A Common Weak-Link in the Security Chain

Gregory B. White, Ph.D.
SecureLogix Corporation
greg.white@securelogix.com

Keywords: Dial-up connections, Modems, Network Security, Intrusions/Penetrations

Abstract

The need for computer security is commonly accepted today in government and industry. Numerous studies have shown both an increase in security incidents as well as an increase in interest by organizations to address security issues. Many security tools such as firewalls and intrusion detection systems are becoming commonplace in organizations yet intruders still are able to penetrate computer networks. Often this is because security administrators neglect to address one of the most common weak-links in the "security chain" – modems attached to individual machines inside of the security perimeter. The use of "war-dialers" have been discussed in numerous articles and have been made famous though movies such as *War Games.* Many security professionals, however, commonly neglect to use this or similar tools as a means to audit their organization's modem use. This paper discusses this common weak-link in security and proposes methods to address this aspect of computer security

Introduction

Computer security has gained enough attention in the last few years that it no longer is as difficult to convince managers of its importance. Increasingly we see companies and government agencies addressing the problem. Of 212 companies contacted in a survey conducted by Zona Research, 58 percent reported that they were increasing their security budgets. Just because over half of the companies contacted in the survey are increasing their security budgets does not mean that industry and the government have arrived at a point where they have control of the situation. In fact almost the opposite can be said to be true. In early 1998, the FBI reported that the number of cases involving computer intrusions over the previous two years had increased over 250 percent. [Yas:1998] 64 percent of respondents to a 1998 Computer Security Institute survey of 520 companies claimed to have had a security breach in 1997. [Mac:1998] At the same time, only 48 percent claimed to have had break-ins the previous year and only 42 percent were victims in 1995. While that number dropped slightly in the 1999 survey to 62 percent, a corresponding increase in the number of organizations that couldn't tell if they had been the victim of an intrusion occurred. [Pow:1999] The adage that companies have more to fear from their employees than from outsiders also seems to be somewhat changing as the 1999 survey reported that 57 percent of the companies had frequently been attacked through the Internet compared to 54 percent in 1998 and only 37 percent in 1995. Another alarming increase took place in 1999 as 28 percent of the respondents reported that remote dial-in was the point of attack as opposed to only 24 percent the previous year.

If companies are more security conscious and are spending more on securing their computer systems and networks yet at the same time are experiencing an increased number of intrusions, one has to ask if they are spending money on the correct defenses. While undoubtedly a major part of the reason that intrusions are on the rise is the increasing number of individuals participating in this sort of activity, one still has to examine where money is being spent and ask if the countermeasures being employed are sufficient. One aspect of security often overlooked and which often allows a backdoor into a computer system or network are modems attached to systems inside the security perimeter.

A Weak-Link Often Overlooked

One of the recent trends seen in the security arena is an increasing number of successful attacks on computer systems and networks that are a direct result of organizations making their systems accessible via dial-up connections. Highly visible cases in the media have only served to further aggravate the situation. Cases such as the July 1998 attack on Time Warner Cable's Chatsworth, California system illustrate this point. In this incident, intruders claimed that they gained access to the channel modulator, communications satellite, and channel switching server.[Cho:1998] The intruders further claimed to have been able to gain directional control of one of the system's satellites. The intrusion itself was reportedly perpetrated by dialing directly into Time Warner Cable's system through a maintenance port. [Cho:1998] In a public statement about the incident, Michael Luftman, Time Warner Cable's Vice President of corporate communications provided a carefully worded statement stating "There was no impact because never at any time did they try to do anything to the system itself." This obvious non-denial of the incident only serves to excite one's imagination as to what the intruders could have done had they chosen to.

In another case involving intrusion via an unguarded modem, also well reported in the media, a 'juvenile hacker' was charged with shutting down telephone service at the Worcester, Massachusetts airport control tower as well as the town of Rutland, Massachusetts. [Bor:1998; Gla:1998] Unfortunately for the airport, its ability to communicate with its fire department and other services as well as its main radio transmitter relies on its ability to use local telephone lines. The youth, apparently unknowingly, cut this service for over six hours on March 10, 1997. The systems attacked by the intruder had been left accessible via telephone connections so NYNEX employees could remotely access them in case of problems.

