# Survey of Layered Defense, Defense in Depth and Testing of Network Security

Young B. Choi[*], Chrisopher Sershon, John Briggs, and Chad Clukey
Department of Business, Leadership, and Information Systems
College of Arts & Sciences
Regent University
1000 Regent University Drive
Virginia Beach, VA 23464-9800
USA
[*]E-mail: ychoi {at} regent.edu

***Abstract*— The threats that face a network is overviewed, and the difference between Defense In-depth and Layered Defense is established. The functions of Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Firewalls are explained. Best practice for securing and testing a network is described.**

**Keywords – Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Penetration Testing**

## I. INTRODUCTION

Preparing an organization's physical assets against threats can be considered common sense, however when it comes to protecting nonphysical assets, such as an organization's network, everything changes. Threats to physical assets generally come in the form of natural disasters and theft and can easily be protected again with insurance, locks, and security guards. Despite these being a good way for an organization to protect the network's infrastructure, the threats against that data on that network face far difference threats and require a completely different approach to safely guard it.

## II. SECURITY THREATS TO NETWORKS

According to SOPHOS *Security*, "Modern malware is all about stealth" [11]. The Advanced Persistent Threat (APT) has become the most vicious, specifically targeting individuals, organizations and governments. The security landscape is changing and companies no longer have an option to implement standard security practices. Companies, governments and even individuals must shift to a more tactical deployment of security technologies and strategies to combat not only these new threats but the threats to come. These sophisticated attacks are "well planned and well-funded; carried out by highly-motivated, technologically advanced, and skilled adversaries [11]."

### A. Adversaries

Gone is the stereotypical profile of a computer hacker being a long greasy haired introvert living in his parent's basement probing government computers to find the source of all the conspiracies. Today's hacker profile is very different and they come from all socioeconomic, religious and political spectrums. Though, the script kiddies and packet monkeys are out there, they have more or less become unwitting pawns in a much larger game. As SOPHOS mention, these hackers are more organized and well-funded [11]. They generally fall into to two categories of organizations, Hacktivist, such as the decentralized movement known as Anonymous or organized crime syndicates such as Zeus Gang. Hacker groups can come from any country and most people wrongly suspect Eastern Europe and Russia as the top countries where hackers originate. The top two countries, the United States and China account for "nearly 40% of the world's hacking attempts, costing the global economy over $44 billion each year [3]."

### B. Motivations

The motivation of attacks plays a large role in planning security measures for an organization. Understanding what drives these individuals and groups allows organizations to anticipate some of the threats and establish effective countermeasures to guard against attacks. Randy Weaver, Dawn Weaver and Dean Farwood in their book Guide to Network Defense and Countermeasures (3rd ed.) list some of the motivations associated with attackers. The list consist of; status, revenge, financial gain and industrial espionage. In addition to these motivations, cyber terrorism and political espionage are very real threats [16]. An example of financial gain can be seen through the distribution of the ZeuS Botnet code. This malicious code has undergone a number of changes and updates and is distributed over the Internet for cost ranging from $3,000 for the latest cybercrime toolkit up to $10,000 for a module that allows attackers to completely take control of a compromised computer [9].

### C. Classes of Attacks

There are a number of different ways attackers use to gain control of sensitive data and information. Microsoft TechNet provides a list of the common types of network attack to guard against. Some of the common attacks are:

- Eavesdropping - referred to as sniffing or snooping allows an eavesdropper to monitor the network. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.
- Data Modification - Attackers can modify the data in the packet without the knowledge of the sender or receiver.
- Identity Spoofing (IP Address Spoofing) – Allows attackers to falsely assume an organization IP address allowing them to modify, reroute, or delete your data.
- Password-Based Attacks - Attacker finds a valid user account and has the same rights and privileges as the real user.
- Denial-of-Service (DoS) Attack - Prevents normal use of your computer or network by valid users by flooding a computer or the entire network with traffic until a shutdown occurs because of the overload [13].

