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

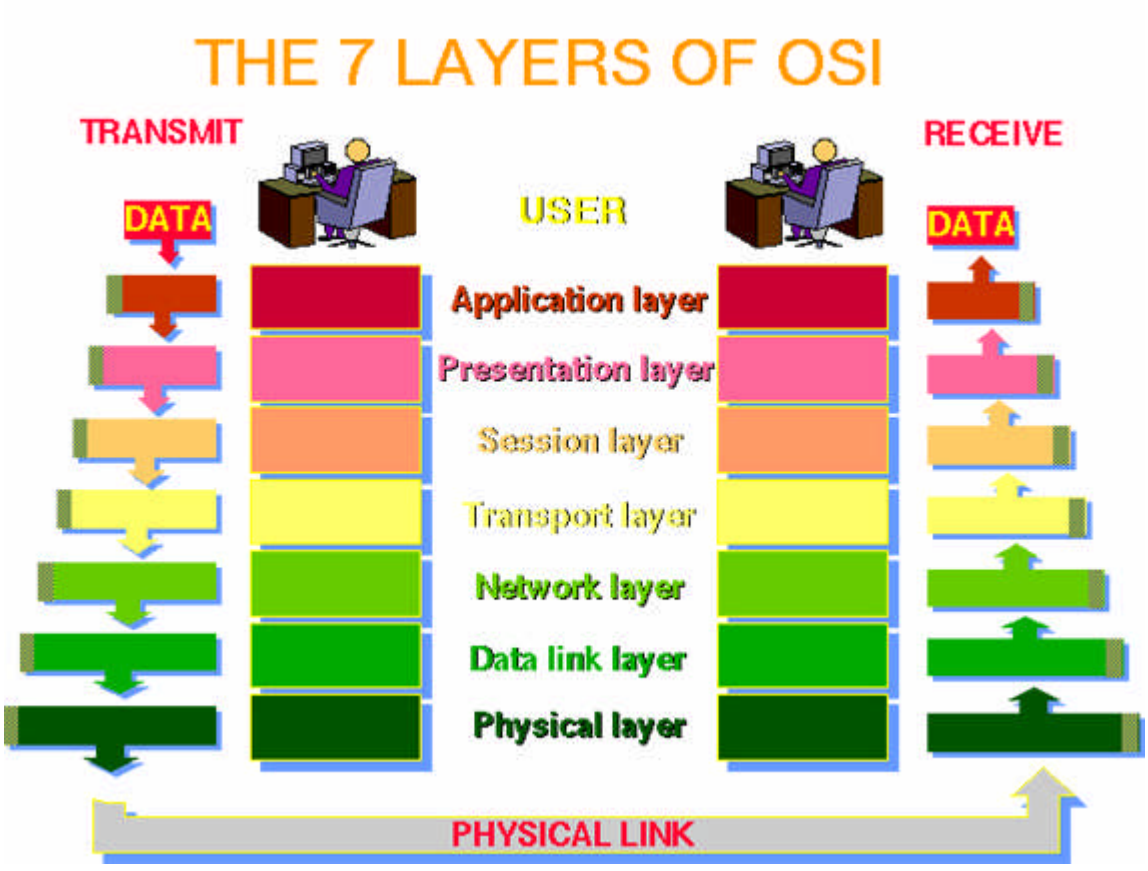
Abstract

Information is the heart of any business or industry. It provides sustenance to organizational units: empowering and strengthening its users as groups and individuals. It can be used for or against us, naturally concerning us with the safety and integrity of our information. If the nature of our information is to be distributed for accessibility then so must our efforts to secure it.

Over the past two decades, the distributed computing industry has utilized the International Standards Organization's (ISO) Open System Interconnection (OSI) Model [1] for better standardization of hardware and software components. Some layers have more impact than others when securing information. Together, they can be used to build a comprehensive solution. Utilizing the OSI Model's seven layers, this paper will demonstrate a logical, comprehensive and achievable approach to securing an organization's information resources.

Understanding the OSI Model

Figure A[1]



[1] The 7 Layers of the OSI Model [1]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure A is a visual representation of the OSI Model. Manufacturers of networking hardware and software, to improve standardization and interoperability, map each layer, at least roughly. Therefore, the model assumes a peer layer on another system. Throughout this paper, the layers are addressed in terms of general functionality and purpose from a security perspective.

