GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

SANS Security Essentials
GSEC Practical Assignment Version 1.4b

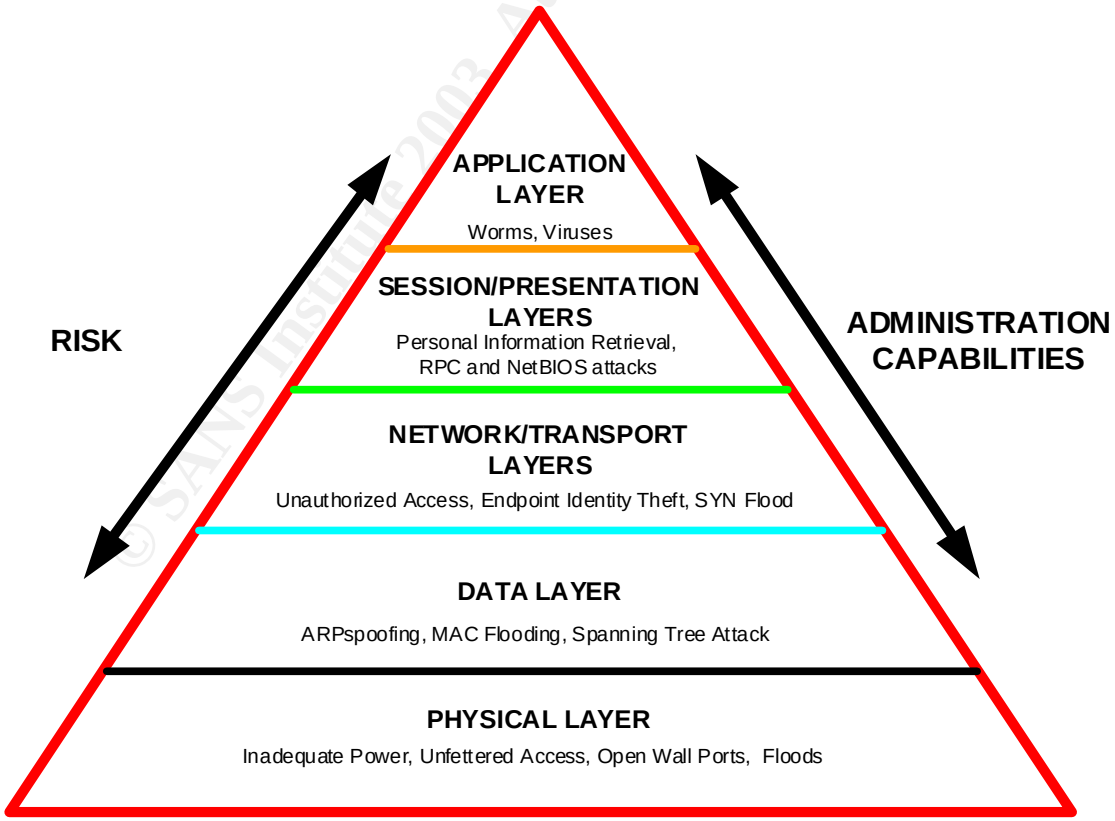
OSI Defense in Depth to Increase Application Security

Kim Holl

Abstract

"OSI Defense in Depth to Increase Application Security" explains how enterprise applications are at risk and sets forth one approach by which Information Technology (IT) managers can mitigate these risks. In the OSI model approach, security is addressed at each layer of the OSI model, shown below. By comparing in depth the OSI model with the concept of Application Security by Defense, IT managers better understand that securing enterprise application is more than authentication, encryption, OS hardening, etc. At each level of the OSI model there are security vulnerabilities and, therefore, security prevention measures that can be taken to ensure that enterprise applications are protected. Importantly, the capability IT managers have to mitigate risks decreases at the higher OSI model layers.

Figure: OSI Pyramid



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

One reason IT managers have less power to protect applications at the higher OSI layers is that at these higher layers, developers have much more influence over security measures. However, security measures are possible at every OSI layer. Addressing security threats at every layer reduces the risk of enterprise application compromise or Denial of Service. Examples of vulnerabilities and solutions at each layer provide a better understanding of the topics presented.

The OSI Physical layer represents physical application security, which includes access control, power, fire, water, and backups. Many of the threats to security at the Physical layer cause a Denial of Service (DoS) of the enterprise application, making the application unavailable to enterprise users.

The Data, or Data Link, layer of the OSI model encompasses switch security topics such as ARP spoofing, MAC flooding and spanning tree attacks. Simple configuration changes to the network switch can help protect enterprise applications from Data layer attacks.

The Network and Transport layers of the OSI model are where the most common security precautions take place — this layer is where routers and firewalls are implemented. Threats that occur at this level are unauthorized retrieval of endpoint identity, unauthorized access to internal systems, SYN flood attacks and "ping of death." Implementing Network Address Translation, Access Control Lists, and firewall technologies mitigates these risks.

The Session and Presentation layers are the lower layers of the Application Set of the OSI model. At these layers the IT manager's ability to mitigate application security risk begins to diminish as developers take a bigger role in protecting applications. IT managers can prevent unauthorized login/password accesses and unauthorized data accesses, which are common attacks at these layers, by using encryption and authentication methods.

The Application layer is the final layer of the Application Set and the OSI model. Many security protection methods are the responsibility of the programmer at this layer. Backdoor attacks occur at this level and it is the programmer's responsibility to close those doors. IT managers can use access control methods described to assist in preventing backdoor attacks; also, IT managers can set up tools such as virus scanners, WebInspect, and intrusion detection devices to help prevent compromise of enterprise applications.