SOPHOS, Security Threat Report 2014, reports, "The creators of malware, exploit kits and botnets became smarter and more aggressive in 2013. They identified new forms of attack, new ways to repurpose older approaches, new targets, and new techniques for hiding their activities [11]."

### D. Security Perimeter

The network security perimeter is the first layer of defense in network security designed to prevent unwanted access to an organizations data, information and systems. The security perimeter is the point where an organizations network connects and interfaces with everything outside of the organization commonly referred to as untrusted networks. According to Microsoft TechNet, "the network perimeter encompasses every point where the internal network is connected to networks and hosts that are not managed by the organization's IT team [14]." There are a number of devices that can be employed at the perimeter to guard against attacks which includes, VPN clients and servers, remote access clients and servers, border routers, firewalls, proxy servers, and intrusion detection and prevention systems.

### E. Layered Defense or Defense in Depth

There are a number of people that used the terms layered defense and defense in depth interchangeably believing that they are the same thing. Though they are very similar in context, the application of each is vastly different. It is important for security professionals to understand the differences and address each one separately within their security policy. Implementing a security device such as an antivirus program is good but by itself it will not stop the malicious traffic entering the network leaving gaps in an organization's defense. Layered defense or layered security is a means to layer additional different defenses to compensate for the flaws or gaps in other security measures at each layer covering the gaps and holes of other layers. Defense in depth was originally a military concept which is similar to layered security but it addresses the strategy of network defense as opposed to the actual defense of attacks. Use of firewalls, IDPS and antivirus software are components of layered defense. Layered defense itself is one component of a defense in depth strategy. Chad Perrin explains, "layered security is extremely important to protecting your information technology resources … A defense in depth approach to security widens the scope of your attention to security and encourages flexible policy that responds well to new conditions, helping ensure you are not blindsided by unexpected threats [10].

## III. LAYERED DEFENSE

As mentioned previously, layered defense is combining various network technologies and procedures, each one compensating for the gaps or holes left by others. Layered security can be as simple or as elaborate as an organization wants however a balance between security, cost and operability needs to be defined. Systems Engineering presents an article on the layered approach to managed security in which they identify layers of defense:

- Security Policy is the first step in securing your network.
- Perimeter Defense includes a traditional firewall, Intrusion Prevention Software, Botnet and Malware Filters as well as Network Monitoring.
- Core Network Protection of your network includes Patching, Network Monitoring and Server Endpoint Protection that goes beyond the protections afforded by firewalls and antivirus software to provide browser protection and advanced threat prevention.
- Endpoint Protection for desktops, laptops and mobile devices reduces the vulnerability of the weakest links in your network.
- Web Content Filtering addresses cybercriminals' preferred method for delivery of malware to gain network and data access - the Internet [12].

When developing the organizations layered defense, John Mello in his article cautions, "One pitfall to avoid with layered security is using products from the same vendor. That's because all of a single vendor's products are based on the same technology and security intelligence [8]."

### A. Layered Security and Configuration of Perimeter

Protection of our network is critical to the success of businesses and their operation. Having a breach inside a network can be devastating to most businesses. Theft of information can not only destroy a business but it will also destroy the business brand. Once intrusion has occurred there are limited options for the company to take. Therefore, being proactive to defending the network will help secure organizational data. According to Whitman, Mattord,and Green the cornerstone of most network security programs is an effective perimeter defense [17]. Perimeter defense is the protection of boundaries of the organization's networks from the insecurity of the Internet. The heart of any good perimeter defense is an effective firewall that has been properly configured to be safe and effective.

In order to achieve network security there are different types of network security configurations. Having the configuration rules will allow who comes into the network and what goes out of the network. The configurations rules also specify the users who can use the Internet with the network and its resources.

