1998

Building a Secure Intranet

Fred J. Berryman
Lindenwood College

BUILDING A SECURE INTRANET

Fred J. Berryman, B.S.

A Culminating Project Presented To The Faculty Of The Graduate School Of Lindenwood College In Partial Fulfillment Of The Requirements For The Degree Of Master Of Business Administration

1998

ABSTRACT

This thesis will explain the vulnerabilities of computers in a networking environment and demonstrate proper procedures for building a secure Intranet.

The Internet is built around the concept of open communication. Data is shared around the globe just as easily as it is from one office or cubical to the next. Corporations are skeptical about putting company data on such a public transport mechanism as the Internet, but the tools used on the Internet are exciting and everyone wants to use them. Out of a desire for the best of both worlds, the Intranet was born.

An Intranet that has no connection to the Internet can safely make a significant amount of company data available to employees, but when hosts are connected to the Internet, things change. Each application on the Internet comes with a threat to a company's data.

More office managers would probably install and use an Intranet if they understood them better and trusted them more. The purpose of this paper is to educate the non-technical manager in the subject of Internet applications and security mechanisms so that he or she can make an informed decision about installing an Intranet.

There is so much software available for building and securing a Web site that many feel overwhelmed at the prospect of getting started. The goal will be to define the terms and acronyms used in this technology, and to evaluate the services and software available for building a secure Intranet.

Securing a Web site requires some knowledge of TCP/IP, routers, firewalls and data encryption. These subjects will be covered at an introductory level with the goal of enabling the reader to understand the issues involved.

The work will terminate in a project that builds an Intranet that shares data with a selective audience while securing it from others. The hardware and software configuration will be documented as a sample that can be duplicated in any office environment. The Web site will be built using some HTML coding to demonstrate the complexity of the language and some high-level software that demonstrates the value of these new tools.

Two security specialists evaluated the project. They agreed that an Intranet built with the specifications in the project would be functional and secure.

BUILDING A SECURE INTRANET

Fred J. Berryman, B.S.

A Culminating Project Presented To The Faculty Of The Graduate School Of Lindenwood College In Partial Fulfillment Of The Requirements For The Degree Of Master Of Business Administration

1998

COMMITTEE IN CHARGE OF CANDIDACY:

Associate Professor Daniel W. Kemper, Chairperson and Advisor

Associate Professor Gareth Gardiner, PHD

Adjunct Professor Ben Kuehnle

Table of Contents

List of Tables iv

List of Figures v

I. Introduction..1

History of the Internet 1

Internet / Intranet Tools 7

Microsoft vs. Netscape 10

Return on Investment 14

Summary & Statement of Purpose 15

II. Literature Review..17

TCP/IP Protocol Stack 17

Domain Name System 22

Security 24

Routers, Gateways and Firewalls 40

Conclusion 42

III. Methods & Evaluation

Materials 43

Subjects...43

Instrument 44

Procedure 45

IV. Results...46

V. Discussion 52

Summary of Evaluator Comments 52

Details of Evaluator Comments 52

Limitations 59

Suggestions for Future Research 60

Predictions for the Future 61

Appendix A – The Project 63

Network Diagram 91

Appendix B - The Questionnaire 92

Appendix C – Cover Letter 102

Works Cited 103

Vita Auctores 108

List of Tables

Table 1 Classes of IP Addresses 18

Table 2 Top Level Domain Names 22

Table 3 Security Areas of Concern 27

Table 4 Encryption Terms Defined 28

List of Figures

Figure 1 Internet Investments 1995-2000 2

Figure 2 Cost Breakdown of Building an Intranet 3

Figure 3 TCP/IP Protocol Stack 20

Figure 4 Fraud Rate 25

Chapter I
INTRODUCTION

History of the Internet

The World Wide Web (WWW) is a collection of data stored on computers that are interconnected by wires, trunks and routers. The Internet is the backbone that allows these inter-connected computers to share information. The data is available to anyone with a computer running the right software and a connection to the Internet. Data is shared via services like chat groups, e-mail, newsgroups, file transfers and the World Wide Web. The Internet is not owned by anyone, therefore, each user is liable for the safety and consequences of sharing his or her own data.

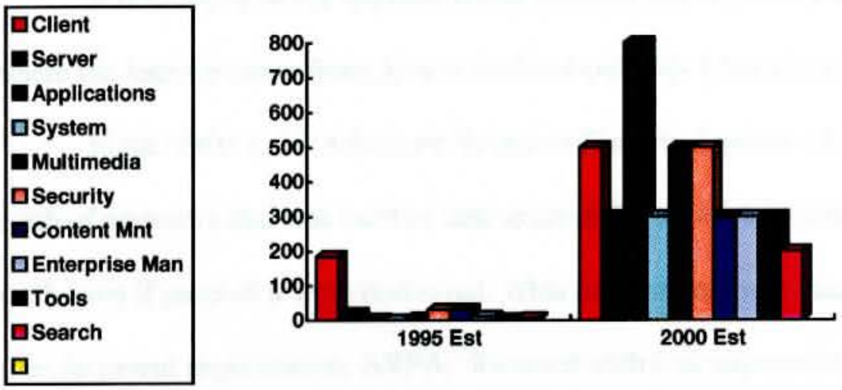
Most countries have backbone networks that are connected via high-speed trunks to other backbone networks in a hierarchical structure. Internet Service Providers (ISP's) have high speed access lines to one or more of the backbones and they sell low speed access via modems and frame relay circuits to individuals who want connectivity.

Ryan Bernard describes the Internet in his book The Corporate Intranet as "a biological organism that is self-replicating, self-sustaining and self-governing" (Bernard 3). The Internet has no governing bodies and its structure has simply evolved over time. There are commercial sites that require users to register and some that charge for access. Anyone who purchases and installs the right hardware and software on his or her computer can also publish information on the Web (3).

In 1994 there were approximately 17,000 Web servers in operation. A year later there were 70,000 for a total expenditure of twenty million dollars for server hardware alone. Aside from servers, there are administrative costs, client software and management costs that go into the Internet each year. Figure I illustrates the breakdown of money spent in 1995 compared to an estimate for the year 2000:

Figure 1

Internet Investments 1995-2000

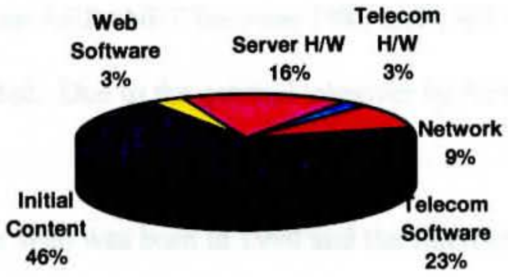


Source: "Spectacular growth for the Internet" ZD Internet Magazine. Dec. 96: 32. Study by Hambrecht & Quist.

Peter Meade, a writer for America's Network, estimates the cost of building an average corporate Web site to be $109,000. Figure 2 illustrates the breakdown of costs for building a single Intranet.

Figure 2

Cost Breakdown of a Corporate Web Site



Source: Meade, Peter. "Spinning a web, It costs more than you think." America's Network. October 15, 1996: 21.

A discussion of the Internet would not be complete without explaining where the Internet came from, how it evolved and why it has grown so rapidly. In the 1960's, the Advanced Research Projects Agency (ARPA) created a mesh of networks that was built so that some of the network would continue to work even if parts of it were destroyed. This first Internet was named ARPANET after its parent organization, ARPA. It started with four supercomputers strategically placed around the United States. The threat of nuclear attack lessened during the 1970's and scientists found themselves with a high-speed network to use as their personal post office. ARPANET decided to allow connections to other networks in 1977. This required a common protocol, which they designed and named Transmission Control Protocol / Internet Protocol (TCP/IP). In 1983 ARPANET broke off and became MILNET, leaving the rest of the world connected on what eventually came to be known as the Internet (Johnson).

The National Science Foundation (NSF) took over all the educational and business connections from ARPANET between 1985 and 1989 at which time ARPANET was disbanded. Due to the gradual takeover by NSF, ARPANET was hardly missed.

The World Wide Web was born in 1990 and the Internet started to double in size every year. Much of the growth was due to Hypertext Transmission Protocol (HTTP) developed by a physics laboratory in Geneva Switzerland commonly referred to as (CERN). HTTP is a means of sending text, pictures, sound, music, voice, animations and video over TCP/IP networks (Johnson).

When the Internet was first created, the tools were rudimentary and difficult to use. Finding information was slow and tedious. Initial Web pages were simple ASCII text documents without graphics. A program known as Gopher was used to serve the first Web pages while Lynx and Veronica were the popular browsers of the day. Archie searched for content in Web pages and WAIS was used to find files of interest in (File Transfer Protocol) FTP sites. Many of these original tools went from notorious to nostalgic in less than four years, but that does not mean they are extinct. Some educational institutions still use text only browsers. Web designers should keep this in mind, and offer text substitutes for graphics. HTML allows for easy substitution, but it is often neglected (Johnson).

Today, search tools like Yahoo and Excite create indexes during off-line searches of graphics rich Web sites. Browsers then search the abbreviated index, which is much faster than looking through every page on the Internet.

The Internet has been around for over a decade, but the Web has only become a household name in the past several years. The popularity of the Internet has spawned a vast amount of software and hardware. Managed internets are beginning to be used by corporations for the same purposes as the public Internet, but in a more controlled environment called an Intranet.

When Internet tools are used to create a common backbone for sharing internal corporate information in a way that is productive and secure, it is called an Intranet. Intranets take advantage of the TCP/IP family of open standards and protocols used on the Internet. These standards make possible not only Web pages, but applications and services like email and database access systems that are as powerful as traditional proprietary systems such as Lotus Notes or Microsoft BackOffice. Because Intranets are built on open standards, users reap the benefits of platform independence and they gain the ability to use the products created by an entire industry, not just a single vendor (Bernard 18).

Many corporations put these tools to work and produce internal Web sites allowing employees instant access to company information. Each department may install its own server to store procedures and other information they wish to share with others, or the company may install one server and let a Web master (the individual with the skills and responsibility for administering the Web server) post data for the individual departments.

Intranets have all the advantages of the Internet such as generic tools that can be used on any platform, low cost of implementation, a fast learning curve and the added advantage of speed. Many Internet users are individuals at home, dialing up on a modem. Downloading large files including graphics, sound and video is slow. Intranet users are often in the office, connected via an Ethernet cable or equivalent at ten megabits per second or faster which means graphics and sound files are quick and stimulating (20).

Transferring large files over modems takes significant time. Since the Internet is often accessed via modems, a display protocol is needed to minimize the size of files. The required protocol is called Hypertext Markup Language (HTML). It uses ASCII code with a few control characters to create files that give the appearance of being created by a much richer instruction set. HTML files are up to 10 times smaller than their Microsoft Word and Frame Maker counterparts. HTML files that include graphics are also smaller because HTML requires the use of the GIF and JPEG formats instead of proprietary PCX, EPS and BMP formats (21).

The Internet created the ability to integrate diverse types of multimedia information on a variety of hardware and software platforms. It has created the ability to create a paper-less office. Because of the Internet, business transactions can be conducted with no human interaction whatsoever. It taught its users to overcome corporate and governmental boundaries and restrictions. According to Bernard, businessmen have learned to share knowledge more efficiently to promote their businesses for financial gain (22).

A closer look at some of the Internet tools will help the reader understand each of their functions.

Internet / Intranet Tools

TCP/IP is the network language used by the Internet and within this protocol are many resource types. The resource used to locate and connect to Web sites is Hypertext Transfer Protocol (HTTP). When Web users surf the Web, they have to tell their browser software where to look. The tool they use to do this is the Uniform Resource Locator (URL). A URL takes the form `"resource://server.host.name/[path]" (e.g., http://www.att.com/index.html).`

HTML as explained earlier is the language used to standardize Web documents. Web documents usually contain titles, headers, some graphics for ascetic appeal and some text. They are stored in logical collections on a host computer and together they make up a Web site. There are standards being developed insuring that a Web page built by one program will be readable by another. Servers sold by companies like Netscape and Microsoft are the tools that allow a computer to post Web pages for others to browse (54).

Web pages can be complex entities. Aside from sounds and pictures, they can provide access to databases that reside on the server. There is a special programming language that acts as a translator between the browser and the database. These translators belong to a family called Application Programmer Interface (API's). One form of an API is a Common Gateway Interface (CGI) which is a script file that takes a request from the browser, translates it into a query and sends it to the database (63).

The two main competitors in the server/browser market are Microsoft and Netscape. Netscape has a web page that compares its products to those produced by Microsoft. Microsoft's Internet Information Servers (IIS) use data link library (DLL) routines to build interfaces to Web forms called Internet Server API's (ISAPI). Netscape uses a similar tool but calls it Network Server API (NSAPI) (Compare).

Another form of API is Java. Originally designed by SUN® Microsystems and now used by many Internet software vendors, Java goes beyond the power of conventional CGI scripts. Java allows graphics rendering, real-time two-way interaction with users, live information updating and instant interaction with servers over the network. JavaScript is an industry-standard Internet object scripting language with a built in API that allows scripting of events, objects and actions within HTML pages. JavaScripts have opened new possibilities for Intranets and they are changing the way people buy software for PC's. Given the proper JavaScript, a corporation could feasibly avoid buying multiple copies of a database program and let their users access data through Web browsers (Netscape.com).

The advantages of Java do not come without cost. Java has security problems that are considered a serious threat to networks that run them according to an informative Web site dedicated to the subject of Java and JavaScript. It has been demonstrated that improperly written scripts open doors to unauthorized access that are hard to protect against (Java).

Hyperlinks are used in HTML documents to allow the reader to jump from one area of a Web page to another or to a new page. A hyperlink can be a special symbol inserted in the document or it can be a section of text that is highlighted so it stands out from the rest of the text. When the user clicks on the hyperlink, he or she is taken to another section of the document or to another document on the network. Special symbols can be inserted that when clicked, take the user back to the point where the hyperlink was selected.

Electronic mail (email) is used for delivering electronic messages and it is much faster than the US Postal Service. Email is handy, but also one of the more dangerous applications on the Internet according to Cheswick & Belovin in Firewalls and Internet Security. For example, Sendmail is a UNIX mail program that runs in the privileged mode called root. It is a large and complex program that gave hackers the ability to break into servers by sending commands imbedded in mail messages. This is a technique known as a Trojan Horse. Sendmail has since been fixed, but there could be sites that are still using the old version (Cheswick 30).

There are many TCP/IP tools that are considered dangerous to Web administrators. Some are UNIX tools that were in use before the Web came into existence and must be guarded against. Telnet for example, is a tool used to access another host on the network. It requires the use of a login and password, but once on the destination machine, the user can execute programs just as though he or she were sitting at the remote keyboard. Telnet is often abused after an unauthorized user breaks into a Web server (Cheswick 31).

File Transfer Protocol (FTP) is an application that is used to transfer files to and from a host. FTP requires users to log-in, but since passwords are not always disguised while traveling on networks, hackers with access to the right equipment such as a Sniffer (computer used to capture data as it traverses networks) can observe and use logins for mischievous deeds (39).

Anonymous FTP is a form of FTP that accepts "anonymous" or "ftp" as the login with no real password required. An email ID is generally expected as a password, but anything will usually do. This is done so anyone can send files or retrieve them from a host. Anonymous FTP can be the Achilles heel of Unix servers if it is not configured properly (Hunt 338).

