharing of diskettes or CDs, across the Internet through e-mail attachments and downloaded files, as well as through infected web servers. A worm is a type of virus that replicates itself in memory. A worm may not be evident to the human user until its uncontrolled replication causes the system to lose performance. A Trojan horse is a program containing malicious code which may appear to be a normal program or file until it produces its destructive behavior.

The impact of infection from these malicious programs may take many forms ranging from minor annoyances to widespread damage across the Internet. Examples of relatively minor annoyances include the Freehand virus which displays a message on the screen and then erases itself. Many users remember the display of "Happy New Year 1999" followed by fireworks graphics when the worm Happy99.exe infected their systems. The LoveLetter virus and the Nimda worm created significant increases in network traffic. These two malicious programs created security breaches by making the hard drives of infected systems sharable. Newer, more virulent viruses such as Nimda may include characteristics of macros, worms, and Trojan horses as they attempt to propagate in multiple manners and exploit multiple system vulnerabilities.

Each year organizations and individuals incur costs in the hundreds of millions of dollars resulting from loss of productivity related to computer viruses. For example, the Nimda virus infected 2.2 million computers and caused $370 million in damages. [Reuters, 9/21/01] The LoveLetter virus caused as much as $10 Billion in damages while damages associated with the Melissa virus are reported to be approximately $385 million. [8]

The CERT(Coordination Center is a federally funded research center that analyzes security incidents and publishes security alerts. CERT defines security incidents as:

1) attempts (either failed or successful) to gain unauthorized access to a system or its data
2) unwanted disruption or denial of service
3) the unauthorized use of a system for the process or storage of data, and
4) changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. [3]

Statistics published by CERT and given below in Figure 1 show a dramatic increase in the number of incidents over the last five years. Many of these incidents are related to infection from malicious software. [8]

Year	Incidents
1997	2,134
1998	3,734
1999	9,859
2000	21,756
2001	52,658

Figure 1
Estimates of Incidents of Virus Infections

Companies and individuals often install protection software on their machines to attempt to protect their machines and networks from malicious programs. McAfee, Symantec and other organizations have active centers where people work to discover emerging threats and write patches that can protect customer machines from these threats. If users of protection software update their protection frequently they can hope to avoid the new infections. However, this approach is reactive and is premised on the continual vigilance of those who manage the most active computers. Malicious programs can infect large numbers of computers very quickly, sometimes in a matter of hours. Extensive damage can occur during the time required for companies like Symantec and McAfee to identify the threat, analyze it, and create and distribute a necessary patch. The emergence of a new threat can cause a significant increase in the sale of protection software. For example, during the week following the discovery of the Melissa virus the sales of virus detection software increased by 67 percent. [6]

The spread of computer viruses, especially worm viruses such as Nimda, has several characteristics in common with spread of biological viruses and sexually transmitted diseases. For example, both computer viruses and biological viruses are self-replicating. Preparation of antiviral agents for both computer and biological viruses requires access to the virus and is thus reactionary. More virulent computer and biological viruses both require a symptom less incubation period allowing growth to a critical level before detection. [2] The worm virus may spread slowly among a small number of machines until one or more very active machines becomes infected. Then what was a local problem suddenly becomes potentially a global problem very quickly.

Those who release malicious software have the advantage of decentralization and the advantage of a "head start." The head start can result in the infection of large numbers of networks prior to the creation of the patch and during the time when the new patch is being distributed. Furthermore, while the virus or worm moves quickly from network to network the patch is likely to be distributed in a more disciplined but slower way. What is needed are ways to distribute the patch very quickly so that the great majority of systems receive (and install) the patch before they encounter the computer virus.

The remainder of this paper addresses ethical issues related to different methods of responding to the threat of infection from malicious software. Where appropriate, medical analogies are used as guidelines. A "Protection Mechanism Grid" containing five categories related to the distribution of protection software is presented. The ethical implications of each method of distribution are discussed.

PROTECTION MECHANISMS

The implementation of system protection mechanisms potentially involves actions by both the system owner or administrator and the organization that provides the protection software or service. The behavior of the protection provider can be either passive or active. Passive distribution means that the provider of the protection waits for owners of computers or networks to request the download and installation of protective software. Active distribution means that the provider takes the initiative either by notifying the owners of computers or networks of the availability of protective software, by probing the machines or networks, and/or by actually downloading and deploying the protection without the owner's knowledge or permission. The system owner or administrator may wish to respond to threats or vulnerabilities individually as they occur or they may wish to subscribe to a service which automatically provides protection to threats as they occur. Also, it is possible that there is no mutually agreed upon relationship between the protection service provider and the system owner or administrator. In this later case there is no consent by system owner or administrator for the protection service provider to provide their services.

