

Computer Set-Up and Security

Pamela Schoffstall

John Carroll School

08/17/01

Lab: ARL/CISD

Mentor: Dr. John Brand

Abstract

The purpose of this research project was to investigate the mechanisms and execution of computer security. Initially, a computer was built and a network constructed to better understand the physical aspect of computer security. Subsequently, different methods of protection from intrusion were studied and deployed.

Introduction

The purpose of the research was to investigate computer security. Computer security will be important in the future because information needs to be kept secure. Politics, the economy, social life, education – all will be linked in the relatively unexplored world of “cyberspace.” In this world, malicious intruders can and will do everything they can to break the community’s trust to serve their own needs. There is a need for people to fully understand and study computer security to maintain the workings of society and to protect the flow of information. If no one protects cyberspace, intruders will be free to do as they please. Even today, business transactions and data transfer take place electronically all the time, and the informed intruder knows how to disrupt these inner workings. To maintain order, this cannot happen. People with good intentions need to know more about computer security than the malicious intruder. This is the purpose of the research experiment – to learn more about the world of tomorrow to better protect it.

Computer Set-Up and Security

Equipment:

- case and ATX-compatible power supply
- motherboard
- Central processing unit (CPU)
- memory
- hard drive
- floppy drive
- CD-ROM drive
- video card
- Etherlink card
- monitor
- keyboard
- mouse
- drive cables (2)
- jumpers
- screws
- screwdrivers
- flashlight
- Partition Magic CD or floppy
- Disk Wizards boot disk
- Windows 98 installation CD

- Red Hat Linux 7 installation CD
- floppy disks for emergency start-up disks

Procedures for constructing a computer:

1. Test the power supply for ATX compatibility. Begin by checking the wire colors, and then checking the voltages. Compare with the known ATX values:

Color	Signal	Pin	Pin	Signal	Color
Orange	+3.3 volts (v)	11	1	+3.3v	Orange
Blue	-12v	12	2	+3.3v	Orange
Black	Ground (GND)	13	3	GND	Black
Green	PS On	14	4	+5v	Red
Black	GND	15	5	GND	Black
Black	GND	16	6	+5v	Red
Black	GND	17	7	GND	Black
White	-5v	18	8	Power Good	Gray
Red	+5v	19	9	+5VSB (Standby)	Purple
Red	+5v	20	10	+12v	Yellow

(Mueller, 1105).

2. Dispel electrostatic discharge (ESD) by touching the case, and then install components on the motherboard. Install the CPU, fan, and memory before installing the motherboard inside the case. The CPU used in this project has a Zero Insertion Force (ZIF), so it should not be forced into place. The CPU fan is set on top of the CPU by way of a special clip. The memory should also not be forced into its socket, as it can only go in one way. If it does not fit, it is backward or in the wrong socket.
3. Next, install the motherboard inside the case. Count the connectors before placing the motherboard inside the case. Align the ports of the motherboard with the corresponding openings in the case. Ensure the connectors line up with the holes in the motherboard and none touch the circuitry. After screwing in the

- motherboard, count the number of screws and ensure they equal the number of connectors. This prevents shorting the motherboard.
4. Now the cards can be installed. Place them carefully in the sockets on the motherboard with the metal end facing the outside of the case. Rocking the card back and forth will help to overcome the springiness of the contacts. After screwing them in, cover any unused openings with metal plates.
 5. Install the internal drives by first placing them in their individual drive bays and then screwing them into place. Connect the IDE cables from their drives to the motherboard by aligning the red wire with the number 1 pin on the motherboard's and drive's IDE port. Connect the power connectors from the power supply to their sockets on the drives, with the red wire closest to the IDE cable. The cables are keyed, so do not force the plug into the IDE port. The floppy drive uses a special cable with a twist on one end. The twisted end should be closest to the drive.
 6. Finish the internal connections by connecting the power switch, reset button wires, and the power supply to the motherboard.
 7. Plug in external peripherals (the monitor, keyboard, and mouse). The monitor's cable attaches to the external port on the video card. The keyboard and mouse have similar keyed connectors that connect directly to the motherboard.
 8. Turn on the computer and monitor to test to see if everything works. The BIOS should boot and either a setup screen or a message will appear saying to press any key to restart.

