Journal of Theoretical and Applied Information Technology
15 June 2012. Vol. 40 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTRUSION PREVENTION SYSTEM: A SURVEY

DERIS STIAWAN[1&2], ALA' YASEEN IBRAHIM SHAKHATREH[1] ,
MOHD. YAZID IDRIS[1], KAMARULNIZAM ABU BAKAR[1], ABDUL HANAN ABDULLAH[1]

[1] Faculty of Computer Science & Information System, Universiti Teknologi Malaysia

[2] Faculty of Computer Science, University of Sriwijaya, Indonesia

E-mail: deris@unsri.ac.id, yis81@hotmail.com, yazid@utm.my, knizam@utm.my, hanan@utm.my

ABSTRACT

For the last few years, the Internet has experienced tremendous growth. Along with the widespread evolution of new emerging services, the quantity and impact of attacks have been continuously increasing. Defence system and network monitoring has become an essential component of computer security to predict and prevent attacks. This article presents a survey, open issues on early detection, and response toward prevention network intrusion. Roadmap of intrusion prevention of current approach is also presented. Furthermore, relevant issues and challenges in this field are subsequently discussed and illustrated. This research is expected to obtain learning phase. Finally, this work concludes with an analysis of the challenges that still remain to be resolved.

Keywords: *Intrusion Detection / Prevention System, Heterogeneous Parameter*

1. INTRODUCTION

Intrusion Detection was developed to identify and report the attack in the late 1990s, as hacker's attacks and network worms began to affect the internet, it detected hostile traffic and sent alerts but did nothing to stop the attacks [1]. It has been a long road for Intrusion Detection System (IDS), almost two decades since it has become a major issue. In other words, Intrusion Detection is passive. It is not able to detect all malicious programmes and activities most of the time and incompatible to integrate with control restriction to stop traffic inbound-outbound from attacking; which means it was only capable to detect attack actions, without prevention action.

Intrusion Prevention System (IPS) is primarily a network-based defence system, with increasing global network connectivity and combines the technique firewall with that of the IDS properly with proactive technique. This system is a proactive technique which prevents attacks before entering the network by examining various data record and detects demeanour pattern recognition sensor. When an attack is identified, intrusion prevention blocks and logs the offending data. Currently, requirement for a system to provide early detection / warning from intrusion security violation with knowledge based has become a necessity. Therefore, the system must be active and smart in classifying and distinguishing packet data, if curious or mischievous data are detected, alert is triggered and event response is executed. This mechanism is activated to terminate or allow packet data to process associated with the event. It prevents attack before entering the network by examining various data records and prevents demeanour of pattern recognition.

Currently, requirement for a system to provide early detection / warning from intrusion security violation with knowledge based has become a necessity. Therefore, the system must be active and smart in classifying and distinguish packet data, if curious or mischievous data are detected, alert is triggered and event response is executed. This mechanism is activated to terminate or allow packet data process associated with the event. It will prevent attack before entering the network by examining various data record and prevent demeanour of pattern recognition.

The main contribution if this paper is the enhancement of the learning phase and part of the research have being done [2],[3]. The remaining of the paper is structured as follows: Section 2 presents related work in roadmap of intrusion detection, early detection, response, and prevention system. Section 3 discussed on issues and challenges in this research. Finally, section 4, summarized our concluded and present additional works to be continued.

2. ROADMAP OF IPS

Based on the earlier section, in order for places to counter security threat, this current needed an integrated solution that is renewable and not avoidable. The roadmap for development of detection, early detection and prevention system are depicted in **Figure 1**. It started earlier in the IDS solution by [4], presenting the taxonomy and existing tools used of IDS. Furthermore, work by [5], proposes automatic early warning system to make prediction and advice regarding malware based on database and repository of threat.