Microsoft vs. Netscape

An Intranet can be built on one of many hardware and software platforms. Lotus Notes and BackOffice are a couple of proprietary packages that offer a

wide range of services. They may be expensive and the application is restricted to the services provided within the confines of these programs. Many Information Systems (IS) managers are looking at the wide range of software being built on Internet standards which allow them to pick and choose the tools and services they need and want to build their applications. Many managers feel it makes

sense to deploy an Intranet as their platform and adopt the same open standards as the Internet (Netscape.com).

The HTML language is not user friendly, but initial Web masters became experts out of necessity. Today, most sites are built by high level interpreters that convert ASCII text and word processing documents into HTML format. HTML TRANSIT, for instance, will convert word documents written in languages like Microsoft Word and Word Perfect to HTML, plus it creates an index and table of contents at the same time. Many programs are now coming out with a "save-as-html" option, which allows for a document to be created in the word processor or spreadsheet application and saved in HTML format (Netscape.com).

Microsoft Exchange is Bill Gates' Internet server offering along with his browser, Internet Explorer, which he offers free of charge with every copy of Windows 95. Many Information Systems (IS) managers feel Microsoft has tried to force customers to use their full line of products by making certain functions work best when all Microsoft products are used together rather than deploying an open architecture. This marketing philosophy may be costing Microsoft substantial market share at this time and may subject them to anti-trust laws in the future.

Microsoft's main competitor in the Web publishing industry is Netscape who seems to feel that standardization is the key to the success of the Internet. Netscape's promotional material pushes the concept of cross-platform, cross-database design. This means that any browser should be able to access any server and any database (Netscape.com).

Netscape's clients and servers run on all common platforms including Windows 3.1, Windows 95, Macintosh and most versions of Unix. Netscape products support databases from vendors including Computer Associates, Informix, Microsoft, Oracle and Sybase. "This open systems architecture is one reason Netscape has won such an impressive lead in Internet sales to date" (Netscape.com).

In another feasibly one-sided home page, Netscape compares its Suite Spot of server software to Microsoft's BackOffice. If the statements are true, Netscape may be the platform of logical choice. Netscape claims that Microsoft BackOffice barely qualifies as an Internet/Intranet solution due to its proprietary architecture. Netscape claims an open systems design along with being less expensive to create, deploy and maintain. SuiteSpot claims to be a cross-platform, cross-database solution that lets customers leverage all their investments in hardware, operating systems, databases and applications (Compare).

While Netscape claims Java and JavaScript as the standard of the future, Microsoft is promoting its own API, ActiveX. Microsoft refutes Netscape's accusations about marketing schemes, and declares that Active X will be the standard of the future (Langa 11).

Netscape not only claims to have built its tools with open systems and integration in mind, it has gone one step further by conducting a melting pot for application software built on these tools. Netscape's Application Foundry is an Internet based collection of business applications that are available to enterprise developers at no charge. Netscape wants developers to use their products like Java, Java Script and Live Connect. They openly invite developers to join in creating business applications, which use their products and place them in the Foundry for all to use (Suitspot).

Intranet software is being developed and improved everyday. Security issues are being dealt with in a progressive manner, and the tools are reasonably inexpensive, so there is little reason to put off building an Intranet. There is no limit to the uses and applications. A few examples of how corporations are using Intranets should demonstrate the potential of this technology.

John Deere uses a Netscape-based Intranet to improve its operation according to a testimonial by Phyllis Michaelides, head of the Methods Architecture and Data Team at John Deere. They use the Intranet to access an on-line catalog of equipment that integrates data from multiple sources and allows company-wide access to results from remote test sites. It provides technical documentation to employees all over the world and it offers a visual front-end to a parts database. The Intranet has extended the useful life period of otherwise obsolete PCs. John Deere believes that while useless for many applications, 486 PC's have enough power to run Web browsers to access the Intranet. The company chose Netscape client and server technology because it is available on most major platforms and John Deere has a variety of systems. Netscape Commerce Server provides security features that John Deere believes meets or exceeds its security requirements (Michaelides).

At another Netscape Customer Profile site, a representative of AT&T, Rich Brandwein, discusses how AT&T utilizes Netscape products to solve some of its communications needs. AT&T has created a system that integrates disparate billing systems from various AT&T business units along with an interface to library services, internal research and external news feeds. They also use it for ordering office supplies. It hosts an employee-contact database of over 300,000 employees. AT&T chose Netscape Server for many reasons, but security is the common thread (Brandwein).

AT&T chose Netscape Communications Server because they considered it to be cost-effective, stable and easy to administer. They chose Netscape Commerce Server partially because of its security features. Netscape Proxy Server is used due to its performance and its compatibility with AT&T's firewall structure. The proxy server sits between the firewall routers and the Internet to deter unauthorized access to the applications running inside (Brandwein).

Intranets, like any other new venture, cost money and since they don't usually produce an income flow, many IS managers want to know if the cost is justified in building an Intranet for their organization.

Return on Investment

Ian Campbell is the Director of Collaborative and Intranet Computing at International Data Corporation. Campbell has researched the return on investment (ROI) for corporations that deploy Intranets and published his findings on the Web. Two companies surveyed were Cadence Design and Silicon Graphics Inc. They both reported ROI's of over 1000% and the payback period was measured in weeks, not years. ROI on a project can be measured in increased sales, labor costs or one of a dozen other areas. Based on these two examples, a well managed Intranet environment is a project that should not be overlooked (Campbell).

Campbell was scientific in his research, defining costs for hardware, software and personnel. Personnel costs were broken down into initial development costs and ongoing training. Development cost was high, but training new employees and getting them up to speed with an Intranet actually saved the companies money. Substantial savings were seen in the reduction of paper products, and initiatives such as ISO 9000 were drastically improved (Campbell).

Summary and Statement of Purpose

The Internet has opened the doors for communication on a global scale. It is built on standards that are being honored by software developers. Aside from minor differences, all browsers can display Web pages written in any programming language. Using the Internet is less expensive than using proprietary networks and it is far less restrictive.

The security of data sent over the Internet is the only issue remaining to be solved. Many companies have accepted the risks and are currently sending confidential data and financial documents over the Internet. Others have gone part way by developing Intranets within their firewalls, but still refuse to open the gates to the outside world.

Some feel that Cryptology is advanced enough to secure their data while others are still waiting for something better. Some individuals who read the headlines about hackers braking into the Social Security system probably think the Internet will never be safe. Others feel technology is ready and that a combination of Cryptology and firewall administration can guarantee safe transmission of their data.

The reason for this study is to learn more about Web design and the security mechanisms that are available for securing Web sites. The claims made by Netscape and Microsoft will be compared by employing and evaluating some of each manufactures' products. The knowledge gained will be used in building an Intranet using a wide variety of software including some raw HTML coding and some Web design software that writes the HTML code behind the scene. The reader should obtain a clear understanding of the security issues involved, and gain insight as to what can be done toward putting his or her data online based on in-house programming skills and his or her budget.

Chapter II
LITERATURE REVIEW

TCP/IP Protocol Stack

The language used to communicate over the Internet is TCP/IP. Every piece of information transmitted is placed inside an IP packet. The most important pieces of information in the IP packet are the origination and destination addresses. The routers need the destination address to deliver a packet to the desired recipient and the origination address is required if the recipient is expected to answer.

IP addresses are used for navigating TCP/IP packets through the Internet. An IP address is a 32-bit integer, most often expressed as four decimal bytes (or octets) separated by a period ('.') delimiter as follows: 192.23.4.1 which is called dotted decimal notation. IP addresses may also be seen represented in hexadecimal and binary formats.

In order to satisfy a variety of needs, IP addresses are broken down into classes. Classes are used to assign organizations the smallest number of addresses possible to satisfy their needs based on the number of hosts on each network. Classes can be further sub-divided by the use of sub-nets, which will be explained briefly below. The IP address range is a finite number, which means there is a limited number of available addresses. The original designers of the IP protocol did not anticipate the rapid growth of the Internet and thought a 32-bit address would be sufficient, but they were wrong. Work is in progress to increase the number of bits used in the IP address scheme (Washburn 51).

There are only 128 class "A" addresses available, but each class A network can have over 16,000,000 hosts. There are 16,128 class "B" addresses with 65,536 hosts, and 2,097,152 class C addresses with 256 hosts in each network.

The first three bits of the address indicates whether it is a Class A, B or C address. If the first bit of the address is a "0", it is a Class A address, if the first two bits are "10", the address is a Class B and if the first three bits are "110", the address is a Class C. The chart below shows the address classes represented in binary and decimal.

Table 1

Classes of IP Addresses

FIRST BYTE DECIMAL	FIRST BYTE BINARY	CLASS	# OF NETS	# OF HOSTS
001-126	0111 1110	A	128	16,777,216
128-191	1000 0000	B	16,128	65,536
192-223	1100 0010	C	2,097,152	256

Source: TCP/IP Running a Successful Network. Wahsburn, K. and Evans, J.T. Workingham

Some addresses are special and not included as standard class addresses. The address ranges beginning with 127 and 224 are used for testing and 0 is never used (Washburn 60).

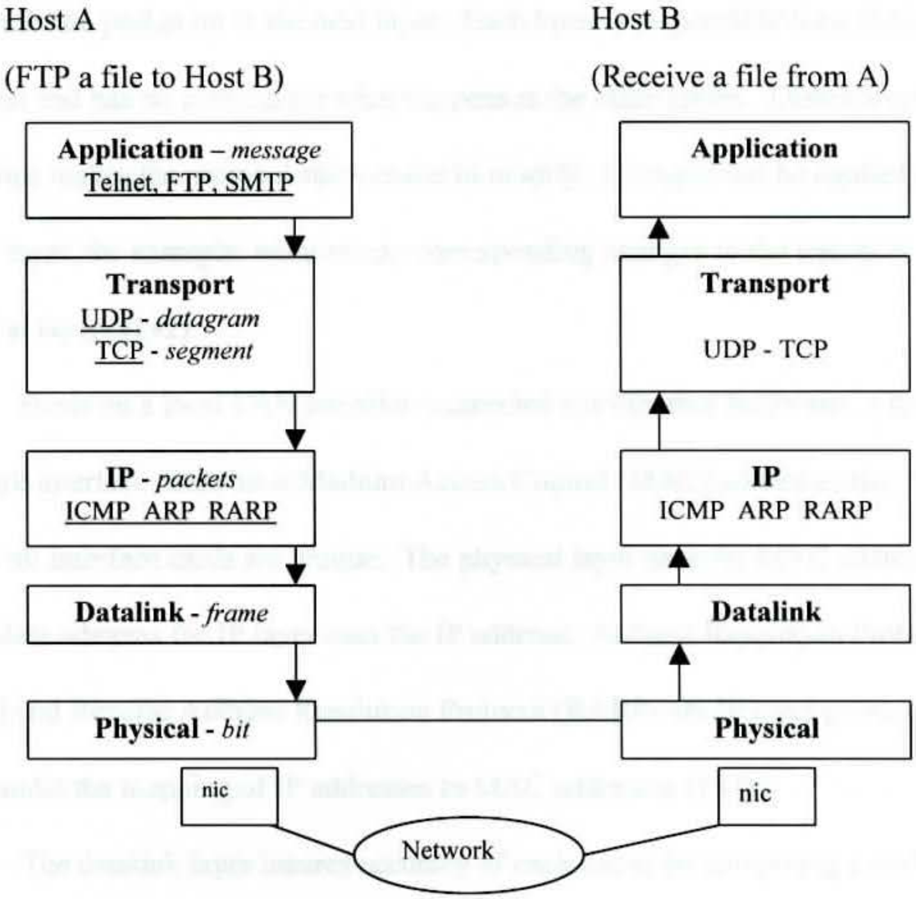
IP networks are often further divided into sub-networks to localize IP broadcast traffic and improve network performance, reliability and security. A sub-net mask is a 32-bit integer that is used to change the function of the host and network bits. The sub-net mask is applied to an IP address using a logical 'AND' function where a '1' 'Logically Anded' to a '1' equates to '1', a '1' Anded with a '0' equates to '0', and a '0' Anded with a '0' equates to '0'.

While this discussion may seem tedious, the Web Master who has to configure the firewalls and routers must be able to relate to binary, octal and hex IP addresses as well as he relates to dollars and cents.

The following discussion of the TCP/IP protocol stack illustrated in Figure 3 is only an introduction to a topic that must also become second nature to the Web Master and firewall administrator.

Figure 3

TCP/IP Protocol Stack



Source: TCP/IP Running a Successful Network. Wahsburn, K. and Evans, J.T. Workingham, pp.141.

The TCP/IP protocol stack contains five layers. The layer names in the diagram are in bold letters. The information in Italics is the data format used at each layer. The underlined data is the service provided at each layer (141).

The example in Figure 3 uses the FTP service to send a file from host A to host B. For outbound messages, each layer interprets the data it receives from the layer above it, adds information in a header of its own, and then sends the entire envelop to the next layer. For incoming messages, each layer reads the header to determine what it must do with the data inside the envelop, strips off that header and sends the packet on to the next layer. Each layer is responsible for a distinct function and has no concern for what happens at the other layers. Distribution of functions makes the protocol stack easier to modify. Changes can be applied to the IP layer, for example, without any corresponding changes to the transport or physical layers (142).

Hosts on a local LAN are often connected via Ethernet hardware. Ethernet network interface cards have Medium Access Control (MAC) addresses that insure all interface cards are unique. The physical layer uses the MAC address to route data whereas the IP layer uses the IP address. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) are IP layer protocols that handle the mapping of IP addresses to MAC addresses (152).

The datalink layer insures accuracy of each frame by computing a cyclic redundancy check code (CRC), which it places in the datalink frame. The receiving node calculates its own CRC and compares it to the one accompanying the data. If the two CRC codes do not match, the data must be retransmitted.

Each physical medium has its own method of controlling the flow of data. Ethernet connections, for example, are controlled by a protocol named **C**arrier **S**ense, **M**ultiple **A**ccess, and **C**ollision **D**etection (CSMACD). The network interface card or NIC, listens for call requests (carrier sense) on the network. If two hosts request to transmit at the same time (collision detection) the NIC commands both hosts to wait a random amount of time before trying again. All stations on the network see the data at the same time (multi-access) (154).

TCP and UDP are the two main protocols in the transport layer. Transmission Control Protocol (TCP) is a connection-oriented protocol that guarantees safe and concise delivery of messages over unreliable circuits. User Datagram Protocol (UDP) is a lightweight connectionless protocol in comparison. UDP is used for traffic that does not warrant the overhead involved with TCP (Washburn 142)

Applications consist of File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Network News Transport Protocol (NNTP), Hypertext Transfer Protocol (HTTP) and a growing list of others. Understanding the functions of each of the layers is necessary when studying the operation of Cryptology and firewall functions discussed later (Hughes 24).

Computers are designed to handle low-level structures like IP addresses and protocol stacks, but humans need constructs that are easily remembered like names and acronyms. Browsers are the interface to Web pages, and they are designed to contact Web sites via IP addresses. A tool used to translate IP addresses to a more human friendly format is the Domain Name System.