The combination of these various possibilities can be modeled using the Protection Mechanism Grid shown in Figure 2. The grid has two axis - the vertical axis relates to the active or passive distribution of protection service and the horizontal axis relates to the type of relationship initiated by the system owner or administrator, namely, specific informed consent, general informed consent by subscription, or no consent.

Within the six cells in The Protection Mechanisms Grid (Figure 2) there are five categories representing the relationship between those providing protection and the system owners or administrators. Those five categories are: Client Pull, Provider Push with Consent, Care-Taking, Subscription, and Invasion. Passive distribution implies that a relationship is initiated by the system owner or administrator thus, the cell corresponding to passive distribution and no consent is empty.

PARTICIPATION OF SYSTEM OWNERS

Figure 2 displays a grid regarding the possible behavior of those offering or providing protection. The remainder of this section explores these five categories and associated ethical implications.

BEHAVIOR OF THOSE OFFERING OR PROVIDING PROTECTION	**PARTICIPATION OF SYSTEM OWNERS**		
	Specific Informed Consent	**General Informed Consent by Subscription**	**No Consent**
Passive Distribution	*Client Pull*	*Care-Taking*	*NULL*
Active Distribution	*Provider Push with Consent*	*Subscription*	*Invasion*

Figure 2
Protection Mechanisms Grid

Client Pull

Sample Scenario: The owner of a machine or network checks the Symantec web site to learn about new viruses and chooses to download protective agents.

Explanation: "Client pull" protection implies that the individual takes the initiative to obtain and install protection on their system. Individuals have a right to protect their property just as they have a right to get a flu shot if they feel that the cost, inconvenience, and potential side-effects of the shot are less important than the potential benefits of the flu shot. This involves a personal calculation regarding the probability of getting the flu and the potential consequences of getting the flu. The same kind of risk/benefit analysis applies to the decision regarding installation of protective software.

Ethical Implications: On the surface this situation presents no significant ethical issues. Downloading electronic protection does not prevent others from also downloading that same protection. Any unanticipated side-effects of the protection are not likely to adversely affect others. However, does an owner have an obligation to protect his or her equipment so as not to become a potential source of infection to other systems? In evaluating the tradeoffs between benefits and risks, how should the individual owner assess externalities? By choosing to risk infection rather than risking possible side-effects of personal protection, the owner may increase the risk of infecting other systems through online communications. This decision might be more the result of neglect than of calculation. While it is probably not a breach of ethics to not update a system's protections against computer viruses frequently, failure to do so can contribute to the overall propagation of computer viruses. Drawing an analogy to public health, few people would argue that individuals have an ethical obligation to get a flu shot primarily in order to prevent others from getting the flu.

Provider Push with Consent

Sample Scenario: Microsoft Corporation sends e-mail to owners of machines running IIS and warns them about a recently discovered vulnerability. The owner can then choose to download the software that will secure the problem, or may choose not to do so.

Explanation: Provider push with consent implies that protection is actively distributed. That is, those agents seek out systems that require the immunization service they offer. However, individuals responsible for each system can decide whether to either allow these agents to examine their system or to allow the agents to immunize their systems. This could be analogous to the U.S. Postal Service determining which employees may have been exposed to anthrax and then offering treatment to those potentially infected. The employee would have the right to refuse the treatment.

Ethical Implications: If users can select whether or not they wish to allow their systems to be examined (or perhaps if they can turn-on and turn-off access to their systems by active agents) then this becomes much like client-pull and the ethical issues may be related to responsibilities and proper control. If the user cannot control access to their systems by these active agents then this situation becomes somewhat like invasion. The privacy of the system is violated. This might be analogous to an individual being required by the state to submit to a physical checkup to screen for a deadly disease. Even if the treatment is optional should the disease be found, the required screening itself would raise ethical concerns. There is also the concern that the protection provider might also exploit this situation as an opportunity to collect information for other purposes.

Subscription

Sample Scenario: An owner enters into a service agreement with Gibson Research for software to protect the owner's system. A part of the agreement is that when the vendor updates the software product that provides protection, the update will automatically be downloaded onto the owner's machine. The agreement may or may not specify that the owner will be notified after the fact that the upgrade has been made. The owner may at any time opt out of the update service agreement.