One such way to provide network security is the use of a properly configured firewall. "A firewall is a security guard placed at the point of entry between a private network and the outside Internet such that all incoming and outgoing packets have to pass through it. The function of a firewall is to examine every incoming or outgoing packet and decide whether to accept or discard it. This function is conventionally specified by a sequence of rules, where rules often conflict [4]." In order to properly configure a firewall the company needs to specify a set of filtering rules, known as a policy, is typically complicated and error-prone. The policy is a set of rules that will allow what comes in and out of the network. It also provides a list of who has access to the network. Liu Gouda describes, "There are two types of firewalls: stateless firewalls and stateful firewalls. If a firewall decides the fate of every packet solely by examining the packet itself, then the firewall is called a stateless firewall. If a firewall decides the fate of some packet not only by examining the packet itself but also by examining the packets that the firewall has accepted previously, then the firewall is called a stateful firewall [4]." According to Whitman, Mattord, and Green a firewall is anything, whether hardware or software (or a combination of the two), that can filter the transmission of packets of digital information as they attempt to pass through the network boundary [17]. They perform two basic security functions: packet filtering and application proxying.

### B. Intrusion Detection and Protection Systems

Another way we can achieve network security is a properly configured Intrusion Protection System (IPS). Intrusion Detection Systems (IDS) help information systems prepare for, and deal with attacks. IDS is a perimeter defense is a layer of network when configured successful the IDS can do a number of security functions for the organization. They accomplish this by collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems. "Thus intrusion detection can be defined as technology designed to observe computer activities for the purpose of finding security violations or we can say intrusion detection is the process of identifying and responding to malicious activity targeted at computing and networking sources [1]. Once an ID system is selected, a number of decisions will determine whether it is deployed effectively. These include decisions about how to protect the organization's most critical assets, how to configure the IDS to reflect the organization's security policies, and what procedures to follow in case of an attack to preserve evidence for possible prosecutions. Organizations must also decide how to handle alerts from the IDS and how these alerts will be correlated with other information such as system or application logs [1].

Once a company has a set of guidelines it is up to the senior management to implement these configurations to the firewall and IDS. Network engineers can turn on and off ports and configure the network to the security policy in order to comply with polices regarding configuration. With the IDS placed on the network and configured there are several uses it can provide to administrators. According to Jawhar M. Mehrotra, the techniques for Intrusion Detection (ID) fall into two major categories depending on the modeling methods used: misuse detection and anomaly detection [6]. Misuse detection compares the usage patterns for knowing the techniques of compromising computer security. Although misuse detection is effective against known intrusion types; it cannot detect new attacks that were not predefined. Anomaly detection, on the other hand, approaches the problem by attempting to find deviations from the established patterns of usage. Anomaly detection may be able to detect new attacks. However, it may also cause a significant number of false alarms because the normal behavior varies widely and obtaining complete description of normal behavior is often difficult. Architecturally, an intrusion detection system can be categorized into three types: host based IDS, network based IDS and hybrid IDS.

The IDS has the ability to provide the following:

- Greater degree of integrity to the rest of you infrastructure
- Tracking of user activity from point of entry to point of impact
- Recognition and reporting of alterations to data
- Automation of task for monitoring the Internet searching for the latest attacks
- Detection of system attacks
- Detection of system configuration errors
- Policy design guidance of computing assets
- Reduction in the need for expert security management staff.

The IDS may not have the ability to provide:

- Compensation for a weak identification and authentication mechanisms
- Investigations of attacks without human intervention
- Compensation for weaknesses in network protocols
- Compensation for problems in the quality or integrity of information the system provides
- Analysis of all the traffic on a busy network
- Handling of all problems involving packet-level attacks
- Handling some of the modern network hardware and features (SANS 2012).

As the age of technology has exploded in recent years having our information protected is becoming and ever increasingly challenge for companies. Planning ahead and following the security polices and configuration rules that the upper management has put together is one way of protecting our networks. Protection of the network from outside intruders will always be a challenge. Having a great perimeter defense is one way companies can avoid a critical disaster. Having a firewall that is configured properly is a key for who has access to the network and what is going in and out of the network. The firewall alone won't completely stop an intrusion. Having also an IDS is a good idea to see what is on the network at all times. They can see if the network is being under attack and alert a response team to help handle the incident. These couple of hardware and software changes can greatly reduce the odds of an intruder trying to get into the system.