Domain Name System

The Internet would not likely have grown as fast as it has if users had to remember IP addresses of every site they visit. TCP/IP allows for workstations to be assigned meaningful names as opposed to more cumbersome IP addresses by using the Domain Naming System.

Domain names are built in a hierarchical fashion and the top-level domain must be one of the acronyms listed in Table 2. A period ('.') delimiter is used to separate the partitions or labels that make up domain names.

Table 2

Top Level Domain Names

Domain Name	Meaning
• COM	Commercial organizations
• EDU	Educational institutions
• GOV	Government institutions
• MIL	Military Groups
• NET	Major network support centers
• ORG	Organizations other than those above
• INT	International organizations

Source: TCP/IP Running a Successful Network. Wahsburn, K. and Evans, J.T. Workingham, England: Addison-Wesley, 1993. pp.319

The name-server software is the mechanism that performs the mapping and conversion process. The name server that has responsibility for a particular sub-domain is said to have authority over that domain. Client domain name software is called the name resolver. When a name sever receives a query from a client, it checks to see if the name is in the sub-domain for which it has authority.

If the name server has authority, it converts the domain name to an IP address, appends an answer to the query, and sends it back to the client (Washburn 323).

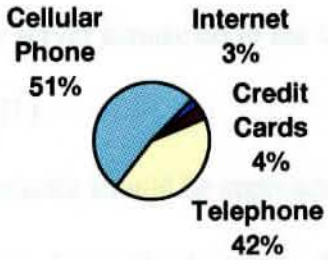
Security

Web servers must be protected from hackers. The measure of protection varies from system to system and from user to user. Cheswick and Bellovin humorously define a secure computer as "one that has no connections to the outside world, has a lock on the keyboard and the computer itself is locked inside a steel vault with a guard at the door." This sounds like overkill, but some IS managers tend to treat security this way. The fact is, some systems need not be secured at all, and no system is useful if it is secured to the level described above. (Cheswick XI).

Hackers work in two realms, they steal credit card numbers and they corrupt data on servers and hosts that don't belong to them. The cost of data destruction is hard to measure and statistics are not readily available. Internet credit and phone card theft is easier to measure and statistics are readily available, but often overstated. Keizer tries to put this form of Internet fraud in perspective in his article "Online Money Matters". Keizer suggests using a credit card on the Internet is less risky than using it at a department store. He compares Internet fraud to using a credit card, a telephone calling card and a cellular phone in dollars stolen per one thousand dollars spent. Figure 4 converts these numbers to percent of fraud by type.

Figure 4

Fraud Rate



SOURCE: Computer Life Magazine "Online Money Matters" by Gregg Keizer 49.

These figures suggest a relative safety compared to other forms of financial transaction fraud, but as mentioned above, they do not cover data corruption.

Cheswick explains how hackers get into systems and what they often do once inside. A decade ago, hackers broke into computers to steal valuable processing time. They would typically run programs that were available on the victim's host computer then exit without a trace. Computer time is relatively inexpensive now, so hackers usually have more criminal and destructive things in mind than merely borrowing computer cycles (Cheswick 3).

inexpensive now, so hackers usually have more criminal and destructive things in mind than merely borrowing computer cycles (Cheswick 3).

Sometimes the first machine broken into is merely a tool to get to other machines attached to it via tools that may or may not require passwords. IS managers often mistakenly neglect this threat and base their security policy on the information contained on the server connected to the Internet instead of all the machines on their network (11).

Cheswick believes security should be approached in three steps. First, define the data to be protected. Secondly, determine the access methods hackers might use to gain access to it. Finally, implement a system that protects against such break-ins. For the teenage hacker with a modem, a good password system might do. For intelligence agencies with high tech tools, wire tapping and monitoring of spurious electronic emissions must be guarded against (6).

John Fontana makes a valid point in his article "Pragmatic Plan Eases Security Fears". He says an overload of information and the fear of unknown security problems are two strong factors that weaken network administrators' attempts to build a secure Internet presence. But proper planning can overcome those problems, said Jay Batson, vice president of engineering at ON Technology Corp., Cambridge, Mass. Batson says, "Your plan should include what you can do, not what you should do". The result of a pragmatic approach to security according to Batson is "a system designed to balance between business opportunity and business exposure" (Fontana).

Trusted Information Systems (TIS) is a company that designs firewalls and other computer security systems. TIS has an extremely informative Web site where they share knowledge about Internet security. David Dalva, TIS Web Master, believes the two major security problems are those caused by browsers and those caused by servers. Internet users browse through Web sites looking for information to help them do their jobs, plan a vacation or just for fun. Files downloaded from the Internet are usually innocent printer drivers, pictures or games, but they are often times Trojan Horses in the form of URL's designed to bypass the security mechanisms of firewalls and cause damaging code to be run on the client. URL's support many communication protocols, and hackers have found ways to use them for gaining illegal access to systems (Dalva).

The HTTP protocol allows clients to read data from and write data to servers. The write capability can be used for unauthorized modification of data. So even if Web hosting is the only service being offered, there are risks to the files on the local network that must be considered. Securing a Web site is a multi-faceted project. The first thing that comes to mind is the security of sensitive data like credit card numbers and employee record data. Like any valuable asset, there are many possible avenues for corruption and theft. Locking the computer in a guarded room with a lock on the keyboard might secure the server itself, but when the cables are connected and strangers suddenly have access to files and data that was once secured in personnel files, other precautions must be taken. Table 3 illustrates four general areas of concern.

Table 3

Security Areas of Concern

- *Access* can be restricted by user or by IP address. Routers perform access control at the IP level. Servers and proxies perform access control when it is based on logins and passwords.
- *Authentication* is the act of proving who or what something is. Often times, it is only significant that the client knows the server is authentic. At other times, it is important that the server knows the client is who he says he is.
- *Confidentiality* is important for web applications that involve sensitive data. Data exported by web clients or servers may need to be protected from eavesdroppers. Data encryption can insure the needed confidentiality.
- *Integrity* of data is the assurance that what was sent is what is received. In some cases cleartext passwords provide sufficient protection, in other cases they must be encrypted so hackers cannot intercept them.

Source: http://www.tis.com/docs/research/papers/wwwarticle.html
Dalva, David. Trusted Information Systems Web Site.

Internet software can be run on any type of computer and operating system. Some have asked if running an Internet server is safer on one machine than another. The answer is yes, according to MIT in an article found on the web and maintained by Thomas Boutell. According to Boutell, UNIX systems are known for their power and flexibility, but this power comes with a price. For every service offered there is a portal for entry by hackers. Some feel the Windows operating systems are easier to administer, which means fewer mistakes and possibly fewer portals. On the other hand, most UNIX administrators believe that a UNIX system properly administered is more secure than a Windows system set up by a novice (Boutell).

CGI scripts are programming tools that enable web pages to extract data from databases. While useful, CGI scripts are a major avenue for hackers. CGI scripts must be written with extreme care. Boutell says "Untrained programmers write faulty scripts and trusting Web administrators install them at their sites without realizing their dangers" (Boutell).

The potential dangers listed above are enough to keep some potential Internet users offline. According to Larry Hughes, most of the threats can be minimized if the proper tools and configurations are used. Many security tools involve data encryption. Table 4 defines some of the terms used in the study of data encryption.

Table 4

Encryption Terms Defined

- Cleartext – Text written without scrambling the characters.
- Encryption - The scrambling of data so it is incomprehensible by humans.
- Ciphertext – Data that has been encrypted.
- Decryption – Algorithm used to unscramble encrypted data.
- Cryptology The study of secret encoded communications.
- Cryptosystem – A system of encrypting and decrypting data.

Source: Actually Useful Internet Security Techniques. Hughes, Larry. pp. 43

There are many varieties of cryptosystems. Some are simple and easy to crack. Others are complex and require many compute cycles to generate, but they are harder to crack. Each system has its place depending on the need for more or less security (Hughes 50).

Digital signatures are one example of the use of data encryption. Digital Signatures on electronic messages serve the same purpose as hand written signatures on letters. They attempt to verify the authenticity of the sender. Hughes describes digital signatures as mathematically calculated attachments that verify the sender's authenticity and the integrity of the data (Hughes 43).

Each of the cryptosystems discussed below uses a key to lock and unlock data. The strength of a key is relative to the amount of time required to decode it. The number of bits used to calculate a key is called its keyspace. Codes using twenty five bits can be broken with pen and paper in minutes, forty bit keys have been broken by computers in a matter of hours and fifty-six bit keys can be broken but with a great deal of computer power. There are keys available that use 128 bits that are virtually unbreakable, but there are government restrictions that regulate where they can be used (Hughes 46).

There are two basic types of key systems, secret and public. Secret key systems are so named because the key used to encrypt messages is the same key used to decrypt them. Both parties must know the key and it must be kept secret. Secret systems are symmetric since the keys must be synchronized between sender and receiver (47).

Public key systems are asymmetric. User A has a secret key and a public key and they are not synchronized in any way. User A tells anyone that needs to communicate with him the public key. Any messages signed with the public key are only readable by the holder of the private key (user A). This eliminates the need for synchronization or sharing the secret key with anyone (48).

Keys must be authenticated before they can serve their intended purpose. In the beginning, secret keys were passed between two parties in cleartext, which left room for theft and modification of the key. Newer systems protect the transfer of the keys. Centralized trust is used when certificate authorities (CA) hold the keys. The CA verifies the authenticity of each participant and applies his digital signature as a seal of authenticity. The Internet Policy Registration Authority (IRPA) is the top level of a hierarchical tree of CA's. Applications are available that apply a decentralized trust approach in which a user trusts a friend's signature who trusts someone else's signature creating a web of trust without a central agency (49).

According to Hughes, the strength of any key system is measured by its ability to keep the keys secret, the absence of loopholes in the key technology, and the ability to resist a brute force attack on the key. In theory, any key can be broken given enough computing power and enough time. The following is a brief explanation of some popular encryption mechanisms.

There is an old technique called the "One Time Pad" which was invented by AT&T for use on telegraph messages and later used by the Germans in battle situations. The sender and receiver each had a pad of keys. The key on the top of the pad was used for the next transmission, then it was discarded. The computer generated One Time Pad algorithm applies a logical exclusive or (XOR) function on the data and the key. The resulting ciphertext can be deciphered by performing the XOR function again. The key must be completely random and each key may only be used once in order to be secure. The key must be kept secret until it is used, then it may be discarded (52).

Encryption software is complex computer coding that will not be discussed in detail, but some differences between types of encryption systems is useful. Hughes explains that encryption is performed on a bit, a byte (8 bits), or a block of bytes at a time. Stream ciphers act on each bit or byte as they are received while block ciphers wait until a block of data is available. Block ciphers are the most common and they come in 4 flavors; the electronic code book (ECB), cipher block chaining (CBC), cipher feedback (CFB) and output feedback (OFB). These techniques are listed in order of strength (54).

Encrypting large data files with some of the aforementioned cryptosystems can take a long time due to the mathematical calculations involved. A faster technique is to create a code called a hash value from the cleartext and encrypt only the much smaller hash value. Ron Rivest of RSA Data Security Systems created one of the first versions of hash technology. Rivest called his programs Message Digest versions MD2, MD4 and MD5 (55).

MD2 was first used to secure electronic mail by applying it to Privacy Enhanced Mail (PEM). Running data through the algorithm twice, results in 2-

times the security, so Rivest calls this technique MD4. MD5 was written to correct weaknesses in MD4 (55).

Hash and encryption constructs have been used to develop a variety of cryptosystems, the most popular, Data Encryption Standard (DES), was created by The National Institute of Standards and Technology (NIST) in the 1970's, and is still considered a secure model today. DES can use any of the four block cipher modes ECB, CBC, CFB and OFB discussed earlier. It uses a fifty-six-bit key and encrypts data in sixty-four-bit blocks. It was designed to run on a hardware chip that does most of the work. DES, however, has undergone some criticism due to the relatively short fifty-six-bit keyspace. There have been some enhancements to DES over the years; the new model is called Triple DES (TDES).

Hughes mentioned a couple of varieties of TDES. One variety uses two keys and runs the data through the algorithm twice, much like MD4 did for MD2. This produces a keyspace of 112 bits. The other variant of TDES uses three keys for a total keyspace of 168 bits (Hughes 57).

The European cryptologists Xuejia Lai and James L. Massey invented IDEA, another sixty-four-bit block encryption routine that has a 128-bit keyspace that emulates the functions of the DES hardware. It is believed by some to be more secure than DES without the hardware restriction (58).

Ron Rivest later created RC2 and RC4 to replace DES. The block routine runs at about the same speed as DES, without the required hardware, and the stream cipher model RC4 runs many times faster than DES according to Hughes.

The encryption algorithms discussed so far have been based on secret keys, which leaves them vulnerable to hackers (59).

The Diffie-Hellman algorithm solves this problem by providing a mechanism to secure key exchanges over public networks. The designers accomplish this by enabling both sides of the exchange to derive a key without passing any secret information. User A generates two public numbers up to 150 bits long and sends them to user B. Both users generate a secret number, which they keep to themselves. Both users run the public numbers along with their secret numbers through the Diffie-Hellman algorithm, which produces the key for all further transmissions between them.

One of the first alterations of the Diffie-Hellman algorithm is RSA which is an acronym derived from the names of its creators Ron Rivest, Adi Shamir and Leonard Adleman. The result is a program that generates key pairs that are impossible to decode according to Hughes. Sender A no longer has to generate the large numbers for the algorithm, RSA does it for him. RSA is strong, but it requires too many compute cycles to be used for every application where encryption is needed. It is currently being used in conjunction with other algorithms such as TDES to derive an extremely secure yet timely application according to Hughes. It is also used for creating secure digital signatures by applying RSA to the hash of the message. The receiver decrypts the signature using the sender's public key (61).

The US Government would like to control hard encryption technology and the storage of encryption keys in the interest of national Security. The NIST has one solution to the problem. Their answer was a software package called SkipJack, which was a potential replacement for DES. There is a microchip made for commercial use that runs the SkipJack algorithm. The clipper chip is supposedly secure from attacks of all kinds, but it has hidden inside, a threat of its own according to Hughes. Since clipper communicates symmetrically, it must have a secret number to work with Diffie-Hellman to produce the secret key. Each connection between two clipper chips is a session. One secret key is used for the entire session, so if a hacker learns the key, he can intercept and manipulate the entire session. Keeping these keys secret (key escrow) is the major issue concerning clipper chips.

Solutions being offered include variations of key escrow that moves control of the keys out of the government's hands, but many businesses refuse to accept the concept at all. Net Guide Magazine featured a debate over key escrow in an article called "The Encryption Debate" by Kate Gerwig. Gerwig explained that White House administration has been trying to shove the key escrow down the Internet's throat since it came out with the Clipper Chip proposal, which required registering access keys with the government. This idea did not go over, so the government has since suggested registering keys with non-governmental agencies as long as law enforcement agencies can gain access in emergencies.

Gerwig feels that putting key escrow in the hands of the government can be as damaging to the needs of individuals as not having them is to law enforcement agencies. TIS has developed a Commercial Key Escrow that they feel is secure. Others maintain that if the government can get to the keys, so can hackers (Gerwig 98).