Though most well-publicized incidents involving intrusions via dial-up connections are recent, the problem is not new. The 1983 movie *War Games* featured the star, Matthew Broderick, utilizing a "war-dialer" to obtain phone numbers for connections to computers. Thirteen years later, in a well-known security test, individuals at the WheelGroup Corporation accepted a challenge from *Fortune* magazine to "hack" into computer systems at an anonymous Fortune 500 company located in New York City – 1600 miles from where WheelGroup was located in San Antonio, Texas. [Den: 1999; Beh:1997] The security specialists utilized several techniques to attempt to gain access to the target systems but were ultimately blocked by a firewall and the rules of engagement. Though given time they might have been able to either circumvent or penetrate this obstacle, the parameters of the test did not permit them this luxury. Instead they relied on the same technique used by Matthew Broderick thirteen years earlier – they used a war-dialer to find 55 numbers answered by systems connected via a modem. Within two hours of obtaining these numbers the company's network had been successfully penetrated.

The WheelGroup Corp. (which has since been purchased by Cisco Systems) is not the only organization that knows of and utilizes war dialing. Mark Abene, a security consultant (known in computer "hacking" circles by the name *phiber optik*), also employs this method to gain access to systems an networks he has been asked to penetrate (from a "white hat" perspective in his security consultant role). In an article for CPMnet, Abene and his co-authors, Gerald Kovacich and Steven Lutz, described the steps that they take when performing a penetration test. [Abe:1997] Abene stated that after attempting more common means of penetration through the Internet, they eventually move to "identifying any dial-up terminal servers or workstations/servers with directly connected modems." He went on to state that this "gives us a stealthy and almost guaranteed way into the network." The extent of this problem is illustrated in a statement by Jeromie Jackson, a security consultant at Garrison Technologies. In an interview conducted in 1996 he stated: [Poo:1996]

I would say that none of the companies that I work with are totally secure. Ninety-nine

> percent of the time we go in we see modems sitting on people's desks; people are allowed to bring in pcAnywhere software. They can get into their computer with nothing: no id or password. Then they connect with T1 lines out to their vendors; they have no security between them and their vendors.
>
> I mean, the Internet is nothing. They have plenty of problems internally already. If your management's freaking out about getting on the Internet because of security, then they're under the false assumption that their network is already secure. I would bet your and my bottom dollar I could go into just about any company in the United States and find huge, gaping holes…everywhere…

The common thread through all of these examples is that while access to an organization's computer systems or network through the Internet may be protected, intrusions can still occur because of the common practice of installing modems on systems that are inside the organization's "security perimeter."

Current Methods to Address the Problem

One way to handle the problem is to take the approach that Sun Microsystems took in 1998. Their policy is that any employee found with a modem on their desk will face possible termination from the company. [Ran:1998] According to Mark Graff, network security architect at Sun, dial-up Internet access from desktops is the "second-biggest security risk in corporations." While many may feel this approach is a bit extreme, the fact that modem usage must be regulated is a generally accepted premise. On the subject of modems, the September 1997 Site Security Handbook (RFC 2196), for example, makes several recommendations:

> Although they provide convenient access to a site for its users, they can also provide an effective detour around the site's firewalls. For this reason it is essential to maintain proper control of modems.
>
> Don't allow users to install a modem line without proper authorization. This includes temporary installations (e.g., plugging a modem into a facsimile or telephone line overnight).
>
> Maintain a register of all your modem lines and keep your register up to date. Conduct regular (ideally automated) site checks for unauthorized modems.

One current approach some take is to purchase modems with internal security features which can provide, for example, some level of password authorization. Another common feature is to employ a method to provide a dial-back capability. The use of Remote Access Services (RAS) to introduce authentication and encryption technology is also becoming common for organizations that permit dial-up access to their computers or network. The problem of "rogue modems", unauthorized modems which individual users have installed, can still be an extremely dangerous threat to an organization's security. To combat this threat, companies will frequently employ the use of war-dialers to scan for rogue modems connected to company telephone lines. Public domain software such as ToneLoc and THC-Scan (**T**he **H**ackers **C**hoice) have been employed to perform this task. Originally developed by and for those in the computer 'underground' these tools can nonetheless be used by security auditors to scan a series of numbers to determine if modems are connected to them. These freeware versions of war-dialers, while useful, suffer from several deficiencies that make them less desirable in commercial environments. Specifically, both of these lack easy-to-use interfaces and perform no automated vulnerability assessment should a modem be detected. In addition, both only allow the use of a single modem which limits the usefulness of the tool for large organizations with many numbers. Obviously the one factor both of these

tools have in their favor is that, as freeware, the cost to the organization to obtain them is nonexistent – of course the same can be said of their customer support.

