Internet security 300

Seminar Paper

Security on the Internet

The Internet is the community of the future, but if security measures are not put in place and enforced, then it will become more of a slum and less of a community. The primary question is, therefore, who has the obligation to put these security measures into place? Is it the individual users of the computers and the Internet? Is it the responsibility of the companies that develop the different computer applications to place certain security measures in place? Or is it the responsibility of the governments of the world to unite and create rules and regulations that secure the Internet and guard the citizens of the world from the malicious activities of the hackers? In my opinion, the responsibility belongs to them all.

Security on the Internet is a very important issue in the world today. Billions of people have an on-ramp to the Information Superhighway, and more are finding one every day. The Internet transcends geographical locations, and is the first example of a true global village. Unfortunately for regular users of the Internet, much like the real world, criminals exist on the Internet as well. “ Hackers,” the computer wizards who use their knowledge for evil, are rampant on the Internet. Sometimes they do seemingly harmless acts, such as just going into a computer system and observing, but at other times, they steal, destroy or alter data. On some occasions, these cyber-felons perform even more malicious acts, such as infecting systems with “ viruses,” computer programs that “ infect” the systems by latching onto other programs and eventually destroying them. Another favorite activity of the hacker is to gain access to the computer system and then manually either delete files or cause the computer to do “ strange” things, such as placing messages on the screen that either make no sense or have an unusual meaning.

Before we look at who has the responsibility to protect the end user, we must first look at what the truth is behind all the “ security breaches.” There is almost regular notice in the media of a “ backdoor” or “ bug” in a program: an error in the coding of the program that allows the knowledgeable hacker to access the computer system of someone using that program. Most frequently, we hear about this regarding a World Wide Web browser, such as Microsoft’s Internet Explorer or Netscape’s Navigator. While we associate Microsoft and Netscape with the United States, they are used internationally. Netscape and Microsoft both have large market shares in countries such as Japan and Canada, as well as all throughout Europe.

A prime example of the sorts of bugs found is one which recently affected Microsoft’s Internet Explorer. On May 8, 1997, C-net’s online news service, News. com, reported that yet another bug had been found in Internet Explorer. According to the article, “ The glitch could allow a malicious Web site to execute any program on a user’s computer without permission, including deleting files and uploading private information.” The article continues to describe how Microsoft had found out about the bug, and would very shortly have a fix available on their web page. However, further reading of the article, brings some interesting points into view. The article describes how the “ glitch” launches a PowerPoint presentation. PowerPoint is an application included in Microsoft’s Office Suite; however, not everyone either has this program or chooses to install it. In other words, the only way for the " glitch" to affect a user is if PowerPoint has been installed on the individual computer system. That important item of information failed to make it into the more mainstream reports, such as the television news, leaving the uninformed worried about a " glitch" that had no affect on them. This caused thousands of people to hurry onto the Internet to find a patch to the " glitch," thereby slowing down the connections to the Internet.

More recently, on June 12, 1997, the Associated Press reported on a bug in Netscape's Navigator web browser. According to the article, the glitch " lets Web site operators read anything on a hard drive of a personal computer logged onto the site." PC Magazine and CNNfn ran their own tests for the bug and determined that even firewalls (security measures put in place to try to protect against just this type of security breach) were not effective in protecting against this bug. Unfortunately, this article, much like most articles about software bugs that are from mainstream media sources, offers no technical information about the bug and, therefore, it is hard to determine what the reality is behind this bug. This is the type of article that the typical Internet user sees and most likely will frighten them enough to make them take time away from their usual regimen to find a patch for the bug. This may become an enormous waste of time and resources since these users do not realize that this bug most likely does not affect them or their computer systems.

Another popular form of scaring the public is virus hoaxes. According to the National Computer Security Association, ten hoaxes currently are making their way around the Internet, most of them by E-mail. One of the most popular hoaxes is the “ Good Times” virus.

“ This hoax originated back in 1994. Created as a joke by some students at Swarthmore College, it has caused quite a stir in the Internet community. Claiming to be the first multi-platform virus and able to create massive destruction to whatever hard drive it might infect, the recipients of this message were in a panic. We have seen this particular hoax rise and fall in circulation. It circulates all over the USENET groups and every once and a while it springs to the surface and makes its rounds, most likely due to new users that ‘ get on the net’ and have no idea that these types of messages are false. Give someone an idea and they’ll run with it; that’s the true result of this hoax. Good Times is the first generation of hoaxes. Granted there were a few before this, but they were not as proliferated as this one”

As one can see from this, people are as easy to fool in the computer world as they are in everyday life. This is just one of the many hoaxes going around the Internet and it is interesting that it has been active for three years now. The trick is that the message sent out changes occasionally. The original message was just a warning about it and everyone quickly realized it was a hoax. The message said “ What makes this virus so terrifying, said the FCC, is the fact that no program needs to be exchanged for a new computer to be infected.” To those of us who have been using computers and the Internet for a long time, this is obviously impossible, but to those Internet users who are not as computer savvy, this seems frighteningly real. Since it seems real to them, imagine how distraught they are when they cannot find a protection against this virus.