Explanation: The benefit of a subscription update service for software protection is convenience and the fact that the system being protected is likely to be updated almost immediately once the security patch is available. The provider is clearly a trusted source in that the owner of the machine or network has voluntarily entered into the service agreement and is probably paying for the subscription. The fact that the machine or network is patched quickly helps assure that it is not used by a new computer virus to help spread the new virus. The owner or administrator of the network may prefer to be notified of the completed security update although having that information may be of little help if the update has caused a side effect and no uninstall (rollback) is available. If the automatic installations of patches cause side effects, the owner should be able to terminate the agreement with the vendor and change to the "provider push with consent" arrangement.

Ethical Implications: Ethical implications for the vendor are similar to those in the client-pull category previously discussed. Also, the vendor has ethical responsibilities to protect the privacy, security, and integrity of customer systems.

Care-Taking

Sample Scenario: AOL (America Online) maintains a firewall to prevent e-mail virus attachments from reaching the owner's machine or network.

Explanation: Care-taking implies that protection is available without direct action of the individual whose system is being protected. It does not involve placing protection directly on owners' machines or networks but rather taking some action "upstream" to protect the owner. If an ISP installs and maintains the protection software on its equipment then its customers receive the benefit of that protection. That protection, however, may interfere with something the customer wants to do. For example, some firewalls prevent the use of some instant messaging services.

Ethical Implications: In terms of a public health analogy this may be like the responsibilities of a water district to remove known contaminants from water before the water goes to households. Water districts have legal as well as moral obligations to maintain water quality. It is more difficult to define the jurisdiction of an ISP than of a water district. It is less likely that an ISP is legally required to filter out computer viruses. However, it may well be in their best interests to attempt to do so. Also, there may be an element of distributive justice in this. In other words, customers who can't afford individual protection should receive some protection in the public domain.

Another ethical aspect of care-taking might be forcing customers to receive protection that they do not want. In terms of the water treatment analogy, this might be analogous to fluoridation of water. However this line of thought seems more relevant to the filtering of content rather than to protection against computer viruses. Some ISPs attempt to filter adult content in the interest of children and advertise this as part of their service. Some governments attempt to limit the political ideas communicated across the World Wide Web. It is very unlikely that any customer wants to receive computer viruses. Therefore, screening out computer viruses upstream is not likely to raise ethical issues.

Apparently the only major ethical issue here is if the upstream protection prevents the customer from doing something he or she wants to do or if it has performance implications for the customer. Assuming that the customer has the ability to choose another ISP that offers less or different upstream protection, it is hard to envision that the provision of upstream protection against computer viruses would cause any significant ethical concern.

Invasion

Sample Scenario: A well-intentioned person releases an electronic antibody (EAB) onto the web believing that it will help prevent the spread of a particularly destructive and fast-spreading computer virus. The EAB multiplies and spreads itself from machine to machine and network to network in the way a computer virus does. The EAB does not announce itself and does not obey robot exclusion rules. [5] The EAB does not carry the identity of its source. A machine or network receives the EAB without the owner's permission or knowledge. The EAB installs itself on the machine and uses the machine to send copies of itself to other machines. Once on the machine the EAB does no damage and (hopefully) protects the machine from an intentionally harmful computer virus.

Explanation: The EAB is essentially a benign virus designed to fight the computer viruses. The only distinction between those who release the EAB and those who release the virus is intent.

Ethical Implications: The release of the EAB has invaded the privacy of many systems and the fact that the EAB is not intended to damage a system does not insure that it will do no harm. Good intent alone does not justify what is otherwise unethical behavior.

The responsibility of protecting a system belongs to the owner of the system or to the owner's agent who is likely to be a system administrator. It is inappropriate for others to attempt to protect that system without the knowledge and agreement of the owner. The exception may be a situation in which there are large negative externalities and a timely action is absolutely necessary. In other words, if a system might be used as a vehicle to damage other systems (as in a denial of service attack), the ultimate consequence may be very significant. For example, the ultimate consequence might be a sudden failure of the air traffic control system or a significant financial system. As in time of war, an immediate preemptive action may be necessary. Even in this circumstance, the burden of ethics falls heavily on any person or organization that releases EABs regardless of good intent.

DISCUSSION

Informed Consent

Informed consent is one of the cornerstones of medial ethics. A competent adult can give informed consent for personal medial treatment. Medical providers have legal and ethical obligations to inform the patient of the possible consequences of treatment. A legal guardian can give informed consent regarding medical treatment decisions for children or others not able to give informed consent. Giving informed consent involves attempting to weigh the risks and the benefits of treatment in order to make a decision regarding what treatment to select, if any. Informed consent does not imply complete and perfect knowledge regarding possible risks.

