2011 International Conference on Computer Communication and Management
Proc .of CSIT vol.5 (2011) © (2011) IACSIT Press, Singapore

Pitcher Flow: Unified Integration for Intrusion Prevention System

Deris Stiawan [1&2], Abdul Hanan Abdullah [1] and Mohd. Yazid Idris [1 +]

[1] Faculty of Computer Science & Information System, Universiti Teknologi Malaysia
[2] Faculty of Computer Science, Sriwijaya University, Indonesia

Abstract. In the last few years, the Internet has experienced explosive growth. Along with the widespread evolution of new emerging services, the quantity and impact of attacks have been continuously increases. Defense system and network monitoring has becomes essential component of computer security to predict and prevent attacks. A hybrid technique is one of solution for classification and detection intrusion threat. There are some researchers combine misuse-based and anomaly-based to solve this problem. Moreover, there are also performed works using other approaches. In this paper, we analyze fundamental requirement to be satisfied defense network from any intrusion threat will be present, then propose a framework to identify, recognize, prevention and reacting threat, this method is called Pitcher Flow, it combines anomaly-based and misuse-based with event parameters database using data mining approach, which is approach with modular blocks. Throughout this paper, we represent to evaluate system security for help security officer and Network Operating Center (NOC) team to overall network monitoring.

Keywords: Network Security, Intrusion Prevention System, Hybrid Approach, Intrusion Threat, One Integrated System

1. Introduction

There are three interconnection factors in security field [1], [2] and [3]; (i) vulnerability, (ii) attack, and (iii) countermeasures. Vulnerability, application or software vendor update patch regularly. System software and application software is often released without being fully tested and evaluated as free from bugs, due to the complexity of large-scale coding. Implementation vulnerability exits when during the implementation of the protocol or application there was either an error in the code, a misinterpretation, an unforeseen method of attack was discovered. Reports from CERT (cert.org/stats/cert_stats.html), the number of incident reported total of catalogue vulnerabilities has increased from only 5.990, to 6.058 in Third Quarters in 2008. Attack, can occur due to vulnerability from network configuration and application has a bugs, even if the vulnerability is discovered, there may not be an easy way to exploit the systems. According to CERT (www.cert.org/stats), most successful attack result from targeting and exploiting know, unpatched software vulnerabilities and insecure applications running on system.

Along with the widespread evolution of new emerging services, the quantity and impact of attacks have been continuously increases. Countermeasures, there are many method and mechanism to attack, consequently is difficult to tackle it with conventional defense methods, thus requiring new techniques for detecting and adapting to emerging threat. Therefore, enforcement protection network resource must cover prevention to reduce system vulnerabilities, detection to identify ongoing cyber attacks that break through prevention mechanism, and response to stop and control the attack. The solution for identify and recognize security violation is urgently needed. Intrusion Detection System (IDS) have been actively investigated by researchers for about two decades. Obviously, IDSs is one of solution defense system for organization and in other sides many researchers continue to develop it.

[+] *Corresponding author: Faculty of Computer Science & Information System, Universiti Teknologi Malaysia, 81310, Skudai, Johor Bahru, Malaysia. Tel: +60137260814; fax: +6075532210. E-mail : deris@unsri.ac.id*

Increasingly accuracy detection and reduce the false based one unified integrated system is main contributions of this paper. Therefore, a new mechanism have been propose to overcome this problem, which combine between anomaly-based and misuse-based with event parameters from global threat correlation. The novel element in this study is a mechanism to identify and recognize threat based on hybrid systems, combine event parameters with different structure, label and variable of data from heterogeneous data input. The remaining of the paper is structured as follows: In Section 2 we present and briefly discuss background and related work. Section 3 proposes exploratory and our approach. Section 4, summarized our conclusions and present additional issues on which research can be continued.

