

Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems

Moses Garuba, Chunmei Liu, and Duane Fraites
Department of Systems and Computer Science, Howard University

Abstract

Organizations require security systems that are flexible and adaptable in order to combat increasing threats from software vulnerabilities, virus attacks and other malicious code, in addition to internal attacks. Network intrusion detection systems, which are part of the layered defense scheme, must be able to meet these organizational objectives in order to be effective. Although signature based network intrusion detection systems meet several organizational security objectives, heuristic based network intrusion detection systems are able to fully meet the objectives of the organization. Through a comparative theoretical study, this paper analyzes several organizational security objectives in order to determine the network intrusion detection system that effectively meets these objectives. Through conclusive analysis of the study, heuristic based systems are better served to meet the organizational objectives than signature based systems. The analysis was based on which system provided definitive security objectives and offered the flexibility, adaptability, and reduced vulnerability that an organization requires.

1. INTRODUCTION

The movement towards a more secured computing system continues to rise as management becomes cognizant of the numerous threats that exist to their organizations. Currently, there are numerous controls; of a technical, physical and administrative nature that are implemented to mitigate threats. This paper is focused on technical controls, primarily on network intrusion detection systems (NIDS) and the benefits that are drawn from implementing a heuristic based NIDS in comparison to a signature based NIDS. The role of NIDSs as Pfleeger and Pfleeger describe, lends to the defense in depth schematic by providing one layer in the layers of protection required for a network [10]. Although, there are skeptics as to the feasibility of detection systems, Chuvakin asserts that “the nature and complexity of electronic communication lead one to believe that 100 percent effective prevention is unachievable” [1]. Consequently, the importance of detection devices cannot be understated; rather they should be used in conjunction with other types of security devices. Furthermore, an organization’s network cannot be secured through one security device; neither can it be secured through multiple security devices. Pfleeger and Pfleeger assert that secure

systems are impossible because it entails securing a system for both present and future threats [10]. Pfleeger and Pfleeger indicate that a “trusted system” can be developed through a layered defense and supports the use of IDS as part of this layered defense [10]. Therefore, identifying an adequate NIDS is of paramount importance to the overall security objective of any organization.

The structure of the paper is organized as follows. The third section introduces intrusion detection systems (IDS), in particular the two types of NIDS, which would be the focus of the paper. The fourth section justifies the necessity for NIDS by identifying the various network threats that exist. The fifth section explores topically, the cost benefit analysis of implementing a NIDS. The sixth section develops a comparative study delineating the benefits offered by heuristic and signature based NIDS. The following two sections draw conclusions from the preceding sections and introduce future works, respectively.

2. RELATED WORK

Many works have been conducted in the area of IDSs and other network devices including defining and comparing the two various types of NIDS. Work also has been done in defining the cost benefit analysis of IDSs. However, work as to my knowledge, has not been done in comparing the security objectives for the purpose of management.

3. INTRUSION DETECTION SYSTEMS

Intrusion detection systems are classified into two general types known as signature based and heuristic based. Pfleeger and Pfleeger describe signature-based systems as “pattern-matching” systems that detect threats based on the signature of the attack matching a known pattern. Heuristic based systems, which are synonymous with anomaly-based systems, detect attacks through deviations from a model of normal behavior [10]. IDSs that operate on a single workstation are known as host intrusion detection system (HIDS), while those that operate as stand-alone devices on a network are known as NIDS. HIDS monitor traffic on its host machine by utilizing the resources of its host to detect attacks. NIDS operate as a stand-alone device that monitors traffic on the network to detect attacks. NIDS come in two general forms; signature based NIDS and heuristic based NIDS. These two types of NIDS provide a varying degree

of security based on several objectives that will be analyzed in forthcoming sections.

4. NETWORK THREATS

NIDSs are normally one of the first lines of defense, along with firewalls, in a typical network security model. Consequently, NIDS must be able to monitor extensive and differing attacks. The tasks of monitoring the traffic throughout the network is becoming increasingly difficult as new threats and vulnerabilities are exposed every year. The problem is further compounded by the exorbitantly high number of sites that contain malicious code and the ease in which these codes can be deployed. Lemke indicates through a report by Symantec, that there are more than 38,000 Web sites containing source code for virus and worms [7]. McHugh, Allen and Christie provide further evidence by stating that “anyone can attack Internet sites using readily available intrusion tools and exploit scripts that capitalize on widely known vulnerabilities”[8]. The period where skilled and knowledgeable hackers developed and deployed attacks are now being replaced by novices with malicious intentions, readily deploying malicious code against unsuspecting organizations. The diagram found in Appendix 1, developed by McHugh, depicts a ten year period between 1990 and 2000 where the growing trend of intruder knowledge decreases while the sophistication of attacks increases [2].