Journal of Theoretical and Applied Information Technology
15 June 2012. Vol. 40 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

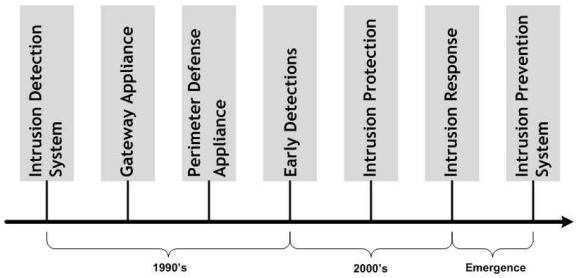

Figure 1. Roadmap of detection & intrusion prevention

These early detection concept has been introduced by [6], which describes differentiate types of operation mode IDS, IPS and Intrusion Response System (IRS), they compare it based on literature product with features proactive, reactive and passive. Therefore, IRS can be categorised as a basic method of IPS. On the other hand, performed work by [7], outlines the future trends of IPS functionality such as: gateway appliance, perimeter defence appliance, all-in-all capability, and network packet inspection or prevention. Additionally, work from [8], encountered challenges in intrusion detection of early detection. The trend of behaviour analysis to efficient data collection is describe to improve the performance of sensors in the real-traffic network, due to network traffic capture on high-speed links is always a challenge to capacity issues.

This means that early detection, protection and response system act as an elementary of IPS. The researcher strongly argued that the intent of early detection and response system is the main concept of IPS. It is expanded on the functionality provided by IDS by enabling to prevent attack against of network. As mentioned above, early detection and intrusion response has the fundamental and part of intrusion prevention mechanism in recent network security challenge, this was confirmed performed work by [9], [10], [11], [6], [5], [12] and [13]. Responding to this issue, some researchers have proposed several detections and response mechanisms to complement the existing prevention mechanism by stakhanova in 2007 [13], 2009 by Salah [14], work by Anuar in 2010 [6], and in 2011 work by Elshoush [15], they were declared intrusion response as having similar function to IDS and part of it, by maintaining detection, alerting and response to security operator.

IPS functions as radar to monitor stream network traffic; detecting, identifying, and recognising any signal that could be considered a security violation. With respect from proposal work by [16], they present real-time intrusion prevention and anomaly system. In 2011, Hu [17] declared IPS has correlation between intrusion detection and firewall, also design and implementation of trusted communication protocol based on XML is provided , and then [18] had predicted the future of IPS technology, such as (i) better underlying intrusion detection, (ii) advancement in application-level analysis, (iii) more sophisticated response capabilities, and (iv) integration of intrusion prevention into other security devices. Moreover, the prediction concerns on intrusion prevention technology which are very positive in market.

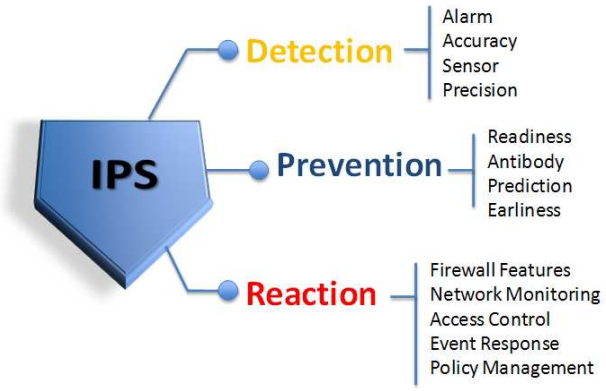

Figure 2. Features of IPS

Previously, in 2004 [19], has predicted IPSs to have a bright future, this technology will continue to be used by a growing number of organizations to the point that it will become a commonplace as intrusion detection technology. More recently, performed work by [20], describes superior characteristic of host based IPS and use the term detection approach to show how IPSs work. As seen from Figure 2, the feature function of IPS is shown Intrusion Prevention provides numerous capabilities at both the host level and the network level, but from a high-level perspective, the capabilities provided by IPSs fall into two major categories: (i) Attack prevention, and (ii) Regulatory compliance [21]. Additionally, much type of IPSs potentially avoid the weakness of signature-based intrusion detection systems and it can learn classes of harmful system behaviour and the types of events that they attempt to produce in targeted system. Therefore, it is much better suited to react appropriately to zero-day attacks. Hence, from this analysis, it is identified that. IPS will also become more proficient because IDS, early detection, intrusion response is a fundamental aspect when intrusion prevention in developing.

