Global Information Assurance Certification Paper

Glen Sharlun
GIAC Security Essentials Practical

Defense in Depth
The lessons from Troy and the Maginot line applied

For centuries, warriors have known that to properly protect anything of value, multiple measures of protection are the most effective. If it was a medieval castle, the defenses generally started with a distant perimeter of rock fences and ditches to slow the approach of an enemy. This was often followed with large open areas that sloped up to the castles well-selected high ground that provided superior observation and protection. Finally at the perimeter, the attacker was faced with a moat that was immediately followed by a seemingly insurmountable wall barrier. This wall was strategically designed with limited access that were co-located with defendable guard houses. Once inside these formidable barriers, the attacker still only had access to the expendable, peasants. To get to the "crown jewel" or ruler, this attacker would need to continue to battle through a number of formidable barriers that had channelizing openings, and that were well observed and defended. A pictorial depiction of the defense in depth concept as it was applied to the Heidelberg castle can be seen at the following link. (http://www.cheswick.com/ches/talks/heidelberg.html)

Though the concept as a whole is as valid today as it was then, the application has evolved with the tactics and technology of the day. The use of the Trojan Horse, and the employment of cannons, are solid examples of the learning that the attackers undertook to overcome static, fortified emplacements, to the point that castles as a defense tactic, have become obsolete. Functionally, the attacker learned that instead of working harder to defeat the strength of the defense, he learned to think harder on how to avoid and mitigate the strengths of the defense.

This layered defensive tactic needs to be employed in our computer network defense strategy as well. The rationale for this is not any different than that used by the King for his castle and riches: Stop the enemy as far from "home" as possible to minimize damage to important infrastructure (screening router if possible). Positions and/or equipment must be located and tuned to look for and identify the attacker (router ACL's, firewall rules, IDS's, anti-virus). There must be a barrier that separates the outside from the inside, as well as each sub-unit within the perimeter (firewall, routers, switches). Access through each of the barriers must channelize the attacker so that they can be repelled (the rule base applied to each packet in the firewall, router and switch).

The Department of Defense (DoD) defines defense in depth as, "The siting on mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver his reserve". While perfect security is a myth that cannot be achieved, there is much that can be done to minimize system vulnerabilities and counter potential threats. This implies that we need to shift from a risk avoidance strategy, to a

risk management strategy. The confidentiality, integrity, authenticity and availability of information and IT systems are the goals of an IT defense strategy. The castle example may make for a good parallel of the multiple layers of a defense system; it does not easily reflect the varying technologies that are available at each of these layers of the computer network defense system.

Encryption, the art of turning data into ciphertext and decryption, the reverse process, not only provides information confidentiality but also integrity and mutual authentication of the parties that are communicating. This ability to make data illegible to unauthorized parties allows for the tunneling of sensitive information across a non-secure Internet. This also allows for the cryptographic assurance that the transmitted data could not have been altered or read by anyone who is not authorized to decrypt the information. The Virtual Private Network (VPN), using IPsec, is becoming a very common application of this technology and can be used at any layer of the defense where secure communications are required. Secure Sockets Layer (SSL) is typically used to protect communications between web a server and web browser. Of course saving this data in its decrypted form can defeat the entire process of the secure communications, if that system is compromised.

Firewalls have largely been seen as the panacea of perimeter defense. There ability to selectively allow authorized external users access, and to deny unauthorized users, has been misinterpreted as the only defense mechanism necessary. Much in the same way the soldiers in Troy learned from the Trojan Horse, and the French learned from building the Maginot Line, any single defense will fall to an opponent who has the intelligence to find a way through, or the will to go around. It is an integral layer to the defense and serves to protect a network from much of the noise on the Internet, but it does not have the resources to do it on its own.

Content checking and intrusion detection provide the vital inspection of packets that are allowed through the firewall (or that hit the firewall). By having a large signature base of viruses and attacks, these can quickly identify malicious traffic and generally prevent the infection or attack from progressing beyond a perimeter or near perimeter location. Essentially, anti-virus programs and IDS's are the internal guards that know (hopefully) what the enemy looks like and are charged to isolate and eradicate them on sight.