The lack of knowledge required to attack an organization’s network using existing attacks is compounded further by the development of new software vulnerabilities through which attacks exploit. Messmer, who uses the study performed by Internet Security Systems indicates that software vulnerabilities recorded for the first eight months of 2006 exceeds all vulnerabilities found in 2005 [9]. As a result, security devices such as, NIDS must be able to detect and identify the various threats that exist. These threats require a robust system capable of defending against existing threats while having the flexibility to adapt to new threats.

Alternatively, much emphasis is placed on external threats, but NIDS must also be able to defend against internal threats. There are two types of internal threats: intentional attacks and unintentional attacks. Intentional attacks are malicious attacks carried out by employees for various reasons such as, financial payment from outside sources or disgruntled employees. Unintentional attacks such as, deleting important data files cause unwarranted performance and financial damage to the organization. Although seemingly unnoticed and inconsequential, internal attacks occur more frequently than outside attacks. Lynch proposes that between 60 to 70 percent of the attacks that occur within an organization are internal [18]. The threat of internal attacks are further magnified when the origin of most internal attacks are coming from the technical and network security personnel. CERT/CC (n.d.) conducted a

survey on insider attacks and found that over 80 percent of the attackers held technical positions within the organization [6]. Although a robust system is needed, a system that has a wide coverage scope is also required that can track the activities of external traffic in addition to the internal activities.

5. COST BENEFIT ANALYSIS OF IDS

Upon identification of the various threats to an organization, management should determine the financial savings that are incurred through acquiring a NIDS. The return on investment of an IDS and more specifically a NIDS, is beyond the scope of this paper, but its cost of implementation will be discussed. The cost of implementing and maintaining a NIDS should be considered in comparison to the potential risk impacts that can occur when not implemented. One consideration that an organization must account for before purchasing such a security device is whether their organization is large enough to justify such a purchase. Additionally, the probability of threat to various assets and resources must factor into the discussion. NIDS are suitable for medium to large scale organizations due to their volume of data and resources. For this reason many smaller companies are hesitant in deploying IDS as contended by Chuvakin [1]. The benefit of acquiring a NIDS is dependent on the fact that it costs less to implement and maintain than the loss that can be incurred due to vulnerabilities being exposed. As proposed by Iheagwara, Blyth and Singhal, the cost effectiveness of an IDS is determinant on any estimated loss from intrusions [6]. Several cost factors must be considered for acquiring and maintaining a NIDS. Cost factors such as, initial cost, ongoing maintenance cost, and personnel required for monitoring. McHugh provides estimated costs for these factors listed: initial cost is listed at \$10,000; maintenance cost is listed at 15 percent of the initial cost per year; and personnel cost is defined by the organization based on the level of monitoring they requires, whether continual or periodic monitoring [2]. The implementation and ongoing costs should then be compared to the potential risks impact that can be incurred by the organization to determine if there are the cost savings.

External attacks such as virus attacks and other malicious code can prove to be quite costly for organizations. Jacques identifies a research study indicating that malicious code attacks cost businesses between \$169bn to \$204bn for the year of 2004 [12]. Although this amount is a cumulative total for all businesses, it shows that financial losses are real for businesses affected. Then again, the cost of internal threats can prove even more costly as indicated by CERT/CC (n.d.) where they revealed that insider attacks can cost millions of dollars to any one organization [6]. With this in mind, it is safe to infer that acquiring a NIDS is justifiable based on the probable loss to the organization and the potential savings through implementation. Calculation

of the cost benefit of a NIDS allows organizations to focus on the basis of this paper, which is to determine the NIDS that fulfills the security objectives for an organization.

6. COMPARATIVE STUDY OF SECURITY OBJECTIVES

The comparative study of the security objectives of the two NIDS provides the basis of the paper. The two types of NIDS, heuristic and signature based, provide varying functions that can be beneficial to any organization. In light of these functions identified, the security objectives are analyzed and observations derived as to the more effective NIDS for an organization.