Physical Layer

The logical first step in securing our information is to insure that the physical resources are not compromised. The physical layer of the OSI Model reminds us to not overlook the obvious. Quite often, technologists fail to recognize the importance of the simple measures, like properly locking storage units, server cabinets, equipment rooms and office spaces. Gaining access to resources is the first step in compromising them. Where is the information stored and who might have physical access to it?

Physical locks, both on equipment and facilities housing the equipment, are imperative to keep intruders out. In order to use information one must have access to it. Security cables on laptops and system cases with power button locks are examples of procuring equipment with physical security capabilities.

Typically, efforts to physically secure information are a shared responsibility between technologists and those who manage the facility in which the information resides. In some organizations, you must have a card key or hardware key to enter areas where sensitive information can be accessed. Biometrics integrates biological identifiers such as a fingerprint and sophisticated hardware and software when proper identification is critical regardless of cost.

Even with the resources physically locked, they are at risk. Social engineering is a form of infiltration that takes advantage of common social interaction to gain physical access. With fake identification, the right uniform, or saying all the right things, an intruder could walk in and gain access to critical information resources they would otherwise be denied. Training information users is the best defense against Social Engineering.

Up to this point, we have addressed the threat of intrusion and access to critical information. It is also necessary, when addressing the physical layer of our security approach, to be concerned with other factors that could have a negative impact on the physical state of our information. Environmental factors should also be considered.

In extreme circumstances, a good disaster recovery plan is essential in the event that information resources are compromised. Off-site data storage, asset inventories and vendor contacts are critical to knowing what to replace, where to get replacements and how to restore access. Other, not so obvious threats to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

our resources include power supply threats, radio frequencies, electromagnetic interference, dirt, moisture and temperature.

Data Link Layer

The Data Link layer of the OSI Model is a bit more obscure than its predecessor. Its responsibility is to place frames on the network medium and insure that delivery is error free. This is where the MAC (hardware) address of communication devices is utilized and checksums for error in delivery are applied.

A device running in promiscuous mode [2] and a packet filter could be helpful or harmful tools at OSI Layer two. Allowing flow analysis, problem determination and code debugging can be helpful. However, in the wrong hands the ability to copy datagrams poses a threat.

An example of a layer two threat is Libpcap [3], a packet capture driver that forces a NIC in to promiscuous mode allowing it to absorb traffic destined to other machines. Perhaps a hacker prefers using software to spoof a MAC address, capturing traffic destined for a specific machine. In either event, contained in the traffic could be important data or even usernames and passwords for access to even more sensitive information. Other known threats at this layer include MAC Flooding, ARP and Spanning-Tree Attacks. How does one protect against these and other Layer 2 onslaughts?

Layer 2 switches provide the ability to create logically separate LANs on the same physical device, called VLANs [4]. Using traffic and protocol access control lists or filters provides us with some form of protection at this layer. Quality-of-Service marking and prioritization control protocols give us the ability to control and better utilize existing bandwidth. This is typically accomplished using appropriate class-of-service or differentiated services code point (DSCP) values.

Also, disabling untrusted Layer 2 ports will reduce traffic to and from hosts. Another measure is to disable the default VLAN 1 port [5]. As you tighten up your defenses at Layer 2, you will need to leave a port open for management purposes, preferably out-of-band. When it comes to securing a Layer 2 device, your most secure bet is a console cable with telnet capabilities completely filtered.

Network Layer

Some switches operate at Layer 3 [6] of the OSI Model, although pessimism of its success still abounds. More often than not we will find routers and firewalls operating at this layer. It is at this layer that best path is determined from source to destination host on a network.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

IP addresses are assigned and utilized at this layer for unique identification. In order for a system to communicate with the Internet, it must have an associated public IP address. This address allows a system to contact the outside world and allows the outside world to contact the host. It is logical to consider this border to our system vulnerable.

Defense through obscurity augments a comprehensive solution at this layer. Network Address Translation (NAT) is a service that temporarily assigns a private IP address to a public IP address. In this sense, for a time, there is a one-to-one relationship between a private and a public address. It is necessary to lease a pool of public IP address for NAT to work. **Figure B** illustrates the public and private IP address relationships using NAT.

