Global Information Assurance Certification Paper

ALPHA 1:
Building Blocks for a Secure Network

Michael Trotman
Version 1.2d

Introduction:

In order to have a secure network, many security issues will present themselves in order to achieve a "defense in depth" network. Depending on the size and complexity of the network, a Security Administrator (SA) can go from the exotic to the sublime in firewalls, Intrusion Detection Systems (IDS), and encryptions. This paper will attempt to provide the basic building blocks when considering a secure network with connection to the Internet. A SA considering such a system that will transmit and receive sensitive Ecommerce data should consider the following before implementing such a system.

Security Policy:

First thing to address is consideration of a security policy; it defines the overall security posture. A security policy is representative of an organization's position on particular security issues. These policy statement are backed-up by specific standards and guidelines that provide details on how an organization is to achieve its stated posture. A good security policy will help identify risk, and test procedures for soundness. In order to accomplish the above, the formation of a security committee is extremely important in establishing the security policy. When the security committee is established, the task of putting the policy together must be tackle.

Site Inspection:

The facility where the equipment and personnel is located should be assessed with a through site inspection. In this inspection, the SA should have a description of the facility's location and a description of the facility itself. Some things to consider are:
Geologic and seismic activity, floods, wildlife fire, road access, fire, power to the facility, effect of explosions, wind, communications, unauthorized access, hackers, employees theft, airline flight paths, hazardous material spills, civil disturbance and others that are important to the facility's protection.

Change Management:

In the Change Management process a policy for change control or management should be implemented through the network environment. Some things to consider are:
Production input/output controls: controls used for the marking, processing, storage and disposal of input and output information and media as well as the labeling and distribution procedures for information and media. The controls used to monitor the installation of system software updates should be set out. In addition, hardware and software maintenance controls, virus protection, security awareness training and incident response capability should be set out.

Technical controls such as user authentication and logical access controls (restricting activities of users) should be considered. Other things to consider are public access controls and secure communication, audit trails, security testing, firewalls, routers, servers and database security.

Risk Management:
Risk Management is the total process of identifying, measuring, and minimizing uncertain events affecting assets. The primary objective of risk management is to identify specific areas where safeguards are needed against deliberate or inadvertent unauthorized disclosure, modification of information, denial of service and unauthorized use. With risk management, the security policy should address such things as: Unique features in the system, software application functions, identifying system assets and various threats to the network. Threats like natural disasters, utility failure, human error, fraud or theft, competitors or improper disclosure of information that could cause harm to individuals.

Securing the Network:
Once the above is in place or taking form, the network itself has to be design, implemented or upgraded. Aside from the usual servers, workstations, software and other peripheral devices the following security devices should seriously be considered to ensure "defense in depth" is throughout your network.

Firewalls:
Two types of firewalls dominate the market today: application proxies and packet filtering gateways. While application proxies are widely considered more secure than packet filtering gateways, their restrictive nature and performance limitations have kept their adoption limited to traffic out of the company rather than traffic into a company's web server. Packet filtering gateways, or the more sophisticated "stateful" packet filtering gateways, on the other hand, can be found in many larger organizations with high performance requirements.

> **Packet Filters:** This type of firewall provides for examination of IP packets and makes a decision based on specific criteria. The criteria are generally the source and destination IP addresses and source and destination TCP and UDP port numbers. Packet filter firewalls look solely at the header information of a packet and not at the data contained within the packets.
>
> **Stateful:** In addition to examining the IP packet headers a "Stateful" firewall also look at some of the contents by transparently intercepting the packets and reviewing the contents. The criterion this firewall uses is based upon the packet header information and the data within the packet. A "Stateful" firewall however, does not inspect all the data in a packet.
>
> **Proxies:** In order to inspect the entire data in a packet an application level/proxy firewall is needed. The proxy firewall is capable of operating in

the application layer of the OSI Model. It views information being passed over them and ensure that the information is acceptable, based on its own set of rules.

Networks firewalls are susceptible to different vulnerabilities: Three common ones are buffer overruns, IP spoofing and ICMP tunneling. Buffer overruns typically occur when data sizes inside a buffer exceed what was allotted. IP spoofing is simply sending your data to a source, in this case a firewall and faking a source address that the firewall will trust. In this particular scenario, the hacker would be able to access internal machines since he compromised the firewall. ICMP tunneling allows a hacker to insert data into a legitimate ICMP packet. Since the network firewall cannot probe the packet past the IP header, it cannot deny the connection. Even if IDS detect the intrusion, the system has already been compromised.

Application level/proxy firewalls uses proxies based on the specific application that needs to be used. For example, http, telnet, and SSL traffic will be checked at the firewall with the specific rules that were applied for these applications. These firewalls view information as a data stream and not as a packet. In this way, they are able to scan information being passed over them and to ensure that the information is acceptable, based on its own set of rules.