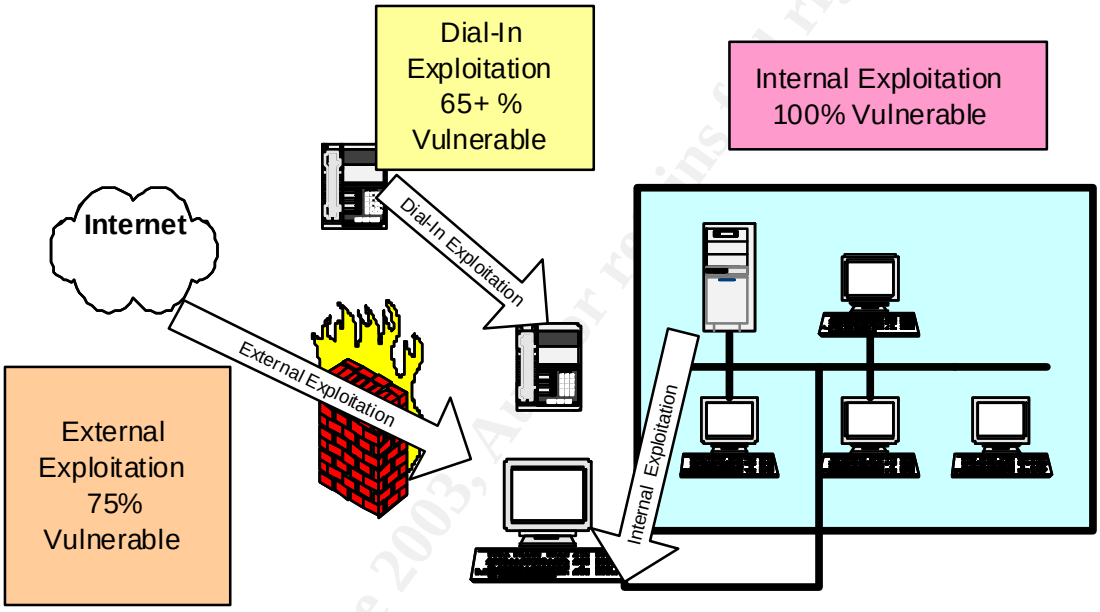
This paper presents some ideas on how to better protect enterprise applications. Implementing security at each and every layer of the OSI model cannot prevent any and all unauthorized access to enterprise applications. The more layers that are protected, the lower the probability an intruder will access valuable information. Each IT manager must determine how cost-effective network protective measures are.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Introduction

Many Information Technology (IT) managers believe application security requires merely installing a perimeter firewall, or taking a few configuration measures to prevent applications or operating systems from being attacked. This is a dangerous fallacy. Instead, application security can be likened to a Tootsie Pop® in that it is hard on the outside but soft and chewy on the inside. Firewalls and router access filters, though important security measures, cannot by themselves protect an enterprise from attacks on application security. Based on statistics from Cisco Systems, the idea that most attacks come from the Internet is a serious misconception.

Figure 1: Attack Vulnerability [1]



As depicted in Figure 1 above, enterprises are 100% vulnerable to inside attacks; in addition, Cisco's statistics show enterprises are 65–75 % vulnerable to attack from outsiders.[1] Insider exploitation can originate from local networks, local systems, and/or malicious code. These attacks may be accidental or malicious, and they can come from employees, visitors, or contractors.

In approaching an effective application security scheme, the first question that should be addressed is: what is a security breach or threat? A security breach occurs when a compromise or denial of service (DoS) takes place due to an accidental or malicious exploit of vulnerability. Attacks may occur when outsiders gain access to the internal network via the external access points or remote dial-in; when insiders gain unauthorized access to network devices or systems; or when malicious code in the form of a virus or a worm comprises system integrity. A security threat, then, can be thought of as any condition or event that makes a security breach more likely.

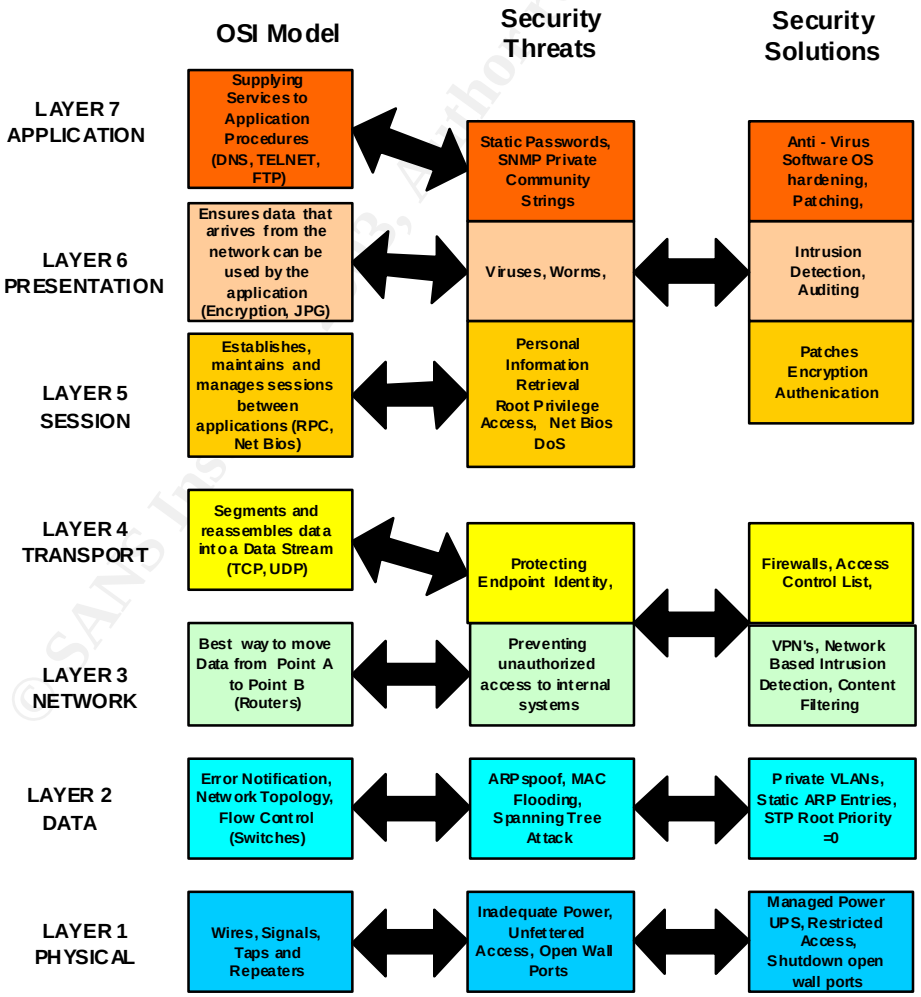
The foundation for protection and attack of application security has three building blocks: Confidentiality, Integrity, and Availability (CIA).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- **Confidentiality** – Making sure no unauthorized visibility of information you are sending or that is on a server
- **Integrity** – Assurance the information on the network or server has not been compromised or altered (beyond reproach)
- **Availability** – The information can be accessed when required

Most IT Managers have a working knowledge of the OSI Model. "The OSI (Open Systems Interconnection) Model is a conceptual model defined by the International Organization for Standardization (ISO), describing how any combination of devices can be "connected for the purpose of network communication and troubleshooting."[2] Comparing the OSI model's layers to the levels of application security will shed light on application vulnerabilities. This paper illustrates examples of security breaches and possible solutions at each OSI layer to provide a better understanding of how this affects application security. The OSI model is a hierarchical functional representation consisting of seven layers, with the Application layer at the top and the Physical layer at the bottom (see Figure 2).