Figure B - Network Address Translation Table

Private IP Address	**Public IP Address**
10.1.1.21	192.168.5.122
10.1.1.22	192.168.5.123
10.1.1.23	192.168.5.124
10.1.1.24	192.168.5.125

As you can see from **Figure B**, there is a one-to-one relationship between the private IP address of a host and the public IP address seen on external networks such as the Internet. This relationship is temporary, unless statically mapped, so that the public IP address can be recycled by other privately addressed hosts.

Port Address Translations (PAT), on the other hand, allows a single public IP address to be bound to multiple virtual ports. In this way, multiple networked hosts can share a single public identity on the Internet, providing a more cost effective and secure solution. In either event, the internal IP address is hidden to the outside world, providing us with some anonymity. **Figure C** illustrates the public and private IP address relationships using PAT.

Figure C - Port Address Translation Table

Private IP Address	**Public IP Address**
10.1.1.21	192.168.5.122
10.1.1.22	192.168.5.122
10.1.1.23	192.168.5.122
10.1.1.24	192.168.5.122

Notice each private IP address is represented by the same public IP address to outside networks such as the Internet. This is possible by using port assignments to properly direct incoming traffic to the requesting or destination network host.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Perhaps it is necessary for users outside to access information resources within an organizations network. Remote access through Internet tunneling takes place at Layer 3. Virtual Private Networking (VPN) allows us to establish credentialed connections and transmit encrypted payloads across preexisting Internet channels. The presence of a VPN implies encryption of transmission. This is not to be confused with encryption of data. With a VPN, it is of no consequence to the Layer 3 device if the packet it must deliver contains encrypted data or not.

Up to this point, we have assumed that the risk at Layer 3 is external to our LAN. This is not a safe assumption considering that statistically, most information breeches take place from the inside. If a system requires an IP address to participate in network communications, then perhaps we may need to consider how IP addresses will be assigned.

Dynamic Host Configuration Protocol (DHCP) has been widely accepted and used due to its ease of administration, lower risk of human error and flexibility. It is possible, however, for any system to plug into a DHCP network, receive an IP address and participate in IP transmissions across the infrastructure. When securing a network from unauthorized access is more important than the benefits of DHCP, static IP assignment should be considered. IP conflicts could be a result of unwanted hosts on your network. When identification of specific hosts on a network is particularly threatening, then DHCP with a very short lease length may be more appropriate.

Transport Layer

Finding a system on the Internet requires knowing the public IP address assigned to it. To target a specific application on a system, an intruder would need to know the IP address to locate the system and the port number assigned to the application, collectively referred to as a socket. A computer system has 65535 ports. These ports can be further broken down into three categories: well known, registered and dynamic. This is where Layer 4 security is applied.

Many applications utilize well known TCP and UDP ports [8]. An FTP server will, by default, utilize TCP port 21. If the file server providing the FTP service is not meant for public domain, it is best to change the default port number and divulge the new port number to authorized users only. In this way, we can confuse and stall potential intruders by using private ports in place of well-known ports.

Trojans, malicious programs masquerading as benign programs, tend to target specific TCP and UDP ports [8]. An open port that is infected by a Trojan will require cleaning. Virus scan software helps to protect systems at this layer. Updated lists of known ports used by Trojans can be obtained on the SANs Institute website.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Security issues at the Transport Layer are concerned with availability of end-to-end data transmissions. Layer 4 switching [7] provides the ability to control traffic, not only utilizing IP addresses and MAC addresses of the lower layers, but also by specific application incorporating the upper layers of the OSI model. Prioritization based on application allows us to better control and utilize our bandwidth. Better control measures offer a more secure a level of service.

Further securing of this layer can take place by using a secure form of TCP [9]. Extended Three-way Handshake extends traditional TCP handshaking techniques to deliver negotiation data and key exchange data. State Transition is a secure TCP method that utilizes host state to differentiate authorized transmissions. Data integrity can be achieved through MAC (Message Authentication Code) to identify if an attacker has modified data. Data confidentiality can be achieved through encryption and must be addressed at the same time as data integrity.

Session Layer

Layer 5 of the OSI model deals with session handling between systems. Its job is to facilitate communication with a receiving device by establishing, maintaining, synchronizing, controlling and terminating connections. During this process of communication, verification of entities can take place.