To design an efficient IDS for an organization, a comprehensive readiness assessment framework for identity theft can be considered [18] and a multi-dimensional classification framework for developing context-specific Wireless LAN (WLAN) security attack taxonomies can be used [19].

## IV. CONFIGURINGAND TESTING NETWORK DEFENSES

Once devices have been purchased and properly configured according to the organizations security policy, there are two final steps that must take place to ensure that the network is properly protected with a layered defense: configuring the physical layout of the network and testing your defenses.

### A. Configuring and Designing the Security Architecture

Configuring and designing the physical layout of security devices is the most crucial stage of development for security through layers. This is because if a network is not properly connected, all the bells and whistles of the firewalls and IDPS (Intrusion Detection and Protection System) and the security policies established on them become useless and no amount of testing would be able to fix it without a complete overhaul of the policy configuration. One of the best examples to use when explaining the importance of a layered defense is a castle. This is because they too have layered defense to protect what is inside. When a castle is designed it is built to protect the people it governs. Soft targets like farms need lots of resources but are at little risk so they are placed outside the network. A township that requires some resources but also needs protection from the outside is placed behind a light wall. If these were both to be attacked those inside would fall back to the barbican or a small miniature fort that protects the entrance to the castle [5]. If this too fails, then citizens would further remove themselves across a moat into the castle itself and finally to the castle keep where the last stand will be held.

Much thought went in to the designs of castles medieval times. If those in charge did not properly layout the lands defenses if would mean the castle, its citizens, and all its riches would quickly fall and be plundered. In the same way, layered networks can also suffer the same fate if they are not properly laid out. If assets are placed outside the firewall in what is supposed to be a DMZ (Demilitarized Zone), and the IDPS is placed inside the firewall than there is effectively no true DMZ and those devices become completely vulnerable to the outside. In the same way, if the IDPS and firewall are both configured properly on the network but the web server is placed inside them for complete protection then it will slow down access to an organization's webpage while many benign requests must be filtered through.

### B. Designing the Architecture

Before a network can be properly designed an organization must review what its needs and modus operandi or method of operations are. Part of this is reviewing the types of software configurations that are on the hardware. If an organization is going to be using internal email that is never to be used outside the network and a firewall is placed on the network to prevent in and out traffic on port 110 then it makes more sense to place the mail server inside the firewall than in a DMZ. At the same time, if a banking website needs to have access to the financial database for online banking, the organization must figure out which is safe and efficient; having the database in the DMZ with the web server or having it full protected with web server having limited VPN access to the database. Another part of this is defining the different working groups and their required systems. If a user works in accounting they should not have access to the same systems as IT and therefore should not be placed in the same area of the network as IT. At the same time payroll and human resources both require intercommunication, so putting them each in their own secured area of operations will also cause problems.

There are thousands of different ways that an organization can configure its network architecture for layer defensive. However, no matter your company needs there is a single basic design that should form the backbone of your security strategy. Starting from the outside the first thing that should be on the network is a signature based IDPS [2]. This will look at all traffic coming from the Internet and examine it for traces of attacks. This works like a watch tower on the boarder protecting everything in the network from now malicious signatures.

The next item on the network should be routers [2]. The first router serves two purposes. First, it can mask what is on the network by taking the address from the ISP and converting it to a private address scheme. Secondly the router helps to move traffic through the DMZ. The DMZ is an area that will be created between the first router and the firewall. This midway defense allows objects that need access to certain ports or resource to operate. Regardless of what an organization decided to put in its DMZ everything on the DMZ should have an application based behavioral IDPS. Working like a village militia the IDSP on the DMZ hardware works as a second form of review for packets allowed on the network. The guard tower on the boarder might let three men in with an innocent cargo but the town militia will be able to see that the cargo is being configured into a bomb. Similarly with network security, it is possible to get a malicious payload past a signature based IDPS by fragmenting a packer, but the behavioral based IDSP on the hardware in the DMZ will pick up on the malicious intent of the payload as the fragments are reassembled.