Software providers are working hard to get around the key escrow issue. Banks want to put applications on-line, but not until they trust Internet software to the point they are willing to guarantee transactions. On Jan 8, 1997, PC Week featured an article "Encryption Technology SET for Final Testing". IBM, MasterCard and RSA have announced an application for sending secure transactions over the Internet using a program called Secure Electronic Transactions (SET) which they claim "provides the added measure of security many users have been waiting for" (Moeller 1).

SET is a protocol being promoted as an absolutely safe way to send financial data over the Internet. SET uses digital certificates to verify purchases on the Internet. It is an online credit card verification system. Keizer says "SET insures integrity all the way to the bank" (Keizer 46).

Netscape has also attempted to escape governmental control. Netscape's Certificate Server is a new class of software that enables organizations to issue, sign and manage public-key certificates using Secure Sockets Layer (SSL) for secure, private communication over the Internet.

Companies like HP, RSA and Netscape are all working within the law to utilize available encryption technology, trying to stay one step ahead of the hackers. Given this short lesson in Cryptology, the applications available for securing Internet services can now be evaluated.

PEM or Privacy Enhanced Mail for example uses digital signatures to insure confidentiality, originator authentication and message integrity. According to Hughes, "PEM is a standard, not a program". It can be applied to mail messages or files being delivered by other programs such as Sendmail in UNIX. PEM comes in 3 flavors, MIC-CLEAR, MIC-ONLY and ENCRYPTED (Hughes 147).

MIC-CLEAR offers originator authentication by attaching an encrypted digital signature to a plain text message. It is often used in mailing lists where originator authenticity is assured.

MIC-ONLY messages are specially coded in a universally accepted format so they can be read by routers and firewalls but not easily read by humans. This provides a slightly higher level of security.

ENCRYPTED PEM messages are not readable by man or machine. The signature is outside the message but inside the PEM envelope. Since RSA is too complex to run on large messages, PEM uses MD2 or MD5 to hash the message, then sends the hash value of the message to RSA for generation and hard encryption of the signature (148).

Whether a user registers with a public CA or not, he can use the PEM technology and sign his own certificates by deploying a program called RIPEM. RIPEM is available for free download at `ftp://ripem.ssu.edu`. The user can digitally sign cleartext messages and encrypt messages that are more sensitive. Once a user knows other RIPEM users and their public keys, he can send secured messages across the Internet without fear (151).

RIPEM is probably a great product for the price (free), yet widespread use has not occurred. Pretty Good Privacy (PGP) on the other hand has received much popularity. Its creator, Philip Zimmermann stands accused of distributing illegal encryption software outside the US and of pirating some of his technology from RSA, but his program is still used by many security conscious administrators (156).

PGP uses some of the same techniques as RIPEM but it goes a few steps farther according to Hughes. It uses IDEA instead of DES. It generates the hash, encrypts the signature and embeds it inside the ciphertext instead of leaving it outside the message. This way, only the recipient can see the signature. Zimmermann compacts the entire message with the ZIP utility before the encryption process which makes it run twice as fast, then he breaks the messages up into chunks and sequences the blocks which makes for easy congestion at the other end (158).

Hughes describes the Internet as "a non-application specific mail super-highway". It sends IP packets from city to city and it cares not about the hardware or software running on the other end. Since e-mail is one of the most highly used applications running on this highway, a standard for e-mail was produced to ensure all mail programs send their packages in a format that can be interpreted by the recipients. The Multipurpose Internet Mail Extension (MIME) specification defines exactly how mail is addressed. It allows for multi-part messages. Binary sound and video files can be sent so that the recipient can interpret them as long as he has the required readers and viewers running on his computer (167).

HyperText Transfer Protocol (HTTP), like e-mail has its own security issues. In its original form, HTTP had little to offer in the way of security. Subsequent protocols like SHTTP and SSL have enhanced web page delivery to include secure transmission over the Internet according to Hughes (271).

Secure Hyper Text Transfer Protocol (SHTTP) was developed by Integrated Technologies Corporation (EIT) to be completely compatible with HTTP, but it offers encryption of web pages and the ability to digitally sign or authenticate each page much like PEM and PGP do for e-mail. There is an extensive amount of negotiation that must take place between server and client before transmission commences. They negotiate security protocols for traffic in both directions. They might decide it is acceptable for the browser to download a plain text page, but any data sent back to the server must be encrypted or signed. The negotiation is prompted when a browser requests a URL that begins with "shttp://" (269).

Secure Sockets Layer (SSL) is Netscape's protocol that encrypts and secures data from server to client. When the client is connected to an SSL secured host, it will display a symbol to indicate security. In the Netscape browser, it is a picture of a full key if it is safe to transmit data and a broken key if it is not safe. In Microsoft's Explorer, which also uses Netscape's SSL technology, the picture for safety is a closed padlock. Alerts concerning the safety of sensitive data are configurable in the browser (271).

EIT's SHTTP mentioned earlier, is an extension of HTTP, whereas Netscape's SSL is basically an extra layer that handles the encryption of HTTP documents and it runs between the TCP layer and the application layer. This way, application programmers need not concern themselves with security according to Hughes. When an SSL compliant browser sends a request to an SSL equipped server, the handshake protocol determines which encryption methods to run in which direction. SSL uses a new form of key called a session key. The key is used for the entire connection or session, not for each message or file transferred (272).

Routers, Gateways and Firewalls

A major link in the Internet chain is the router. Routers control the delivery of IP packets from one local network to another. Simple Network Management Protocol (SNMP) allows remote administration and monitoring of routers. SNMP uses a small instruction set. It uses "get" and "set" commands to transfer information from and to the Management Information Databases (MIB) in the router. The MIB stores management and configuration data for the operation of the router. SNMP can use UDP or TCP for its transport layer. SNMP version 1 uses clear text passwords for authentication, and while version 2 allows for strong authentication, it is not yet widely deployed (Amoroso 102).

Some routers perform checks on traffic and make decisions to pass or drop packets based on access-lists configured by the administrator. When used in this fashion, routers are called packet filters or firewalls.

Ed Bott explains the difference between packet filters and application gateways in his article "Secure Firewalls". Bott says packet filters are hardware devices that sit between a user's network and his Internet Service Provider's router. It can be a router or a computer running router software. Packet filters can look at the origination or destination address or the packet type. They can therefore filter out certain web sites, or specific users on the network. They can also allow TCP packets while denying UDP packets (368).

Application gateways filter out specific services such as HTTP, FTP, Telnet or Internet News. Gateways can therefore stop employees from accessing Playboy's homepage or downloading files from FTP sites that may contain viruses. A combination of packet-level filters and application gateways can isolate a network and keep employees on track while protecting company information all at the same time (368).

Proxies may be used in firewall environments to enable hosts on protected networks to use the web. Proxies sit between the protected networks and the Internet and relay requests between both sides of the firewall, a function called proxy mediation. According to Dalva, this technology can solve some of the security issues involved with connecting to the Internet (Dalva).

Installing a proxy server has its own security problems according to Dalva. Since the proxy server sits outside the protection of the firewall, it must use mediation to authenticate and provide access control to the services that it provides.

Dalva says the proxy should be able to check protocols for ill-formed commands. Proxies can also look for data constructs and detect programming languages that are known hacker tools like PostScript. If the proxy prevents this data format from entering the client, it eliminates the threat. Code analysis is an approach to mitigating some of the security issues by analyzing the software ran on files downloaded from the web. Code analysis is a complex and time-consuming task according to Dalva (Dalva).

Conclusion

The tools defined in this chapter are used in a variety of applications found in corporate Intranets today. The reader should not be overwhelmed by all the possible solutions to securing an Intranet, but rather comforted by the amount of work that has gone into the subject. Engineers and programmers are trying to stay a step ahead of the criminals that would love to gain access to confidential data.

The project description and guide to follow will use much of the technology described in the first two chapters. The project will explain how to administer and use a variety of Web servers and browsers. It will demonstrate the use of HTML authoring and conversion tools. Some fundamental firewall configuration will be explained. The design and maintenance of a Web site will be discussed along with the political and budget issues that are sure to arise in almost all Web projects. It is a guide that will give the reader an idea of the simplicity or complexity (depending on the reader's perspective) involved in setting up a secure Web site.

Chapter Three
Methods and Evaluation

Materials

This research culminates in a project to construct a secure Intranet for the dissemination of inter-departmental data and procedures. The environment will consist of two Web servers protected from other environments by a SunScreen SPF-100 Firewall. The work will be performed inside an existing Intranet environment, so it will be an Intranet inside an Intranet. The Firewall configuration will be built on a live machine, but it cannot be activated, as this would disrupt the operation of the site. The configuration will be analyzed on paper only.

The plan (Appendix A) will include a diagram of the configuration, a security policy, Firewall configuration instructions, Web Server administration instructions, HTML conversion techniques, and Web publishing procedures. The goal of the plan is to document the actual work that goes into building the site so the reader learns from the mistakes and the accomplishments of the project.

Subjects

Dennis O'Brien is head of AT&T Network Security for Operations and Engineering (NSOE). O'Brien has 28 years experience in his current position as a network security specialist. He has written some of the security tools used by AT&T and discussed in this project.

O'Brien has two degrees; AAS in Electrical technology and AOS in electrical technology, both from Rockland Community College at Suffern, NY.

The FBI, Secret Service, USAF Office of Special Investigations and the NY State Police learn from his experience as he teaches for the International Association of Computer Investigative Specialists and he is a guest lecturer at many conference and professional association meetings. He has taught computer intrusion detection and other computer espionage subjects to the Federal Law Enforcement Training Center (FLETC) Instructors.

Bob Perrey is Manager of Information Security at MasterCard International. With over twenty years of experience with hardware, software and computer networks, Bob is responsible for the security of MasterCard's world-wide network systems. Perrey graduated from the University of Missouri – Rolla with a degree in Electrical Engineering, specializing in the fields of Computer Aided Design and Non-Linear Control Theory.

Instrument

O'Brien and Perrey will provide feedback via a questionnaire (Appendix B). The instrument consists of 9 open-ended questions. Open-ended questions admittedly have several disadvantages, including:

- Higher cost of coding, editing and analyzing
- Categorizing and summarizing takes time
- Interviewer bias is greater than with fixed-alternative questions
- The length of answers is proportional to the respondent's education

Open-ended questions are used for this project because none of the negative factors apply and they provide some advantages not allowed with fixed-alternative questions. The sample size is small, so the time to evaluate the results is not an issue. Most importantly, both evaluators are highly educated and well versed in the area of study. Giving them ample room and opportunity to express their views gives me a great deal of useful input that may not surface with a multiple-choice instrument.

Procedure

O'Brien will be allowed to evaluate the WEB server first hand. He has access to the Server and to the Firewall where the configuration file exists. Perrey will not be able to test the actual Web Site, so the HTML files will be sent to him and he can view them on his PC. The content will be exactly as though he was looking at the data on the Server. O'Brien and Perrey will base the majority of their evaluation on the written project. The cover letter, the project and the questionnaire will be e-mailed to the evaluators. They will fill in their responses to the questionnaire and return them via e-mail. Their return e-mail address will serve as their signature.

The questionnaire is self-administering, but there will be a follow-up interview conducted with both evaluators. What is expected of the evaluators will be explained in a cover letter (Appendix C) that will accompany the questionnaire and the written project.

Chapter IV

RESULTS

This chapter will report on the results from the survey sent to the subjects described in chapter three. The questions will be listed, followed by the comments from the readers. O'Brien's comments will be listed first each time simply for the sake of consistency. Evaluation of these comments is reserved for the last chapter.

Was the material in this manual written in a clear and concise manner, making it easy to follow and understand? O'Brien said it was clear and concise, and stated that "The project goals described what actually did follow with reasonable accuracy". He also stated that "While the step-by-step procedures were exactly like a check-off sheet, the personal experience (1st person) starting on p22 gave me confidence the procedures would, and did indeed work".

Perry agreed that the project was well written and made particular notice of the attention to detail, and he appreciated the inclusion of the thought processes that went into the firewall rules.

Was the choice of hardware and its configuration appropriate and or adequate? O'Brien said, "The hardware selected provided the ability to implement the security policy on page 2 in a cost effective manner".

Perry noted that the question asked about the choice of routers, but in the conclusion, it was stated that the router rules were not discussed due to the complexity of the subject. Perry also noted that the project did not go into the reasons for selecting the SPF100 firewall. He added that the paper should have discussed the pros and cons of a few different types of firewalls.

Was the discussion on securing the UNIX environment clear and adequate to protect the Web Server? O'Brien said yes, but noted that even though the comments on pp5-7 were accurate and reasonable for this project, there is much more to know and consider in dealing with securing a UNIX environment. He also stated that he has recently developed and delivered a 527 viewgraph, 2-day course on the subject.

Perry was mixed on this topic. He liked the discussion of utilities such as Crack, but insisted that ACL's do not protect UNIX machines. He added that remote access (allowed by an ACL) gives a user the same capabilities as being at the console.

The Security Policy is clear and adequate to protect the OurNet environment, assuming everyone follows it. O'Brien suggests rewriting the question to include "the implementation of the security policy". A policy is just a set of rules that can and will be broken according to O'Brien. He therefore responds with a qualified YES, stating that the firewall rules will protect the network and servers from the Internet.

Perry thinks that the strict control placed on the use of .netrc., .rhosts and /etc/hosts.equiv was accurate and comprehensive and he agrees that having a tiger team test firewall rules is a necessity.

The administration of the SunScreen firewall is adequate and helps to fulfill the requirements of the security policy. O'Brien said the rules for the Internet and for the Intranet are reasonable.

Perry feels the rules pertaining to UNIX security are well defined and adequate and that the only access to the firewalls is through an encrypted tunnel is a good touch.

The network diagram clearly depicts the network described in the project and it is useful in discerning the security issues discussed. O'Brien checked both the YES and the NO boxes on this question. He said the drawing is a good representation, but that it was not as tightly coupled to the text as he would have liked as a reader. He made several notes on the drawing and his suggestions are discussed in the next chapter.

Perry stated that the diagram was a good logical depiction and that there was lots of labeling. He did suggest labels for DMZ-A and DMZ-B.

Were the instructions for configuring and using the software clear and well documented? O'Brien stated that " a degree of personal experience was made evident" and that "the step by step check-off was fine".

Perry felt the project included an accurate description of each of the packages used in the project.

The manual covers all the basics for selecting options to insure the functionality and security of the server, the host it runs on and the environment surrounding the server. O'Brien says yes and that "While apparently fairly comprehensive, a review of firewall logs might yield errors" He explained this by saying that the project described a 2-level security strategy (host and network) but it did not mention application level issues.

Perry praised the selection of the administration login and password and the restriction of hosts that are allowed to administer the server.

Did the manual adequately cover the setup and installation of a Web-site that will be functional? Consider the discussion on HTML Transit, Front Page and Netscape Enterprise Server. O'Brien said yes, because "it offers step by step instructions on the configuration of a web server and showed evidence of success at the operation by making it experiential". It will not be certain until our follow up interview, but he probably means that he tested the site and it works.

Perry was impressed by the discussion on how to install and run each of the packages. He also said he appreciated the explanation of HTLM Transit.