6.1 False Negative and Positive Alarms

The first organizational objective for consideration is the accuracy of the NIDS in detecting attacks and the frequency of its accuracy. The capability of the two types of NIDS; heuristic and signature based are then analyzed to determine their accuracy rate. In order to determine the accuracy of these two systems, the false negatives and false positives of these systems are deduced. Pfleeger and Pfleeger identify a false positive as an alarm being raised for benign activity and depict a false negative as no alarms being raised for a real attack [10]. Delving into the premise on which heuristic and signature based NIDS are structured through analysis, it can be inferred which type of system would create a particular type of false alarm.

False negatives are associated with signature based NIDS. Signature based NIDS require the use of signatures incorporated into its database to match the signatures of packets of data entering into the network. Signatures of known viruses and other malicious codes are placed in the database for signature matching. As a result, any attack for which it has the signature can be accurately identified and detected. Unfortunately, newly created malicious code or known viruses with modified signatures are allowed to go undetected within the system and are classed as a false negative. Such a drawback is owed to the inability of signature based NIDS to detect new attacks as stated by McHugh et al. [8]. False positives are also generated by signature based NIDS as supported by Conorich, who indicates that outdated malicious signatures could be the signatures of a new benign application programs [3] and a subsequently flagged due to these amendments.

Unlike signature based NIDS, the rate of false negatives are rare for heuristic systems as supported by Liston [13]. The non-dependence upon signatures and the use of statistical and behavioral patterns as the means to detect new types of malicious code allows for a low false negative rate. Heuristic based NIDS use behavioral patterns of users, applications and other program files to develop a pattern of normal and abnormal behavior, which is then used to detect

the occurrence of an attack. Subsequently, any deviation from normal behavior by a user or program within the system would be detected and flagged, thereby generating an alarm. Unfortunately, most alarms are benign and false positives are derived as a result. For example, a programmer with authorization to all aspects of the system, but usually works with programs files, may access log files and would be flagged as a result, since it deviates from the normal behavior of the programmer. High false positives, as asserted by Pfleeger and Pfleeger can lead to administrators becoming disenchanted with heuristic systems by investigating less, alarms raised [10]. Although, the high rate of false positives are solvable. In accordance with the structure of a heuristic based NIDS, refinement of its detective analysis is based on continued sampling of statistical and behavioral patterns. The greater the volume of data available for sampling correlates to its ability to distinguish between deviating behavior of benign applications and the behavior of malicious applications.

6.2 Updates

The organizational objective of updates is directly tied to the organizational objective of false alarms. For signature based NIDS, the inability of network personnel to provide timely updates of signatures, leaves an organization vulnerable against attacks and increases the number of false negatives as a result. Incompetent personnel can cause security vulnerabilities within an organization that utilizes a signature based NIDS, but this problem can be easily resolved through the hiring of a competent staff. The main problem of concern is not the competency of security personnel; rather, the dependency upon updates that creates vulnerabilities.

McHugh et al. indicates that the rapid change of product lists, surveys, and reviews cause software to become quickly outdated [8]. Correspondingly, CERT (2006) has identified over 5300 new software vulnerabilities for the first three quarters of 2006 [14]. The direct correlation is evident as the necessity for frequent updates becomes mandatory, which is compounded further by the obsolescence of the signatures within the database. As a result, the detective ability of a signature based NIDS is cast in doubt. The probability of identifying all new and existing vulnerabilities and malicious codes is significantly low. Furthermore, the constant deployment of new vulnerabilities and threats compounds the problem. Consequently, security personnel are unable to determine their level of preparedness against diverse threats.

The dependency of signature based NIDS on updates is at the root of the problem. A system that requires updates of newly created signatures in order to identify attacks is therefore limited by the signatures that it contains. This inherent limitation allows the system to suffer from attacks that have not been accounted for. Vulnerabilities are established, not from signatures that are contained within

the database, rather, from signatures that are not updated to the database. As a result, it requires that personnel must be able to identify vulnerabilities and threats before they are actually developed, which is unfathomable. The reactive nature of signature based NIDS supports such a premise. Signatures are only identified after conception, but attacks against the network have already taken place before signatures are developed to identify such attacks. Therefore, the system employs a reactive approach that minimizes its detection rate. Additionally, a high rate of false positives is also associated with this type of NIDS. Conorich indicates that updates are required to delete outdated signatures that are being utilized by software developers as new application programs [3]. Therefore, monitoring of signatures that are being used for benign programs is also required in the update process in order to lower the possibility of false positives.