Figure 2: OSI Model as It Relates to Security



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Layer 1 (Physical Security)

The Physical layer of the OSI model is responsible for converting data packets from the Data Link layer (Layer 2) into electrical signals. The Physical layer consists of the actual physical connections to and within the network, including wiring, devices used to connect the NIC to the wiring, the signaling involved in transmitting and receiving data, and the ability to detect signaling errors on the network media. The OSI Physical layer comprises the enterprise's physical and site security concerns, which includes all these aspects:

- Access Control
- Power
- Environment
- Smoke & Fire
- Water
- Backups

Access control is in place when only authorized personnel are allowed physical access to computers and the network. This concept includes permitting only authorized personnel to possess logins and passwords and closing unmanaged wall ports which, if open, could provide unauthorized persons access to the enterprise network. An unauthorized person need only connect a laptop with Sniffer software to an open wall port to obtain proprietary information, including trade secrets and customer data, or gain access to mission-critical applications. This is why mission critical systems should be kept behind locked doors to prevent access. Physical security also involves keeping hardware (particularly laptop computers) from being stolen. Closing open ports, locking doors, using surveillance monitors, restricting access to critical servers, and using strong passwords can prevent many common attacks.

While unauthorized users are an obvious security threat, anything that can cause a denial of service (DoS) must be considered an additional threat. That is why the loss of electric power is considered a vulnerability. Hardware failures are much more likely in systems subjected to power loss or power spikes. Without regular backups, disk drive failure can cause data loss, or at least a DoS. An uninterruptible power supply (UPS) or surge protector can help prevent such losses at minimal cost. A managed UPS requires its own security, because an unauthorized person who gains access to it using remote management tools can shut down attached systems.

Environmental issues at the Physical layer include fire, smoke, water, food, and drinks; all are physical security threats that can cause a DoS incident. Poor control over environmental factors such as temperature, humidity, dust, and ventilation can cause frequent failures, lower Mean Time Between Failure (MTBF) and DoS. Use of climate-controlled rooms with proper dust filters and ventilation can significantly reduce the incidence of hardware failure. Smoke and fire damage to systems can be mitigated or avoided with appropriate fire extinguishers and automated fire suppression systems installed in rooms containing mission-critical applications. Proper sensors, if installed, can also help to minimize water damage. Finally, food and drink should be prohibited in rooms containing mission critical hardware, to lower the risk of spills.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

When applications and/or operating systems have been compromised, lacking backups can have devastating results. Backups should be tested on a regular basis to assure their integrity. Ideally, backup media should be taken off-site and stored in an environmentally controlled space so they are safer, readily available in case of catastrophe at the enterprise computing site.

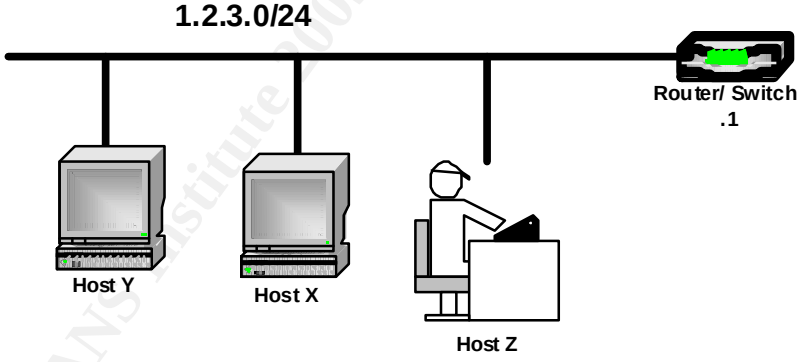
Layer 2 (Switch Security)

OSI Layer 2, the Data Link layer, is primarily concerned with physical addressing, line discipline, network topology, error notification, ordered delivery of frames, and flow control. Devices such as switches and bridges work at this level. Security threats that may occur at this level are the following:

- Gratuitous ARPs or ARP spoof
- MAC flooding
- Spanning tree attack

Gratuitous ARPs/ARP spoofing can be used to maliciously take over a machine's IP address. ARP spoofing is targeted to fool a switch into forwarding packets to a device in a different VLAN by sending ARP packets containing appropriately forged identities. The security vulnerability occurs at the lower layer but affects upper level security without the upper layer knowing about it. Figure 3, below, depicts a malicious user attempting to gain access to traffic from Host X and Y.

Figure 3 ARP Spoofing [3]



To gain control of the data flow, Host Z sends gratuitous ARP replies, telling all the network devices that he is 1.2.3.1 (router/switch) and sending his MAC address. Since ARP replies are broadcast, all hosts on the same Layer 2 subnet see and accept the gratuitous ARP. If Host Z is more persistent than the actual router/switch in asserting its identity, Host X and Y will believe that Host Z is the router/switch. Host Z has effectively inserted himself as a man in the middle (MiM attack), and Hosts X and Y will send Host Z their IP traffic. [3]

To prevent these attacks, some switches and routers can be configured to ignore gratuitous ARPs. Cisco switches offer Edge VLAN segregation (Private VLANs) and ARP inspection to mitigate this threat.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