O'Brien went beyond what was asked of him, by adding comments throughout the project margins. He noted for instance, that the project stated the diagram would indicate the trusted and non-trusted environments. The paper assumes that the labels OurNet and Outside were enough to distinguish the two environments.

O'Brien made several suggestions concerning the diagram. The most important point is that the Intranet LAN segment could be placed on the 4th interface of the firewall (QE3) isolating it from the Internet and making it more controllable by firewall rules. A few of the interfaces on the diagram did not show the IP addresses, causing the reader to have to figure them out which complicates reading and comprehension. He also noted the following points that he felt would make the diagram more useful:

1. FJBPC runs FPWEB (Front Page Web)
2. TSHP is a Web Publisher
3. LWHP is a Web Publisher
4. JONHP is a Web Publisher
5. BADPC is a consultant's PC
6. NET-D is the Personnel LAN
7. The routers are Cisco 2500's
8. NET-E is the Intranet

O'Brien said "Simple things like reminding the reader of names of equipment makes their job much easier". On page two, there is a reference to "the Web Server inside OurNet", but there are two servers and the intended one was not specified.

The security policy on page two states that there will be not e-mail service running inside OurNet. The rule explains that e-mail servers present the risk of allowing in Trojan Horses and flooding of junk mail, but O'Brien asked for the logic behind this rule. Since the readers did not get to read chapter two, which dealt with the dangers of running e-mail servers, he felt an explanation was in order.

O'Brien asked why remote execution was not allowed from the DMZ on page two. He suggested that the paper should specify which LAN segment will not have access to the Web Servers on page three. On page four, SPF-100 was misspelled. He suggests that UNIX is a trademark and that it should be acknowledged by adding the trademark symbol (UNIX ®).

O'Brien noted more syntax errors on page five and suggests that the rhosts and netrc files are preceded by a "." and hosts.equiv is more accurately written as /etc/host.equiv. Also on page five, it was stated that using these constructs is convenient, but not worth the risk. O'Brien thinks a comment to this affect should be added to the security policy.

O'Brien found a construct on page seven that was truly misunderstood and misrepresented. According to O'Brien, the .netrc file stores passwords on the originating machine, not on the destination machine.

O'Brien asks if the Cisco 2500 router can control access at the service level and the answer is yes. He is referring to the fact that the project left access control from Net-B to the router, not the firewall. The same issue is addressed again in the list of hosts on page eight where O'Brien asked how Net-B would be controlled. He suggests login and passwords on RJLHP.

On page ten, O'Brien suggests replacing TCP services with TCP or UDP services. He points out on page eleven that the SunScreens do not have to encrypt all data between themselves, but it is an option.

Chapter V
DISCUSSION

Summary of Evaluator Comments

Based on the feedback, it appears the evaluators liked the work and feel that it was a valuable project. There is plenty of room in a technical project for differences of opinion, but even though a few of the comments were ignored, the majority of them were substantial and warranted action. Most of them will be implemented directly and others will be rectified by adding clarification in other areas.

O'Brien received the first draft of the project, but Perrey received a copy that was modified based on the feedback from O'Brien. The result is that Perrey's comments should not and did not include any of the problems pointed out by O'Brien, but he did find some issues that O'Brien either let slide based on their relevance compared to the other issues he brought forward. The final result is a project that has gone through and extra level of refinement.

Details of Evaluator Comments

On the first issue, whether the document was well written and easy to understand, both readers agreed that it was. O'Brien had an advantage over Perrey in that he had access to the test configuration of the firewall and to the Web site itself. His quote about 1st person experience means that he personally verified the functionality and that based on his personal work experience with firewalls, he felt the rule-set was adequate to protect the environment. Perrey did not have the 1st person experience of checking out the actual Web site or the rule-set, but based on the project, he felt a great deal of thought went into the design of the network.

Results were mixed on the issue of hardware selection. The question asked "Was the choice of hardware and its configuration appropriate and or adequate?" O'Brien simply agreed that the hardware selection would accomplish the task in a cost-effective manner. Perry pointed out that the question asked about the router configuration, but that it was clearly stated in the project that the router configuration was not covered for reasons specified. The point was well taken, but the correction is in the wording of the questionnaire, not in the project itself. Perry also noted that the paper did not go into the reasons for selecting the SPF100 firewall. He added that itcould have discussed the pros and cons of a few different types of firewalls. Again, point is well taken, but there was a discussion of firewalls in chapter two of the paper and repeating the information in the project seemed fruitless. For clarification, the re-work of the project contains a reference to the area of chapter two that should put a reader at ease, knowing it had been covered elsewhere.

Perhaps the most important issue aside from the firewall-rules is the choice of options applied to the UNIX® systems. The next question asked "Was the discussion on securing the UNIX® environment clear and adequate to protect the Web Server?" O'Brien said yes, but noted that there is much more to know and consider in dealing with securing a UNIX® environment. He made reference to a lengthy project that he recently developed on the security issues on UNIX®. He was not bragging, but simply wants the reader to know that UNIX® security is not a two-page subject. O'Brien is correct, but space constraints of this project did not allow for such a lengthy discussion of the topic. Therefore, no changes were made in response to this comment. Perry was mixed on this topic. He liked the discussion of utilities such as Crack, but insisted that ACL's do not protect UNIX® machines. He added that remote access (allowed by an ACL) gives a user the same capabilities as being at the console. Perrey is correct, but security is implemented on the basis of risk and cost of protection. The workstations that are being controlled by ACL's in the router are in the same building as the console. With this in mind, these users have access to the console if they wanted to hack the system, so spending money for another firewall would be a waste of money in this case.

A security policy is a set of rules that the organization wishes to enforce in order to protect its information assets. The question that asks if the security policy is clear and adequate to protect the environment was missing an important phrase according to O'Brien. O'Brien suggests rewriting the question to include "the **implementation** of the security policy". Perry thinks that the strict control placed on the use of .netrc., .rhosts and /etc/hosts.equiv was accurate and comprehensive and he agrees that having a tiger team test firewall rules is a necessity. Again, it is not the project, but the questionnaire that could use some re-wording.

The question about the configuration of the SunScreen Firewall received nothing but praise and there is a good reason for this. The firewall was of particular importance in securing the environment, so more time and space was allocated for it. After all, the firewall is what makes Intranets feasible and they are the newest of subjects in the computer-networking arena.

The next question asked if the network diagram was accurate and complete. O'Brien saw the first draft and had several valid points, which were all corrected on the diagram before Perrey saw it. Examples of O'Brien's findings were;

1. There was no IP address for FJBHP
2. Add "Enterprise" to the comment under RJLHP
3. Add "Front Page Web" under FJBHP
4. Add the Firewall admin station
5. Add "Web Publisher" under work stations that have this privilege
6. The Intranet cloud was not labeled as such
7. The BADPC should say "consultants"
8. Net-D should say "Personnel LAN

Since he received the drawing after O'Brien's suggestions were applied, Perrey responded by saying there were plenty of labels, except that it should distinguish between DMZ-A and DMZ-B, which was done in the final drawing.

The question concerning the installation of the software packages received casual approval. Modern software packages are typically easy to install, but as in the case of the Netscape server, there are a few points that can slow down installation and these are the highlights the project tried to emphasize. While not an exciting subject, there were some issues that demanded attention.

The next issue on the questionnaire was the security options used to protect the Web server RJLHP. O'Brien says that while the project was quite comprehensive in covering the host and network issues, it did not cover application level issues. The fact is, this research did not include much about application issues. This would be a good topic for further research.

The last question asked if the manual adequately covered the setup and installation of a Web-site that will be functional considering the discussion on HTML Transit, Front Page and Netscape Enterprise Server. Both readers agreed that these subjects were adequate and gave examples of points of particular interest to them.

Since O'Brien went beyond answering the questionnaire by making notes on the margins of the project and on the diagram, it seems appropriate to respond to his sidebar-comments as though they were part of his formal response.

His comment about the distinction between trusted and non-trusted areas of the diagram is noted, but there is a problem with saying that a DMZ area is either one or the other, because it is trusted more than the outside, but less than the inside. No changes were made to the diagram for this reason.

The most important point O'Brien made on the diagram is that the Intranet LAN segment could be placed on the 4th interface of the firewall (QE3) isolating it from the Internet and making it more controllable by firewall rules. After some study, it was concluded that he was correct and the recommended changes were made. The result is a much more controllable environment.

A few of the interfaces on the diagram did not show the IP addresses, causing the reader to have to figure them out which complicates reading and comprehension. I added the IP addresses that were missing.

O'Brien made several other suggestions concerning the diagram. Changes were made to the diagram to reflect O'Brien's comments in the following list.

1. FJBPC runs FPWEB (Front Page Web)
2. TSHP is a Web Publisher
3. LWHP is a Web Publisher
4. JONHP is a Web Publisher
5. BADPC is a consultant's PC
6. NET-D is the Personnel LAN
7. The routers are Cisco 2500's
8. NET-E is the Intranet

Comments O'Brien made in the margins of the text, which were used to improve the document, include the following suggestions. On page two the project referred to "the Web Server inside OurNet", but it did not say which one. Since there are two web servers, the paper now specifies RJLHP.

The security policy on page two states that there will be no e-mail service running inside OurNet. Since the evaluators did not get to read chapter two, which dealt with the dangers of running e-mail servers, O'Brien felt, with good reason, that some explanation was required. Since this project was restricted to securing a Web Server, the space was utilized on other subjects.

O'Brien asked why the security policy did not allow remote execution from the DMZ. Simply a matter of trying different options in the firewall rules. Since there are consultants on the Personnel LAN, it was decided that restricting them from access to hosts inside OurNet would be appropriate. He suggested that the LAN segment that will not have access to the Web Servers should be specified. This was done in the final writing. His reminder about the UNIX® trademark resulted in changing all references to include the trademark symbol.

O'Brien suggested the paper should change the spelling of file references on page five, specifically that the rhosts and netrc files are preceded by a "." and hosts.equiv is more accurately written as /etc/host.equiv. Also on page 5, it was stated that using these constructs is convenient for users, but not worth the risk. O'Brien thinks a comment to this affect should make this part of the security policy. The spelling corrections were made and the appropriate rules were added to the security policy.

O'Brien found a construct on page seven that was misunderstood and misrepresented. According to O'Brien, the .netrc file stores passwords on the originating machine, not on the destination machine. When FTP is used in conjunction with a .netrc file, the passwords are transmitted over the network in clear text, making them available to network sniffers. With this in mind, it becomes clear that we cannot control the use of .netrc because we do not have access to the originating machines. We can however, insist that our administrators do not give accounts to users outside OurNet, and FTP from non-trusted networks can be prevented by the application of rules in the firewall. The appropriate rules are implemented in this project.

O'Brien asks if the Cisco 2500 router can control access at the service level and the answer is yes. He is referring to the fact that the network disign left control of access from Net-B to the router, not the firewall. The same issue is addressed again in the list of hosts on page eight where O'Brien asked how Net-B would be controlled. He suggests login and passwords on RJLHP. Logins and passwords are a standard operating procedure for all UNIX® systems. What O'Brien may have been suggesting is that there should be no anonymous FTP allowed and that there would be no group or shared passwords. These items were added to the security policy. On page ten, O'Brien suggests replacing TCP services with TCP or UDP services. This is true and the correction was made.

He points out on page eleven that the SunScreens do not have to encrypt all data between themselves, but it is an option. The ability to hide or disguise administration information is one of the most valuable attributes of the SPF-100 and there is no situation where running administration data in clear text is logical when an encrypted tunnel is available. While it is an option, it is by far the best option.

Limitations

After interviews with the evaluators and other system-administrators, it appears obvious that there is no such thing as a web-master-network-security-expert. Most security experts are not concerned with web publishing and most web-publishers are more concerned with content than with security. The books read in preparation for this project were collections from groups of administration experts and web-masters, so they offered a blend of knowledge. Finding one person with expertise in both arenas is not that easy. The evaluators chosen to read this project are highly respected men with outstanding credentials, which made them more than qualified and there input was very much appreciated.

High levels of respect come from high levels of visibility and work. Asking these men to interrupt their busy schedules was not a trivial thing. Every effort should be made to present these busy professionals with a polished document, not a work in progress.

Suggestions for Further Research

The project was extremely complex and probably should have been narrowed down to a more finite area of concentration. The paper could have dealt strictly with the host level security issues surrounding a web server, or it could have concentrated on the network level security issues of routers and firewalls. If the former had been chosen, the readers could have become web-masters, but they would not have learned anything about firewalls and their web sites would probably be hacked and destroyed in no time. If the later option had been chosen, the readers would be more grounded in firewalls, but they would still be lost when it comes to publishing a web page. The research uncovered a great deal of information on both subjects and an attempt was made to include enough detail to aid the reader who is new to the subject of securing a Web server in an Intranet environment.

One of O'Brien's comments was that the project did not discuss the application level security issues. This would be an excellent topic for further research. This extended research could include such topics as e-mail, pcAnywhere, proxy servers and DNS. Actually, any one of these subjects would be a good topic on its own.

There are many benefits and rewards for doing research and one of them is improved job skills and qualifying for promotions. This writer has already received a job change into the network security arena and it is largely due to the knowledge gained while working on this project.

Predictions for the Future

Since this project has taken over a year to complete, many of the predictions in the first two chapters have already come true. The new developments in Internet security such as SET and Virtual Private Networks (VPN) have eased the fears of many businesses around the globe.

Internet service providers are guaranteeing security of information and offering more and more services such as Voice over IP (sending long distance phone calls over existing IP networks). The government is sticking to its promise to not tax IP services like it does the analog phone services, which makes long distance cheaper and more competitive.

The price of PC's has been reduced to a level that makes them available to more families. Schools are installing high speed Internet connections with help from the government. Web publishing tools are available that make HTML editing almost a thing of the past. Encryption, SSL, and VPN's are making

Internet financial transactions safer day by day. Young students are doing business over the Internet at the astonishment of their parents.

The only problem left is how to transmit billions of packets over a network that was designed to handle millions. The answer to that issue is nearly solved. Fiber optics was the great advancement of the eighties, but the newest member of the telecommunications family is the technology that enable thousands of times the traffic over the same fiber that was laid 15 years ago. The technology is Wavelength Division Multiplexing, which increases the capacity of a fiber from 80 simultaneous calls to 16,000 calls. This, along with the fact that the speed of the Intel Pentium chip has doubled since the start of this paper makes it obvious that the predictions made two years ago will be material for technical nostalgia in the near future.

Appendix A

Building a Secure Intranet

Fred Berryman

Introduction

This plan will document the installation of an Intranet environment, which includes a web server secured by a firewall. The web server distributes company confidential information that is needed only by employees directly connected to networks inside the firewall and a few select computers located outside the firewall. The project will contain a diagram of the network indicating the trusted and non-trusted environments. Detailed procedures for configuring the web server and the firewall will be provided along with the steps used to setup the home page. A security policy will list the restrictions deemed necessary to protect the network hereinafter called OurNet.

General Description of Network

The data stored on the Web server (RJLHP) inside OurNet is confidential and must be hidden from outsiders. Access must be controlled and limited to necessary functions and users. A firewall is considered necessary for protecting the server from the Internet and from certain other users within the environment. The following policy lists security guidelines that will be enforced by company regulations and firewall configuration rules.