Source authentication is very important to network components that rely on being updated by their peers within the network. Routers and domain name servers (DNS) are the most common components that fall into this category. The routing tables and name/address translations tables that are shared among peer components are critical to the correct functioning of a network, and the Internet as a whole. If malicious data can be inserted into either of these two vital components, it can result in a denial of service (DOS) or unauthorized access. Cryptographic authentication of routing protocols (BGP and OSPF) allows for the secure updating of these vital components.

Access control is the security measure that the common user is forced to confront most often. Consequently, this is often the easiest means for the malicious intruder to gain access to an otherwise restricted network. Because user ID's and passwords are maintained by the individual user, they are often very simple to crack or observe (written on computer monitor). File access control is another means of securing data by restricting access to folders or files based on permissions set to the user or group. This access is based on user ID and password though. Tools that test passwords for length, originality, and complexity, complimented with regular physical inspections, are an integral way of protecting a network from its users.

Finally, auditing and updating all of the above techniques and tools is an ongoing process. All of the systems that have been listed are only as good as they are current. With the increased complexity of each of these systems, there is increased likelihood that there are dependencies and voids that can and will be exploited and therefore regular preventative maintenance will be required.

As the complexity of each of the individual systems increases, the complexity of managing a system of these systems goes up as well. The likelihood that there are firewall rules that are erroneous or in the wrong order increases significantly as the number of rules increases (say beyond 30 rules). So it is with the router access control lists (ACLs), anti-virus updates, operating system patches and bind updates. To further complicate matters, the lack of skilled network administrators and security administrators decreases the number of trained eyes that are looking for abnormalities and potentially malicious traffic.

To make matters even worse, very simple actions can nullify numerous layers of this defense in depth. If a user, which is connected to the network, has connected his modem to a phone line (so that he/she could get their Hotmail "once" when the network was down) and has forgotten to remove it, he/she has negated multiple layers of the networks defense. What if a business partner that you have established a VPN with does not work as diligently to provide security to their end of the encryption tunnel? In both of these cases, this is similar to providing the enemy a boat to cross the moat and keys to slip in the back door of the castle.

The final depressing note is to comment on the malicious insider who not only has access to the inside, but who is likely to know where the "jewels" are. The ability to identify this intruder is much more difficult because of his authorized access and potential knowledge of the defense systems in place.

DoD's definition of defense in depth succinctly highlights the purpose of the tactic: Build mutually supporting defense positions; absorb and progressively weaken the attack; prevent initial observations of the whole position by the enemy; and allow for the appropriate response. The screening and inspecting of packets, strong source and access authentication, encrypting of sensitive traffic and data and finally, the regular auditing and updating of the security system, is the best means to accomplish this. The potential for

simple "mistakes" or insiders to cause grave security breaches by nullify multiple layers of defense, is a reinforcing reality. For an information system to have an adequate chance of surviving in today's environment, it must have the layered defenses that it can withstand even the loss of multiple layers, and still maintain integrity.

Sources:

Cheswick, Bill. "Defense in Depth- an example from Heidelberg." URL: http://www.cheswick.com/ches/talks/heidelberg.html (3 Nov. 2000)

Galik, Dan. "Defense in Depth: Security for Network-Centric Warfare." URL: http://www.chips.navy.mil/chips/archives/98_apr/Galik.htm (10 Nov. 2000)

Wilson, Michael. "Defense-in-Depth: Design Notes." 7Pillars Partners. 1997. URL: http://www.7pillars.com/papers/didfinal.htm (7 Nov 2000)

Alberts, David S. "Building Defense in Depth." Defensive Information Warfare. August 1996. URL: http://www.ndu.edu/ndu/inss/books/diw/ch8.html (12 Nov. 2000)

Northcutt, Stephen and Novak, Judy. *Network Intrusion Detection: An Analyst's Handbook*. Indiana: New Riders, 2000.

McClure, Stuart and Scambray, Joel and Kurtz, George. *Hacking Exposed: Network Security Secrets and Solutions*. California: McGraw Hill, 1999

Brenton, Chris. *Mastering Network Security*. California: Sybex, 1999