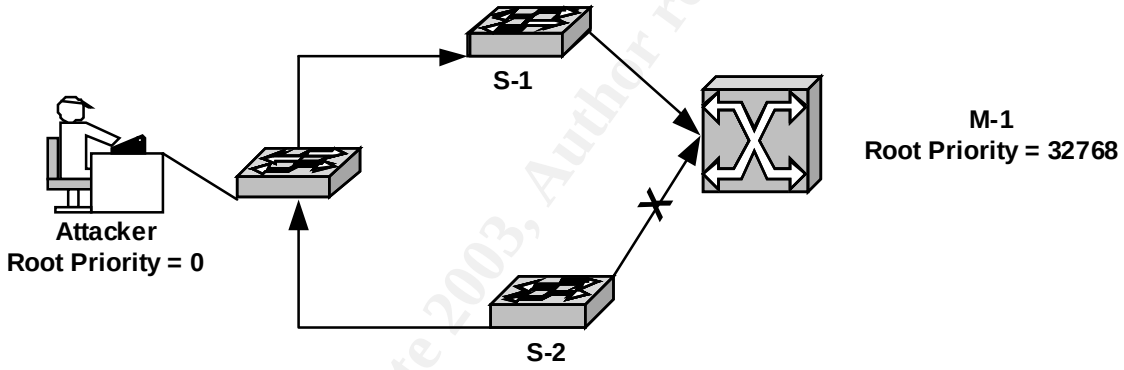
MAC Flooding occurs when the hardware-learning table of a switch reaches capacity and floods onto the VLAN. Many tables reach maximum capacity at 131,052 MAC entries.[4] A malicious user can sniff (Dsniff) the flooded traffic to obtain network information such as passwords. Some switches, i.e., Cisco switches, have a port option that prevents such flooding:

```
set port security 3/21 enable age 10 maximum 5 violation restrict
```

The "restrict" parameter will fail under a load and cause the port to shutdown. The Dsniff (macof) utility can generate "155,000" [4] MAC entries and therefore cause MAC flooding.

Spanning tree attacks occur when an attacker's computer inserts itself into a data stream and causes a DoS attack. A spanning tree attack begins with a physical attack by a malicious user who inserts an unauthorized switch between two existing network switches. The attacker assigns a lower root priority to the invading switch than that of the master or root switch (M-1), as depicted in Figure 4 below.

Figure 4: Spanning Tree Attack [4]



Assigning the lower root priority causes the network connection between Switch 2 (S-2) and M-1 to be dropped. The attacker's switch thereby becomes the root switch, and the attacker gains full access to data transmitted between S-2 and the rest of the network. One-way of mitigating this problem is configure a network's root switch with Root Priority = 0. (The attacker must have physical access to the network for this kind of DoS attack to succeed.)

The Data layer security threats discussed in this section are only a few examples of Data layer vulnerabilities. Other examples not discussed include the following:

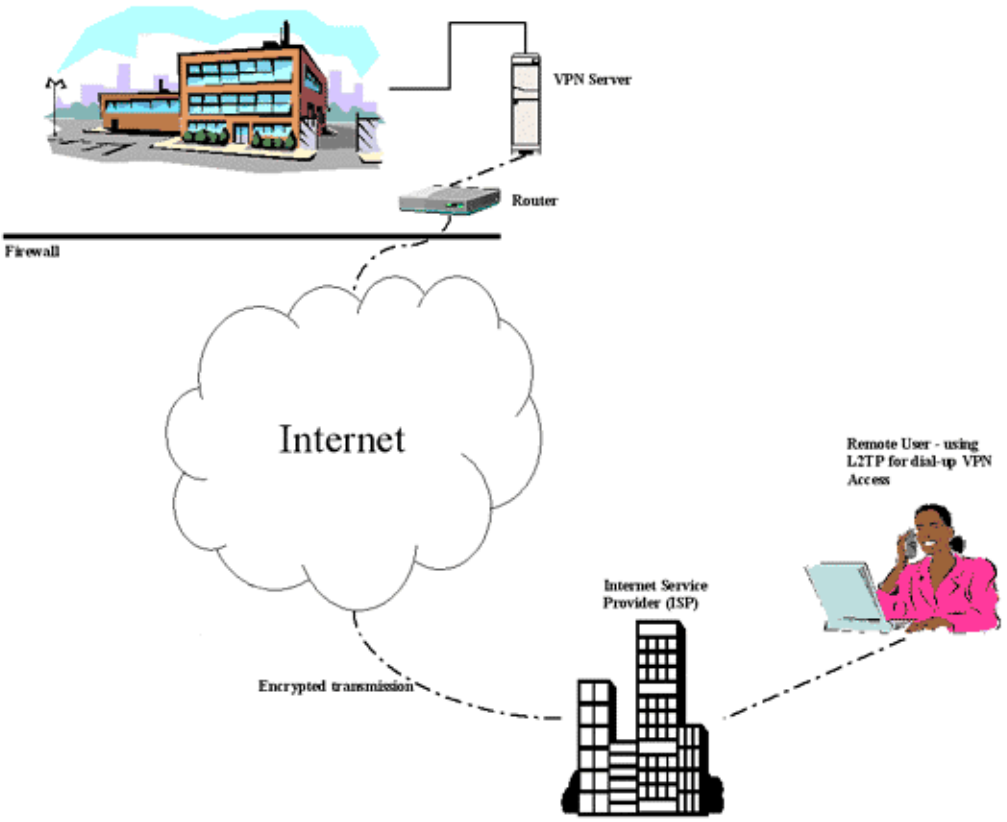
- 802.1Q and ISL tagging attack
- Double-encapsulated 802.1Q/nested VLAN attack
- Private VLAN attack
- Multicast brute force attack
- Random frame stress attack

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The link below can provide further descriptions of the above threats: http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

Tunneling and Virtual Private Networks (Figure 5) are also implicated in OSI Layer 2. Tunneling is a method using the Internet framework to transfer data from one network to another. Tunneling encapsulates packets in a base protocol format within some other protocol over the Internet. Virtual Private Networks (VPN) encapsulates packets within an IP packet. Virtual Private Networks exist on OSI Layers 2 and 3 and are dependent on what VPN protocols are used. OSI Layer 5 also supports a VPN protocol (Figure 5). VPNs work hard to prevent hackers from gaining access to data crossing the Internet.

Figure 5 VPN Connection [5]



At the Data layer of the OSI model, Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP) are implemented. PPTP is popular because Microsoft was one of the developers of this protocol and PPTP is used on their OS platforms. PPTP supports non-IP standards but does not support a single standard that will work across platforms. L2TP was created by Cisco to improve upon PPTP. L2TP also supports non-IP standards but includes Frame Relay, ATM, and Sonet. Like PPTP, L2TP does not support a single standard. IPsec VPN protocol is more popular with less expensive routers and will be discussed further in the next section. Because the appliances normally used to implement VPNs are routers and firewalls, further discussion will occur in the next section under Layer 3 (Router/Firewall Security).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Layers 3–4 (Router/Firewall Security)

Layer 3, otherwise known as the Network layer, and Layer 4, otherwise known as the Transport layer, are the most common forms of application/network security. In these layers, firewalls and router Access Control Lists (ACLs) can be found. The Network layer of the OSI model is where routing, layer 3 switching and IP addressing are defined. At this layer traffic is passed between network devices that are not on the same segment. At the Transport layer, data is divided into packets and then reassembled at the final destination. Data flow control of and error checking are also provided at this level.