The other frightening thing is that sometimes the more destructive hackers take these hoaxes and make them realities. Recently, one of the hoaxes, the AOL4FREE hoax, claimed that if you got an E-mail message discussing getting free access to America Online and open the message, it will open a window and delete all the files on the hard drive. The original version of this hoax stated how no virus programs could detect it, including the one that comes with Windows 95. The better informed of us knew that it was a fake, since there is no virus program included with Windows 95. Recently however, someone took this hoax, and made it a reality. A message now is going around the Internet with an attached file called AOL4FREE. COM. This file is really just a program that calls another program that actually does delete all the files on a hard drive.

Recently, the Social Security Administration made available on their web site a service that was supposed to allow people to get information about their Social Security status. To get this information, all that was necessary was for the user to supply some demographic information. Unfortunately, this information was available on other sites on the Internet, thereby making the information easily accessible. The Social Security Administration took this feature off their web site immediately, but was in trouble with United States citizens nonetheless for putting up this information on the site to begin with.

The main part of the responsibility to protect the users of the Internet lies with the users themselves. Computer users themselves must be ethically responsible enough and knowledgeable enough to use computers correctly. If they are not sufficiently prepared for the Internet, then they are putting themselves into a situation analogous to a man walking into the middle of a gunfight without a bulletproof vest.

People in different countries see different levels of need for protection. I surveyed some “ Net-izens,” people who spend much time on the Internet, to find out how they protect themselves. I surveyed six Americans, including myself, three Canadians, three Europeans, and three Japanese. While this may seem like a small cross section of people, they seem representative of most of their respective countries. The one thing that all these people share is that they are not people who use the Internet exclusively for business. They all use it for entertainment purposes as well. Of all the questions asked, only one was universally agreed upon; of those surveyed, no one encrypts important data files. I assume that they do not do so because they realize that there is no one who would want to get to their individual data files.

The majority of people surveyed have some form of virus protection on their computer system, the most widely used one being McAfee’s Virus Shield. Only one person who did not have any virus protection on his computer and he was from Japan. From what I gathered from the people surveyed in Japan, different people have different views as to the level of security needed on their personal computers. The one who had no form of virus protection is only on the Internet via e-mail, and views no attached files. For that reason, he has no need to worry about a virus coming onto his system via the Internet. Of the rest of those surveyed, most update their virus protection data files once a month. It is important to keep these files updated if one is a frequent and/or heavy Internet traveler because new viruses are being created every day.

Only one American surveyed uses a credit card for purchases on the Internet. Most people never use their credit cards on the Internet because they are afraid that someone may be able to intercept the data transfer and grab the information about their credit card and be able to use it falsely and illegally.

While most people do check once a month for updates to their programs that are supposed to protect against bugs and backdoors, the majority never bother to download those upgrades as these programs do not seem important enough nor are they felt to apply to these users.

Some of the responsibility for security on the Internet must, however, lie with the companies that produce computer programs. These companies have a responsibility to make sure that the programs they sell will not have adverse effects on the user's computer system. As was mentioned above, " bugs" and " backdoors" are frequently in the news media. The companies that release these programs must make sure that there are no bugs or backdoors, and if it is later determined that there is one, they must provide their customers with an upgrade immediately.

Microsoft was very quick in fixing a recent bug. Once the bug was known publicly, there was a patch (repair) available for it within a matter of hours. Microsoft may have an extensive track record of bugs and backdoors in their programs, but they have a great history of quick repairs as well.

Netscape Corporation, Microsoft's chief competitor in the " Browser Wars," has a much worse track record for repairing their glitches. When a bug was found recently in Netscape's Navigator web browser, the company was very apprehensive about the situation and claimed that they did not have enough information about the bug. Netscape claimed that their lack of information was because the company that reported the bug to them was asking for a large amount of money for the technical specifications of the glitch. Netscape refused to pay this since they considered it similar to a bomb threat and blackmail. They could not verify that the glitch existed, nor that it did not, and because of that, they could not create a patch for it. Netscape would never have gotten into that position had they fully tested their Navigator program before releasing it to the public. Netscape does offer $1, 000 and a T-shirt to anyone who does report a valid bug. The company that reported the bug felt that this was too little in comparison to the security problems the glitch could cause. Surprisingly, this greedy company was not an American firm, but was actually a Danish software company that felt that the information it had was worth much more than Netscape was offering.