Commercial-grade war-dialers are now also available. These products are generally designed to locate modems and connect to them, identify the type of system connected to, and finally attempt to gain access to the system using some very basic techniques. Commercial dialers are often capable of using multiple modems and phone lines so that a larger series of numbers can be scanned in a shorter period of time. While these commercial dialers are a big step forward in war-dialing technology, they still suffer from a few deficiencies. Chief among the deficiencies are manual collation of multiple-site sweep results and a non-distributed architecture.

Despite the problems described, how effective can war dialers be? In an experiment run by Peter Shipley, a computer security consultant in Berkeley, California, several million San Francisco Bay area phone numbers were searched for exploitable modems. Of the phone numbers that he found which were connected to modems, 75 percent were insecure enough for intruders to gain access to the computer systems attached to them. [Rad:1999] These numbers included a fire department deployment system and environmental controls for some large buildings. [Stu:1998]

What is Needed

The traditional approaches to addressing the security problem associated with the use of modems are not adequate in today's business environment. Taking Sun's approach of terminating employment with the company for anybody who connects a modem is not realistic for most large corporations today who have legitimate reasons for allowing dial-up access to their systems and network. Allowing unrestricted modem use, however, is also not the answer as the numerous incidents involving intruders gaining access through dial-up connections attest to. Even if policies for the use of officially approved modems are developed, enforced, and followed, "rogue modems" are still a threat. Firewalls may be in place to block insiders from being able to transmit certain types of data over the Internet but an insider who connects a modem to a system can easily circumvent this safeguard. War-dialers can greatly enhance an organization's chance of detecting rogue modem use but the dialers are only useful when they are actually in operation and are not used to actually prevent such usage – just detect it. In addition, war-dialing only provides a "snapshot" of the telephone network at the time the dialing is accomplished. A modem could be attached seconds after the war-dialing scan and it would go undetected until the next scan.

What is needed is a coordinated approach to addressing the problem with modems similar to the way security problems are addressed in the traditional TCP/IP networked environment. It will take more than just policies and detection equipment, however, it will take systems designed to control and manage the use of modems and the telephone lines themselves. Three types of technology have provided the visibility and control of the TCP/IP network discussed here. These technologies are scanners, firewalls, and intrusion detection systems (see figure 1). Scanners are used in the TCP/IP environment to discover vulnerabilities in systems and networks. Programs such as the Security Administrator's Tool for Analyzing Networks (SATAN) have been designed to recognize common network-related security problems. The tools generally report on problems they find—usually without actually exploiting them. Commercial-grade war-dialers are the first step towards providing this same scanning capability in the telephone network. With the global nature of many large corporations these commercial dialers need to be able to address the distributed nature of the resulting corporate telephone network. This means they should be able to consolidate scanning data from remote sites and, in order to perform the dialing in an economic fashion, should handle distributed dialing from a centralized site. *Telesweep Secure*, from SecureLogix Corporation, is designed to handle both the small local business performing a sweep of just a

few telephone lines as well as large international corporations with thousands of lines throughout the world.

Detecting what type of device a telephone line is connected to (e.g. modem, fax, or telephone) is only the first part of the scanning function. Commercial dialers also need to perform vulnerability checks to determine if a possible backdoor into an organization's network exists. A vulnerability check would entail the determination of what software or operating system is running on the system a detected modem is connected to. Many access mechanisms come with default passwords. Telephone line scanners should check for known vulnerabilities, such as these default passwords, and provide a report of them so they can be corrected. Commercial telephone scanners, such as *Telesweep Secure*, often provide this capability.

