Chapter 10

EARLY SYSTEM SECURITY IMPROVEMENTS

INTRODUCTION

Due to the current popularity of international commerce on the Internet, the topic of computer security has moved quickly from being a low priority for enterprises and government agencies to a high priority. This interest has been heightened by computer break-ins at places like Los Alamos National Laboratories and NASA. Admissions by the United States government that many attempted military computer break-ins were successful has only added fuel to the fire. Your computer systems are at risk, but the good news is that you can do something about it [1].

The creators of the Internet never envisioned that it would become the hub of international commerce. They designed the Internet for the open and free exchange of research information between universities and government. They did not design it to be secure and Internet firewalls [4] were an afterthought. Some firewalls are good and others are not. Are proxy firewalls better than filtering firewalls? Nobody really knows and maybe both are necessary depending on the risks involved. However, firewalls may not be enough protection. Secure network routers are coming on line, but they have yet to prove themselves. Potential security problems exist anytime a government or an enterprise computer is connected to the Internet. Furthermore, fragments of previously deleted e-mail and files may linger for years in the heart of a computer's hard disk drive and discarded floppy diskettes. Computer secrets never go away. Many crooks have learned this lesson the hard way. However, things may not be as bad as they appear from a computer security standpoint [1].

Through the implementation of proper computer security policies and strategies, network connections to the Internet can be made more secure and sensitive data can be secured by using file encryption [5]. Also, computer storage media [6] can be effectively cleansed of sensitive information. Knowing the risks up front makes the job much easier for computer users and security policy makers. Firewalls and secure network routers haven't come of age yet and security tied to them may not be adequate protection for trade secrets and sensitive

computer data. However, these technologies have their place and only a fool would connect a computer network to the Internet without some sort of a firewall [1].

Given enough time, desire and resources, it is a safe bet that almost any computer security system can be broken. The only totally secure computer system is one locked in a room, without people and without connections to other computers. Since such a security strategy is impractical, other security strategies and policies must be implemented. Government and enterprise management cannot ignore the Internet just because of potential Internet security problems. The wealth of free information available on the Internet and inexpensive worldwide E-mail access can result in significant cost savings and increased productivity. Don't forget. You do live in the information age. An enterprise cannot remain competitive if it doesn't take advantage of all available technologies [1].

Internet firewalls serve a very good purpose. Much like the perimeter fence at a military base, firewalls act as the first important line of defense. However, they are not the total answer. Encryption should be wisely used to protect sensitive information from unauthorized eyes. It is no secret that foreign competitors of large U S enterprises gainfully employ former Eastern Block intelligence agents. You see, it is more cost effective to steal the secrets of your competition than it is to spend millions of dollars for research and development. Unless good encryption is employed, they can make copies of the computer secrets without leaving any trace or clue that they even compromised such secrets. Lets face it. Most written communications today are created on computers. Most of these computers are not secure and to make matters worse many computers involved are portable notebook computers. File encryption helps here also [1].

An Internet firewall is essentially one or more systems that control access between computer networks. In this regard, the Internet is nothing more than a very large computer network. An installed firewall on a computer network serves two basic purposes: it controls access to the network from outside servers, and it also controls the transfer of information from the network to outside servers. It is not enough to just install an Internet firewall. The type of firewall(s) needed is usually dictated by the needs of the enterprise and the level of risk involved. The most important thing to remember about a firewall is that it creates an access control policy for the enterprise. Executive management and the computer security staff must be involved in defining what the access policy will be prior to purchase and installation. Absent of such planning, the enterprise will set its security policy based on the on the whim of the installer, or worse, the default configuration of the manufacturer. Let's not forget that hackers love default security settings [1].

Once the mysterious focus of spy stories and movies, encryption is really nothing more than the scrambling of data to make it unreadable. There is strong encryption and weak encryption, and an entire chapter could be written on the topic. Most word processing, spreadsheet and database applications that provide encryption as an option, are not secure. In fact, commercial applications exist which can be used to quickly defeat the security afforded by these applications. For the purposes of this chapter, standalone file encryption products will be discussed. To keep things simple, let's just say that the longer the encryption key the stronger the security. This assumes, of course, that a solid encryption algorithm has been employed. Unfortunately there are several algorithms to choose from. With the preceding in