As stated earlier, these firewalls work at the application level, so they tend to be equipped with a certain level of logic. This allows the firewall to make some intelligent decision about what to do with packets that are passing through it. Proxy firewalls can be configured to check for "known vulnerabilities" and can support the ability to report to the intrusion detection software.

Enclaves:
Enclaves are use for identifiable, critical and securable components that need protection. Network guardians manage access between enclaves and the enterprise. Within enclaves, the security objective is to apply traditional controls consistently and well. In the enclave, every system and network component will have security arrangements that comply with the enterprise policy and industry standard of due care.

Network Guardians:
Network guardians mediate and control traffic flow into and out of the enclaves. Network guardians can be implemented initially using network routers. The routers will isolate local area network traffic from LANs used for other purposes. The next step in the deployment of network guardians is the addition of access control list (ACLs) to guardian routers. ACLs functions as border routers in the

Internet firewalls – screening incoming traffic for validity, screening the destination address of traffic within the enclave, and restrict enclave services visible to the remainder of the enterprise to the set of intended services.

Intrusion Detection Systems (IDS):
Intrusion detection system (IDS) encompasses techniques that help to filter intrusion attempts from normal system usage and alerts the SA. An IDS provides protection from the outside world by monitoring and logging the attempts to subvert your system's devices.
As work environments become more interconnected and exposed, service providers will need increasingly to rely on a wide range of anti-intrusion techniques, not just IDSs. Anti-intrusion research and deployment shows promised in combating intrusive activity from external crackers and insiders abusing their privileges. Following are considerations for anti-intrusion techniques:

- **Intrusion Prevention:** Intrusion prevention techniques (enforced internally or externally to the system) could seriously limit the likelihood of success of a particulate intrusion. These technique help ensure that a system is so well conceived, designed, implemented, configured, and operated that the opportunity for intrusion is minimal.
- **Intrusion Preemption:** Intrusion preemption techniques strike offensively before an intrusion attempt to lesson the likelihood of a particular intrusion occurring later.
- **Intrusion Deterrence:** Intrusion deterrence seeks to make any likely rewards from an intrusion attempt appear more troublesome than it is worth. Deterrents encourage an attacker to move on to another system with a more promising cost-benefit outlook.
- **Intrusion Deflection:** Intrusion deflection dupes an intruder into believing that he/she has succeeded in accessing system resources, whereas instead he/she has been attracted or shunted to a specially prepared controlled environment for observation.
- **Intrusion Detection:** Intrusion detection encompasses those techniques that seek to discriminate intrusion attempts from normal system usage and alert the SA. Usually, system audits is processed for signatures of known attacks, anomalous behavior, and/or specific outcomes of interest.
- **Anomaly Detection:** Anomaly detection compares observed activity against expected normal usage profiles which maybe developed for users, groups of users, applications, or systems resource usage. Audit event records which activities fall outside the definition of normal behavior and tag them as anomalies.
- **Misuse Detection:** Misuse detection checks for "evil deeds" with comparison to abstracted descriptions of bad activity. This approach attempts to draft rules describing known undesired usage rather than describing historical "normal" usage.

- **Hybrid Misuse / Anomaly Detection:** Hybrid detections adapt some complementary combination of the misuse and anomaly detection approaches run in parallel or serially. A misuse detector monitoring against description of known undesirable activity may not notice activity, which is flagged as anomalous. For example, an administrator account may have access to sensitive files and have a profile to permit such action, but it would be informative for this access to still be checked against misuse signature.
- **Continuous System Health Monitoring:** continuous active monitoring of key "system health" factors such as performance and an account's use of key system resources may detect Intrusion.
- **Intrusion Countermeasures:** Intrusion countermeasures empower a system with the ability to take autonomous action to react to a perceived intrusion attempt. This approach seeks to address the limitations of intrusion detection mechanisms, which rely on the constant attention of an SA. Intrusion countermeasure equipment can be used to not only detect but also autonomously react to intrusion in real-time. Such a tool would be entrusted with the ability to take increasingly severe autonomous action if damaging system activity is recognized, with or without an SA on duty.

Encryption:
Encryption comes in two basic types, Symmetric and Asymmetric. With symmetric a single secret key is used for both encryption and decryption. Asymmetric encryption uses a pair of mathematically related keys, commonly called the private and the public key. It is not computationally feasible to derive the matching private key using the encrypted data and the public key. Public key encryption is the enabler for a wide variety of electronic transactions and is crucial for the implementation of E-commerce.

