INTERNET SECURITY

Cecilia B. Henry, Texas A&M University – Kingsville
Dr. Richard Aukerman, Texas A&M University – Kingsville
Dr. Jack D. Shorter, Texas A&M University – Kingsville, j-shorter@tamuk.edu

ABSTRACT

After a long period of relative obscurity when it was solely the domain of technically oriented individuals, the Internet has burst onto the national scene and is playing an increasingly important role in an ever-widening spectrum of activities involving an exponentially increasing number of people. The Internet is a loosely structured network of computers that cross company, educational and government boundaries. There's no organizing body, and there are no rules. There's only controlled anarchy. And that control exists to ensure that my computer can talk to your computer fairly well. Topics more relevant to national security than to social and commerce use of the Internet are provided in order to establish a broader importance of the Internet in the daily affairs of individuals and institutions, and its potential for reaching wide audiences. The Internet is a powerful resource for information. The threat from "crackers", "hackers", and computer viruses is always present. Internet security is now in the mainstream.
Keywords: Broadband, fiber optics, cable-modems, DSL, Satellites

INTRODUCTION

The Internet is a powerful resource for information. People from all walks of life use this tool for various reasons. Whether a person would like to share personal ideas with others or start a home business, the Internet opens the door to both. The Internet provides information, resources, humor, and contact with others in the world, news, and an extraordinary avenue for business transactions. The scope of the Internet has broadened within the last few years, now you can shop online, bank online, and find information for research papers online. However, this wonderful information resource can also be misused**.** The threats from "crackers", "hackers", and computer viruses are always present. Internet security is a great concern of millions of people worldwide. In global terms, Americans are by far the heaviest users of the Internet, and the proportion of American homes with personal computers and modems is increasing at a very fast rate. There are so many Websites on the Internet now that when you search for certain terms utilizing search engines, some terms are found on millions of sites.

Computers have changed drastically. They were "centralized in locked rooms and looked after by people with arcane vocabularies. Security threats in those days were mostly from insiders: people abusing their accounts, theft of data and sometimes vandalism"(2). In keeping the computers in locked rooms, they were securely managed. "Today computers are here, there and everywhere, including people's private offices. So central management isn't feasible and security is harder to manage"(2).

HISTORY OF THE INTERNET

The Internet is a publicly enormous global network of computers (7). The Internet grew out of a U.S. Defense Department program called ARPANET (Advanced Research Projects

Agency Network) (15). It was established in 1969 with connections between computers at UCLA, Stanford Research Institute, UC-Santa Barbara, and the University of Utah (7). "ARPANET's purpose was to conduct research into computer networking in order to provide a secure and survivable communications system in case of war" (7). As the network quickly expanded, academics and researchers in other fields began to use it as well. "In 1971, the first program for sending E-mail over a distributed network was developed. By 1973, the year international connections to ARPANET were made (from Britain and Norway), E-mail represented most of the traffic on ARPANET. The 1970s also saw the development of mailing lists, newsgroups and bulletin-board systems, and the TCP/IP communications protocols, which were adopted as standard protocols for ARPANET in 1982-83, leading to the widespread use of the term Internet" (15). In 1984 the domain name addressing system was introduced (15). "In 1986, the National Science Foundation established the NSFNET, a distributed network of networks capable of handling far greater traffic, and within a year more than 10,000 hosts were connected to the Internet. In 1988 real-time conversation over the network became possible with the development of Internet Relay Chat protocols (see chat). In 1990 ARPANET ceased to exist, leaving behind the NSFNET, and the first commercial dial-up access to the Internet became available" (7). In 1991 the World Wide Web was released to the public (via FTP) (15). The Mosaic browser was released in 1993, and its popularity led to the proliferation of World Wide Web sites and users (15). "In 1995 the NSFNET reverted to the role of a research network, leaving Internet traffic to be routed through network providers rather than NSF supercomputers" (7). That year the Web became the most popular part of the Internet, surpassing the FTP protocols in traffic volume. "By 1997 there were over 10 million hosts on the Internet and over 1 million registered domain names. Internet access can now be gained via radio signals, cable-television lines, satellites, and fiber-optic connections, though most traffic still uses a part of the public telecommunications (telephone) network" (15). The Internet is widely regarded as a development of vast significance that will affect nearly every aspect of human culture and commerce in ways still only dimly discernible.