Heuristic based NIDS are not dependent on updates and only require periodic adjustments to refine its behavioral analysis. The ability of heuristic systems to detect new and existing abnormal or malicious activity provides network personnel with the assurance of its preparedness against attacks. One of the drawbacks identified for heuristic systems as indicated by the National Institute of Standards and Technology (NIST), is their propensity for false positives because of their ability to detect new attacks [15]. This drawback of false positives is actually an understated advantage for heuristic systems in regards to updates and maintenance.

As discussed prior, signature based systems are disadvantageous because of their established dependency on updates and their reactive nature, whereby vulnerabilities are produced through signatures that were not captured. Conversely, a high number of false positives for heuristic systems indicate their non-dependency on updates and allows for a proactive approach, which reduces the possibility of creating vulnerabilities within the system. The basis for such a premise is based on how false positives are derived. As introduced prior, false positives occur for heuristic systems when benign programs, applications and users perform abnormal patterns deviating from past behavioral patterns. Although, false positive are a nuisance, the human element is eliminated from the updating process where most of the vulnerabilities are introduced. The capability of the system to update its behavioral patterns and take a proactive approach, allows for a higher level of security. As a result, threats are not detected based on information provided by personnel, but rather based on empirical behavioral patterns over a period of time. Therefore, heuristic systems are truly standalone devices and are able to avoid the introduction of vulnerabilities associated with updates. The problem of false alarms, while disconcerting to personnel, provides indefinite security coverage. False positives indicate a proactive approach to the identification of threats. Being proactive implies that the system is capable not only of identifying known threats,

but is also capable of identifying new threats by utilizing patterns of known behavior to depict a new attack. Therefore, it does not react to the development of a new attack; rather, it identifies the attack based on its deviation from known patterns. Therein lays the strength of heuristic systems in its ability to identify old and new threats likewise, as asserted by McHugh et al. [8]. Eliminating the dependency on updates creates a robust and secure system allowing for an adaptive system against all threats.

6.3 Competency

The organizational objective of competency of network personnel is directly tied to the issue of vulnerabilities being introduced through updates. A detection system that is dependent directly upon the competency of personnel is an insecure system. NIDS are developed to be standalone devices whereby only monitoring and minimal maintenance by personnel is required. As discussed in the previous subsection, the dependency of signature based NIDS creates the necessity of intervention by personnel to update the signatures of the system, which brings the issue of competency into focus.

Signature based NIDS are entirely dependent upon the competency of network personnel to detect attacks. Halme & Bauer further illustrate the dependency of signature based NIDS by indicating that their developers (and subsequently their system security officers) have to be knowledgeable about various software vulnerabilities [4]. It is therefore evident that an incompetent network security personnel correlates to an ineffective signature based NIDS. Technical detection controls whose performances are dependent on the human element are not beneficial to an organization. As McHugh et al. postulates, administrators are better served minimizing vulnerabilities through patches and other security measures than utilizing commercial IDSS, which attempt to detect known vulnerabilities [8]. Vulnerabilities are introduced, not because of incompetent workers, but because of the requirement placed on workers to identify all known threats. Therefore, the security purpose of an organization is not realized if the signature based NIDS cannot be trusted. Ultimately, competence of personnel should not be the only factor in determining the effectiveness of a security device.

The issue of competency does not impact upon the performance of a heuristic based NIDS. Conversely, its ability to detect threats is dependent upon its ability to determine abnormal patterns within the network. Its capability of learning, through statistical interpretation or modeling of behavioral patterns, whether accepted normal and abnormal behavior, allows for its performance to be driven independent of network personnel. Pfleeger and Pfleeger posit that heuristic systems should be targeted to the information that they are to analyze. Apart from monitoring, providing the focus for a heuristic based NIDS is the only function provided by personnel. Consequently,

the competency of personnel is discounted when evaluating the system, which provides a secure environment in contrast with the environment offered by a signature based NIDS. Moreover, its detection rate is not inhibited by incompetence. An independent system that requires minimal intervention provides an adequate security environment than a system that requires competent workers in order to maintain its level of security.

