Journal of Information Security, **2013, 4, 144-149**
http://dx.doi.org/10.4236/jis.2013.43017 Published Online July 2013 (http://www.scirp.org/journal/jis)

Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth

Lance Cleghorn
School of Information Technology and Computer Science, East Carolina University, Greenville, USA
Email: Cleghornl08@Outlook.com

Received May 17, 2013; revised June 18, 2013; accepted June 26, 2013

ABSTRACT

The defense in depth methodology was popularized in the early 2000's amid growing concerns for information security; this paper will address the shortcomings of early implementations. In the last two years, many supporters of the defense in depth security methodology have changed their allegiance to an offshoot method dubbed the defense in breadth methodology. A substantial portion of this paper's body will be devoted to comparing real-world usage scenarios and discussing the flaws in each method. A major goal of this publication will be to assist readers in selecting a method that will best benefit their personal environment. Scenarios certainly exist where one method may be clearly favored; this article will help identify the factors that make one method a clear choice over another. This paper will strive not only to highlight key strengths and weaknesses for the two strategies listed, but also provide the evaluation techniques necessary for readers to apply to other popular methodologies in order to make the most appropriate personal determinations.

Keywords: Defense in Depth, Defense in Breadth; Network Defense; Security Architecture; Defense Methodology; Information Assurance

1. Defense in Depth

Defense in Depth is an information security practice adapted from a military defense strategy where an attacker is forced to overcome a great many obstacles that eventually expend the attacker's resources [1]. In terms of information security, an administrator layers their assets in defensive measures that will deter casual attackers seeking to gain unauthorized access [2]. Layers of defense often overlap in order to ensure that traffic is processed multiple times by heterogeneous security technologies in hopes that the shortcomings of one security control are covered by another [3]. A well-tuned defense in depth architecture will prevent a vast majority of attacks and alert an administrator to intrusions that pass through [4].

Evaluating the Defense in Depth strategy in terms of current threats will provide additional insight into the key aspects of the strategy [5]. Automated attacks occur almost constantly against any public-facing service; however, these attacks lack sophistication as they often are carried out by a program rather than a live, skilled person [6]. Defense in Depth is a superb method of minimizing and preventing automated attacks, considering automated attacks seek out the most vulnerable assets facing the public Internet [4]. An active attacker scenario in which a live attacker is attempting to exploit an information asset is more difficult to analyze. Depending on the source of the attack (internal or external), the Defense in Depth architecture may provide differential protection [4].

In a scenario where an attacker is actively attempting to gain access from the internet, a defense in depth strategy will deflect the attack, assuming that security measures like Network Address Translation (NAT), a firewall, a Demilitarized Zone (DMZ), and gateway Intrusion Detection System (IDS) are in place [6-8]. Each of the aforementioned security devices provides an obstacle that an attacker must navigate; even skilled attackers who lack motivation will be deterred by a plethora of security controls [2]. In contrast, networks saw a large increase in attacks from inside a network when attackers learned that penetration from the inside was significantly easier since it bypassed a majority of the perimeter defenses [9-11]. While the defense in depth methodology should be applied to all assets equally, many practitioners clustered defenses at the perimeter [9]. Advances in the practice of defense in depth have led to a more comprehensive security deployment [5].

Advanced Persistent Threats (APT) provide an entirely new challenge to administrators, who now have to face organized attackers with resources and motivation that have never been seen before [11,12]. Admittedly, the defense in depth architecture is adapting lethargically to this new category of threats; however, the basic concepts of the strategy hold true even against these new threats [5]. An administrator must apply security controls continually and keep up with the threat spectrum that is attempting to gain unauthorized access to data assets [13,14]. One major aspect that puts APTs at the top of the threat food chain is the ability to adapt zero-day vulnerabilities into an attack [11]. As a result, a well-tuned defense in depth architecture should be able to adapt new zero-day malware detection immediately. A system like FireEye boasts the ability to detect malicious payloads in zero-day vulnerabilities [14].