- **Pretty good Privacy (PgP):** PgP is considered a powerful cryptographic product that will allow people to exchange messages securely. It will also provide security for files, disk volumes and network connections with authentication.
- **Data Encryption Standard (DES):** Although not considered safe anymore, DES is a widely used method of data encryption that uses a private or secret key. A key is chosen at random from among an enormous number of keys (72 quadrillion possible keys); the sender and the receiver must know and use the same private key. "Triple DES" is stronger and will apply three keys in succession.
- **Kerberos:** Kerberos is a method for authenticating a request securely. It provides a way for a user to request an encrypted "ticket" from an authentication server that can them be used to request a particular service, like telnet.
- **Public Key Infrastructure (PKI):** PKI can enable secure data exchange over an unsecured public network such as the Internet; it is done through the use of a public and private cryptographic key pair, which can be

obtained and shared through a trusted certificate authority. The private key system has a major flaw, if the key is found, stolen, discovered or intercepted by someone other than whom it was intended for, messages can easily be decrypted and stolen.

- **Internet Protocol Security (IPsec):** IPsec is a standard for security at the network layer, layer 3. This layer is the Internet layer or packet-processing layer of network communication of the OSI model. IPsec will be crucial in implementing secure VPNs and for remote user access through dial-up connection to private networks.
- **Secure Sockets Layer (SSL):** SSL is a protocol for managing the security of message transmissions on a public network, the Internet. It is programmed to work between the HTTP (layer 7) and TCP (layer 4) layers. Netscape developed SSL; it is in both Microsoft and Netscape browsers as well as most Web server bases programs.
- **Advanced Encryption Standard (AES):** AES is an encryption algorithm; AES is more robust and may replace DES and/or triple DES. AES can support key sizes of 128, 192 and 256 bits.
- **Rivest-Shamir-Adlemon (RSA):** RSA is an Internet encryption and authentication system; it uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir and Leonard Adlemon. The RSA algorithm is the most commonly used encryption and authentication algorithm. Netscape and Microsoft Web browsers both use RSA.
- **MD5:** Md5 is a hash algorithm; it is a one-way cryptographic function. When applied to a data object, it outputs a fixed-size output. It is conceptually similar to a checksum, but is much more difficult to corrupt.
- **Steganography:** Steganography is the practice of hiding data; this differs from encryption, which makes intercepted data unusable, but does not attempt to conceal its presence. Traditional form of steganography includes invisible ink and microdots. Cryptographic steganography uses data transformation routines to hide information within some other digital data. Multimedia objects, such as bitmaps and audio or video files are the traditional hiding places; recently steganographic file systems were announced as a new hiding place.

Virus Protection:
Every organization should have an anti-virol policy; more importantly, an organization should have enough of an understanding of viruses so that it can determine its next step towards implementing antiviral protection for protection of assets.

- **Virus:** A virus is a piece of code or a small program created to execute by the user without the user knowing. A virus can merely be a nuisance or it can be very damaging; it will attach itself to files, and boot sectors in hope of replicating.
- **Trojan Horse:** A Trojan horse is a malicious program contained within a seemingly harmless or even trusted program.

- **Worm:** A worm is a computer program, or set of programs that can spread across a network to other computer systems; its full intention is to replicate itself.

Some virus types are boot-record or sector infectors, multipartite, which can spread over an entire network (a hybrid of boot infectors and program viruses), and Macros; Macros uses the Visual Basic (VB) editor and usually target word documents.

Auditing:
Auditing should be every organization's last line of defense; many problems occur that force us to audit. Audits are performed to identify when an intrusion occurs; if an intrusion is detected, audits can be used to determine what portions of the system have been compromised. Auditing will not stop intrusions from occurring, it will help to determine facts about the intrusion and what is normal activity for a system.

Penetration Testing:
Once all of the above are in place, an organization needs to determine the effectiveness of its security measures. Penetration testing is designed to bypass the security controls of a system or organization for the purpose of testing that system or organization's resistance to such an attack. Penetration testing is performed (with upper management approval) by using the tricks and techniques of a real-life attacker to uncover and mitigate the security weaknesses of a system before a real attacker discovers them. Penetration testing can materialize in three ways:
First, physical infrastructure of the subject; this test will test the adequate access control and physical security of the facility. Second, operation procedures of an organization; test if anyone can get help from the help desk, social engineering and improper disposal of old data, etc.
Third, electronic testing; outright attack on the computer systems, networks or communications facilities.

Conclusion:
In concluding, a good security policy with a strong secure network is only as good as promulgated by the Corporate Executive Officer (CEO). Without the support of the CEO and constant vigilance the well built "defense in depth" network can be compromised, crumble and fail. This paper was written to provide a starting point for the Security Administrator when considering building a network system; additional considerations will apply depending on the complexity of the network.

Tipton, Harold F, Krause, Micki. "Information Security Management", vol. 2, 4th Ed., CRC Press, LLC.

McClure, Stuart, Scambry, Joel and Kurtz, George. "Hacking Exposed". 1999.

Halme, Lawrence R and Bauer, R Kenneth. "AINT Misbehaving: A Taxonomy of Anti-Intrusion Techniques".
www.sans.org/newlook/resources/IDFAQ/aint.htm

www.brainbuzz.com/

www.3com.com/nsc500619.html (18 Sep. 2000)