2. Background & Related Work

Currently, IDS technologies are not very effective against prediction a new mechanism of attack. There are several limitations, such as performance, flexibility, and scalability. Intrusion Prevention System (IPS) is a new approach system to defense networking systems, which combine the technique firewall with that of the Intrusion Detection properly, which is proactive technique, prevent the attacks from entering the network by examining various data record and detection demeanor of pattern recognition sensor, when an attack is identified, intrusion prevention block and log the offending data. In other hands, IPS adopts techniques from intrusion detection, such as detection approach, monitoring sensor, and alert mechanism. IPS can be defined as an in-line product that focuses on identifying and blocking malicious network activity in real time [4]. Wherefore, as mentioned above, IPS introduces the new technology to defend themselves with the ability, intelligent to accurately indentify and block malicious traffic and activities. As resume in proposal [5], [6] and [7], they present two main intrusion prevention techniques: (i) anomaly detection, and (ii) misuse detection. However, intrusion threat usually curious and unpredictable or evolve continuously. The goal of an IPS is to monitor network assets in order to prevent misuse or anomaly behaviour. In other hands, refers to [8], [9] and [10], there are three way to combine hybrid approach, based on misuse and anomaly detection: (i) anomaly detection followed by misuse detection, (ii) misuse and anomaly working in parallel, and (iii) misuse detection followed by anomaly detection. Misuse detection system is a mechanism to identify behavior patterns that are characteristic of intrusion threat. Unfortunately, it can be difficult if have a novel attack.

During the past years, a variety of approaches have been proposed by using hybrid approach techniques with combine advantage anomaly-based and misuse-based. As basis beginning of hybrid intrusion prevention research work in 2000 by [11], introduce the earliest method of hybrid, their present architecture of a hybrid Intrusion Prevention based on real time user recognition. They work motivated and implications to other researchers to investigate various hybrid mechanisms. In currently 2010, there are some effort [12], [13] and [14] propose in hybrid early detection and intrusion prevention. All the results arrived at the same conclusion to using hybrid for solution mechanism. The mainly problem in network traffic is a label the training data for classification and identifying normal or malicious traffic. In 2009, from proposal [15], is concerning the robustness and generalization capabilities of machine learning methods in creating user profile based on the selection and subsequent classification of command line argument. That is from the test result work by [16], they describes some preliminary result concerning the robustness and generalization capabilities of machine learning methods in creating user profile based on the selection and subsequent classification of command arguments. We should cites [15], [16], and [17] for critically and inspiration part of our approach, we seem similarity in term of user profile with anomaly-detection. Nevertheless, we use habitual activity user to recognized behavior user, while during previously researcher they uses learning vector.

3. Exploratory Our Approach

Currently, required a system to provide early warning from intrusion security violation with knowledge based has become a necessity. Therefore, the system must be active and smart in classifying and distinguish of packet data, if curious or mischievous are detected, alert is triggered and event response execute. This mechanism is activated to terminate or allow process packet data associated with the event. Prevent attack before entering the network by examining various data record and prevention demeanour of pattern recognition. An intrusion prevention function as a Radar to monitor stream network traffic detecting,

identifying, and recognized any signal that could be considered a security violations. From the preliminary observation and experiment, initial thoughts of this system illustrate mark (a) in Figure 1, given named pitcher flow [18]. From our experiment and observation made in ubiquitous spread and scattered heterogeneous information to collecting in data warehouse, and behavior approaches to recognized and habitual activity user and using data mining to classify and making knowledge information from it.

There also some effort and problem from [19] and [20] to introduce the concepts hybrid approach effectively with detecting normal usages and malicious activities using heterogeneous data. What makes this solution different from others, this approach improvement and enhances mechanism with combine anomaly-misuse based and event parameters from sixteen heterogeneous data input. We identified the problem is to collecting information from different structure, label, and variable of data. Here data can refer to heterogeneous data, is a set bulk in information and growing from provider, community or security services. We propose improvement mechanism which using data from sources. There are sixteen parameters with different structure, label, and variable of data have been collected, such as (1) Public DNS Registry, (2) IANA authority, (3) Public IP Block list, (4) URL blacklist, (5) Snort rules, (6) Crawler data, (7) Vulnerability from Common Vulnerability and Exposures, (8) Data pattern from Honey pot, (9) Signature, dynamic update patch, (10) Traffic Flow from Service Provider / Network Provider, (11) Log events (Server, Web applications, Firewall and network environment), (12) Spam Rules (images spam, spam fingerprint, spam IP Block list), (13) Virus Definition, (14) Policy definition, (15) Alert from IDS, and (16) Regular Expression.