SCOPE OF THE INTERNET

Individuals connected to the Internet using their desktop computers can perform the following functions:

- Exchange electronic mail, or e-mail with any other user at any location
- Participate in offline discussions via e-mail with large groups of individuals interested in particular topics, using "mailing lists' and "News Groups"
- Participate in online discussions with large groups of individuals using the "Internet Relay Chat" function
- Log on to remote computer sites and users, and upload files to remote sites and users via FTP, or File Transfer Protocol, function
- Read complex documents composed using "Hypertext" (clicking on a highlighted phrase on the screen takes the user into another domain); a standard protocol fetches the desired component from its home location and presents it transparently to the user, who is unaware of the underlying processes.
- Read "multimedia" documents, resident at "World Wide Web" sites, consisting of text, graphics, sound, and video (7)

HACKERS AND CRACKERS

There are many hackers (it's hard to know exactly how many). Many of them have unimpressive skills, aren't creative, and simply borrow someone else's hacking software for their exploits (9). Some hacker masterminds can find new ways to break into computers. But such people are rare.

"A hacker is simply someone who explores computer systems without stealing information, altering information or cracking codes. Hacking, the common term for unauthorized use of computer systems, has been a problem for system operators since modems became common equipment with home PCs a decade ago" (9). Knowledge and exploration is the goal of a hacker. Often hackers "contact the owners of the systems that they explore to inform them how effective their security systems work; this service allows security systems to be improved and secure facilities to be made more so" (9). Danger becomes evident when hackers toy with private information. "The term cracker is broader in scope, referring to someone who enter a computer system and "cracks" codes. The main difference between a hacker and cracker is intent: exploration or conquest. Where the hacker strives to learn about computer systems, the cracker enters systems for personal gain. Often, a cracker steals information and/or programs for personal use or to sell; this person is a criminal" (9).

How can hackers and crackers be stopped? You are potentially safe if you use a dial-up connection to connect to the Internet. However, you are susceptible to intrusion "if you use a full time network connected to the Internet or use a full time connection like cable modem or Digital Subscriber Line (DSL)" (4). Software companies continuously produce new and advanced methods of security, which enhance hacker prevention (3).

VIRUSES

A computer virus is "typically a short program designed to disperse copies of itself to other computers and disrupt those computers' normal operations." (5) "A virus will not act until the file it is hiding in has been executed, or until certain pre-established conditions have been met – trigger condition (a specific date, an operation carried out by the user, etc.)" (8). Some viruses are annoying, while others can destroy information or cause an operating system or application to crash (5). "A computer virus usually attaches or inserts itself to or in an executable file or the boot sector (the area that contains the first instructions executed by a computer when it is started or restarted) of a disk; those that infect both files and boot records are called bimodal viruses" (5).

There are thousands of known viruses that are spread through networks, CDROMS, infected floppy disks, and the Internet via e-mails. "Some actions that can be carried out by a virus are obvious enough to be recognized and could include: messages displayed on-screen, operations slowing down, the properties of some files changing, files and/or folders disappearing, the computer will not start, the content of the infected disk is lost, etc" (8).

Some people think that if they connect to the Internet, their computer systems will immediately start picking up "Internet" viruses. It can happen, but it's also one of the easiest risks to manage. To combat viruses, antivirus programs and hardware have been developed to scan incoming files. Antivirus programs "search for evidence of a virus program (by checking for appearances or behavior that are characteristic of computer viruses), isolate infected files, and remove viruses from a computer's software" (5).