TCP and UDP occur at the Transport layer. Security threats that occur at these levels include the following:

- Endpoint identification
- Unauthorized Internet access
- SYN flood
- Ping of death

It's easy to forget when connecting a device to the Internet that the Internet is also connected to that device. That is why protecting endpoint identity is of great importance in protecting today's applications. IP addressing and subnetting are important methods; mission critical applications should also be protected by private IP addressing (RFC 1918).

For example, compare the following "public" IP addresses to their "private" equivalents:

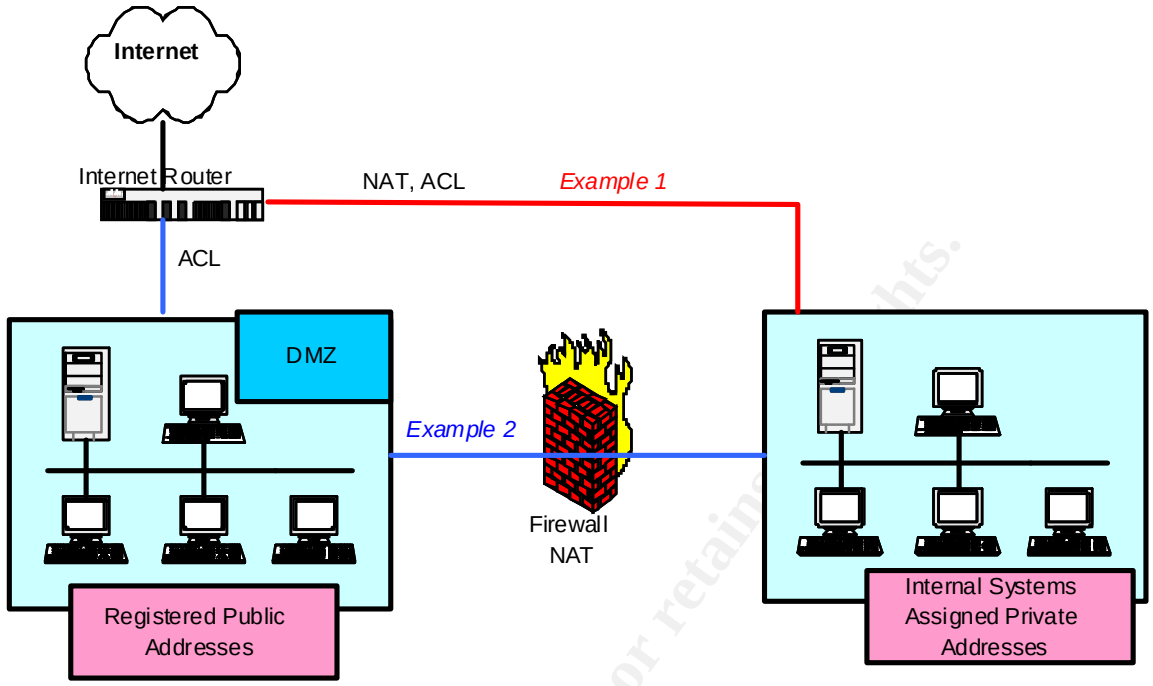
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Application private addresses are protected via Network Address Translation (NAT), firewalls, and router Access Control Lists (ACLs). Figure 6, below, shows two examples of how routers and firewalls can protect internal private addresses from Internet intrusion. Example 1 (red network connection) shows the internal systems protected by a router with NAT and ACL.

The fundamental purpose of NAT is to hide private addresses from the Internet. To the rest of the world it appears that there is only one address associated with an enterprise network. NAT requires that connections needing to discriminate between private addresses originate from the internal network. That is why networks using NAT usually have systems located in a demilitarized zone (DMZ) that allow outside clients to establish connections for FTP or Web services without giving access to the internal network. Firewalls and routers have NAT capabilities; these services can be made available to internal systems by either creating tunnels or opening ports in firewalls and routers. Open tunnel or port access does open the internal network to attack and should be carefully considered before being implemented.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 6: Protecting Internal Private Addresses



SYN flood and "ping of death" attacks target the TCP/IP stack. Both of these attacks cause DoS by causing systems to crash or become unavailable to other connections. SYN flood sends a large number of TCP connection requests without sending anything else, making systems unavailable. Pings of death overrun the size limits of TCP/IP stacks by sending ICMP pings of 65,535 bytes, causing systems to crash or reboot.

Using ACL and firewalls can prevent unauthorized Internet access. There are four types of ACLs: Standard, Extended, Reflexive and Network Base Access Recognition (NBAR).

- **Standard** - Uses only the source IP addresses as a network filter.
- **Extended** – Uses logical address, protocol field, and port field as network filters.
- **Reflexive**- IP Packet filters based on Session layer information. This filter is used to allow outbound traffic and limit inbound traffic based on sessions originating from the inside network.
- **NBAR** – Uses Packet Description Language Modules (PDLMs) to filter applications (see Figure 7 for a list of applications that can be filtered). By using a PDLM, created by Cisco Systems, certain applications can be filter via an Access List. Further information on NBAR can be found at the URL http://www.cisco.com/warp/public/cc/so/neso/ienesv/cxne/nbar_ov.htm

Standard, Extended, Reflexive and NBAR Access Control Lists are all implemented at the network infrastructure level.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 7: Applications Filterable with PDLMs [6]

citrix	http	nntp	ssh	*streamwork*
cuseeme	imap	notes	smtp	syslog
custom	irc	novadigm	snmp	telnet
exchange	kerberos	pcanywhere	socks	secure-telnet
fasttrack	idap	pop3	sqlserver	tftp
ftp	napster	realaudio	sqlnet	vdolive
gnutella	netshos	rcmd	sunrpc	xwindows

Figure 6 shows ACLs being used in both Examples 1 and 2. Adding ACLs to the router can increase security to the internal network by allowing address, port, protocol, and application filtering on both inbound and outbound ports.