9. Partition and format the hard drive with Partition Magic. The Linux partition should have 2 or more gigabytes (GB), the Windows operating system and programs partition should have 3 or more GB, and the rest of the space should be left for a data partition. The Linux partition uses the EXT2 file system, and the other two partitions should use the FAT32 file system. FAT32 is readable by Windows 98 and other higher versions, which gives flexibility of upgrading.
10. Boot from the Disk Wizards boot disk, and choose the option that will install the CD-ROM driver. Insert the Windows 98 CD in the CD-ROM driver, and type “setup” at the CD’s command prompt. Follow the on-screen instructions. The setup program will prompt for the computer to be restarted several times.
11. Install Red Hat Linux 7 from its CD. The Linux partition may need to be configured from the Linux setup. It will need an extended swap partition, and the rest of the partition can be left to the root directory.
12. Install drivers for the video and Ethernet card.

Results:

The computer case had one ribbon cable designated for the power switch, reset button, LED, and other components. Since the new motherboard had a separate connector for each of these, the cable was cut and the wires stripped individually. The resistances of the possible wire pairs were tested for the power and reset switch, and the respective wires soldered to connectors. These makeshift wires were then plugged into the corresponding spots on the motherboard. Upon first test, the computer did not boot. The LED on the motherboard was not even lit. Upon further investigation, it was found that the power supply was not ATX compatible (the first step of the procedure was not

followed upon first trial). A new power supply was obtained and installed. The computer finally booted. Oddly enough, it worked even though I had accidentally switched two of the wires while soldering. This was easily fixed. After booting, the BIOS did not recognize the hard drive. The hard drive was swapped for another, and the BIOS recognized it. However, Partition Magic did not recognize the new hard drive. Removing the master/slave jumpers on the hard drive caused the computer to accept it. After the hard drive was partitioned and formatted, Windows NT was installed. It was discovered that NT was not easily compatible with the Linux operating system, because of Linux Loader, a Linux function which offers a choice of which operating system to load after boot. NT was uninstalled and Windows 98 was installed without problem. After installing the video card driver more problems surfaced. The computer's resolution was too large to see the entire screen. Loading Windows 98 in VGA mode and adjusting the resolution seemed to help, but the computer would freeze often. The hard drive was re-partitioned and re-formatted; Windows 98 was reinstalled to eliminate the video card driver, but it remained resident on the computer. Finally the drivers for the video card were uninstalled using the Add/Remove Programs option in Control Panel, and the computer had fewer problems. In the meantime, Linux was installed successfully. This experience emphasized the importance of troubleshooting.

Procedures for setting up a network:

1. Connect multiple computers to a hub by way of cables. One cable links a hub and an Ethernet card together.

2. Configure Windows 98's network settings for the network. The IP address, subnet mask, and network name should be entered into their appropriate fields.
3. In MS-DOS mode, test the Ethernet card and the connections by pinging the card first, then pinging the other computer. Ping the network card by the loopback address 127.0.0.1 and then the installed network IP address.
4. Configure Linux's network settings. This is normally done during installation of Linux.
5. Test the settings by pinging the other computer, and press Ctrl+C to stop it if the ping is set for a large number of attempts.

Results:

For cables, category 5 uniform twisted pair (UTP) with RJ45 connectors were used. The network functioned normally. The IP address used was 128.1.1.5, and the subnet mask was 255.255.255.0. The name of the network was kidnet. It was observed that network settings are often configured during installation, but they should always be checked afterwards. On the hub, there are lights that indicate whether or not the Etherlink cards are detected. These lights should also be checked.

Procedures for securing Windows 98:

1. Disable file and printer sharing. Go to Network Properties and click on the File and Print Sharing button, and clear the check boxes. This prevents the intruder from scanning shared files or planting hostile programs on the user's machine.
2. Disable dial-up server or set an encrypted password by using the Server Type dialog box in the Dial-Up Server Properties. An alternative is to authenticate

- through a Windows NT domain controller or NetWare server. This prevents the intruder from using file sharing on the dial-up server for his own means.
3. Do not install the Remote Registry Service. The Remote Registry Service would enable an intruder to modify the Windows Registry. The Windows Registry contains key components which allow Windows to function properly, but could cause the computer to crash if abused.
 4. Install and use antivirus software to scan for Back Orifice (BO) or NetBus, or use a backdoor scanning tool such as The Cleaner (<http://www.moosoft.com/cleaner.php3>). Backdoors such as BO enable an intruder to remotely administer the system. Intruders could perform any action they wished without the actions showing on the display of the victim computer.
 5. Keep software, especially internet software such as Internet Explorer, patched and up-to-date. For Internet Explorer check out <http://www.microsoft.com/security/bulletins/>, and for Netscape, use <http://home.netscape.com/security/notes/index.html>. Most backdoor programs take advantage of holes in internet client software, so it is important to keep the internet client software patched.
 6. Beware of downloading from untrusted sites, for BO or NetBus could be disguised as helpful programs.
 7. Use a host-based firewall such as ZoneAlarm for Windows machines or the Firewall Toolkit for Linux.
 8. Set a BIOS password. In the BIOS setup, choose the BIOS password option. This discourages console hacking.