According to some reported work, [22] describes IDS and IPS fundamental, currently IDS can be seen as a traditional second line of defence system, it is becoming more difficult to apply security access control. On the contrary, IPS can be used to alarm for attacks within a network and provide for acting on attack preventive with Firewall and IDS function mechanism. In comparison to IDS and IPS with features of both depicted in Table 1. The illustrated fundamental difference between IDS and IPS can be seen in Figure 3. As mentioned in Table 1 and Figure 3, the basic difference of both, such as (i) event notify, (ii) response, (iii) alert, and (iv) knowledge.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. OPEN ISSUES & CHALLENGES

The address difference of challenge of detection, response and prevention, various analysis techniques have been proposed in recent years. In this section, the observation during recent years is discussed. There are some significant gaps, challenges and preliminary results for future direction in IPS to improving, mining and reducing false alarm. With respect from previous proposal [23], this work is improvement of statement on research gaps and extension from performed work [24].

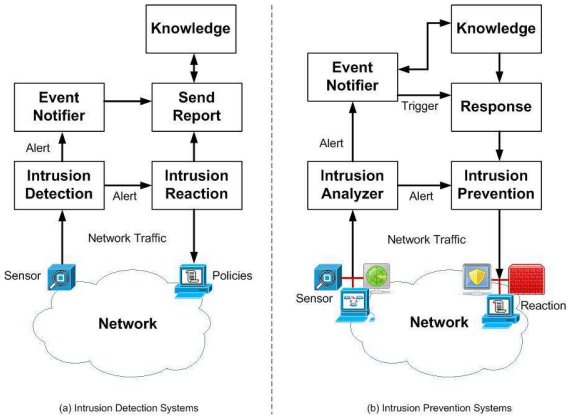

Figure 3. Basic Fundamental IDS / IPS

3.1 Data sets

Although this current is required to collect data from network behaviour, specific log data from stream traffic and develop network environment with normal access or attack actions, it is greatly and heavily desired to have some publicly available data for researchers to evaluate various algorithm or mechanism. DARPA MIT, KDD 99, and University New Mexico has become this study's standard as a data sets. From the observations, this existing datasets are not sufficient and mostly outdated, since new suspicious threats have been increasing in recent years. Furthermore, there are several reasons that required the new data to be investigated, *Firstly*, the new model attack, more recently next application technologies are changing the Web 2.0 security landscape, new attack pattern, and attack mechanism. *Secondly*, the new emergence application, Web 2.0 applications are faced with all the threat associated from past approach application, because of inherited traditional resources in addition to new ones. *Thirdly*, there are new approaches (architecture and technology) in web technology. This will result in payload of application. According to [25], they described sample of some well known Web 2.0 application.

Table 1. Comparison IDS and IPS

	Intrusion Detection System	Intrusion Prevention System
Usefulness	IDS design just only identify and examined to produce alarm	IPS design is to enhance data processing ability, intelligent, accurate of it self.
OSI Layer	Layer 3	Layer 2, 3,4 and 7
Signatures Action	• Simple pattern matching • Stateful pattern matching • Protocol decode-based analysis • Heuristic-based analysis	• Recognize attack pattern • Blocking & response action • Stateful pattern matching • Protocol decode-based analysis • Heuristic-based analysis
Activity	• A passive security solution • Detect attack only after they have entered the network, and do nothing to stop attacks only just attacks traffic and send alert to trigger.	• Reactive response security solution • Early Detection, proactive technique, early prevent the attack, when an attack is identified then blocks the offending data
Component	• Cannot expect to detect all malicious activity at all time • Handling alert to trigger false positive or false negative alarm	• Can be detect new signatures or behavior attack • Handling alert to trigger false positive or false negative alarm
Blocking future traffic	Cannot integrated with filtering rules security to stop traffic from attacking	Have the capability to block and can apply policy at perimeter router or firewall
Event Response	Capability only to recognize and report to security operator in the event of attack.	• Have mechanism allow, block, log, and report • Integrated mechanism threat management to security operator
Sensor	• Commonly collected in source sensors • Multisensory architectures	• Enable to integrated with other platform • Have the ability to integrate with heterogeneous sensor