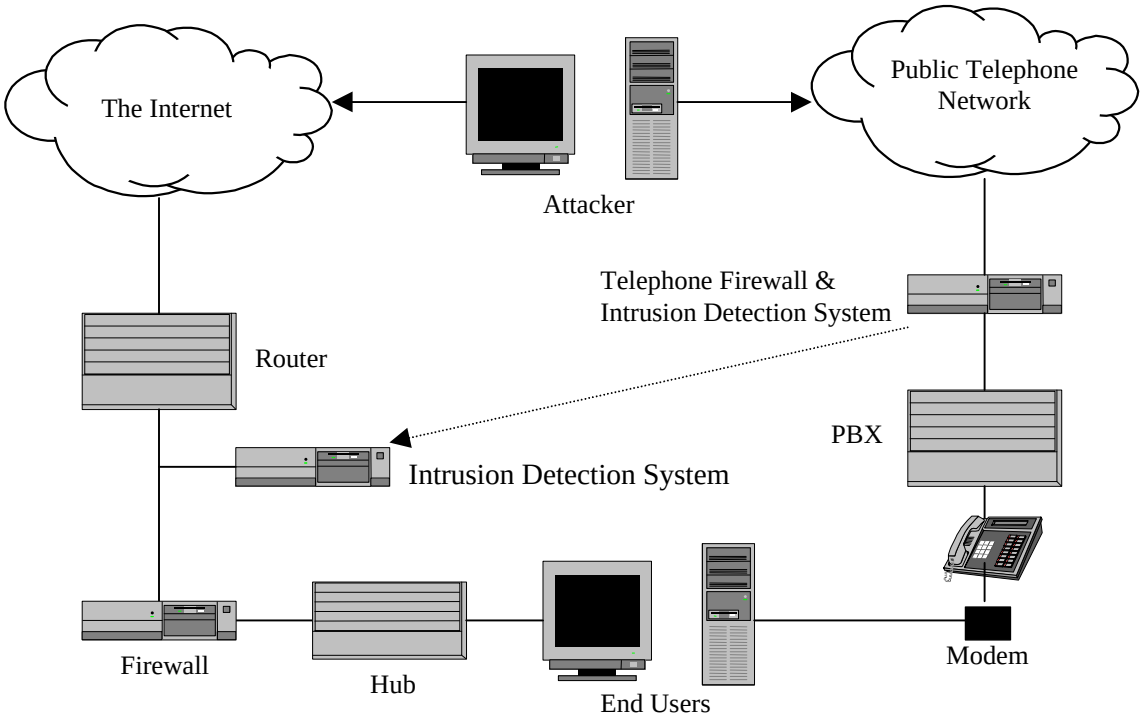

Figure 1. Protection of the TCP/IP and Telephone networks

The second technology needed in the telephone network arena in order to provide visibility and control similar to that now provided in the TCP/IP environment is a firewall for the telephone lines. In TCP/IP networks, firewalls are used to control the services and systems that are visible or usable to individuals outside of the corporate environment. In this way they can limit the damage that can be done to internal networks from the "firestorm" that exists on the public network. A firewall designed to be used on telephone lines should be able to enforce corporate security policy in terms of which lines are intended for voice, data, or fax data. It should be able to block connections that are in violation of security policies and should have a reporting mechanism to inform security officers in real-time. A robust reporting mechanism can also provide an auditing mechanism for telephone call traffic which can be used to not only better manage telephone resources but also as a mechanism to perform audits of telephone line charges. *TeleWall*, from SecureLogix Corporation, provides this capability.

A third technology needed is the ability to detect intrusive activity that is occurring via the telephone network. A first step towards providing this capability is to be able to detect war dialing

attempts against an organization's telephone lines. Technology in devices such as *TeleWall* provides this capability. More extensive intrusion detection capabilities, such as detecting attempts to gain access to computer systems via telephone lines authorized for data communication, are also possible and can be handled in two ways. The first is to have the firewall device on the telephone network also perform the intrusion detection activity. A second method would be to have the firewall on the telephone network serve only as a sensor which then feeds connection information to other intrusion detection devices already attached to the TCP/IP network (both of these methods are depicted in figure 1.). The first method has the advantage of simplicity as it limits the domain knowledge necessary for the telephone firewall. The disadvantage is that it results in the treatment of the networks as two separate entities. The second approach, the one the author recommends be developed further, has the advantage of consolidating intrusion information for both networks in a single manager. This provides security professionals a better view of the security status of the entire network. While no product currently provides this capability, a product which would combine information not only from these sensors but from all others as well (e.g. all brands of firewalls, routers, and intrusion detection systems) would be extremely valuable in detecting concerted attacks from multiple avenues and in providing an accurate, real-time picture of the entire network.