Security Policy

- Downloading files from the Internet will be limited to printer drivers and other files necessary for company business. Files will only be allowed from secured sites and virus checkers will be run against them.
- Outbound WEB access is allowed as stated above, but there will be no WWW access to OurNet from the Internet.
- There will be no e-mail server inside OurNet.
- There will be no inbound FTP from the Internet.
- Remote execution of programs will be allowed from certain hosts inside OurNet, but not from outside the firewall on interfaces Qe0, Qe2 or Qe3.
- Risks that cannot be mitigated by the firewall such as Trojan horses and viruses injected via removable media will be controlled by strict enforcement of established guidelines on virus checkers and the use of pirated software.
- Hackers are equipped with sniffers (packet capturing software and hardware). They can capture session data and try and hack their way into the network by pretending to be a valid user. The firewall will validate the authenticity of the "from address" in all packets based on the point of entry to the network.
- There is a LAN segment inside OurNet (Net-D) that is used by consultants and the personnel department who will not have any access to the Web Server.
- When changes are made to the firewall, a tiger team will run tests against the new configuration to insure no new holes have been opened.
- The security team will run Satan, Swan, Itrust and Crack on a regular basis.
- The use of .netrc, .rhosts and /etc/host.equiv will be strictly controlled.

- There will be no anonymous FTP accounts.
- There will be no shared logins on any host in OurNet.

Hardware

A Gateway Pentium PC with a 3-Gigabyte disk drive and 64 megabytes of ram will run FPWEB (Front Page Web). An HP/A4304A:XC will be the host for the Netscape Enterprise server (RJLHP). The firewall is a SunScreen SPF-100 configured to enforce the security policy listed above. Rtr1and Rtr2 are Cisco-2500 routers. Router and firewall selections were based on logic discussed on Page 40 of chapter two.

Software

Although a Web site can be developed with a text editor and a thorough knowledge of HTML, it is not the method of choice. There are many tools that make the job easier. The installation and use of the following software will be demonstrated.

- HTML Transit
- Microsoft Front Page
- Netscape Enterprise Server

UNIX® Host Administration

There are many security issues that must be addressed to insure a secure operating environment. The UNIX® security options will be dealt with first, and then the firewall rules will be discussed.

The web server is going to store confidential information. Some employees have a need to know this information while others do not. The administrator and others who are given permission to publish web pages will have a login for remote access through Telnet and FTP.

Personnel with publishing rights will want easy access to the web server, but security will not be sacrificed for convenience. These employees have workstations from which they can gain access to the Web server. They could create an environment whereby they could gain access without typing a password. This is done through the use of .rhosts, .netrc and /etc/host.equiv files. These three files are UNIX® constructs, created to allow convenient access by trusted users on other hosts. The danger in using them is that an unauthorized user on one host can gain access to other hosts. The convenience is not worth the risk when sensitive data is at stake.

Adherence to security guidelines will be monitored through the use of software packages much like those used by hackers. The first step for a hacker is to find a login and password pair that will gain him access to a host. The login is stored in the password file and the encrypted password is typically stored in the shadow file. Crack is a program that tries to guess passwords by going through a list of rules. First, it tries the login-name as the password. Then it adds numbers to the login, then it reverses the login, etc. It can take weeks to run though all the possibilities, but hackers are in no hurry. Using such tools, weak passwords are guessed allowing access by intruders. By running this sort of program, the system administrator can detect and correct weak passwords before the hackers find and use them. It should be assumed that a hacker will find the password file.

Itrust is a script that verifies conformance to guidelines concerning .rhosts, .netrc and /etc/host.equiv files. Itrust lists occurrences of these files and makes note of the ones that give unreasonable read and write permissions. It also checks the permissions on each user's home directory. This directory should not give write permission to anyone except the owner. If it does, a hacker can drop a .rhosts file in it, giving himself easy access from any machine he chooses.

The /etc/host.equiv file is similar, and even more dangerous than the rhosts file. The hosts.equiv file is a list of machines that this machine trusts. Once enabled, this construct allows users to move from machine to machine without a password. Situations exist in many corporations where one machine trusts another machine, which trusts yet another machine, until users on the network can login to almost all other machines.

The .netrc file does the same thing for FTP as the .rhosts and /etc/host.equiv files do for the R-commands. One distinction is that the .netrc file is maintained on the originating host and stores passwords for the destination hosts. When used, these passwords are transmitted over the network in clear text. While we want to maintain security inside OurNet, we do not wish to prevent our users from performing critical work, which often includes using FTP to outside hosts. As a compromise, we will allow outbound FTP, but we will reprimand any users deploying .netrc files.

When a computer such as the Netscape Server connects to a network, it immediately becomes vulnerable to hacking by other hosts on the same LAN segment. When there is a path from this network to an Intranet, the Web Server becomes vulnerable to anyone in the Intranet. When there is a path from the Intranet to the Internet, it becomes vulnerable to intruders all over the world. The attached diagram details the connections of workstations to the servers and the associated firewalls. The diagram page is at the end of the project, feel free to set it aside and refer to it during the remainder of your evaluation.

Detailed Description of Network

Our Web server host (RJLHP) is on network Net-A. The other hosts on Net-A will have more privileges compared to hosts on other LANs inside OurNet. Some of the hosts on Net-B will be allowed FTP access to the Web server for publishing web pages and some will only have HTTP access. Since Net-B is inside the Firewall, access control to RJLHP is controlled by rules in Rtr1.

The Corporate Intranet is a number of LANs and hosts interconnected via routers. The Intranet has access to the Internet via proxy servers, which are beyond our control. FW1 and Rtr2 control access to OurNet from and to the Intranet.

The firewall is a Sun SPF-100 with 4 Ethernet ports. The firewall will be configured with a set of rules that will allow certain hosts to send packets to and from OurNet. The exact rules will be defined later.

Hosts and LAN Segments

- **Net-A** is the most trusted LAN segment in OurNet.
- RJLHP is the host for Netscape Enterprise Web Server (NES).
- FJBHP is my HP workstation. It will be used for remote administration of NES.
- FJBPC is my PC, which runs Front Page. From there, I can develop Web pages and publish them up to NES.
- **Net-B** has a number of HP workstations belonging to staff. Some have publishing privileges on the Web server. Other hosts on this LAN can only browse the NES server. Access is controlled via router rules and Access Control Lists (ACL's) on RJLHP ie; inetd.sec. Since these are employees of the company, access control via a firewall would be more expensive than the damage an employee in this category would likely cause.
- **Net-D** is a demilitarized zone (DMZ) explained later.
- BADPC is a host used by consultants that need limited access.
- **Net-E** connects the corporate wide Intranet to the Internet and it connects to QE3 of the firewall. All users in the Intranet will be allowed to browse the NES web and one of them (JONHP) will be allowed FTP access for publishing to the Web.
- **Net-F** is the worldwide Internet.
- **Net-X connects** the Firewall to OurNet.

- **Net-G** connects the Firewall to the Intranet and the Internet

The SunScreen firewall is an SPF-100 Sun Sparc5 computer running a condensed version of UNIX® System5 Release 4. The only application that should run on the unit is the firewall software. Installing any other software is not recommended and a violation of corporate policy. The operating system boots from a CD ROM drive and components needed for operation are automatically transferred to the 535-Megabyte hard drive on boot up. The SunScreen uses dynamic packet screening and public key cryptography. The security rules and the encrypted tunneling options must be configured before the interface cables are connected.

Another required component of the SunScreen system is the Administration Station. One SunScreen is required at each physical connection point where the Intranet touches the Internet. One Administration Station can service multiple sunscreens. The Administration Station is used to create and modify rule-sets and to monitor the operation of the SunScreen.

The SunScreen can filter on TCP services such as TELNET, SMTP, FTP, DNS, Gopher, finger, News, Rlogin, rsh, lpr, WWW and other user-defined services. It can also filter on UDP services such as DNS and SNMP. It runs Simple Key-management for Internet Protocols (SKIP) software using 1024 bit Diffie-Hellman modulus and X.509 certificates. It encrypts traffic using RC2, RC4 and 56-bit DES. The main component is the rule-set, which determines which packets are allowed and which ones are denied.

Firewall Configuration Details

Four Components of a Firewall Rule-Set

1. **Service** – can be individual TCP or UDP services or a group of several services.
2. **From** addresses –individual devices, networks, subnets, or groups of addresses from which packets are received.
3. **To** addresses – destination addresses and can be grouped as above.
4. **Action** – determines what will be done with a packet once it matches on a service and address. Options include pass, encrypt, decrypt, log or drop the packet. Actions are divided into Pass and Fail rules.

The SunScreen uses source address checking to verify that packets are coming from a valid source network and they are not an attempt to spoof an address assigned to a different network. If the packet is encrypted, it is decrypted then sent back to the rule-set to determine its fate. It is then checked against the Pass rules. If all the requirements of the Pass rule are fulfilled, the Action dictated by the rule is carried out. The Pass action will normally be to pass or encrypt and pass, but it can also cause a log entry or send an SNMP packet to the SNMP manager. Logging of passed packets is usually not necessary because only trusted packets are passed and there is no need to log them.

If the packet fails all the Pass rules, it goes to the Fail rule-set. Failed packets are often logged and certain malicious looking traffic can generate alarms or syslog entries to inform the administrator of danger. If it is dropped at this point, a special fail action will take place and the default Fail rule will not be applied. If none of the Fail rules apply, the packet passes to the default Fail rule, which normally logs failed attempts.

The SunScreen encrypts all traffic between itself and the Administration Station. It can also encrypt traffic between itself and another SunScreen. Encryption often requires fragmentation because packets are larger after encryption. The encrypted packet is placed inside another IP packet, a SKIP header is added for decryption and the process itself adds padding. If the sender applied the "don't fragment bit" the packet is sent back to the sender requesting a smaller packet.

The packet is then encrypted using the encryption technology chosen at configuration time (DES, RC2 or RC4). A random traffic key is generated based on the encrypted data packet. To make the packet more secure, the traffic key is encrypted with the chosen technology DES or RC2 and a key received form the SKIP key manager. Upon arrival at the destination SunScreen, the SKIP manager provides the SKIP key to decrypt the traffic key, which is used to decrypt the traffic packet.

Functions Performed by the Administration Station

1. SunScreen Administration Application – Two sub-programs
2. Configuration Editor – Used to create the rule-set.
3. SunScreen Manager – Used to connect to and manage the SPF-100.

   Operations available are;

   - Information – last boot, system name, etc

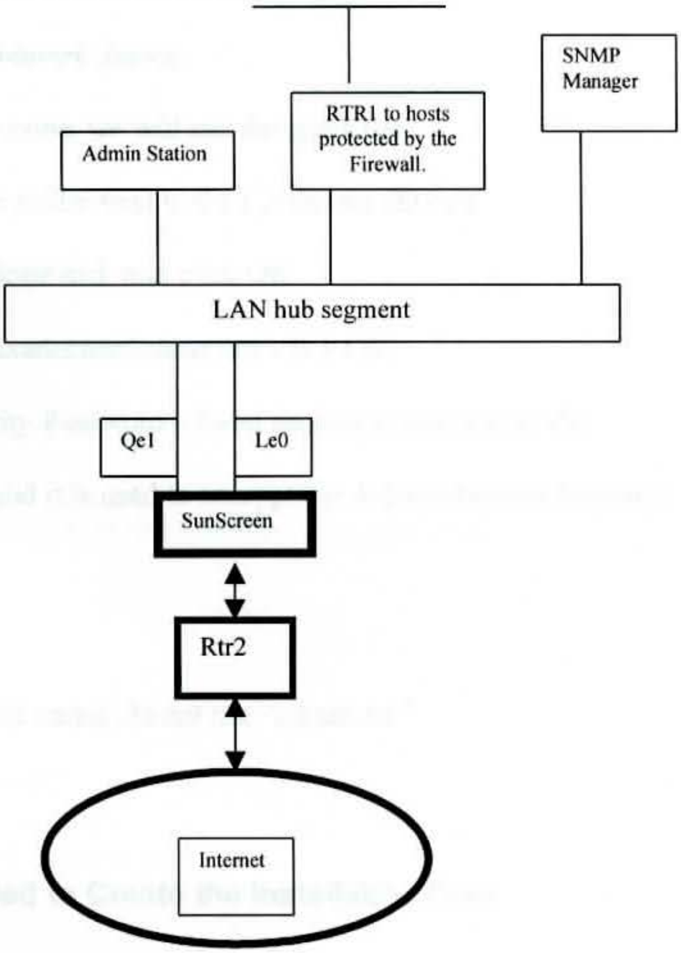
- Key Statistics – number of lookups, key manager requests, etc.
- Emergency – stops all traffic through the SunScreen
- Routers – address of router connected to an interface
- Access Control – list of Administration Stations allowed access.
- Traffic Statistics – packets passed, logged or dropped on interfaces
- Miscellaneous – set date, get logs files, issue specific commands.
- SNMP Alerts – address of SNMP manager
- Certificates – copy SKIP certificates between SPF-100 and the Administration Station.
- Configuration – shows the active configuration and allows for copying configurations to and from the Administration Station.

4. Configure Application – Used to set the initial parameters of the Administration Station, including the IP address, DNS and the Administration Station's SKIP certificate.
5. Create Installation Disk Application – Used during initial installation. The installation disk is created on the Administration Station and is used to boot the SPF-100 the first time. The name of the SunScreen, its IP address and DNS information is entered here.
6. Certificate Manager Application – Used to associate encryption certificates, names and device types to SunScreens and Administration Stations. Also defines the key encryption technologies used for data and key encryption. SKIP certificates can be copied from SPF-100's or from the public certificate diskettes.

7. Log Browser Application – Used to view logs retrieved from SunScreens.
8. Reports Application – Used to generate reports from the Certificate Manager database and from the rule-set database.
9. Configuration Backup Application – Used to backup Administration Station files including local copies of SPF-100 configurations and local certificates.
10. SKIP Host Application – Used to create an unencrypted connection for printing or moving a file from the Administration Station to a network printer or to another computer. Everything else going to or from the Administration Station is encrypted.

Now that we are somewhat familiar with the tools available, we will setup and configure the SunScreen and Administration Station for OurNet. The SunScreen is placed directly between the router interface and the network it feeds. In our case, Rtr2's interface E0 goes to the Internet, E2 goes to the Intranet and E1 goes to the network inside OurNet, which is what we want to protect. The SunScreen interface Qe1 connects to the LAN segment that feeds OurNet. The Administration Station could connect directly to the Ethernet port on the SunScreen called LE1, but we may want to send SNMP traps from the Administration Station to an SNMP Manger and that requires a LAN connection.