9. Use a commercial security tool that provides system locking or disk encryption beyond the BIOS, such as RSA SecurPC 2.0 (<http://www.securitydynamics.com/products/datasheets/securpc.html>) or Pretty Good Privacy (<http://www.nai.com>). This also discourages console hacking.
10. Disable the CD auto-run feature. This prevents an intruder from bypassing the screen-saver password by using the CD auto-run feature. The CD auto-run feature is disabled by going to Device Manager and double-clicking on the CD-ROM driver entry. On the Settings tab, click the “Auto Insert Notification” check box to clear it.
11. Disable password caching by creating the DWORD Registry key:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching = 1`. Otherwise, an intruder could crack the file for system passwords.

Results:

The problem with the Windows 98 operating system is that it was not designed to be a secure operating system. Instead, security was sacrificed for ease of use. However, remote administration features are limited, which deters the intruder slightly. An intruder can take over a Windows 98 system by tricking the system and/or its operator into executing the intruder’s code, or by gaining physical access to the system. Steps 1-3 protect against intrusion through shared resources. Steps 4-6 protect against back doors, programs used by the intruder to take over the system. Step 7 protects against different ways of hacking, such as denial of service. Steps 7-10 protect against console hacking. Should an intruder gain physical access to the console, the computer is basically his due to Windows 98’s lack of security features. The security measures listed here can only

deter the intruder and make taking over the system more difficult. On the experimental machine, I carried out steps 1, 2, 3, 7, 9, and 10. On my home machine, I installed ZoneAlarm, a host-based firewall. Within ten minutes a port scan was attempted from a remote machine, emphasizing the importance of securing one's system.

Conclusions

This summer, I have learned about the hardware of the computer and how it relates to the computer's operations and networking, as well as how to set up a network and to secure individual computers. Now that I have a working knowledge of computer security, I know I still need to learn how to secure more operating systems beyond Windows 98. I also want to be able to investigate the different firewall and antivirus software available. I have also learned how to troubleshoot a problem -- sometimes it is necessary to do everything over to ensure all steps of the process were performed correctly. I am confident the knowledge I have gained will be beneficial to me in the future.

There is still much more to learn about computer security. The information to be learned could be endless. Yet, there are steps any person can take to protect him/herself and his/her data. My SEAP experience has taught me that the future frontier of cyberspace may be a scary place, but someone has to take the initiative and protect it. There may always be intruders with evil intents that will haunt this world and keep it from being a peaceful place. But as long as people keep studying and working to secure their information, there is hope the future world may be a utopia of free information exchange and open relations between countries all over the globe.

Acknowledgements

I would like to thank my parents, for encouraging me to apply for and pursue this apprenticeship program. A special thank you goes out to my mentor, Dr. John Brand, who has done everything in his power to provide me with the best information and resources that I could hope for. Thanks to Ms. Ann Brodeen, who helped me with paperwork, badging, other administrative duties, and revising my writings. Thanks to Ms. Pat Jones, Branch Chief, for supporting this program and acquiring materials for us. Thank you to Ms. Maria Lopez, for her informative classes on C programming. Thank you to all of the other employees in the building where I worked, for their kindness and conversations about their jobs. Finally, thank you to my fellow apprentices, Juvy Santos and Mike Juhasz, for sharing their knowledge with me.

Bibliography

- Campen, Alan and Douglas H. Dearth, ed. Cyberwar 2.0: Myths, Mysteries and Reality.
Fairfax, VA: AFCEA International Press, 1998.
- Gilster, Ron. A+ Certification for Dummies. Foster City, CA: IDG Books Worldwide,
Inc., 1999.
- McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed: Network Security
Secrets and Solutions. Berkeley, CA: Osborne/McGraw-Hill, 1999.
- Mueller, Scott. Upgrading and Repairing PCs, Eleventh Edition. Indianapolis, IN: Que
Corporation, 1999.