Defense in Depth is a tried and proven method of preventing automated attacks and many attacks with an active attacker participating in the intrusion [15]. The security methodology is also able to adapt to new threats by layering in new security controls as they become available. In a properly tuned environment an administrator should at least receive log alerts on threats that pass though some security controls and an active administrator should be able to step in and prevent further compromise. A fine-tuned architecture of defense in depth technologies includes motived and educated administrators [2].

Layering many heterogeneous technologies in an environment often leads to extensive administrative overhead [16]. Often this administrative overhead results in administrators becoming overwhelmed, and in this case the administrators may allow security responsibilities to slip, opening the door to security threats [16]. Additionally, administrators may be inclined to rely on homogeneous security architecture like that of a Unified Threat Management (UTM) system [17]. Homogeneous environments present a single attack surface that may allow an attacker to circumvent all security controls by compromising the UTM system [17].

Defense in Depth is a tool which is only as useful as the administrators using it. Improperly deployed, the defense in depth architecture weakens the human component and makes this system difficult to maintain [5]. A lack of higher education and extensive experience in information security professionals intensifies the difficulty of maintaining a defense in depth architecture. The entire methodology depends on the motivation, determination, and skill of human resources that often work 9 to 5 and easily become complacent [18].

The defense in depth architecture concedes several points inherently that are worth noting as many criticisms of the methodology focus on these concessions. The architecture concedes that attacks will occur, and given enough time these attacks will begin to circumvent security controls [19]. Given infinite time the attacks will circumvent all security measures. The architecture must layer defenses in such a way that balances security with overhead and adequately defends resources at different Open Systems Interconnection (OSI) layers throughout the network topology; this inherently produces overhead which must be managed and countered [1,6].

2. Defense in Breadth

Defense in Breadth is a methodology that came about suddenly with little legitimate acknowledgement in the information security community. Rather than a fully developed methodology, Defense in Breadth appears to just be a patch for the Defense in Depth architecture already in place that promises to fix the issues without addressing the root causes [9]. Aspects of the Defense in Breadth methodology are sound; however, the similarities to the Defense in Depth method are apparent. The founding principal of Defense in Breadth is layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another [9,10].

Some companies like F5 used the Defense in Breadth methodology to market security technologies to corporations already protected by other companies [10]. The entire methodology is comparable to installing multiple anti-virus software programs on a single host to make sure that what one misses the others catch. Any administrator worth his or her salt would scoff at the thought of installing multiple anti-virus programs, and the reasons that make this example unsound are the same that make Defense in Breadth impractical. Many security technologies are not designed to work in concert with competitive technologies providing the same benefits, and doing so can cause more problems than it solves [3,17].

The return on investment for the acquisition of redundant heterogeneous security devices would be nonexistent save for the promises of preventing security breaches that could cost the organization dearly in loss of reputation and proprietary information. Defense in Breadth is a grand idea; however, the practice just does not make sense in a real-world scenario. Layering defense technologies in concentrated areas throughout the network forces administrators to devote exponentially more time and resources, leaving other areas of the network vulnerable [7,20]. Just as the uptake in internal threats occurred when perimeter technologies became layered and redundant, we now see a reverse of this phenomenon as external threats become more prevalent [20].

Defense in Breadth lacks foresight and adaptability to new threats. Zero-day exploits will hit where no signature-based intrusion detection system can defend; how-

ever, adding an anomaly-based intrusion detection system adds significant overhead with little likelihood of catching exploits [11]. Diversifying security controls and dispersing them throughout the network is the only way to ensure that a conscious effort is being made to defend the network and data assets. Adding a zero-day analysis technology like Fire Eye diversifies the security infrastructure and actually addresses new attack vectors [13]. Clustering redundant technologies just does not solve the issues facing information security professionals.