OurNet SPF-100 Configuration Diagram



Data needed to configure the Administration Station

- IP address of the Administration Station – 195.191.172.35
- Network Mask for network – 255.255.255.224
- Common or Host name for the Administration Station – OurNet1
- The Administration Station's key and certificate disk.
- IP address of the default gateway – 195.191.172.33

Steps to configure the Administration Station

1. Click on the SunScreen Administration Configure icon.
2. Fill in the information obtained above.
3. Name resolution order – none, we will use the hosts file
4. Security – Click on open folder next to the Certificate ID box
5. Insert the key and certificate disk and click OK
6. Click next to the long hexadecimal name and click OK
7. Type in the Login Security Password – Used each time you access the Administration Station and it is used to encrypt the Administration Station's private key.
8. Save and exit.
9. Restart Windows from the menu, do not use "ctl alt del"

Data Needed to Create the Installation Disk

1. Name of SunScreen – FW1
2. IP address of admin port Le0 on SPF-100 – 195.191.172.36
3. Network Mask – 255.255.255.224
4. IP address of default gateway router – 195.191.172.33
5. SunScreen SPF-100's key and certificate disk

Steps to create the Installation Disk:

1. Click on the Create Installation Disk icon
2. Fill in the information gathered above
3. Click on OK
4. Insert the SunScreen SPF-100 key disk
5. Insert a blank disk in place of the key disk
6. Remove disk and label "SunScreen Installation Disk"

Steps to Initialize the SunScreen SPF-100

1. Power up the SPF-100
2. Place SunScreen CD-ROM in the CD drive
3. Insert Installation disk in drive A
4. Turn off SPF-100, wait 5 seconds, power on
5. When the Installation disk is ejected, the procedure is complete.

Creating A Rule-Set With the Configuration Editor

The configuration is the set of rules and interface definitions that tell the firewall what to do with each packet it receives. As mentioned earlier, a rule has four components, Service, From Address, To Address and Action. The action is one of two types, Pass or Fail.

Each rule is of one type or another, Pass or Fail. A rule does not have two alternative actions. If the rule parameters of Service, From and To Address are met, and the rule is a Pass rule type, the packet will be passed. If the conditions are not met, the packet falls to the next rule. All packets are checked against the Pass rules, then by the Fail rules. This technique is called parsing.

The first step in constructing the database is to create a new config file. Start the administration station and go to "file, new". I will name it OurNet.mdb. The first section of the database will be the addresses, which define the interfaces on the SPF-100 and the hosts and networks that we will be controlling with the firewall. We can also configure groups of addresses to minimize rules.

There are 4 interfaces on our Firewall, Qe0, Qe1, Qe2 and Qe3. See the map and observe that we have broken our world into four zones. Qe0 is OUTSIDE (the Internet) Qe1 is OurNet, Qe2 is a Demilitarized Zone (DMZ-A) and Qe3 is DMZ-B. Setting up the firewall address structure is a 3-step process.

First we will enter each host address with the **individual address** type. Then we can assign names to the networks involved by using the address type of **network**. After the networks are named, we will create address groups using the **address list** type. The group OurNet includes all the LAN segments that we are protecting with FW1 (Net-A and Net-B). Group DMZ-A consists of only one LAN segment (NetD). Group DMZ-B includes Net-E (the Intranet). Group OUTSIDE is everything else (the Internet). The groups OurNet DMZ-A and DMZ-B are built by including specific Networks while OUTSIDE is defined by excluding the previously configured groups.

After the addresses are configured, the Actions are defined. There are two choices here, Pass or Fail. I will configure the Pass actions first. Configuring

Pass actions is a two-part process. The action names are matched with Pass or Fail, log, encryption and SNMP options. Later, the Actions are associated with addresses in the rule definitions.

Firewall Actions

The Normal Pass Action just passes packets, sends no SNMP traps and logs nothing. The Secure-Outside Action makes a summary log entry, sends an SNMP trap to the SNMP manager and encrypts the packet. Pass-det is a Pass action that creates a detailed log entry for those special users on the Intranet that have selective access to OurNet other than WWW on port 80.

The standard or default Fail action drops the packet and sends an ICMP (Internet Connection Message Protocol) message to the user. This is just to let the user know his message or request failed. It will tell him nothing about the network. The fail-sum action will drop the packet after making a summary log entry. The fail-det-snmp action will make a detailed log entry and send an SNMP trap to the manager.

Associating Address Definitions to SPF-100 Interfaces

Pull down the SunScreen Definition menu to associate the addresses to SPF-100 interfaces. The top entry box is for the SunScreen name. The SPF-100 must have already been added to this Administration Station including its certificate, or it will not show up in the list. There is a box for each physical interface. Choose an address definition from the pull down list that best describes each interface. Ours are OUTSIDE, DMZ-A, DMZ-B and OurNet. Then choose a FAIL action from the right side pull down list. This tells the SPF-100 what to do with packets that do not match any other rule. I will pick the default action, which is pre-configured and drops packets without logging them or sending SNMP messages.

Defining Network Services and Service Groups

Network Services is where we tell the SPF-100 what services to use and assign port numbers to these services. Many of the standard services are pre-configured with standard port numbers. If we want to use a pre-configured service, but with different options, we must configure a new one with a different name. The FTP, Telnet and WWW services are already configured with standard ports, so I am going to leave them alone for now.

Service Groups are similar to address lists in that they are made up of lists of individual services. There are a few pre-configured service groups and I will create at least one of my own. Rather than go through each step of each service and rule, the following tables list the address definitions, special services and rule-sets for OurNet.

Addresses

Address-Name	Use
Badpc 195.191.174.37	Consultants
Bbhp 195.191.176.66	Bruce's HP
Fjbhp 195.191.187.100	Fred's HP – Web Admin
Fjbpc 195.191.187.102	Fred's PC – Front Page
Jonhp 125.151.204.37	John's PC – Web pub from Intranet
Lwhp 195.191.176.68	Larry's HP – Web Publisher
Patspc 195.191.174.36	Personnel Admin – Web access
Dcpc 195.191.174.35	Personnel Admin – Web access
Rjlhp 195.191.187.101	Richard's HP – Home of NES
Tshp 195.191.176.67	Teresa's HP – Web Publisher

Address Lists

Net-A	Web Server, Admin, and others with full access
Net-B	Web Publishers
Net-D	DMZ – Restricted Access in and out
Net-E	Intranet – Restricted Access
Net-F	Internet – Restricted Access
Net-G	Intranet – Another trusted SPF-100 Firewall
Net-X	Interface between firewall and OutNet
DMZ	All DMZ LANs
OurNet	All LANs inside the firewall except dmz
Outside	Intranet and Internet LANs

Pass Actions

Action Name	Log	SNMP	Encryption
normal	none	none	none
secure-outside	summary	yes	yes
pass-det	detail	none	none

Fail Actions

Action Name	Log	ICMP Alert	SNMP
fail	none	Net Unreachable	none
fail-sum	summary	none	none
fail-det-snmp	detail	none	yes

Service Lists

consult_deny	telnet, ftp, www, finger
dmz-allow	telnet, ftp, www, ping, icmp-all, echo, finger

Service Rules

Service	From	To	Action	Type
ftp	jonhp	Net-A	pass-det	pass
consult-deny	dmz	OurNet	fail-det-snmp	fail
telnet	outside	OurNet	fail-sum	fail
dmz-allow	DMZ	OurNet	normal	pass
encrypted-skip	Net-E	Net-X	secure-outside	pass
www	Net-E	Net-A	normal	pass
www	OurNet	outside	normal	pass

All the addresses, services and rules are entered, but they may not work. The true test is in downloading the configuration to the SPF-100. When this is done, the SPF-100 checks for conflicts and approves or fails the configuration. For example, if two rules have the same service, "from address" or "to addresses" and different actions, there is a conflict. Once the configuration downloads without a conflict, connect the cables and activate the configuration. Verify that the configuration allows and denies packets as planned. My configuration is not very complex, but I am proud to say it compiled on the first try.

Front Page – Web Server Installation

Front page is a Windows 95 or NT application. It loads and configures itself as easily as any other Microsoft product, just select the setup.exe utility on the CD-ROM and follow the Wizard. Front Page is only used as a tool to demonstrate how web pages can be developed on one machine and published on another. The Enterprise Server is a bit more complicated.

Netscape Enterprise - Web Server Installation

The other web server chosen for this project is Netscape Enterprise Server 2.01. Enterprise Server was chosen for its security features. The Web server is installed on RJLHP and the administration for the Web server will be performed remotely from FJBHP. The steps listed below will be brief where software documentation was sufficient and detailed in the areas that gave me the most trouble.

- RJLHP does not have a CD drive, so I mounted the CD on another host that has one, and advertised that CD via NFS. This was accomplished with the system administration module (SAM). I created a mount point on the host system called /cdrom and mounted the CD there.
- On RJLHP, I used SAM to mount an externally advertised file system. I created a directory called /cdrom (it did not have to be the same as the directory on the host system) and mounted the CD there.
- On RJLHP, I created a directory called enterprise under the root file system. I found the installation files I needed on the CD in a directory called HPUX10_X/ENTPRISE/HTTPS.TAR;1. The ";" in the filename caused some confusion for me. I am not sure why it was used, but with it in the filename, the ";" was being seen as a delimiter and the copy command failed. Finally, I did a "`cp HTTP* /enterprise`" and the file copied. This way, I did not have to enter the ";" because the wildcard "*" picked up the file I needed.
- I put the TAR file in a directory called enterprise, but it could have been any directory name except tmp. The installation guide advised against using tmp. After the installation is complete, I will delete the TAR file and this directory.
- The command "`tar xvof https*`" was used to un-compress the file. Again, the ";" in the file name prevented me from typing the entire filename. The files uncompressed into a directory call /enterprise/https.
- To start the installation process, be sure you are logged in as root, cd into https and type "./ns-setup. This installs the software into a directory called /usr/ns-

home by default unless you change it. I prefer to take as many defaults as I can.

- Since I am running the server on RJLHP, that is the machine name I entered when prompted.
- When the install process asks for a server port, it randomly generates a default port number. It already checked and verified this port is not being used, so I used the one it suggested port 16791.
- When asked for the admin login, I used the default username admin and I chose a password that I do not use on any other systems. This password is sent during logins with the HTTP protocol and it is not encrypted.
- The install process asks for a list of hosts that can administer the web server. The RJLHP machine is accessible by other users, so I chose not to allow administration of the server from that machine. Instead, I only entered the name and IP address of a machine that is in my locked office, FJBHP.
- Later, I decided that local administration is probably a good idea in case the network or the other host is down. To do this, I edited the /usr/ns-home/admserv/ns-admin.conf file and added rjlhp and its address. I then stopped and started the admin server for the changes to take affect.
- The install process starts the Server Selector. It is used now and in the future to make changes to the server using a Netscape browser. The next time, the Server Selector will have to be started manually before I access it. To start it manually, go to the server root directory /usr/ns-home and type ▒ `./start-admin`".

- From FJBHP, I started Netscape and typed the URL `http://rjlhp.els-an.att.net:16791/ &`. This took me to the Netscape Server Administration screen. First, make sure RJLHP is in the /etc/hosts file.
- To configure a new Web server, I just clicked on the line that said "Install a new Netscape Enterprise Server" The following prompts came up
  - Server name - RJLHP.els-an.att.net
  - IP address - leave blank
  - Port number for server - take default port 80
  - Server identification - richard don't ask me why
  - User name for server - lindauer
  - Number of processes - default
  - Document root directory - /usr/ns-home default

All that is left to do now is to populate the document root directory with a home page. The home page should have the name of index.html. I am going to create my home page with HTML Transit and import it to Front Page on my PC. After massaging it with Front Page, I will publish it to the NES Server. For now, we can verify operability of NES by going to FJBHP and starting the Netscape Browser. In the URL field, type "http://rjlhp.els-an.att.net/richard" The default home page that comes with Enterprise Server will be displayed.

Web Site Development

The first step in actually creating a Web site is to create a home page that is simple, appealing and informative. Many home pages are simply lists of things that can be found on the Web site. Lists can be simple bulleted items or complex drawings that have embedded image maps. The image maps are used as a graphical representation of the Web content. The image map might be a block diagram of a warehouse. When the user clicks on a section of the drawing, he gets transferred to the page with details about that particular area of the warehouse. Since this project is mainly concerned with securing the Web site, we will not get fancy with the content. We will however walk through the steps involved in creating Web content from the ground up. I have chosen to create a site from my thesis. The home page will be an index to the rest of the documents. I will use HTML Transit to convert my word documents into a web site.

I used HTML Transit version 2.0, which was written for Office 95. I currently use Office 97, which has Word version 7.0 installed. That means I must save all my word documents as Office 95 Word documents before I can use them as input files to HTML Transit.

HTML Transit takes a variety of file types such as Word and Word Perfect, as input and creates HTML pages from them. The user has many options from which to choose. He can dictate how styles in the original documents will appear in the HTML pages. Backgrounds and page separators can be chosen from galleries. An index and table of contents are created automatically from headings you select. A template is created with all your favorite options, which can be used to format future projects. HTML Transit converts images in source files to GIF format. There is a wizard to help the new user along the way.

HTML Transit opens with a menu page. From the "Set Up Files" button, select the input files you want to convert. Simply browse to the directory your original files are in and click on the ones you want to include in the web site. The output will go to a default location, but you can change it if you like. Go through the options under "Assign Elements, Format and Globals" and select options like background colors and page separators. Don't worry if you are not sure of the results because it is a simple matter to make changes later.

After all the files are selected and the options are chosen, click on Translate Publication. This will take a couple of minutes because it converts everything in the input files list to HTM including the table of contents and all the links from the TOC to the main documents. When the translation is done, click on Browse Publication and see what it looks like. If you have not chosen a default browser, it will ask which one to use, assuming you have more than one browser installed. If anything is not just the way you want it, go back to the options or to the original documents and make adjustments. Re-run the Translator and check your changes. I had to make minor changes in appearance because some of my documents used different style definitions for headers. I went back to the original documents and made them all the same and re-ran the translator. It is actually very simple and fast. The tutorial that comes with HTML Transit is extremely helpful and only takes a couple of hours to complete.

Now that the web site is built, I am ready to put it somewhere so others can view it. I chose to create my site with HTML Transit, then import it into Front Page for some final adjustments, then move it to my Netscape Enterprise

Server. I could have created it in Front Page or the Netscape Server, but I would have spent hours creating the table of contents and all the links to the other documents. The next step is Front Page.

Start Front Page and create a new Web. There are several options here. I can create a page from scratch, use the Front Page Wizard or import from somewhere else. Since I already have my site built in HTML Transit, I will import it from the output directory of Transit. Front Page uses the name Default.htm for the index file. HTML Transit uses the filename htindex.htm for the index, so after I import all the files from HTML Transit, I just renamed the htindex.htm file to Default.htm. The only thing that doesn't look right is the drawing I created in the project with the draw tool that comes with Word. I will have to go back and create that drawing with another package, probably Visio. I will insert it into the Word document and Transit will take care of it from there.