System owners have rights regarding the maintenance and protection of their networks just as parents have rights regarding the medical treatments of their children. There are at least two significant qualifications that should be made regarding this analogy. Computers and networks are clearly property and nothing more. First, children are not the property of their parents and the ethical treatment of humans is certainly far more complex than the ethical treatment of property. Second, it would be unusual for a parent or legal guardian to delegate the decision about a medical treatment to a small child. However, it is reasonable for the owner of a computer to program the computer to interact with software agents and to make decisions regarding automatic downloading of software upgrades and service patches. The program that does this embodies the delegation of discretion by the owner or system administrator. It is possible to program the computer to make the decision regarding whether the owner or system administrator should be consulted prior to installation of a particular upgrade or patch. While a small child's consent to receive a medical treatment would not constitute the parent's informed consent, we believe that a computer's consent to receive an upgrade or a patch can be a meaningful expression of the owner's consent.

Trusted Sources and the Limits of Regulation

"Trusted source" is not an absolute concept. Every owner can decide which providers of software (including virus patches) are trustworthy. If a vendor is the sole provider of a particular kind of software and the owner needs that kind of software, the vendor is in the position to dictate the conditions of the agreement. If a vender requires that owners accept automatic patches and the owner cannot choose another vender, the vender may have a substantial burden of ethics if the owner's system is subsequently damaged by an unintended effect of a patch. If an owner chooses to download and install patches from multiple trusted sources, the owner must accept the risk of possible interaction effects.

The usual solution in a situation like this is some kind of government regulation. However, the jurisdictions of governments are not well defined in cyberspace, and government agencies are not likely to be agile enough to make decisions regarding distribution of patches quickly. Government agencies test new drugs for their safety and effectiveness, but lack the speed and skills to approve EABs. There may be a role for government agencies and/or professional societies to certify the credentials of companies that provide EABs.

CONCLUSION

The Protection Mechanisms Grid (Figure 2) contains five categories representing the relationship between system owners or administrators and those organizations or individuals that provide protection services. The Client Pull, Provider Push with Consent, and Subscription categories produce no major ethical concerns because the system owner has the opportunity to give informed consent for the service provided. However, even with consent there may be issues related to the system owner's ability to evaluate trustworthiness of the service provider. Also, some might argue that system owners have an ethical obligation to help prevent the spread of malicious infectious agents by protecting their systems.

In the Care Taking category there appear to be no major ethical issues as long as the "care taking" is limited to controlling the spread of malicious infectious agents. The Invasion category has the most serious ethical implications because in this category the system owner has not given informed consent and the system owner has not had the opportunity to evaluate the trustworthiness of the EAB source. The software may do harm even though its intention was benign. The benign intent of the programmer is not a sufficient ethical justification for the release of an EAB.

The number and destructive potential of computer viruses and worms will certainly continue to increase. This increase will produce more proactive and innovative defenses. However, it is important that ethical issues raised by these defenses be considered and that system owners and administrators have the opportunity to give informed consent for the use of these defenses on systems they control.

REFERENCES:

[1] Beauchamp, Tom L. and Childress, James E. (2001) *Principles of Biomedical Ethics* 5th edition. Oxford University Press, New York.

[2] Brissett, A., Shipton, Geraldine. "Some Human Dimensiions of Computer Virus Creation and Infection."*International Journal of Human-Computer Studies,* May, 2000, vol. 52, pp 899-913.

[3] CERT Coordination Center. "Incident Reporting Guidelines."
http://www.cert.org/tech_tips/incident_reporting.html#1.A

[4] Kephart, J. O., Sorkin, G. B., Chess, D. M. and White, S. R. Fighting Computer Viruses: Biological Metaphors Offer Insights into Many Aspects of Computer Viruses and Can Inspire Defenses Against Them. *Scientific American*, November, 1997.
http://www.sciam.com/1197issue/1197kephart.html

[5] Koster, Martijn. "A Standard for Robot Exclusion."
http://www.robotstxt.org/wc/norobots.html

[6] PRNewswire, "Todays News," April 14, 2000. http://www.prnewswire.com

[7] Reuters News Service, reported September 21, 2001.

[8] SecurityStats.com. "2000 Computer Virus Prevalence Survey."
http://www.securitystats.com/reports.asp

[9] Symantec Corporation news release. (May 11, 1999). "Symantec Unveils Digital Immune System Strategy for Unprecedented Level of managed, Intelligent Protection and Control."
http://www.symantec.com/press/1999/n990511.html