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

There are various projects in universities to produces data sets for academic research. From the observation as shown in Figure 4, these work helped this study to get scenario and payload data from past experiments. Unfortunately, this existing datasets are not sufficient and mostly outdated, since new suspicious threats have been increasing in recent years. From this issue, the experiment with new approach is urgently needed to get payload data normal / attack and behaviour activity user based on web 2.0 technology. According to previous works [2] and [26], classify interconnection behaviour is showed. It calls habitual activity with number of connection of activity user. This study argues from the habitual activity, profiles of user's behaviour and user profiles can be generated and have be to be update periodically to include the most recent change frequently.

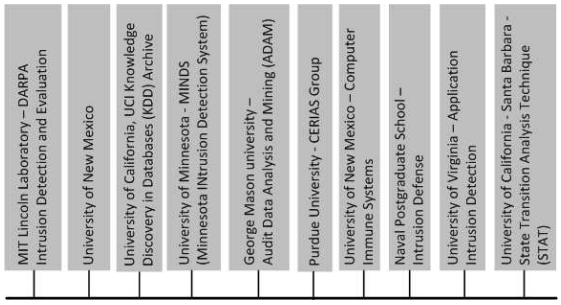

Figure 4. Popular Data sets

3.2 Alert Management

For large network, sensor will be placed with distributed system, the challenge is how to manage alert data from number of sensors used to monitor which is intrusion correlation refers to interpretation, analysis and forensic alert from several sensors. Alert management ability to cluster, merge, and correlate alerts. Its function enables it to recognise alert that corresponds to the same occurrence of an attack. Alert attributes consist of several fields that provide information about the attack in stream network. Furthermore, it has mechanism to generate a new alert that merges data in these various alerts. A method relationship between accuracy alarm, risk rating and event response system is shown in Figure 5.

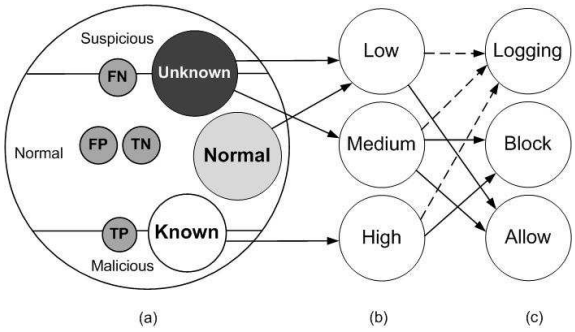

Figure 5. Correlation with accuracy, risk rating and response

According to [27], Alert correlation is defined as a process that contains multiple components with the purpose of analysing alert and providing high-level insight view on the security state of the network under surveillance, and work [15], proposed collaboration IDS (CIDS), they used centralised CIDS to correlated distributed detection unit and alert management correlation based on soft computing. Previously, another method proposed by [28], to developed intrusion alerts correlation system according to the alert correlation approach by using ontology-based intrusion alerts. Additionally, work by [29] and [30], proposed alert management module responsible for collecting the alert generated from the self-corrective IDS, this correlated with the alerts, formulating and more general alert based on individual true positive.