A distinction should be made between a virus-which must attach itself of another program to be transmitted-and a bomb, a worm, and a Trojan horse. A bomb is a program that resides silently in a computer's memory until it is triggered by a specific condition, such as a date. A worm is a destructive program that propagates itself over a network, reproducing as it goes. A Trojan horse is a malicious program that passes itself off as a benign application; it cannot reproduce itself and, like a virus, must be distributed by diskette or electronic mail.

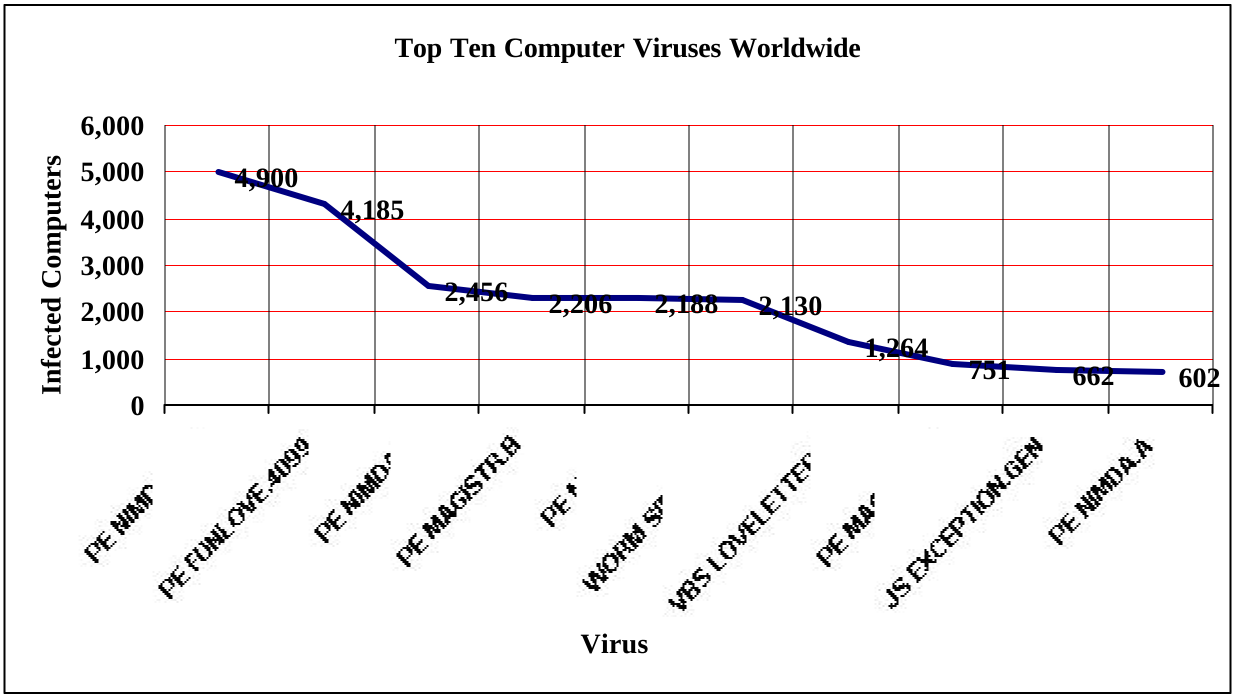

Figure 1. Provided is a list of the top ten viruses that are considered to be major threats worldwide (11)

The latest worms--worms are viruses that can spread without human involvement--don't even require you to open an e-mail attachment to do their dirty work. The recent Code Red and Nimda worms exploited vulnerabilities in Microsoft's server software (12). Microsoft Outlook is another frequent target.

There are thousands of known viruses and related security threats lurking on the Internet today. The number is increasing. Infection from just one of these Internet-borne threats can erase your entire hard drive.

SPYWARE

Spyware is software planted on your computer to harvest and forward information about you to others outside your system (1). "The information collected can range from a survey of your surfing habits passed along to advertisers and marketers, or in malicious cases the passwords and credit card numbers you type being passed along to crackers who will exploit it. The software can be planted through Trojan horses received in e-mail or even included in software you obtain and install for other purposes" (1).

"Web sites present a spyware threat both in the form of cookies and Web bugs. A cookie is a small text file that a Web server sends to your hard drive via your browser" (1).