When properly deployed, Defense in Breadth could hypothetically provide the same benefits of routing attacks as Defense in Depth; however, upon the introduction of a new attack vector this methodology is lethargic and slow to adapt as the resources required to defend new vectors are considerable [10]. If an organization could solve information security issues simply by throwing money at them then we would not see the massive increase in high-profile security breaches [11,12]. Administrators of security technologies have to begin taking responsibility for failures in deployment; scapegoating the principals that govern information security is forcing digression among the security community. **Figure 1** summarizes some of the more obvious strengths and weaknesses that come from comparing the two popular models of network defense.

3. Elements of a Defense Methodology

Both Defense in Depth and Defense in Breadth suffer from human imperfection. Both strategies provide for a more secure network assuming they are implemented correctly. Assuming that as an administrator your primary goal is to improve the security of your network and that human resource elements are mostly beyond your control, there are many improvements that can be made within the scope of the information security department [19]. For whichever methodology appeals to your organization there are some strategies that can be followed to ensure you are prepared for the next threat to hit your doorstep. Five key pillars of information defense may be used to improve existing security architectures or build a new strategy from the ground up.

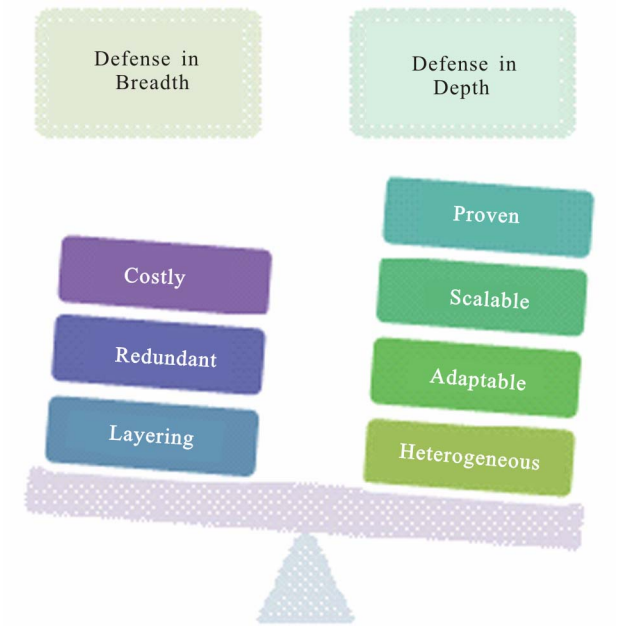

Figure 1. Graphical comparison of methodologies.

First, fortify your network. Begin by covering all obvious attack vectors and bottlenecks with security controls. The fortification of a network is essential to building a working security architecture [3]. At the perimeter of the network traffic should be filtered by a stateful firewall, examined by an intrusion prevention system, and evaluated by an anti-malware technology [17,20] This combination of controls contains elements of Defense in Depth and Defense in Breadth; while all of these technologies provide a distinct function they are layered in such a way that one can detect what another may miss. The stateful firewall filters traffic fairly broadly and should require little in terms of updates and maintenance. The firewall will shield a network from attacks at an array of OSI levels depending on the firewall features [3]. A network based intrusion prevention system at the perimeter can respond to a wide array of threats, a signature-based alternative is best at the perimeter as the learning stage of an anomaly-based system may prove ineffective and cumbersome [13]. Finally an anti-malware system can perform deep packet inspection on traffic and look for zero-day malware [19]. **Figure 2** depicts a multilayer defense perimeter that should be present between major network segments of different trust levels.

The perimeter is a bottleneck that functions as the first and last line of defense in many attacks; attacks that originate from outside the network and seek to exfiltrate data from the network must leave the same way they entered [3,21]. Internal attacks also must leave the network at some point to exfiltrate data [21]. Fortification of the perimeter is key in a defense architecture; however, the DMZ, and the internal network cannot be ignored [17]. Implementing anti-virus, a host-based intrusion detection system, and a host-based firewall should be mandatory on all servers and workstations [17]. Both the internal network and the DMZ could benefit from layering in a network-based intrusion detection system in each network [3]. Hardening servers and workstations should be a priority as this type of control provides a great deal of security with little overhead [17]. **Figure 3** is an example of layering heterogeneous defenses to defend an asset. Multiple controls should be in place and utilized to defend areas where information is at rest.