6.4 Susceptibility to Attacks

The organizational objective of susceptibility to attacks is very important to determine the level of security provided. Understanding the types of attacks that may go unnoticed and measures that are available to resolve this problem is very critical to the level of security offered by the two types of NIDS. Furthermore, the susceptibility to attacks of the two types of NIDS correlates directly to vulnerabilities introduced due to updates and competent workers. McHugh et al. stresses that the greatest threat to IDS is manifested through narrowly focused attacks launched by intruders who make serious attempts to avoid detection by current and proposed IDS [8]. The organizational objective of susceptibility to attacks is determinant on inherent flaws of the two types of NIDS. Therefore, the organization is vulnerable unless countermeasure can be employed to detect or minimize the frequency of undetected threats from evasive attacks.

Deploying countermeasures for signature-based systems against evasive attacks proves to be very difficult. Signature based systems utilize the technique of pattern matching. If known signatures are modified in any way that do not meet the pattern of the signatures contained within the database, no alarms are raised and the attack is undetected. Attackers utilize evasive attacks because they prey upon the weaknesses of the matching system, which can only match in accordance with what is stored in the database. The only countermeasure that counteracts the use of evasive signatures is the recognition by personnel that attacks are evading the detection of the system and add the modified signature to the database. Consequently, this proves to be quite difficult because it infers that personnel are aware of the evasive techniques being used and are able to determine how the signature of the attack was modified. Moreover, this countermeasure is entirely dependent upon the security personnel and the system is unable to develop countermeasures otherwise. Therefore, the susceptibility to attacks that exist within the structure of a signature based NIDS, continues to inhibit its detection rate because of the inability of personnel to identify all possible new or modified signatures.

Heuristic based systems also allow undetected threats into the network system, but its rate of detection to evasive techniques are significantly higher in comparison to signature based systems. As indicated by Taylor and Foss-Alves, heuristic based systems are capable of comparing

previous statistical or behavioral measurements to the measurements generated by the attack [16]. To evade a heuristic system implies that the intruder is aware of the behavioral patterns of normal existing systems on the network, in addition to determining what behavioral patterns would not be flagged by the heuristic system. As discussed prior, a benign program may be flagged as threatening because it exceeds its expected behavioral scope. The sensitivity of the system determines its capability of detecting evasive threats within the network. Additionally, its propensity to detect false positives also provides the ability to detect evasive threats. As discussed prior, heuristic systems raise alarms for benign files and programs that deviate from normal behavior. Conclusively, it is evident that evasive threats will pass by undetected, but through continuous sampling of behavioral patterns the rate of detection is high. The basis for such a premise is that over a period of time the threat will exhibit suspicious activity that is anomalous to normal behavior. For example, files that contain dormant viruses may go by undetected. Activation of the virus may cause the file to perform unusual requests that would be anomalous with its previous behavioral pattern and allow for an alarm to be raised. The issue of susceptibility is inherent with both systems, but heuristic systems are capable of detecting such evasions, when anomalous behavior is performed. Signature based NIDS are entirely dependent upon the ability of personnel to be aware that evasive action is being taken by attackers and remains susceptible.

6.5 Coverage of NIDS

The coverage scope of the NIDS is pertinent to its ability to apply security to all facets of the network. Coverage of the network involves protecting against and monitoring for internal and external threats. For signature based NIDS, its limitation is in its ability to cover attacks containing signatures. Although it is able to identify attacks whose signatures are found within its database, other attacks are excluded from its coverage. Attacks that contain signatures are typically external attacks, such as viruses and other malicious code. Internal users that attack the network do not generate signatures that are detectable. For instance, employees that go beyond their authorized range to record sensitive information or personnel that develop holes and backdoors within the security system are undetectable by a signature-based system. These types of intrusions may cause havoc to the organization, but do not develop signatures to indicate the intrusion to the NIDS. Consequently, this one-sided approach provides a defense against external threats, but leaves the network vulnerable to internal threats.