Outbound filters can be just as important as inbound filters. As mentioned earlier, when an internal user is connected to the Internet, the Internet is connected to your internal network. These connections create vulnerabilities; for example, high bandwidth applications such as peer-to-peer applications (Napster, KaZaa, Morpheus, Grokster, etc.) can occupy enough bandwidth to cause a DoS attack.

The most common topology example shows an Internet router connected to a DMZ. A DMZ is an area between the Internet router and the firewall that allows public access to systems such as Web and FTP servers while prohibiting public access to the private internal network. Standard, Extended, and NBAR ACLs can all be used to protect the DMZ.

A firewall blocks access to the internal network in Example 2 (Figure 6, above). A firewall has three main functions with respect to the internal network:

- Detect
- Reject
- Protect

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Firewalls are composed of rules that either allow or deny traffic. If a packet does not meet any of the "accept" rules criteria it is dropped, or "denied." Firewalls also have NAT capabilities similar to those of routers. There are three categories of firewalls:

- **Proxy/Application Gateway** – Works at layers 3 through 7 of the OSI model. Along with providing NAT and ACL, this category of firewall addresses attacks that manipulate application behavior on browsers and through HyperText Transfer Protocol (HTTP). Raptor™ and Sidewinder™ firewalls are examples of this type of firewall.
- **Packet Filter** – Relies on Destination Ports to filter traffic and is similar to a router's Access Control List. These firewalls are fast but are not as secure as other firewall types because they do not check data content. An example of this sort of firewall is the BlackIce™ product.
- **Stateful Inspection** - Sometimes known as hardware firewalls, these firewalls operate at OSI layers 3 and 4. Since every protocol has a state this type of firewall is more secure than packet filtering. Cisco's PIX™ firewall and router with firewall IOS are examples of this type of firewall.

A firewall is an excellent way to enforce corporate security policies, but none is perfect and all can be compromised. Network Computing commissioned a survey that compared features of popular software firewalls against those of popular hardware firewalls. The software firewalls chosen were Axent Technologies Raptor™ Firewall, and Check Point Software Technologies FireWall-1™. Cisco Systems PIX and NetScreen Technologies' NetScreen-100™ were the hardware firewalls chosen for the evaluation. Network Computing's survey found that the software firewalls supported more security features than the hardware firewalls: virus scanning, intrusion detection, and content monitoring tools were among the additional features found in the software firewalls. The survey also found the software firewalls supported more dynamic protocols than their hardware counterparts. Hardware firewalls, on the other hand, performed better within their more limited parameters. And a software firewall has the burden of its underlying operating system, which must be hardened and maintained against attacks.

Therefore, choosing between a software and hardware firewall requires evaluating needed features. If the additional features of the software firewalls are not required by the enterprise then a hardware firewall should be considered because of its better performance and because a hardware firewall does not require a separate server and operating system to run.

As discussed earlier, VPNs exist at OSI Layers 2, 3, and 5. The IP Security protocol (IPSec) is probably the most popular VPN protocol; its main functions are to authenticate and encrypt. IPSec prevents MiM attacks by hiding internal IP addresses. Normally this protocol is configured on routers and firewalls and protects data traversing the Internet. Note that, when allowing a VPN connection to a corporate network, the security of the VPN is only as good as the security of the remote site. If there is an attack upon the remote site's network, the VPN connection into your corporate location can be compromised.

Because the Internet is unsecured and TCP/IP (OSI Layer 3 protocol) provides no security, Netscape developed the Secure Socket Layer (SSL) protocol, since adopted by IETF as a standard for Transport Layer Security (TLS) and now known as SSL-TLS Secure. Many financial institutions to encrypt data crossing the Internet use these protocols. SSL and TLS are

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

not TCP/IP dependent and can layer on top of any transport protocol. They can run under application protocols such as HTTP, FTP and TELNET. SSL and TLS provide all three of the critical "CIA" security components: confidentiality, authentication, and integrity. These protocols give protection against message tampering, eavesdropping, and spoofing.

Passwords are the most common form of authentication and a common security vulnerability. A "dictionary attack" is defined as the attempt to login to a system by using all possible passwords until the correct one is found. SSL prevents eavesdropping of communication between a client and a server by encrypting passwords. SSL encryption relies on public and private keys. The Web server has the private key to encrypt and decrypt secure messages. The client computer has the public key, which has the installed certificate for that Web server. When the public key is installed, the user can encrypt messages to, and decrypt messages received from the Web Server. Because SSL ciphers uses large key spaces the time to resolve a password becomes long. Therefore reducing the risk that a password is compromised. "SSL is not vulnerable to MiM type attacks as long as the server uses a private key to decrypt the master key and the server has a certificate."[7]

TLS is very much like SSL with the exception there is an interface between the handshaking portion and the record layer. The changes allowed for more ways to authenticate and to minimize network activity. Like all Security efforts there a weaknesses in these protocols and hackers can program to attack their vulnerabilities. TSL appears to have fewer security breeches than SSL and it looks like SSL-TLS Secure improves upon them both.

Layer 5–6 (Encryption/Authentication)

In the OSI model, Layers 5–7 are known as the Application Set. This section will address the Session and Presentation layers as they relate to security. The Session layer (Layer 5) is responsible for creating, managing, and terminating sessions between applications and overseeing data exchange between the Presentation layer (Layer 6) and Transport layer (Layer 4). Login passwords, the exchange of user IDs, and accounting operations can all be handled at the Session layer. The Presentation layer defines how data is formatted, presented, encoded, and converted for use by software at the Application layer. Security threats that occur at these layers involve:

- Unauthorized Login/Password Access
- Unauthorized Personal Data Access
- RPC & NetBIOS Attacks

Web browser "cookies," data files stored on the user's computer by a Web site that contain information about that user, are implemented at these layers. Cookies provide a mechanism by which user movements can be tracked on the issuing Web site. They usually contain a site username and password, but they can contain other personal information such as Social Security numbers or credit card numbers. The lifespan of the cookie is determined by the issuing Web site, but it's not always clear how long a Web site retains personal information. A session cookie, if enabled, can prevent a Web site from retaining personal information. One reason SSL and TSL were created was to encrypt exactly this information.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Encryption is one method of hiding transmitted login and data information. Even though encryption is normally thought of as occurring at the Network layer, it is not always end-to-end. Network layer encryption ends at the firewall or router. Encryption can occur both at the Session and Presentation layers. The Session layer is where peer-to-peer dialogue occurs and therefore peer-to-peer encryption can occur also. End-to-end encryption techniques supported at this layer such as DES, 3DES, AT&T's Encrypted Session Manager™ (ESM), and Authenticated Telnet. SOCKS network security protocol exists at the Session layer and is a VPN protocol. This protocol allows Network Administrators to limit VPN connections to some applications.