There is a challenge to handle alert management. From our observation, this alert information depends on the variant used or diversity of format by different vendor product. Therefore, the solution for correlating alarm with different vendor can be solved with pre-processing the message of a common standard data format. These solution leverages Intrusion Detection Message Exchange Format (IDME) drafted by IETF Intrusion Detection Working Group based (IIDWG) on RFC 4766 which defines a data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to the management systems which may need to interact with them (http://tools.ietf.org/html//rfc4765).

From the observation, it can be defined that for relationship metric between alert, the correlation may occur because correlating alerts based on the similarity between alerts attributes, such as time stamp, IP and ports addresses. Therefore, there are several issues that should be addressed; aggregation of alert, knowledge-based, evaluation of alert and correlation management. Likewise, solution with storing system, these alert efficiently and divided based on their group to depict the overall security violation is needed.

.

3.3 Heterogeneous Data

This current information, an increasingly large volume of dataset and multidimensional data has grown rapidly in recent years. There are also some efforts and problems from [16], [23] and [31] to introduce the concepts of hybrid approach effectively with by detecting normal usages and malicious activities using heterogeneous data.

According to some previous work, [32] described benefits of CVE compatibility, integrating vulnerability services and tools to provide more complete security and alert advisory services, [33] presented a log file monitoring techniques that can be categorised into fault detection and anomaly detection. On the other hand, from proposal [34], they used Honey pot to capture and analyze attacker to database analyzer. In the case of fault

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

detection, the domain expert creates a database of fault message patterns by [35] which presented blacklisted user and notify the user of their blacklist status. Additionally, proposal work [36] collected URL filtering systems to provide a simple and effective way to protect web security, [30] also proposed a method for automatically evaluating alerts of Snort based on metrics related to the applicability of the attack, the importance of victim. It is declared that there are relationship between alert under training and previous alerts, and the social activities between the attackers and the victims.

However, it is possible to propose collecting scattered information in routine update regularly from provider or security community. This data can be useful information to be associated with others. The data sets include 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 that it would occur. These data set bulks in information and growing from community or security services. Therefore, the ability to extract hidden pattern and trends from large quantities of heterogeneous data is important for immune and prediction before attack. There is a critical need of data analysis system that can automatically analyse the data to organise it and predict pattern attack future trends.

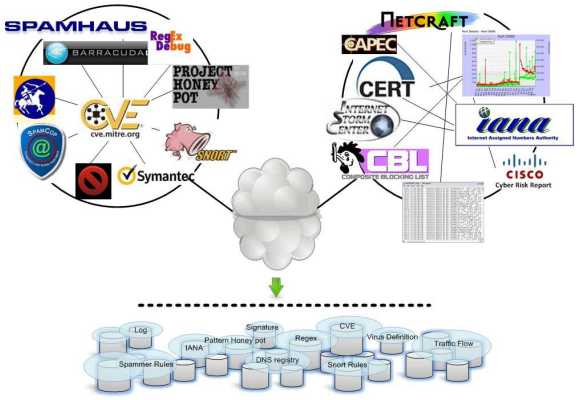

Figure 6. Heterogeneous data

Figure 6, Illustrates an example of heterogeneous data input, there are some problem to addresses; *Firstly*, is collecting and labelling scattered information from security services and community to identify attack patterns possible and the occurrence can be predicted?. *Secondly*, how to correlate heterogeneous event parameters with different structure, format, label and variable of data? *Thirdly*, is it possible to provide threat identification, analysis and mitigation to continuously provide the highest level by using combination event parameters? From the preliminary observation [37], propose data mining approach is utilised to collecting scattered information in routine update regularly from provider or security community. This could be data from the web, library data, logging, and past information that are stored as archives. These data can form a pattern of specific information. It gives a collection of datasets, a sample of such data was examined to look for pattern which may exist between certain pattern methods over time.