Software bugs are common, but the companies that are responsible for the distribution of the software must also be responsible for its upkeep. Most companies are responsible enough to get the upgrades out within a few days after the bugs are discovered. What they need to do, however, is to assure that the programs are bug-free before they release them.

There is yet another place where the responsibility for security on the Internet lies. The governments of the world need to get together and create laws to govern the Internet. As it stands, countries can make laws to prevent security breaches in their own country. There is no legal remedy to deal with someone in a foreign country, one with which there is no extradition treaty, who commits a felony in another country via the Internet. When a crime is committed on the country's soil, the country has some time to capture the felon before he leaves their soil. When a cyber-felon commits a cyber-crime on the Internet, the cyber-felon is never actually in the country to be caught.

The most famous attempt by government to govern the Internet is the Communications Decency Act, or CDA. This was an act that was designed to censor the information on the Internet, specifically pornography. When the CDA was first approved by President Clinton, a major protest was staged on the Internet. It was announced that people should turn the background of their web pages to black to mourn the occasion. Millions of web sites, both personal and commercial, turned their pages to black; this action was taken by both Americans, who would be held to this law, and people from other countries, who this law would not directly affect.

Therein lay the major problem. The United States attempted to make a law to govern the Internet; however, it was just the United States that enacted the law. Since no other countries had made the law, it did not affect web pages hosted in other countries. Another problem with the CDA was that it was close to impossible to enforce. There are millions of web sites and no one source can tell what is on each one. While it may have been possible to find the commercial sites that would have been illegal according to the CDA, it would have been impossible to find all the personal sites on the web that were in violation of this law. The final problem with the CDA, and effectively the one that destroyed it, was that it was against the First Amendment. The CDA was never put into effect because there was such protest against it, and until recently, everyone was waiting for the Supreme Court to make a ruling on the CDA. When the Supreme Court finally made the ruling earlier this summer, the “ Net-izens” breathed a great sigh of relief. The Supreme Court has ruled that the CDA was against the First Amendment, because the Internet is a form of speech.

In early July of this year, twenty-six European countries made a broad declaration of their Internet policies. This group statement basically was the same as the White House’s “ hands-off” policy that had been announced on July 1, 1997. However, one central principle was made: “ what is illegal offline is also illegal online.” The American government wants to make the Internet a worldwide free-trade zone. European officials do not agree entirely. They agree not to seek new Internet taxes, but they do wish to have sales taxes and other real-world levies to apply to anything sold over the Internet. To enforce this however, is yet another problem much like those experienced with the CDA. The international sale of goods on the Internet would require some form of monitoring to guarantee against fraud. While they could examine the record books of the company, those could be falsified as well. The only way to verify that companies were obeying the rules would be if there were people hired with the specific job of scanning the Internet to find out what comapnies were following the rules, and which ones weren’t.

There are groups that are attempting to set international laws governing the Internet. An international meeting has been called for this fall by a Washington-based group. The group, calling themselves the Open Internet Congress, or OIC, stated that a longstanding informal international panel has fleshed out some of the already existing standards of etiquette that Internet users have imposed upon themselves since the Internet was just a newborn idea. The OIC claims that this international panel is attempting to get control of the Internet. The OIC wishes to have a new system of processes that would be both fair and democratic. The goal of the fall convention is to create “ some sort of administrative entity to govern the Internet,” said Wayne Thevenot, the spokesperson for the OIC. This may be a good idea since, right now, the only people regulating the Internet are the people who own and run the Internet Service Providers (the companies that give end users access to the Internet) and the people who operate the different sections of the Internet: chat room operators, webmasters, newsgroup moderators, etc.