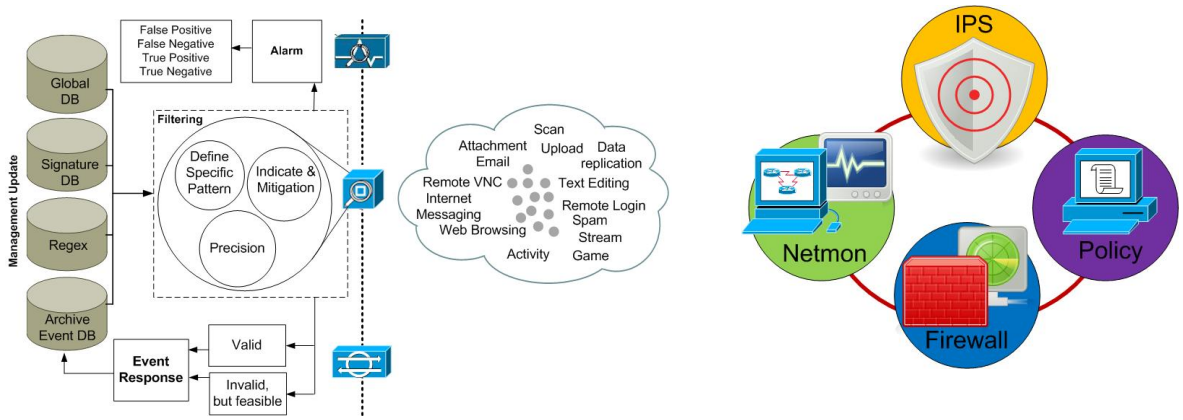

Fig. 1. In mark (a) figure of hybrid intrusion prevention, and mark (b) Unified IPS with others

As mentioned above, to update regularly and newly list of pattern attack and normal activity, signature attack, and archive of history profile user, we employ database records using Data Warehouse approach to known detection behavior has been developed and updated over the time. For that, data mining is an effective technique of discovering knowledge form extensive data sets to match of voluminous data in database. We use spread database to store this events, as following: (i) Global database, (ii) Signature database, (iii) Regex, and (iv) Archive database. In fact, on archive event database, while sensor refers trigger alarm, attempt, penetration, and misuse. An attacker will capture and labelling to specify stored in archive event. From our experiment, we have test several global database to improve and associate with our approach, such as blacklist categorized for defense system (http://cri.univ-tlse1.fr/blacklists/index_en.php).

3.1. Framework & Mechanism

The basic idea of a hybrid intrusion prevention is to make a robust system for identify, recognized and response from security violations, it needs the framework that cooperates with connected and related several component for accurate, intelligent, adaptive and extensible with consists of components are composite to an integrated system. In this approach we divide with modules, as following;

1) Filtering. In this phase, data collecting from training dataset previously, after successfully pass from filtering and screening. In this process, we use filtering, screening and proxy with firewall function, such

as IP Address, Port Address, and Protocol. We propose IP Tables under Linux command. IP Tables approach in Linux command to handles screening and sorting packet with accordance of security policy doing in this process. Refers to [21], Different firewalls usually provide different rule logic with different parameters.

2) Management update to manage the data set includes signature identification, rules, policy, pattern, method attack, URL blacklist, update patch, log system, list variant of virus and regular expression, all this will be collected and labelled to identify attack patterns and can predict it that would occur. These data set bulk in information and growing from community or security services. Therefore, there is a critical need of data analysis system that can automatically analyze the data to classification it and predict pattern attack future trends. This method depends on the input information has been collected in a database. The information in the database come from a variety of information collected and stored from time to time. In some cases, the new types of attacks based on previous patterns, especially the attacks from malicious threat, on knowledge process, performed composite and combining the data residing on the database to be sorted, queries and reused as input. The learning process occurs to combine and choose quickly by comparing the fit of the data in the database.

3) The sensor can take different actions based on how they are configured. Then, after pass threat assessment, the system can trigger event response with status alarm or risk rating status. For example, if sensor detects any attack, it raises alarm to examine valid or invalid but feasible as well as update the newly detected intrusion in archive database. If an alert is triggered, then the alert is fused with other existing alert to decrease the number of alert with the same cause. Risk rating is the quantitative measure of a network's suspicious threat level before event response mitigation. When new events are detected and sensor detect an attack, an analyst can check to see if the event's habitual activity components, store in archive event database if not in list. Database module gets rate mark and lists it within risk rating. As the mentioned above, we assume can deeper inspection with signature matching and behavior analysis is unable to handle the latest threat or can predict the future trends.

4) Meanwhile, in the event response process, we divided in modules: alarm, event response, and risk rating. From our review, these high-level alarms can be used as the base to perform further higher-level threat analysis. We assumed this to be depending on based on approach to produce thousand of millions of alert. The event response can be categorised into two approach; (i) reactive response are activated and executed after intrusion have been detected, and (ii) proactive response, aimed to of pre-empt actions to prevent an intended attack, refers to early prevention system. By using our approach [18], every unknown activity or suspicious threat has labeling.