As stated before the third line of basic defense that should be configured on the network is the firewall [2]. At this point little restriction has been placed on traffic coming into the network. Like a traveler coming into the country only need to have their paper work in line, packets at this point only have to past the test of not seeming malicious. However there are many malicious threats on a network that do not require a malicious signatures espionage and backdoors like an assassin in the kingdom will not be recognized until it is too late. This is where the firewall comes into place. Like the guards at the town gates and the barbican, the firewall scrutinizes everything in and out of the network. The firewall will turn off ports, and deny traffic to and from certain address effectively only allowing authorized traffic into and out of the network. This part of the defense protects the network anything that may not have a malicious behavior. An example would be a hacker only trying to acquire intellectual property (IP). Getting past the IDPS and the router is possible without the use of malicious software by using proper recon. Port Scanning and Ping sweeping will reveal a lot of information on the network. A firewall however will prevent this. By turning off ports, using port forwarding, and denying ICMP (Internet Control Message Protocol) request through a firewall a hacker would only ever be able to determine is on the DMZ because the firewall is masking everything else.

The final basic line of defense is the secondary router [2]. This router works as an internal defense for the organizations. This router will separate the different assets inside the network into the different working groups. This router will establish the VPNs for traffic going to the DMZ and the Internet. This part of the defense works like a castles royal guard determining who is allowed into and out of the castle, which rooms they may or may not enter, and who they are allowed to converse with. The only defenses past this router will be client and application based anti-viruses and operating system hardening which would not protect against internal threats, thus the important of using this second router to disseminate the network traffic in to proper working groups.

While this is a very top down look as a secure network infrastructure with layered defenses it is still important for an organization to review its needs and modus operandi to properly decide what assets go where on the network. However by using this basic design as the backbone of the networks layout it is possible to have maximum protection and efficiency no matter what the location of the other network assets.

With all policies and software configurations in place on the network defenses and all devices are placed in properly layered network architecture. The task of testing is left as the final step to proper network security.

### C. Testing the Defenses

Current military operations have the army establishing FOBs (Forward Operating Bases) in mission critical areas. These unlike established bases are very vulnerable to attack and those manning them must be able to protect against everything from a full frontal assault to a mortar bombardment. Because of this troops must constantly train and test on mock FOBs to establish what does and doesn't work when protecting it. In the same sense of urgency, network security personal must also protect the network from a wide array of attack types. They must constantly test, review, update, and retest the network to ensure that every avenue of attack from DDoS to logic bomb is defended against. This should be done by means of penetration testing.

Penetration testing like having mock fire fights on a FOB is benign hacking attempted done by either a certified contractor or by and authorized tester in the organization [7]. Their job is to periodically stage attacks on company assets and defenses not only testing their strengths but also looking for ways around them. The test will use all tools that a hacker would use to carry out the test and for that test the network security personnel can make needed changes to a defense configuration of an organization's security policy. Every time a change is made to the network a test should be done to ensure that the change has not opened a vulnerability to the network [7].

The General Sun Tzu said "If you know yourself and know your enemy you will be victorious in 1,000 battles [15]." Taking this to heart and regularly testing a network in a war gaming style to gain insight into the mind of those who would cause the network harm, and properly configuring the network architecture and knowing how they work. Network security personnel will be able to effectively defend the network against anything.