Authentication is any method used to ascertain whether someone or something is who or what they say they are. Many methods have been developed to authenticate a user's access to a system or a network. Kerberos is an authentication protocol that uses secret-key cryptography to perform strong authentication. Other authentication and accounting mechanisms are Terminal Access Controller Access Control System (TACACS) and RADIUS. TACACS, a security application created by Cisco, provides centralized validation of users attempting to gain access to a router or network server. RADIUS is a similar service that provides remote authentication for dial in user services.

Remote Procedure Call (RPC) and NetBIOS are common protocols at the Session layer. These protocols also are often subject to attack. If an attacker can access an RPCBIND/Portmapper server, that server can provide access to a list of RPC services running on the machine. This will then allow the machine to become more vulnerable for attack. Another form of RPC attack was the "Snort" WINNT RPC DoS. The "Snort" attack causes 100% CPU usage, which results in DoS. Both attacks are resolved by applying vendor patches. NetBIOS attacks are often DoS attacks. Like RPC attacks, they can be resolved by applying vendor patches. Use of proxy firewalls and intrusion detection devices can prevent many RPC and NetBIOS attacks.

Layer 7 (Application Security)

The Application layer supplies services to application procedures that are located outside the OSI layer. It appears that most of the security breaches occur at the Application layer: a survey by Gartner showed 70% of successful attacks occurred at the Application layer. In 2000 the FBI reported that hackers at the Application layer caused over $300 million in damages.[8] The company @stake determined that 47% of application security flaws fall into these categories:[9]

- Authentication/Access Control
- Cryptographic Algorithm
- Input Validation
- Parameter/Data Manipulation
- Sensitive Data Handling
- Session Management

The @stake report showed that most application security breaches result from authentication and access control failures. IT managers can reduce the exposure of application level vulnerabilities by implementing the security methods discussed earlier. Many application vulnerabilities are

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

accidentally built into the application early in the design process and are best addressed while design is ongoing. IT managers have little control over preventing these vulnerabilities. The developers of enterprise applications should address data manipulation, data handling, and session management protections as well as cryptographic algorithms and input validation.

Because operating systems, Web, email, and SNMP applications are common to most enterprises, the most important application security issues relate to these applications. Vendors of operating systems such as Microsoft Windows®, Macintosh® OS, Linux, etc. are continually hardening their code to prevent attack from hackers. These attacks may come from "back doors" accidentally left in the operating systems or worms or viruses with the power to delete files or alter system files. Vendors are continually providing software patches to protect operating systems from these vulnerabilities. However, the need to frequently load software patches can be difficult to fully meet, and there is always the risk a patch will be published too late. That is why other forms of security protection may be required.

Web application technologies (i.e., HTTP, HTML, JAVA, ISS, etc.) have become standard avenues for today's businesses to provide products, services, and information to their customers. The impact of this technology cannot be realized until users have confidence that these Internet channels are secure. Common vulnerabilities on Web pages are the following:[10]

- Search engines that repeat back the search keyword entered.
- Error messages that repeat back the string containing the error.
- Forms filled out that repeat back the user's inputs.
- Web message boards that allow users to post their own messages.

These vulnerabilities are also known as cross-site scripting. A hacker to execute malicious script in a clients Web browser can use cross-site scripting. Any Web page that renders dynamic HTML based on content that users submit is vulnerable. A common real world example of cross-site scripting is:

> A user receives an email with a link to an online banking site where the user has an account. The email explains that the user is eligible to win 200 dollars as part of a special promotion and should verify the account's balance to check the result. The user clicks the link and visits the bank's login page, logs in, checks the (unchanged) account balance, logs off, and quickly forgets the entire matter, equating it with other "You may already be a winner!" type messages. What has not been forgotten, though, is the user's login information, stolen and recovered by the hacker who sent the email in the first place. With one email, the hacker now has complete access to a user's online bank account, including the ability to transfer funds electronically. [10]

To eliminate these types of vulnerabilities, developers can provide filtering on user-supplied data. Developers or network administrators can use a utility called WebInspect™ to test their Web application for these types of vulnerabilities. By running WebInspect, these types of vulnerabilities can be determined and correct resolution path can therefore proceed. Users can reduce the risk by disabling scripting languages in their Web browsers, though doing this does limit some browser functionality.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Electronic mail (email) has become one of the most popular forms of person-to-person communication, but it is only completely secure if encrypted. Many companies filter email entering and exiting the network, looking for a sender or receiver of confidential information or email with adult content. Web-based email can be vulnerable because account information from the URL can theoretically be passed to a third party server. Email is also the most common way that computer viruses and worms are introduced into internal networks. These usually come in the form of an attachment to the delivered email.

A virus is a program loaded and run on a computer without its user's knowledge. Viruses can replicate themselves: a simple virus that makes copies of itself over and over again is dangerous because it will quickly fill all available memory and bring the system to a halt. Some viruses are capable of transmitting themselves across networks and bypassing security systems.

A worm is a virus that can spread automatically from one computer to the next without user intervention. It is a separate entity that does not attach itself to other program or files. Viruses, in contrast, normally have to be executed by an unwitting user; for an example, the user who receives an unexpected email might click on an attached file, which then executes the virus.

Virus scanners provide a lot of protection from virus and worm attacks. Many mail servers and personal computers use products from vendors like McAfee or Trend Micro that are updated on a regular basis with pattern files to prevent such attacks. All IT managers should seriously consider implementing this form of protection.

Simple Network Management Protocol (SNMP) is a group of protocols used to manage network devices and systems. SNMP contains two components: a manager and an agent. The manager is the console where management functions take place; the agent provides the interface into the device that is being managed. Many network administrators use SNMP to manage devices on their network. Users of SNMP need to be aware of some of the known vulnerabilities associated with this protocol:

- Buffer overflows (crash, lock-up, reboot devices, overwrite application or operating system files, allow unauthorized access)
- Denials of service (past known issues on Cisco IOS, wireless access points, Windows NT/2000, Linux, and HP JetDirect™)

SNMP can become more secure if inbound and outbound filtering is implemented on perimeter routers and firewalls controlling SNMP, ICMP, tracert, and echo traffic. Avoid easily guessed and default community strings (i.e., "public"), because community strings are sent in clear text. Also, isolating SNMP traffic by VLAN will help keep SNMP traffic more secure.