Also referred to as Transport Layer Security, Secure Socket Layers (SSL) [10] is a technology designed to confirm the identity of hosts and servers. Although called Transport Layer Security, this function lies just above the transport layer and is truly session layer based. The obscurity with the OSI layers 4 and above is cause for their collective reference 'upper layers'. SSL is often the protocol used for secure credit card transactions on the Internet. Using server authentication, a server's identity can be verified by a Certificate Authority (CA) using Public Key cryptography. The same can be applied using client side authentication.

SSL uses different ciphers, cryptographic algorithms, to provide encrypted session services [10]. Cipher suits provide a wide range of encryption settings. The SSL Handshake Protocol enables the authenticated client and server to negotiate which cipher will be used. This helps reduce susceptibility to a "man-in-the-middle" attack, where a rouge program intercepts transmissions. Even if the session were intercepted, the data would be protected by encryption.

Presentation Layer

Encryption services are associated with the Upper Layers of the OSI model, specifically the Presentation Layer. When the data is received, what form will it take? Encryption techniques allow us to scramble the packet contents, requiring a special code to reveal them. The more sophisticated the encryption algorithm,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the harder it is to gain access to the data. Obviously, this intense processing function could affect system performance. Proper planning is necessary to calculate security needs and balance them with resource limitations.

In the early 1970s, the United States government acknowledged the need for data encryption standards between federal agencies [11]. Data Encryption Standard (DES) was the standard adopted by the National Bureau of Standards in 1976, although not for use in matters of national security. In 1999, DES was improved by adding two more stages (for a total of three) resulting in a 168-bit encryption key. The result was 3DES, a much more secure encryption standard in frequent use today.

International restrictions must also be considered. Some ciphers are more permissible then others. Products with less than 64-bits are freely exportable United States products with higher encryption are forbidden in certain "terrorist" countries. "On June 17, 2003 the U.S. Department of Commerce Bureau of Industry and Security (BIS) published a new rule, clarifying and making certain modest revisions to the encryption export rules in the U.S. Export Administration Relations (EAR)."[2] Obviously, these laws are dynamic and require consistent attention where international relations are concerned.

Application Layer

Finally, the seventh layer of the OSI model refers to the applications that support the end user functions. Not to be confused with user software, applications at this layer include FTP, SMTP and other low level services. It is at this layer, where services support user applications, that authentication takes place.

The most common form of authentication is username and password. In this scenario, every user has a unique ID and confidential password. The combination of the two grants the user access. Therefore, it is essential to have an effective account policy.

Password length and complexity are crucial components to an account policy. A minimum password length of 8 is recommended to provide any challenge to a well-armed hacker. Combinations of characters, numbers and special characters make a password more robust. Keep in mind that most passwords are case sensitive.

Duration of any given password can also be altered to increase password level security on network. The longer a user uses a password, the better the chance of it being compromised. The task of changing a password is a complex and unpredictable process for many end users, especially if network and application passwords are not synchronized. Therefore, the help desk can expect an

[2] Steptoe and Johnson LLP [13]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

increase in calls whenever this process takes place. A balance must be found between user productivity and an appropriate level of security.

Usernames are frequently overlooked as a key part of authentication security. Usernames should follow a naming convention that is flexible and scalable. However, it is not good practice to use usernames as e-mail addresses or any other publicized means of identification. If the only two credentials required to gain access to protected resources are username and password, why give fifty percent of the puzzle away? Server software provides the use of aliases to link our e-mail accounts to our user accounts for our purposes, while allowing the outside world to see an assumed name. Once again, as we saw with our NAT and PAT implementations, we can use obscurity to provide an assisting level of security.

Encryption of these two credentials, username and password, is also feasible at this level. Application layer encryption adds yet another element of protection. Kerberos, the authentication protocol used by Windows 2000 and greater networks provides for username and password encryption. Kerberos is a time-sensitive protocol that needs to be synchronized with a reliable external time source to work properly.

Malware protection should be pervasive at layer seven of the OSI Model. Viruses, Worms and Trojans [12] are well known types of malware that are commonly confused with one another. Computer viruses come in two flavors, macro viruses and worms. Viruses [12] are malicious code attached to a host file of sorts. This could be application, document or executable file types. Worms [12] are also malicious code that spread from system to system. However, they do not require a host file for delivery. Trojans [12] are non-replicating malicious programs that are embedded into seemingly functional programs that a user would intentionally download and install.