Disperse security controls to key areas of the network. Fortification addresses the technologies necessary for a

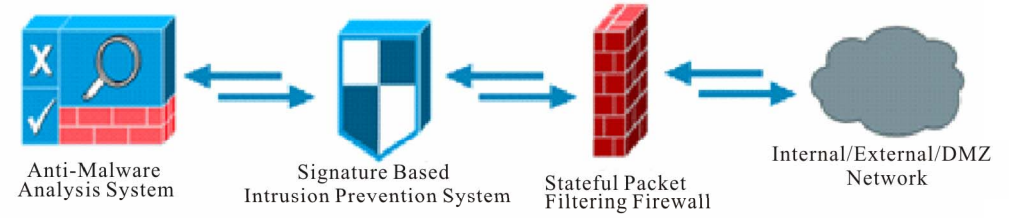

Figure 2. Fortification of the network perimeter.

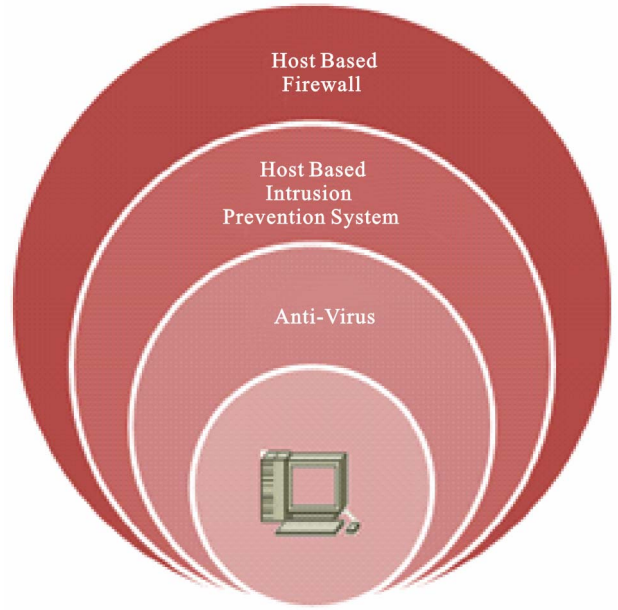

Figure 3. Fortification of host nodes.

good defense, and as mentioned, the placement of these technologies is essential [1]. Dispersing controls throughout the network and on either side of a bottleneck ensures that the attack surface is shielded without gaps. Identify your assets and know where proprietary data is stored, isolate your most important assets, and make sure security controls are in place that will force an attacker to overcome great obstacles [6]. Requiring authentication unrelated to your domain to access key servers may be the key to preventing a successful attack [17]. Dispersing security controls is the best way to contain a breach if one were to occur, this gives the administrator time to stop the attack and protect the network and its assets. Dispersion also forces administrators to evaluate different areas of the network that often go ignored for long periods of time [6].

Diversify security controls and utilize a variety of vendors. While many information security companies make a wide range of products, they often contain some of the same coding and technology that can create a single attack vector [7,16]. Purchasing from a diverse group of vendors will without a doubt add the greatest amount of overhead to an administrator and it is for this reason that it is often avoided, so be cautious with your diversification [9]. Evaluate products not only on their effectiveness but also on their ease of administration. Do not go overboard in diversification [21]. Carefully evaluate where to diversify to make sure you receive the most benefit for your sacrifice in overhead. Try to avoid homogeneous technologies and vendors in any one bottleneck. Place importance on ensuring that data travels through a diverse heterogeneous set of security technologies each time it travels. Mapping out traffic patterns in your network may assist greatly in understanding where to diversify [3].