5) According to some report work [22] and [23], they have identify two set of response type, is active and passive response. Unfortunately, passive approach have gap timing response may range from minute to hours and limitation detecting intrusion to launching a response. Risk Rating (RR), can be describes a threat rating based on numerous factors besides just the attack severity. Wherefore, the RR detects an attack the rule set get rate mark to reduce FP Alarm. We divided risk rating, such as (i) mission critical, (ii) High, (iii) Medium, (iv) Low, and (iv) No value. The target value RR enables to configure an asset rating from specific habitual activity. Therefore, from our observations there are two habitual behavior activities [24], which the asset RR can be one of the values: (i) media rich with activity higher transaction size, and (ii) transactional with activity concurrent connection.

3.2. Unified Integration Solutions

In this section, we discuss to collaboration security system, the Unified Integration Solution (UIS) is respond. There are several variously technology uses in defense system. We proposed UIS to collaborate and integrate between it in one system pitcher flow architecture. The UIS can do collect all security devices monitoring with one network management. The main collaboration and integration is Firewall, intrusion prevention between policy and network monitoring to one control management. Intrusion prevention checking packet of data, which has a sniff and identify all inbound-outbound packet passing and record it and generates some actions (log, blog, deny, alert, report) when intrusion on are discovered. Network traffic consists of a sequence of packet and produces many packets that must be recognized. It is approach used the

anomaly-based and the misuse-based. As the mentioned above, we describes a framework for associated other defense system with IPS, in mark (b) Figure 1, illustrated relationship between IPS, Firewall, network monitoring and policy.

1) Security policy is a crucial step to secure a particular system since it specifies the security properties that must be satisfied and the rules that associate privileges to users, we conclude that standard is closely connected with how to regulate user access from the insides and rules on rights of access other outsiders. There is several standards default to determine framework requirement security policy: ISO 17799 and ISO 27001, which is to declare, indentify, analyze and describes requirement that must be met to accommodate IPS. The previous researcher declared [13], Information Security Management System (ISMS), it requires regulation standard, which in ISO security standards and government compliance regulations guide and enforce organizations about certain requirements and norm.
2) Firewall technology has evolved as defense system requirement have grown and security need. The primary goal of a firewall is to protect the network behind it, essential to every network Firewalls is the ability to examine through each packets and identify pattern that match known attack, which is as a cornerstones of corporate intranet security. Once a firewall is acquired, a security/ systems administrator has to configure and manage it to realize an appropriate security policy for the particular needs of the company [25]. Firewall mechanism (hardware, software and policy) to restrict access from the outside to inside the network. The examined the data of the network layer (Layer 3 : IP Address), transport layer (Layer 4 : Port address, multiplexing) and application layer (Layer 7: application).
3) The conceptual gap between intrusion prevention and management segment provides the most security, monitoring and network management segment. Which it, this integration can do collect all security devices monitoring with one network management. As we know, from a business perspective, enterprise needs to ensure that business-critical application receive proper treatment, defined by a service level agreement (SLA). The most basic function of network management is the collection of the performance utilization overall network devices. We observed there is correlations network management with IPS: (i) performance management, (ii) fault management, (iii) security management, (iv) monitoring, and (v) accounting. The main collaboration and integration are Firewall, intrusion prevention between policy and network monitoring as a one control management.

4. Conclusion &Future Works

The different between [8] with our approach method are: (i), this approach using network-based and behavior-based to evaluate habitual activity; (ii) our approach is more emphasis on accuracy and precision to identify and recognized intrusion threat, and response for this event; (iii) our system check each packet only once on its way to destination, which function in layers data link, network and application; and (iv) this system more emphasis on accuracy of attack, match with event in parameters database. This approach still needs further exploration in future research mainly query correlation each parameters, using data mining approach. In the future research can also include more factors to implement our approach in enterprise network environment and benchmarking with other IPS software solution to tested accuracy and precision.

5. References

[1] H.S. Venter and J.H.P. Eloff, “A taxonomy for information security technologies,” *Information Security*, 2003, pp. 299-307.

[2] S. Zhang, J. Li, X. Chen, and L. Fan, “Building network attack graph for alert causal correlation,” *Computers & Security*, vol. 27, 2008, pp. 188-196.

[3] W. Lin, L. Xiang, D. Pao, and B. Liu, “Collaborative Distributed Intrusion Detection System,” *Higher Education*, 2008.

[4] A. Fuchsberger, “Intrusion Detection Systems and Intrusion Prevention Systems,” *Information Security Technical Report*, vol. 10, 2005, pp. 134-139.