Security on the Internet is more than people think. The responsibility for it does not lie just with the end users, nor just with the software companies, nor just with the governments of the world. The responsibility lies with us all. If we do not check ourselves, and make sure that we are doing only that which is right, then how can we expect the companies or the governments to protect us? If the software companies do not make sure that there are no “ bugs” or “ backdoors” in the programs they write, then how can the end users or the governments prevent those “ bugs” and “ backdoors” from being exploited? If the governments do not make laws regarding what can and cannot be done on the Internet, then how can the end users or the software companies know what guidelines to follow in their interactions on the Internet? Over the past decade, the Internet has grown from a small unknown entity into a wide spread global media with millions of people accessing it world wide and more joining every day. Some people are afraid of the Internet, considering it to be Big Brother from George Orwell’s 1984, realized at last. Others realize that the Internet is a powerful tool, if it is used properly, and strive to get the most out of it. For each person, security entails something different. Some of us will be afraid of the hackers, some of us will realize that the hackers would have no reason to do anything involving us. Some of us will be afraid of computer viruses, some of us will not worry about it since they always have protection against viruses in place. Some of us will always be afraid of the Internet, no matter what security measures are put in place, some of us will never worry about security and will use the Internet for whatever we feel is proper. Overall, the Internet is a global force with which nothing compares and nothing can be compared. Security on the Internet is, therefore, a powerful and important feature that must be attended to and nourished as the cyber-world and real world merge and interact with more frequency.

Bibliography

1. NCSA Anti-Virus Information,

http://www. ncsa. com/virus/alerthoax. html, updated May 1997.

2. Another Bug in Explorer,

http://www. news. com/News/Item/0, 4, 10487, 00. html, May 8, 1997.

3. Netscape Checks for Bug, June 12, 1997 http://www. abcnews. com/sections/business/sectors/HighTech/ap_netscape612/index. html

4. Fox, Robert, Not So Social Security,

Communications of the ACM, June 1997- Volume 40, Number 6.

5. Peter G. Neumann and Lauren Weinsteinh, Inside Risks Spam, Spam, Spam!, Communications of the ACM, June 1997- Volume 40, Number 6.

6. Kanaley, Reid, Will anything ever rule the Net?, The Philadelphia Inquirer, Sunday July 13, 1997, page E3.

7. Survey done via E-mail, results attached.

Annotated Bibliography

1. NCSA Anti-Virus Information, http://www. ncsa. com/virus/alerthoax. html, updated May 1997. This page contains information from the National Computer Security Association about current viruses, as well as hoaxes, viruses that people are saying exist, but in reality are not there. Messages about these hoaxes circulate through e-mail, wasting people’s time, and making the uninformed frantic when they can’t find a protection for the hoax. I will use this site to get information on these hoaxes. Using that information, I will show how the concerns of the people about viruses, and about their computer’s security are blown out of proportion.

2. Another Bug in Explorer, http://www. news. com/News/Item/0, 4, 10487, 00. html, May 8, 1997.

This site gives complete information on one of the most recent bugs in Microsoft’s Internet Explorer Web Browser. This site will be useful in showing an example of a real security problem, and what companies are doing to prevent them.

3. Netscape Checks for Bug, June 12, 1997 http://www. abcnews. com/sections/business/sectors/HighTech/ap_netscape612/index. html

An article from the Associated Press. This article discusses how Netscape Communications Corp. is doing to prevent and fix bugs that can come about. It deals specifically with one bug that has been claimed to exist.

4. Robert Fox, Not So Social Security, Communications of the ACM, June 1997- Volume 40, Number 6.

This article talks about the recent World Wide Web Site that the Social Security Administration shut down because of security issues.

5. Peter G. Neumann and Lauren Weinsteinh, Inside Risks Spam, Spam, Spam!, Communications of the ACM, June 1997- Volume 40, Number 6.

This article talks about the act of " Spamming" and the threats that it imposes upon computer systems.

Etan Weintraub

For my Senior Seminar paper, I wish to research the current global issues surrounding information security on the Internet. While the Internet has evolved from a military communications network to a global data-sharing community, its growth has contributed to this very problem of data insecurity. As it currently stands, much of the information on the Internet is completely vulnerable to unauthorized retrieval and/or manipulation, as well as to piracy. In addition, people can attack others via E-mail by sending harassing messages and/or " Spamming" (the act of sending multiple unsolicited messages that completely fill the victim's mailbox). People cannot protect themselves from these cyber-felons, especially when they can retrieve personal and financial information without the owner's knowledge. There is also almost regular notice in the media that someone can access information from another person's computer system through the use of a backdoor or a bug in a program. I plan to learn what the truth is behind the existence, complexity, and scope of some of these back doors and bugs. I also plan to examine what people are developing to counter these threats and to protect themselves. In addition, I hope to discover what companies are doing to help their customers and to protect themselves. An added question to be answered as well is what the governments are doing to enact laws that will globally govern the Internet.

As a computer science major, someone who deals with computers on a daily if not hourly basis, and a " Net-izen," an Internet citizen, someone who spends time on the Internet in an active nature, the global issues surrounding security on the Internet affect me in more ways than one. The Internet is the community of the future, but if security measures are not put in place and enforced, then it will be more of a slum, and less of a community.