Spyware is another form of malware wreaking havoc on the Internet. Spyware is software that runs on a computer and reports user behavior and system information back to a source location. Many users infect their own systems through thoughtless or uninformed Internet usage. The auditing behavior of spyware is resource intensive, often reducing system performance.

Adware is software that enables the posting of banners and advertisements on the host computer. While not necessarily considered malware, this type of advertising is considered invasive. Adware can also cause the same type of system performance degradation as spyware.

Protection against Malware at the application layer of the OSI model is imperative. Specialized anti-virus software packages, for commercial and home use, can provide a strong level of protection if implemented properly. The problems with these solutions lie in end user, configuration and timing issues.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Due to the volatile and unpredictable nature of malware attacks, it is imperative to update virus definitions on a regular basis. Even if a system is currently running the latest software and virus definitions, it is still possible for a newly released virus or Trojan to infect it. Spyware and Adware require additional specialized software for their detection and removal.

Encryption methods, such as Pretty Good Privacy (PGP) used for e-mail, are also implemented at this level. Multi-layer encryption, although costly in resource overhead, is the best way to ensure data privacy.

Additional protection at all the layers can be assisted at the application layer. This is achieved by maintaining current service packs and patches to operating system and application software. Newer Microsoft products, such as Windows 2000 and Internet Explorer High Encryption Pack, have 128 bit encryption capabilities with the current service packs and software updates. Automatic updates, on Windows 2000, XP and greater Microsoft operating systems are ways to improve consistent application of current patches and fixes with little to no user intervention required. Further automatic update capabilities are available on Windows 2003 server, enabling automatic updates inside the LAN with out every system downloading from the Internet.

Summary

It is clear that sophisticated devices and software can provide services to protect our data. Solutions can vary widely in terms of cost. Costs can be direct, such as procurement of hardware and software. They can also be indirect, through such things as resource utilization and user training.

Training, perhaps the most underestimated tool for defense against intrusion can have the least over-all cost with great returns. Users who are informed can strengthen physical, network and application layer access.

No one layer of the model, in full force, is even a fraction of protection. A comprehensive security solution encompasses consideration of all layers of the OSI model. By using the steps in which the devices that enable distributing computing are created, we are able to build boundaries around our important information

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

[1] Webopedia , "The 7 Layers of the OSI Model", URL:http://www.webopedia.com/quick_ref/OSI_Layers.asp (June 1, 2004)

[2] "UNIX Promiscuous Mode Information and Detection", October 10, 2000, URL:http://www.stanford.edu/group/itss-ccs/security/unix/promisc.html, (June 1, 2004)

[3] "Project: The Libpcap project: Summary", December 29, 2003, URL:http://sourceforge.net/projects/libpcap/, (June 1, 2004)

[4] "Switching and VLAN Security FAQ", URL:http://www.fefe.de/switch/, (June 1, 2004)

[5] "VLAN Security", September 1, 1999, URL:http://www.opennet.ru/base/fire/54.txt.html, (June 1, 2004)

[6] "Layer 2, 3 and 4 Switches*, Moving Data Efficiently and Quickly",* URL:http://www.blackbox.com/tech_docs/tech_overviews/switching_overview.html, (June 1, 2004)

[7] "Layer 4 switching: The magic combination, Network World on High Speed LANs", February 15, 1999, URL:http://www.nwfusion.com/newsletters/lans/0215lan1.html, (June 1, 2004)

[8] "Computer TCP/UDP Ports", URL:http://www.satx.rr.com/support/security/computer_ports.html, (June 1, 2004).

[9] Tsutsumi, Toshiyuki**, "**Secure TCP --- providing security functions in TCP layer", April 29, 2004, URL:http://www.isoc.org/HMP/PAPER/144/html/paper.html, (June 1, 2004)

[10] "Introduction to SSL", October 09, 1998, URL:http://developer.netscape.com/docs/manuals/security/sslin/contents.htm, (June 1, 2004)

[11] Castelino, Kenneth, "3DES and Encryption", URL:http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html, (June 1, 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

[12] "What are computer viruses, worms, and Trojan horses?", November 04, 2003, URL:http://kb.indiana.edu/data/aehm.html?cust=842998.00774.30, (June 1, 2004)

[13] Steptoe and Johnson LLP, "Encryption Export Regulation Update", Summer 2003, URL:http://www.steptoe.com/publications/Encryption_Export_Regulation_Update_2003.pdf, (June 1, 2004)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.