Application/proxy firewalls discussed earlier in this document can be used to block SNMP traffic. Application/proxy firewalls work at Layers 3–7 and are usually packaged with other security tools such as intrusion detection devices, virus scanners, and auditing software. Intrusion detection devices are reactive devices that notify IT managers when an attack is taking place. There are host and network based intrusion detection systems (IDS). The host IDS monitor's

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

malicious activities on a specific host. A network IDS monitors network traffic. Personal firewalls are another means of protecting specific host devices.

Conclusion

Implementing security at each and every layer of the OSI model cannot prevent all unauthorized access to your enterprise applications. But the more layers that are protected, the lower the probability that an intruder will gain access to valuable information. Each IT manager must determine how cost-effective protective measures on the network are.

Unauthorized access to mission critical applications and data can cause disruption in corporate activity to the point of putting an enterprise out of business; this risk should be addressed. This paper outlines only a few examples of common threats and solutions. As shown, some solutions take very little time and money to implement but provide significant added security; for example, shutting down unused wall ports, properly configuring switches and routers, and employing shareware and freeware security tools (i.e., Hping Port Scanner, Tripwire IDS, etc.). Other means such as firewalls, routers with ACL software, and network intrusion detection devices cost more but may be required. To determine what security measures should be taken, a risk assessment should take place. Risk is based on this formula:

Risk = Threat × Vulnerability

In other words, system and network risk from any given threat is affected by both the degree of that threat and the vulnerability of the network to that threat. A risk assessment requires an analysis of what would happen if an attack occurred on key corporate resources and what the consequences of that attack would be. It may be cost effective to protect a system that contains corporate financial data or company secrets, but may not be effective to have the same security protection on a client machine. Before spending thousands of dollars on application security, a qualified security professional's risk assessment is an important tool for measuring need.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Quotations

[1] Cisco Systems. "Securing Mission-Critical Systems", Cisco Networking Forum: Technology Solutions Designs for you Evolving Network, Cisco Systems, 2002 PG 8.

[2] Lammle, Todd. Odem, Sean. Wallace, Kevin. CCNP Routing Study Guide, Sybex Inc., 2001, pg 489.

[3] Cisco Systems. "Securing Mission-Critical Systems", Cisco Networking Forum: Technology Solutions Designs for you Evolving Network, Cisco Systems, 2002 PG 23.

[4] Cisco Systems. "Securing Mission-Critical Systems", Cisco Networking Forum: Technology Solutions Designs for you Evolving Network, Cisco Systems, 2002 PG 28.

[5] Clayton, Sam. "What's VPN", SANS Info Sec Reading Room, March 13, 2001 URL http://www.sans.org/rr/encryption/VPN.php. (2/15/03).

[6] Cisco Systems. " Assuring Mission-Critical Data with Cisco QOS", Cisco Networking Forum: Technology Solutions Designs for you Evolving Network, Cisco Systems, 2001, PG 18.

[7] Erkomma, Liisa. " Secure Socket Layer and Transport Layer Security" University of Helsinki", March 15, 1998. URL http://www.tcm.hut.fi/Studies/Tik-110.350/1998/Essays/ssl.html (2/16/2003).

[8] Ben-Itzhak, Yuval, "Web Application Security—Then Next Evolution", DevX, 2003, URL http://www.devx.com/security/Articles/10236 (2/13/2003).

[9] Middleton, James. "Application Security 'in a grim state', Vnunet, 2/19/2002, URL http://www.vnunet.com/News/1129340 (2/20/2003).

[10] SPI Labs. "Cross-Site Scripting (Are your web applications vulnerable?)", SPI Dynamics Inc. 2002, pp. 3, 4. URL http://www.spidynamics.com/whitepapers/SPIcross-sitescripting.pdf (2/20/2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Wilson, Grant. "OSI Model Layers" Network Essentials Notes, August 6, 2001, URL http://www.geocities.com/SiliconValley/Monitor/3131/ne/osimodel.html (2/5/2003).

University of Chicago. Networking Services and Technologies, "NSC: Physical Security", University of Chicago, Networking Services and Technologies, 2001, URL http://security.uchicago.edu/docs/physicalsec.shtml (2/7/2003)

Horm, Simon. "IP Address Takeover" Ultra Monkey, July 30, 2002, URL http://www.ultramonkey.org/2.0.0/ip_address_takeover.html (2/6/2003).

Cisco Systems. "Virtual LAN Security Best Practices", Virtual LAN White Paper, URL http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml (2/7/2003).

Vicomsoft. "Network Address Translation FAQ", Vicomsoft Knowledge Share –Whitepapers, URL http://www.vicomsoft.com/knowledge/reference/nat.html (2/15/2003).

Fratto, Mike. " Ins and Outs of Firewalls", Network Computing, September 6, 1999, URL http://www.networkcomputing.com/1018/1018ws1.html (2/16/2003).

Erkomma, Liisa. " Secure Socket Layer and Transport Layer Security" University of Helsinki", March 15, 1998, URL http://www.tcm.hut.fi/Studies/Tik-110.350/1998/Essays/ssl.html (2/16/2003).

Blaze, Matt. Bellovin, Steven. "Session Layer Encryption", CiteSeer, 1995. URL http://citeseer.nj.nec.com/blaze95sessionlayer.html (2/17/2003).

Mitchell, Bradley. "Introduction to VPN", Computer Networking, URL http://compnetworking.about.com/library/weekly/aa010701d.htm (2/17/2003).

Clayton, Sam "What's VPN?" SANS Info Sec Reading Room, March 13, 2001. URL http://www.sans.org/rr/encryption/VPN.php. (2/15/2003).

Core, K. "Kerberos, The Network Authentication Protocol", Massachusetts Institute of Technology, January 28, 2003. URL http://web.mit.edu/kerberos/www/ (2/18/2003).

Clifford, Lynch. "A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Network Information Resources" Coalition of Network Information, April 14, 1998, URL http://www.cni.org/projects/authentication/authentication-wp.html (2/17/2003).

Cisco Systems. "Cisco Firewall (Configuring IP Access List)" URL http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml#reflexive (3/21/2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.