## V. CONCLUSION

In closing, layers network security is an ever changing, and continuous evolution. It is important for those designing the network architecture to review what types of threats will be directed at their network. This is a key in designing a secure network. With that said, regardless of where or how the assets of a network are placed designers should ensure that multiple measures are taken to protect these assets. At a minimum these defenses should include a firewall and an IDS or IPS. They should be layered in a way that all traffic coming or going from the network is reviewed. Finally, administrators must configure these and other devices to implement all aspects of an organization's policies. They must also continually test, review, and reconfigure all levels of security measures. While creating a network that is 100% secure is nearly impossible with today's technology, by taking the information described here and applying it to the design and configuration of a network an organization can better protect themselves against the ever evolving threats posed by hackers and malware.

## REFERENCES

[1] Beigh, B, Peer. A (2012) Intrusion Detection and Prevention System: Classification and Quick Review; ARPN Journal of Science and Technology; VOL. 2, NO. 7, August 2012 Retrieved from. www.ejournalofscience.org/archive/vol2no7/vol2no7_17.pdf

[2] Conkil, WM., White, G. (2010). Principles of Computer Security: CompTIA Security+ and Beyond.

[3] Cotton, R. (2012, February 23). Where do hackers come from. Business Works. Retrieved from http://www.biz-works.net/index.php5?SID&fl=y&pgid=bp&art=188

[4] Gouda,M. Liu, A. (2007) Structured firewall design; Computer Networks 51 (2007) 1106–1120" retrieved from www.cs.utexas.edu/.../journal/Firewall.pd

[5] Hull, M. (2011). Castle Defenses. Retrieved from http://www.castles-of-britain.com/defenses.htm

[6] Jawhar, M. Mehrotra, M. Design Network Intrusion Detection System using hybrid Fuzzy-Neural Network; International Journal of Computer Science and Security, Volume (4): Issue (3) Retrieved from www.cscjournals.org/csc/manuscript/Journals/IJCSS/.../IJCSS-288.pdf

[7] Krutz, R., Vines, R. (2008). The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking. Indianapolis, IN

[8] Mello, J. P. (2013, May 24). Layered defenses largely fail to block exploits, says NSS. CSO Online. Retrieved from http://www.csoonline.com/article/733975/layered-defenses-largely-fail-to-block-exploits-says-nss

[9] Messmer, E. (2010). ZeuS botnet code keeps getting better… for criminals. Network World. Retrieved from http://www.networkworld.com/news/2010/031110-zeus-botnet.html?page=2

[10] Perrin, C. (2008, December 18). Understanding layered security and defense in depth. Tech Republic. Retrieved from http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/

[11] SOPHOS (2014). Security Threat Report; Smarter, Shadier, Stealthier Malware. Retrieved from http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

[12] Systems Engineering (n.d.). Layered approach to managed security. Retrieved from http://www.syseng.com/white_paper/managed_security_layered_approach.php

[13] TechNet (2014). Common types of network attacks. Microsoft. Retrieved from http://technet.microsoft.com/en-us/library/cc959354.aspx

[14] TechNet, (2014). Security content overview. Microsoft. Retrieved from http://technet.microsoft.com/en-us/library/cc767969.aspx

[15] The Art of War: And Other Classics of Eastern Thought. (2013). New York, NY: Sterling

[16] Weaver, R., Weaver, D. and Farwood, D. (2013). Guide to network defense and countermeasures. Boston, MA: Cengage Learning

[17] Whitman, M. E., Mattord, H. J., & Green, A. G. (2012). Guide to firewalls and VPNs (3rd ed.). Boston, MA: Course Technology Cengage Learning.

[18] "A Comprehensive Readiness Assessment Framework for Identity Theft Safeguards in Web-based Electronic Government Systems." with Jungwoo Ryoo, Tae Hwan Oh, and Seungjae Shin. The Electronic Government: An International Journal, pp. 19-40, Vol. 6, No. 1, 2009.

[19] "A Multi-Dimensional Classification Framework for Developing Context-Specific Wireless LAN Security Attack Taxonomies." with Jungwoo Ryoo, Tae H. Oh, and Gregory Corbin. The International Journal of Mobile Communications (IJMC), pp. 253-267, Vol. 7, No. 2, 2009.