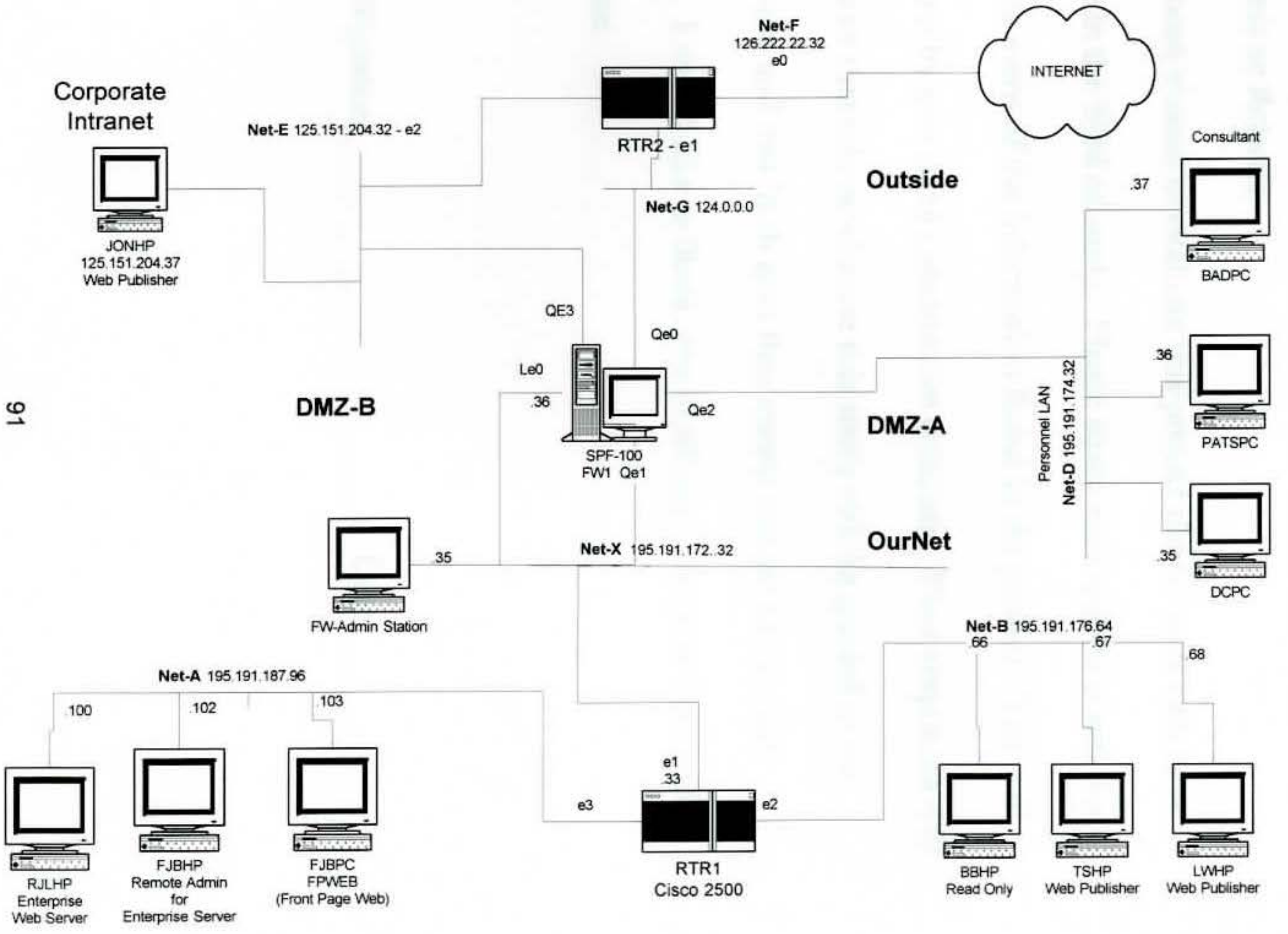
Once the site looks like I want it, I have a couple of options for putting it on NES. I can use an FTP utility on my PC and simply copy the files into the document root directory, or I can use the " File, Publish To" function from Front Page. I used the FTP utility this time, but I have used the Publish- To tool in the past. The Publish-To utility is frustrating because the wizard asks you questions to which the answers are not intuitive. Simple questions like destination directory are difficult to answer if you are not sure of how the document directory is configured on the Server. FTP is just as easy and there are no misleading questions. Once the files were on the server, I had to once again change the name of the index file, this time form Default.html to index.html.

The TOC created by HTML Transit shows up as the home page and all the other sections of my thesis are just a click from there. The site works and I can access it with Netscape Browsers on my PC, my HP and from PC's on the Intranet.

Conclusion

I was beginning to think I chose a project that was beyond my capabilities, but as time went on, and my job function changed giving me access to Firewalls, I started to have hopes of finishing. This project did not discuss the configuration of the routers for a couple of reasons. The Firewall does most of the filtering for OurNet and router configuration is too complex of a subject to cover here. I learned a great deal from the project and it is my sincere hope that my readers see it as an aid to understanding this complex but interesting subject.

OURNET DIAGRAM



APPENDIX B

QUESTIONNAIRE

Dear (Dennis or Robert),

You have been chosen to evaluate this project due to your extensive knowledge in the field of study. Please study each question and reply based on the merit of the information found in the project. You will only help me by providing constructive criticism. Your responses will help to ensure that others who use this study will be guided in the right direction and that Web sites they create will be secure and functional. I would like to thank you in advance for your time and participation.

Evaluator Signature ________________________ Date______________

Was the material in this manual written in a clear and concise manner making it easy to follow and understand?

_____Yes _____No

IF YES, give at least two examples where the manual was exceptionally well written.

1. ____

____

2. ____

____

IF NO, please offer at least one reason the manual was not well written.

1. ____

____

2. ____

____

Was the choice of hardware and its configuration appropriate and or adequate? Consider the selection of the Firewall, the routers and the host running the Web Server software.

_____Yes _____No

IF YES, give at least one example of why the hardware selected is appropriate.

3. ____

____

4. ____

____

IF NO, please offer at least one reason the hardware selection is not appropriate.

3. ____

____

4. ____

____

Was the discussion on securing the UNIX environment clear and adequate to protect the Web Server?

_____Yes   _____No

IF YES, give at least one example of why the security rules are necessary and appropriate.

1. ____

   ____

2. ____

   ____

IF NO, please offer at least one reason the Unix security rules are too strong or too weak.

1. ____

   ____

2. ____

   ____

The Security Policy is clear and adequate to protect the OurNet environment, assuming everyone follows it.

_____Yes _____No

IF YES, give at least two examples of how the security policy insures the integrity of the network.

1. ____

____

2. ____

____

IF NO, please offer at least one example of how the security policy does not perform its intended function.

1. ____

____

2. ____

____

The administration of the SunScreeen firewall is adequate and helps to fulfill the requirements of the security policy.

_____Yes _____No

IF YES, give at least two examples of how the firewall insures the integrity of the network and the Web server.

1. ____

____

2. ____

____

IF NO, please offer at least one example of how the firewall does not perform its intended function.

1. ____

____

2. ____

____

The network diagram clearly depicts the network described in the project and it is useful in discerning the security issues discussed.

_____Yes _____No

IF YES, give at least two examples of how the diagram aids the reader.

1. ____

____

2. ____

____

IF NO, please offer at least one example of how the diagram is incomplete or inaccurate.

1. ____

____

2. ____

____

Were the instructions for configuring and using the software clear and well documented?

_____Yes _____No

IF YES, give at least one example of why the software discussion was helpful and well documented.

1. ____

____

2. ____

____

IF NO, please offer at least one reason the software discussion is not adequate.

1. ____

____

2. ____

____

The manual covers all the basics for selecting options to insure the functionality and security of the server, the host it runs on and the environment surrounding the server.

_____Yes _____No

IF YES, give at least two examples of security options that aid in securing the Web environment.

1. ____

   ____

2. ____

   ____

IF NO, please offer at least one reason the manual is not adequate in the area of setting up the Web server and maintaining security of the server.

1. ____

   ____

2. ____

   ____

Did the manual adequately cover the setup and installation of a Web site that will be functional? Consider the discussion on HTML Transit, Front Page and Netscape Enterprise Server.

_____Yes _____No

IF YES, give at least two examples of how this manual makes the task of configuring a Web site easier.

1. ____

____

2. ____

____

IF NO, please offer at least two examples of how the manual is lacking necessary information or where the information provided is confusing or incorrect.

1. ____

____

2. ____

____

Appendix C

Cover Letter

March 22, 1997

216 Woodmere Way Ct.
St. Charles, Missouri 63303

Dear Dennis and Bob:

As promised, I am sending you a copy of my Intranet project for your evaluation. In order that I might gain maximum benefit from your efforts, I have included a short questionnaire for you to complete. The questions will guide you to the areas of concern while leaving you plenty of room for constructive comments.

Your comments should be detailed and critical. Do not just say you like something; tell me why you like it or why not. I have chosen you as an evaluator because of your expertise in the field of study and I trust you will be honest and thorough with your comments.

This project has been a challenging experience, but I have learned a great deal about a new and interesting technology. I can't tell you how much your willingness to help make it a success means to me. Thanking you in advance for your efforts, I remain,

Respectfully Yours,

Fred Berryman

Works Cited

Amoroso, Edward and Sharp, Ronald. Intranet and Internet Firewall Strategies. Emeryville, California: Ziff Davis Press, 1996.

Bernard, Ryan. The Corporate Intranet. New York: John Wiley and Sons, 1996.

Bott, Ed. "Inter.net Secure Firewalls" PC Computing. November 1996: 368.

Boutell, Thomas. The Whiteboard Institute for Biomedical Research/MIT Center for Genome Research "World Wide Web FAQ"
Last visited on April 5, 1997
http://www-genome.wi.mit.edu/WWW/tools/FAQ/index.htm

Brandwein, Rich. "AT&T Uses Netscape And The Web To Build A New Infrastructure For Information Access And Communications" Netscape Communications Corp. Last visited on April 4, 1996
http://home.netscape.com/comprod/at_work/customer_profiles/att.html

Campbell, Ian. Web Site "The Intranet: Slashing the Cost of Business."
Last updated Nov 96.
Last visited April 4, 1997
http://home.netscape.com/comprod/announce/roi.html

Cheswick, William R. and Bellovin, Steven M.
Firewalls and Internet Security, Repelling the Wily Hacker. Reading, Massachusetts: Addison-Wesley, 1994.

Compare. "Comparing Netscape And Microsoft Server Solutions"
Last visited on April 5, 1997
http://home.netscape.com/comprod/server_central/MS_comp.html

Dalva, David
Trusted Information Systems
Last updated June 1994
Last visited April 4, 1997
http://www.tis.com/docs/research/papers/wwwarticle.html

Falk, Bennett. The Internet Roadmap. San Francisco: Sybex, 1994.
Useful in showing the changes and advances made in just 2 years.

Fontana, John. "Pragmatic Plan Eases Security Fears." CommunicationsWeek. Oct 96: pp

Gerwig, Kate. "The Encryption Debate: What Price for Your Online Privacy?" Net Guide. November 1996: 98+.

Hunt, Craig. TCP/IP Network Administration. Sebastopol, California: O'Reilly & Associates, 1992.

Hughes, Larry. Actually Useful Internet Security Techniques. Indianapolis: New Riders, 1995.

Johnson, Phillip. "History of the Internet" Dec 30, 1996:
Last visited April 4, 1997
http://dragonfire.net/~Flux/ihistory.html

Keizer,Gregg. "Online Money Matters." Computer Life. August 1996: 46+.

Langa, Fred. "Start." Windows Magazine. November 1996: 11.

Meade, Peter. "Spinning a web, It costs more than you think." America's Network. October 15, 1996: 21.

Michaelides, Phyllis "John Deere Harvests The Benefits Of Information Integration With An Intranet".
Last visited on April 4, 1997
http://home.netscape.com/comprod/at_work/customer_profiles/john_deere.html

Moeller, M. and Kerstetter, J. "Encryption Technology SET for Final Testing." PCWEEK. Jan 6, 97: pp 1+

Netscape.com
Last updated April 3, 1997
Last visited April 4, 1997
http://home.netscape.com/comprod/server_central/query/idg/index.html

Spectacular "Spectacular growth for the Internet" ZD Internet Magazine. Dec. 96: 32.

"Suitespot Delivers The Full Service Intranet"
Last visited on April,5 1997
http://home.netscape.com/comprod/server_central/index.html

Wahsburn, K. and Evans, J.T. TCP/IP Running a Successful Network. Workingham, England: Addison-Wesley, 1993.

Works Referenced, But Not Cited

Magazines for Further Reference

Elgan, Mike. "Love The Web? Now You Can Build Your Own." Windows Magazine June 1996: 47+.

Morgan, Cynthia. "Software Reviews." Windows Magazine June 1996: 113+.

Morgan, Cynthia. "What's Hot." Windows Magazine June 1996: 82+.

Heller, Martin. "Getting To Know You." Windows Magazine June 1996: 226+.

Heller, Martin. "Web Server Programming: The Final Frontier." Windows Magazine June 1996: 273+.

Schwerin, Rich. "Web Essentials." PC Computing August 1996: 320+.
A list of Web Tools with short descriptions

Blankenhorn, Dana. "Special Intranet Report." NetGuide Magazine. October 1996: 82+.

Luning, Jon. "Getting There: Software to Launch You on the Web." NetGuide Magazine. October 1996: 117+.

Tadjer, Rivka. "Not All Web Sites Are Created Equal." NetGuide Magazine. October 1996: 143+.

Cataldo, Beth. "Netscape Delivers New Navigator." Computer Life. July 1996: 23.

Cooper, Tom. "Intranet Report: Security and ..." Net Guide. November 1996: 141+.

Rist, Oliver. "Groupware." Net Guide. November 1996: 153+.

Moeller, Michael. "Netscaped Crusaders." PC Week. Volume 13, Number 41. Oct 14 1996: 1+.

Moeller, Michael. "Netscape hooked on intranet." PC Week. Volume 13, Number 41. Oct 14 1996: 144.

vairous authors. PC Week. Volume 13, Number 40. October 7 1996: see reviews.
pg 27 Back Office

Patz, Joel. "PLUG into the OFFICE of the FUTURE." Windows Magazine. November 1996: 194+.

Tackett, Ram. "Server Suite dreams." Windows Magazine. November 1996: 272+.

Ruley, John D. "Let the Buyer Beware." Windows Magazine. November 1996: 279+.

Callaway, Erin. "Assembly Required." PCWEEK. October 21, 1996: 51+.

Camaford, Christine. "GOING ON AN INTRANET SHOPPING SPREE." PCWEEK. Octonber 21, 1996: 60.

Moeller, Michael. "HP's 'Montana' rounds up TP workflow for business." PCWEEK. October 28, 1996: 51+.

WEB SITES FOR FURTHER REFERENCE

http://home.netscape.com/comprod/announce/faq_enter.html
FAQ's on Enterprise 3.0 new for 1997 - new features look good for security

http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html
got this tip from Martin Heller "Web Server Programming"

http://www.microsoft.com/intdev/
this site has info on Microsoft's ISAPI's - the replacement for cgi's

http://www.microsoft.com/intdev/security/
The Microsoft Internet Security Framework (MISF)

http://www.microsoft.com/intdev/security/

http://www.netscape.com/newsref/std/server_api.htm.

http://www.lochnet.com/client/smart/intranet.htm

Complete Intranet Resource - Intranet Reference Site
Nice cite with discussion group, news, book listing, white pages, faq's, and job listings for folks with Intranet experience.

http://www.webcom.com/wordmark/sem_1.html
Intranet training online, you can buy the book or subscribe, the samples have a lot to offer in themselves

http://www.cnet.com/Content/Features/Howto/Design/
Elements of a Web Design
A little tutorial, well done, broken down into topics like graphics and references for software.

http://www.lochnet.com/client/smart/ifaq.htm#6
FAQ's on building an Intranet, questions range from what is an Intranet to how to build a server without an IP connection on a Novell Lan.