Conclusion

With corporate computer security receiving greater attention and with a general increase in security budgets, security professionals must be sure that they are not simply creating the computer security equivalent of the Maginot Line. [Mal:1998] Guarding against one threat while leaving others wide-open only serves to create a weak-link in the security chain. Modems have become this weak link. The ability to use modems to gain access to computer systems and networks is not new but at the same time it is a problem that has not been adequately addressed. Security for this arena is at the same stage security was for TCP/IP networks a decade ago. What is needed to address these problems is a set of solutions similar to those produced in the TCP/IP environment. War-dialers acting as security scanners for the telephone network were the first step. Devices that will serve as telephone firewalls and real-time intrusion detection systems are the next steps in this evolutionary process. Deployment of these devices will provide security professionals a view and control of the corporate data network that has not been available before. It is a view that is necessary to secure all avenues into corporate networks.

References

Abe:1997 Mark Abene, Gerald Kovacich, and Steven Lutz, "Intrusion Detection Provides A Pound Of Prevention", CPMnet Technology News Site, August 17, 1997, available from the internet at www.techweb.com/se/directlink.cgi?NWC19970815S0032

Beh:1997 Richard Behar, "How We Invaded a Fortune 500 Company", Fortune, 3 February 1997.

Bor:1998 John Borland, "Feds Charge Underage Hacker", CPMnet Technology News, 18 March 1998, available from the internet at www.techweb.com/wire/story/TWB19980318S0022

Cho:1998 Joshua Cho, "Looking Both Ways on the Info Superhighway", CableWorld News, 30 November 1998, available from the internet at www.mediacentral.com/Magazines/CableWorld/News98/1998113011.htm

Den:1999 Dorothy Denning: Information Warfare *and* Security, Addison-Wesley, Reading, Mass, 1999.

Gla:1998 James Glave, "Crackers: We Control Your TVs", WiredCom News, 20 July 1998, avilable from the internet at www.wired.com/news/news/technology/story/13838.html

Mac:1998 Malcolm Maclachlan, "Study Shows Hacking Increased in 1997", CPMnet, TechWeb, 03/04/98, available from the Internet at www.techweb.com/wire/story/TWB19980304S0023

Poo:1996 Gary Andrew Poole, "Hack Attack", Forbes ASAP 1996

Pow:1999 Power, Richard, "1999 CSI/FBI Computer Crime and Security Survey", Computer Security Issues & Trends, Computer Security Institute, Vol. V, No. 1, Winter 1999.

Rad:1999 Deborah Radcliff, "Hackers for Hire", www.upside.com, January 14, 1999.

Ran:1998 Steve Ranger, "Sun Sacks Employees For Modem Security Breaches", Network Week, 03/18/98, CPMnet, TechWeb.

Stu:1998 Michael Stutz, "Wardialer Goes Corporate", InfoSec News, 7 Oct 1998.

Yas:1998 Rutrell Yasin, "Security Breaches Surge Over Past Two Years, FBI Says", Internet Week, 04/08/98, CPMnet, TechWeb, available from the Internet at www.techweb.com/wire/story/TWB19980408S0001

Gregory B. White is the Chief Technology Officer at SecureLogix, Corporation, a computer security firm based in San Antonio, Texas. Prior to accepting this position Greg spent 19 years in the Air Force, most recently assigned as the Deputy Head of the Computer Science Department at the United States Air Force Academy. His other assignments in the Air Force included positions as Branch Chief of the Network Security Branch at the Air Force Cryptologic Support Center and as a Systems Analyst at the Strategic Air Command. Greg received his Ph.D. in Computer Science from Texas A&M University in 1995, his M.S. in Computer Engineering from the Air Force Institute of Technology in 1986, and a B.S. in Computer Science from Brigham Young University in 1980. He is the author of numerous articles and conference presentations on computer security and information warfare and is the co-author of two textbooks on computer security.