[5] T.S. Chou and T.N. Chou, “Hybrid Classifier Systems for Intrusion Detection,” *IEEE Computer Society Seventh Annual Commnucation Networks and Services Research Conference*, 2009, pp. 286-291.

[6] S.X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems : A review," *Applied Soft Computing*, vol. 10, 2010, pp. 1-35.

[7] M.A. Aydın, A.H. Zaim, and K.G. Ceylan, "A hybrid intrusion detection system design for computer network security," *Computers and Electrical Engineering*, vol. 35, 2009, pp. 517-526.

[8] J. Zhang, M. Zulkernine, and A. Haque, "Random-Forests-Based Network Intrusion," *MAN and Cybernetics*, vol. 38, 2008, pp. 649-659.

[9] J. Zhang, W. Cao, H. Zhang, and L. Feng, "A Distributed IPS Model Based On Neighbor Distance 1," *IEEE Proceeding Ubiquitous, Autonomic and Trusted Computin*, 2009, pp. 465-469.

[10] K.C. Nalavade and B.B. Meshram, "Intrusion Prevention Systems : Data Mining Approach," *ACM Proceedings of the International Conference and Workshop on Emerging Trends in Technology*, 2010, pp. 211-214.

[11] A. Seleznyov and S. Puuronen, "HIDSUR: A Hybrid Intrusion Detection System Based on Real-time User Recognition," *IEEE Proceeding, 11th International Worskhop Database and Expert Systems Applications*, 2000, pp. 41-45.

[12] Y. Qing, W. Xiaoping, and H. Geofeng, "A Hybrid Model of RST and DST with Its Application in Intrusion Detection," *IEEE Computer Society, International Symposium on Inteligent Information Technology and Security Informatics*, 2010, pp. 202-205.

[13] X. Yu, "A New Model of Intelligent Hybrid Network Intrusion Detection System," *IEEE Proceeding International Conference Bioinformatics and Biomedical Technology (ICBBT)*, 2010, pp. 386-389.

[14] Q. Zhang, H. Yang, K. Li, and Q. Zhang, "Research on the Intrusion Detection Technology with Hybrid Model," *2nd Conference on Environmental Science and Information Application Technology*, 2010, pp. 646-649.

[15] Y.X. Ding, M.I.N. Xiao, and A.-wu Liu, "Research and Implementation on SNORT-based Hybrid Intrusion Detection System," *IEEE Proceeding of the Eighth International Conference on Machine Learning and Cybernetics*, 2009, pp. 12-15.

[16] J. Marin, D. Ragsdale, and J. Surdu, "Hybrid Approach to the Profile Creation and Intrusion Detection," *IEEE Proceeding, Information Survivability Conference & Exposition II, DISCEX '01*, 2001, pp. 69-76.

[17] S.H. Oh and W.K. Lee, "An anomaly intrusion detection method by clustering normal user behavior," *Computers & Security*, vol. 22, 2003, pp. 596-612.

[18] D. Stiawan, A.H. Abdullah, and M.Y. Idris, "The Prevention Threat of Behavior-based Signature using Pitcher Flow Architecture," *International Journal of Computer Science & Network Security*, vol. 10, 2010, pp. 289-294.

[19] A. Singhal, *Data Warehousing and Data Mining Techiques for Cyber Security*, Advance in Information Security Springer, 2007.

[20] W. Junqi and H. Zhengbing, "Study of Intrusion Detection Systems (IDSs) in Network Security," *IEEE. Wireless Communications, Networking and Mobile Computing. WICOM 08*, 2008, pp. 1-4.

[21] T. Katić and P. Pale, "Optimization of Firewall Rules," *IEEE Proceedings Int. Conf. on Information Technology Interfaces*, 2007, pp. 685-690.

[22] R. Perdisci, G. Giacinto, and F. Roli, "Alarm clustering for intrusion detection systems in computer networks," *Engineering Application of Arificial Inteligence*, vol. 19, 2006, pp. 429-438.

[23] A.D. Todd, R.A. Raines, R.O. Baldwin, B.E. Mullins, and S.K. Rogers, "Alert Verification Evasion Through Server Response Forging," *Alert Verification Evaluation Through Server Response Forging, LNCS*, vol. 4637/2007, 2007, pp. 256-275.

[24] D. Stiawan, A.H. Abdullah, and M.Y. Idris, "Classification of Habitual Activities in Behavior-based Network Detection," *Journal of Computing*, vol. 2, 2010, pp. 1-7.

[25] A. Wool, "The use and usability of direction-based filtering in firewalls," *Computers & Security*, vol. 23, Sep. 2004, pp. 459-468.