Heuristic based NIDS, in contrast, are able to cover all aspects of the network, both external and internal threats. External and internal threats are detected based on their abnormal behavior patterns. Halme and Bauer describe the

ability of heuristic NIDS to detect malicious user activity by developing a user profile by which the user is expected to adhere to in future activities [4]. Any deviation from this profile would raise an alarm upon detection. The capability of heuristic systems to model all types of activities from programs, applications and users allow for a full coverage of protection. Any deviation from normal behavior will be detected and raises an alarm. Even impersonation of users can be detected if the activities of the impersonator deviate from an authorized user. Identifying attacks based on statistical and behavioral patterns allow for any entity on the system to be modeled and analyzed. Therefore, coverage is provided for components within the range of the network on which the NIDS is deployed. The ability to detect user activity makes the system more beneficial, since both external and internal threats are accounted.

6.6 Limitations of NIDS

The final organizational objective provides a discussion on the limitations that exist within the two systems. As developed through previous sections, the limitations of signature based NIDS are very clear; the attack is known and is detected or the attack is unknown to the system and allows the attack to proceed undetected. Snort, a leading commercial open source NIDS utilizing a signature based approach, provides a definition of the capability of their system in its ability to perform analysis based against user-defined rules and matches these rules accordingly [13]. Through this definition of the typical signature based NIDS, two inherent limitations can be developed. The first limitation is the dependency on network personnel to provide the user defined rules to detect malicious code. This limitation leads directly to the second limitation whereby signatures that are not placed in its database go undetected.

Heuristic based NIDS do not suffer the same inherent limitations as signature based NIDS, but they do have limitations. One limitation is inherent to its structure, which is the need for abnormality by malicious internal or external activities. McHugh provides support by stating that assumptions are made that intrusions would provide unusual activity that would allow for detection [2]. This assumption creates a limitation if the behavioral patterns of intrusions are similar to those of normal programs. Another limitation inherent to its structure is the changes to behavioral patterns that are not malicious. Abnormal benign activity that deviates from normal patterns creates several problems for heuristic based systems. It creates a high number of false positives and requires profile updates to accommodate these changes in patterns. McHugh et al. categorizes this limitation as a drawback due to the need for retraining of the system to account for natural changes [8]. Pfleeger and Pfleeger further strengthen the contention by indicating that heuristic based systems are limited by the information analyzed and how well the analysis fits into its current

system [10]. Accordingly, the system must be able to cope in a network environment where activities are diverse and not systematic.

7. CONCLUSIONS AND ANALYSIS

Upon review of the main comparative objectives discussed, a summary and conclusive analysis is discussed to determine the most effective system for an organization. In accordance with the purpose of the paper, the organizational objectives as defined in the paper should be met sufficiently by the NIDS to be implemented. In summary, the first objective of false negatives and positives plague both NIDS. From a security standpoint, false positives are tolerable, while false negatives are intolerable because they allow attacks to go by undetected. The objectives of updates, competency and susceptibility to attacks are all directly tied together. For signature based NIDS these objectives are related to its dependency on competent personnel for updates, which as a result leaves it susceptible to attacks. In contrast, heuristic based NIDS utilize behavioral patterns and do not require updates and competent personnel. Additionally, its susceptibility to attacks is reduced based on its ability to refine its detection analysis through continual sampling of normal behavior. The objective of coverage indicates that heuristic based system covers all aspects of the network, both internally and externally. Signature based systems only cover attacks with signatures, which are typically external attacks and leaves the organization vulnerable to internal threats. Finally, the inherent limitations indicate that unknown attacks plague continually, signature based NIDS. In contrast, heuristic based NIDS are limited by the necessity for attacks to exhibit abnormal behavioral patterns. Threats that do not exhibit abnormal behavior are undetectable to the system.

In conclusion, it is evident the thesis is proven as heuristic based NIDS effectively meet the organizational objectives of an organization in contrast to a signature based NIDS. The basis for such analysis is determined by the contrasting composition of the two NIDSS. The dependency upon competent personnel by a signature based NIDS is the underlying factor of its inadequacy. Succinctly, a detection system is not feasible if its performance is based solely on personnel. Additionally, vulnerabilities are introduced regardless to the competence level of the personnel. Therefore, a system that is inherently vulnerable to attack is a system that must be overlooked by an organization seeking an adequate security defense. In contrast, the common underlying factor for a heuristic based NIDS indicates its adaptability and flexibility in detecting known, unknown or evasive threats in the network. Its ability to learn from continual sampling of statistical and behavioral patterns allows the system to determine threats, whether new or existing. Therefore, an organization should utilize this type of system for its security defense because it provides a system that is independent of updates and

personnel and the inherent ability to detect most attacks in the network, whether internally and externally or new and modified.