Cookies are very common and are used to simplify navigation for you and identify you to the site you are visiting. “A cookie can store quite a bit of information about you, and release it again each time you visit the site that generated it. Many ISPs use another type of cookie to keep track of logins. Unless you have told your browser not to accept cookies, which is an option you have, you can continue to visit members-only parts of the service until you close your browser and the cookie goes away” (1).

To defend yourself against spyware, always maintain current anti-virus software on your systems, and be very careful about installing software from unknown sources. Check out independent reviews before installing (1).

DATA ENCRYPTION

Concerns about the lack of security online and potential loss of privacy prevent many computer users from realizing the full potential of the Internet. Encryption systems, which scramble electronic communications and information, allow users to communicate on the Internet with confidence, knowing their security and privacy are protected. However, the U.S. government blocks export of strong encryption, limiting its widespread use (6).

“Cryptography is the art or science of secret writing, or more exactly, of storing information based on the use of algorithms in a form which allows it to be revealed to those you wish to see it yet hides if from all others” (6). A cryptosystem is a method to accomplish this. “The original information to be hidden is called “plaintext”. The hidden information is called “ciphertext”. Encryption is any procedure to convert plaintext into ciphertext. Decryption is any procedure to convert ciphertext into plaintext” (6).

“The operation of the algorithm requires the use of a key” (6). A cryptosystem is designed so that decryption can be accomplished only by persons in possession of both a decryption engine (generally a computer program) and a decryption key (6).

Finally, there is the question of security. The security of a cryptosystem is always relative to the task it is intended to accomplish and the conditions under which it will be used. A secure system becomes insecure if used by people who write their encryption keys on pieces of paper, which they stick to their computer terminals. Encryption schemes can be broken, but making them as hard as possible to break is the job of a good cipher designer. All you can really do is make it extremely difficult for the code breaker to decipher your cipher. Still, as long as both source and encrypted data are available, it will always be possible to break your code. It just won’t necessarily be easy. However, there are many reasons for using encryption, and the cryptosystem that one should use is the one best suited for one’s particular purpose and which satisfies the requirements of security, reliability, and ease-of-use (2).

FIREWALL

In these security-conscious days, a firewall--which controls the flow of data into and out of your PC--has become an essential utility. It also blocks unauthorized access to the Internet by programs running on your system, a lifesaver if a hacker has previously slipped a Trojan horse into your PC or if you've downloaded a program that's spying on your computing activity (13).

Firewalls, like BlackICE, PC Protection, and McAfee Personal Firewall are valuable tools that can protect your data even if you haven’t installed all the latest security patches for your applications. They can also stop some kinds of attacks that Windows wasn’t designed to withstand. A properly configured firewall will withhold all information about your PC from any potential intruder (14).

If you're connected to the Internet, you need antivirus software, and as protection against hackers, you need a firewall, particularly if you have a cable or DSL modem or are part of a local area network. The best-regarded antivirus program has been Norton AntiVirus from Symantec, at http://www.symantec.com. The company also makes an excellent firewall called Norton Personal Firewall and other security programs for individuals and businesses. However, an even better firewall program for individuals is ZoneAlarm from Zone Labs, at www.zonelabs.com. (13)

A firewall is supposed to make you feel safe, but it can make you feel more paranoid than you were before you installed the software. Many firewalls don't just block outsiders—they tell you every time someone scans your computer. The frequent notices can make it seem as if dozens of hackers and crackers are clamoring to get into your hard drive. The scans that firewalls block are always happening. Even if you only occasionally surf the Web and check e-mail, your PC is bombarded by queries constantly—some benign, others more threatening (13).