Monitor the state of your network and look for signs of intrusion. Parsing logs is not the most exciting way to spend any amount of time; however, proper monitoring of security controls can aid in eventually producing effective e-mail alerts [18]. Fine tuning the security architecture will provide a great deal of results and bolster efficiency within the information security department. Even after tuning and learning is completed a daily review of high-priority logs and a weekly review of lower logs may be the key to detecting advanced persistent threats or other intrusions [11]. Monitoring the network will aid in the eventual changes that must occur within the architecture, and while it may not be particularly exciting, it is pivotal to a good security architecture [17].

Maintain the architecture and adapt it as new attack vectors and surfaces become available. Maintenance is not only the method by which new signatures are installed and patches applied, but the maintenance of the architecture itself is also necessary to securing the network [4]. Trends like “bring your own device” create serious challenges to the security architecture as it may remove a key bottleneck from your administration [17]. Implementing security controls that quarantine and evaluate new nodes may become a part of the architecture and these new nodes may introduce a horde of new vulnerabilities and threats to your network [7]. Maintenance is also the catalyst for determining the lifecycle of a control—while a perimeter firewall may last three to five years, the host-based firewall may be changed yearly. Use the habits from the monitoring section to decide how to best maintain your security controls. Remember that the physical devices themselves should not be forgotten as they may also fail [12]. **Figure 4** shows how each of

these pillars is used to form a new defense methodology that is made up of essential security practices rather than checklists and abstracts.

4. Conclusions

The various methods of defense purport benefits and entail consequences that may be counterproductive in practice. An administrator should design a security posture around essential elements and use either defense in depth or defense in breadth as a guideline. Understanding the components and elements of each methodology will help an administrator make a more informed choice; however, the target network must also be considered to ensure that the correct methodology is implemented [3]. As an administrator, you must consider all options and perhaps elements of both the defense in depth and defense in breadth methodologies appeal to and suit your network. Also consider that a hybrid method may be the most favorable of all [9,19].

There are pitfalls to a security architecture design that must be avoided. Haphazardly purchasing and setting up security technologies often will not improve security at all and may even weaken it [17]. Having a carefully considered plan is the first step to design an information defense strategy. Just as important as the plan is the human aspect to security. Understand the human asset constraints that exist in your network. If you know that your organization is exclusively five days a week and 9 to 5 then steps must be taken to ensure that the information assets remain protected and intrusions can be prevented in the off hours. Vulnerabilities in human assets are just as dangerous as those in our information systems [18].

When possible, administrators should choose team members who are motivated and interested in the field of information security. Team members should be interested in learning as the field of information security is constantly evolving, and complacency leads to weakness. Security administrators should understand that higher education in team members is exceedingly valuable; the foundations of information security cannot be imparted in on-the-job training. Choose well-rounded security professionals who combine industry certifications with experience and education. Treat human resources just like any other security control, and choose a good product that requires minimal overhead and yields the greatest benefit to the security posture.

Security postures and methodologies are constantly changing and improving. Often it may be more productive to examine what makes a methodology appealing and use that to create or improve the organization's posture. Fortify, Disperse, Diversify, Monitor, and Maintain: these elements are outlined in this paper as key pillars in a defense methodology and should be included in some fashion in all security postures. Adding additional pillars only strengthens the organization's posture, so carefully consider what factors are most important to your particular network and design your security posture around those factors. To begin to understand your network, evaluate the data and resources that is the most essential to your organization's survival. Tactically it is sound to group your most precious assets in the most defendable position inside the network [4]. Layering defenses can be beneficial to the security posture if it is done with a conscious goal and in such a way that it provides more functionality than overhead [9].

Figure 4. Pillars of a good defense methodology.