8. Future Work

Future work would be to investigate theoretically whether intrusion prevention systems are as advantageous and beneficial as claimed by most in comparison to IDS. Additionally, the benefits of managed security service providers would be investigated in order to determine if it is more feasible for outsourcing some of the security duties on these providers rather than having everything conducted in-house.

References

- [1] Chuvakin, A. (2004). Monitoring IDS. *Information Systems Security* 12(6), 12-16. Retrieved October 2, 2006, from Business Source Premiere database.
- [2] McHugh, J. (2001). Intrusion and intrusion detection. *International Journal of Information Security* 1(1), 14-36. Retrieved October 2, 2006, from Business Source Premiere database.
- [3] Conorich, D. G. (2004). Monitoring intrusion detection systems: From data to knowledge. *Information Systems Security* 13(2), 19-30. Retrieved October 02, 2006, from WilsonSelect Plus database.
- [4] Halme, L. R., & Bauer, R. K. (n.d.) Intrusion detection FAQ: AINT misbehaving: A taxonomy of anti-intrusion techniques. Retrieved October 31, 2006, from <http://www.sans.org/resources/idfaq/aint.php?portal=ab97d321c015e6845470acba5bea5b29>
- [5] Iheagwara, C. (2004). The effect of intrusion detection management methods on the return on investment. *Computers and Security*, 23(3), 213-228. Retrieved October 23, 2006, from ScienceDirect database.
- [6] CERT Coordination Center (n.d.). Management and education of the risk of insider threat (MERIT): System dynamics modeling of computer system sabotage. Retrieved November 15, 2006, from <http://www.cert.org/archive/pdf/merit.pdf>
- [7] Lemke, T. (2004, March 17). Virus creators share code online to create copycats. Washington Times. Retrieved October 22, 2006, from <http://washingtontimes.com>
- [8] McHugh, J., Christie, A., & Allen, J. (2000). Defending yourself: The role of intrusion detection systems. *IEEE Software* 17(5), 42-51. Retrieved October 2, 2006, from IEEE Computer Society Digital Library database.
- [9] Messmer, Ellen. (2006, October 9). Software vulnerabilities already outnumber last year's crop. Computerworld. Retrieved October 22, 2006 from http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonyName=cybercrime_hacking&articleId=9004000&taxonyId=82
- [10] Pfleeger, C. F., & Pfleeger, S. L. (2003). Security in computing (3rd ed.). Upper Saddle River, NJ: Pearson Education.
- [11] Snort: Getting started. (n.d.). Retrieved October 21, 2006, from http://www.snort.org/docs/snort_htmanuals/htmanual_260/nоде3.html
- [12] Jaques, R. (2005, February 1). Cost of malware soars to \$166bn in 2004. Retrieved October 27, 2006, from <http://www.vnunet.com/vnunet/news/2126635/cost-malware-soars-166bn-2004>
- [13] Liston, K. (n.d.). Intrusion detection FAQ: Can you explain traffic analysis and anomaly detection. Retrieved October 30, 2006, from http://www.sans.org/resources/idfaq/anomaly_detection.php?portal=ecf89f730aa7b32ca4ffd0a7117c132f
- [14] CERT Coordination Center (2006, October 23). CERT/CC statistics 1988-2006. Retrieved October 30, 2006, from http://www.cert.org/stats/cert_stats.html
- [15] NIST (n.d.) An overview of issues in testing intrusion detection systems. Retrieved October 31, 2006, from <http://csrc.nist.gov/publications/nistir/nistir-7007.pdf>
- [16] Taylor, C., & Foss-Alves, J. (2001). NATE: Network analysis of anomalous traffic events, a low cost approach. *Proceedings of the 2001 workshop on New security paradigms*, USA, 89-96. Retrieved November 10, 2006, from ACM Digital Library database.
- [17] Schwartz, K. D. (2005). Network anomalies. *Government Executive*, 37(12), 81-82. Retrieved November 13, 2006, from Business Source Premiere database.
- [18] Lynch, D. M. (2006). Securing against insider attacks. *Information Security Systems*, 15(5), 39-47. Retrieved November 15, 2006, from Academic Search Premier database.