E-MAIL SECURITY

The Internet has radically changed the way we communicate with each other. E-mail is obviously an extremely valuable form of communication, but with this technology comes certain pitfalls that should be understood. The path that an e-mail message takes to reach its recipient is a complex and varied one, and while in transit that message may come under the potential scrutiny of numerous people and organizations. There are probably at least a million people in the world with the requisite technical knowledge necessary to intercept Internet-based e-mail. (There are actually probably a lot more than that - maybe several million by now, and more everyday as the populace becomes more networking-literate.) Fortunately, the number of those people who actually have the physical access necessary to intercept e-mail is much smaller, but it is still a very large number. However, there is no way to stop people from intercepting your e-mail messages. The only thing you can do to protect the privacy of your messages is to encrypt those messages so that, if intercepted, they cannot be read and will be of no use (10).

CONCLUSIONS

Computer security is an important issue today for every computer user, whether your computer is part of a huge corporate network, or a single desktop computer used at home to figure your family budget and to shop for things on the Internet. "The increased use of videoconferencing and Internet collaboration technologies, the rush toward Web services, and an emerging class of malicious code that blends virus and wormlike capabilities represent some of the biggest security challenges for 2002." (12)

Virus makers are literally creating new viruses every single day, coming up with ingenious ways to create havoc for computer systems worldwide. Of course the explosive growth of the Internet has made full virus protection a complete necessity for all computers rather than an option. A strategy called "firewalls" has been developed, whereby a second computer (a firewall) is placed between an organization's own computer and the Internet communication lines, to help control access and prevent "break-ins". It has recently been found that hackers have successfully penetrated even triple firewall architecture. With respect to viruses, there is a kind of arms race, whereby anti-virus software writers improve their software to protect against a newly discovered type of virus; the virus writers respond by creating a new virus that can circumvent that new protection.

What is clear is that America's critical information-technology infrastructure is being attacked. Though no lives have been lost, huge amounts of money are being wasted trying to ward off and recover from this intensive onslaught.

REFERENCES

1. Bigelow, S. (2002, January). I know where you surfed last summer. Smart Computing, 42-44.
2. Heath, J. (2001). How electronic encryption works and how it will change your business. [Online]. Available: http://www.viacorp.com/crypto.html [2002, February 25].
3. Howe, W. (2002, January 31). Privacy on the Internet: what can others learn about you? [Online]. Available: http://www.walthowe.com/navnet/privacy.html [18 February 2002].
4. Howe, W. (2002, January 10). Security Guide. [Online]. Available: http://www.walthowe.com/navet/security.html/ [28 February 2002].
5. Infonautics Corporation. (2001, December). Electric Library: computer virus. (6th ed.) [Online]. Available: http://www.encyclopedia.com/articles/03021.html [2002, February 25].
6. Infonautics Corporation. (2001, December). Electric Library: data encryption. (6th ed.) [Online]. Available: http://www.encyclopedia.com/articles/45977.html [2002, February 25].
7. Infonautics Corporation. (2001, December). Electric Library: Internet, the. [Online]. Available: http://www.encyclopedia.com/articles/23350.html [2002, February 25].
8. Panda Software. (2001). What is a virus? [Online]. Available: http://www.pandasoftware.com/library/IntroVir.html [2002, February 18].
9. Schneier, B. (2002). Frontline: Hackers: who are hackers: are hackers outlaws or watchdogs? [Online]. 28 paragraphs. Available: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/outlaws.html/ [2002 February 20].
10. Thurman, M. (2001, December). Making the airwaves safe for corporate e-mail users. Computerworld. [Online]. Available: www.computerworld.com/itresources/rcstory.html [2002, February 22].
11. Trend Micro. (2002, March). Trend world virus tracking center. [Online]. Available: http://wtc.trendmicro.com/wtc.html [2002, March 04].
12. Vijayan, J. (2002, January). Security Challenges Take Toll. Computerworld. [Online]. Available: http://www.computerworld.com/ [2002, February 20].
13. White, M. (2001, November). Keep the wolves at bay. Smart Computing. 78 – 82.
14. White, M. (2002, January). Recognizing Malware. Smart Computing , 32 – 35.
15. Zakon, H.R. (2002, January 3). Hobbes' Internet TimelineVersion: 5.5. [Online]. 39 pages. Available: http://www.zakon.org/robert/Internet/timeline/ [2002 February 25].