There simply is no cookie cutter security template that you can just apply to your network and generate a shopping list of technologies for application. Defense in Depth was never designed to function as a magical solution, and too much emphasis has been placed on the methodology and not enough on the actual concepts involved [4,19]. The defense in depth methodology is only a set of best practices, and like this paper it aims to inform administrators and aid them in designing the best security posture for their organization [4]. The public failings of information security in high-profile organizations led some to blame Defense in Depth and propose Defense in Breadth [9,10,12]. Defense in Breadth does add beneficial concepts to the Defense in Depth methodology; however, it also does not magically solve all information security issues. Administrators should evaluate security methodologies only as best practices and utilize them as resources and not a master plan.

REFERENCES

[1] T. McGuiness, "Defense in Depth," SANS Institute, Bethesda, 2001.

[2] M. Luallen, and S. Hamburg (2009) Applying Security Defense-In-Depth," *Control Engineering*, 2009, pp. 49-51.

[3] R. Weaver, "Guide to Network Defense and Countermeasures," Course Technology, Boston, 2007.

[4] National Security Agency, "Defense in Depth," 2012. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

[5] S. Groat, J. Tront and R. Marchany, "Advancing the Defense in Depth Model," *The 7th International Conference on System of Systems Engineering* (*SoSE*), Genoa, 16-19 July 2012, pp. 285-290.

[6] Defense Information Systems Agency, "Network Infrastructure Technology Overview," Department of Defense, Ft. Meade, 2010.

[7] C. Paquet, "Implementing Cisco IOS Network Security: Authorized Self-Study Guide," Cisco Press, Indianapolis, 2009.

[8] L. MacVittie and D. Holmes, "The New Data Center Firewall Paradigm," F5 Networks, Inc., Seattle, 2012.

[9] P. E. Small, "Defense in Depth: An Impractical Strategy for a Cyber World." SANS Institute, Bethesda, 2011.

[10] L. MacVittie, "F5 Friday: Goodbye Defense in Depth. Hello Defense in Breadth," 2012. https://devcentral.f5.com/weblogs/macvittie/archive/2012/01/27/f5-friday-goodbye-defense-in-depth.-hello-defense-in-breadth.aspx

[11] R. Miller, "Advanced Persistent Threats: Defending from the Inside Out," 2012. http://www.ca.com/~/media/Files/whitepapers/advanced-persistent-threats-wp.pdf

[12] A. W. Coviello, "Open Letter to RSA Customers," 2011. http://www.eweek.com/c/a/Security/RSA-Will-Replace-SecurID-Tokens-in-Response-to-Lockheed-Martin-Attack-409915/

[13] FireEye Inc., "Spear Phishing Attacks—Why They are Successful and How to Stop Them," 2012. http://www.fireeye.com/resources/pdfs/white-papers/fireeye-how-stop-spearphishing.pdf

[14] FireEye, Inc., "Advanced Targeted Attacks: How to Protect Against the Next Generation of Cyber Attacks," FireEye, Inc., Milpitas, 2012.

[15] OWASP, "Defense in Depth," 2012. https://www.owasp.org/index.php/Defense_in_depth

[16] Untangle Inc., "Web Content Control: Five Steps to a Successful Implementation," 2012. http://www.untangle.com/wp-content/uploads/pdf/FiveStepsToWebContentControl.pdf

[17] W. Stallings and L. Brown, "Computer Security Principals and Practice," Prentice Hall, Upper Saddle River, 2012.

[18] U. Rivner, "Speaking of Security: Uri Rivner," 2012. http://blogs.rsa.com/author/rivner/

[19] V. Hazlewood, "Defense-In-Depth: An Information Assurance Strategy for the Enterprise," San Diego Supercomputer Center, La Jolla, 2006.

[20] W. Odom, "CCNP ROUTE Official Certification Guide," Cisco Press, Indianapolis, 2010.

[21] G. Rajaratnam, S. Gnanasundaram and A. Shrivastava, "Information Storage and Management," John Wiley & Sons, Inc., Indianapolis, 2012.