3.4 Extraction Features

Performed work by [38] and [39], proposed in feature extraction as an essential component in anomaly detection to summarise network behaviour from a packet stream. [40], proposed rough set theory to applied threat assessments and classification method that boundary between normal patterns and abnormal, making it more suitable as a part of this system. In 2011 [41], provided comprehensive review of the network traffic features and data preprocessing techniques used by anomaly-based.

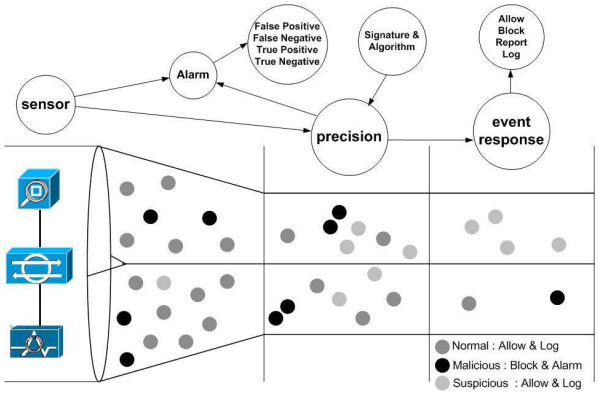

Figure 7. Illustration of Packet data in real network

There are some efforts, working in hybrid technique to select and classify packet. Their performed work has been proposed to combine this advantage of both misuse-based and anomaly-based. [42], proposed a method which includes an ensemble feature selecting classifier and a data mining classifier. We identify through the proposal from [43], as a basis beginning of hybrid intrusion research work, their present architecture of a hybrid intrusion prevention bases on real time user recognition. In the extension work, [42], proposed to use fundamental method from proposal [23] proposal, had shown experimental results to indicate that hybrid approach is effective with detecting normal usages and malicious activities based on machine learning algorithm. Additionally, in 2009, [44] represented their work in optimizing approach work done previously by [45], which used the same concept of frequent episode rules (FERs). In other scenario, [46], analyse the behaviour of the malicious codes based on the behaviour signature with classes.

To recognise threat in real-traffic, feature extraction must exist. Data from network traffic and audit systems,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which is for each type of data that needs to be examined (network packets, host event / server farm logs, payload of data, etc) data preparation and feature extraction is currently a challenging task. This caused real traffic where there are many packet data, audit data were manually inspected to identify network traffic is impossible and was expensive, time-consuming, and inaccurate due to the extremely large amount of audit data. On the other hand, the solution to identify and recognise security violation is urgently needed. In **Figure 7**, show of extraction / classification packet data in real network. Furthermore, the way to enhance recognised method association rule mining, outlier analysis, and classification algorithms in order to characterise network behaviour are issues gap and challenging from this section.

3.5 Minimising False Positives

Accuracy in intrusion prevention a positive alarm is considered as an attack data, while a negative is considered to be a normal data. Furthermore, evaluation accuracy and speed has been proposed by [47], which were measured in terms of FP and FN with timelines activity approaches. Additionally, more appropriately accurate mechanism keeps the number of false negative and false positive low as in work by [48]. Combination anomaly and behaviour activity is a necessarily needed to update pattern and attack taxonomy of attack. It is for countermeasure against of mischievous in security violation. More recent work [34], [49], [44], [50], explored ways to increase accurate with using clustering, percentage and distribute of sensor.

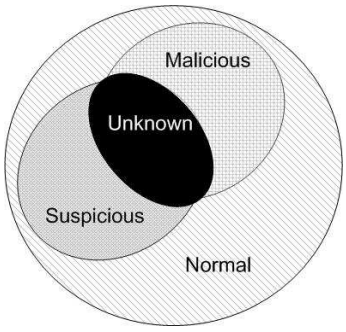

Figure 8. Illustration of classification

The main concerns include capabilities to compromise, identify and recognise detection the pattern, the ability to detect future threats and renew update of signature list, as shown in Figure 8. From this section, there are issues should be addresses, how to enhanced the maturity method with new approach to adaptable from new threat and a new method to increase of true alarm.

3.6 Real-time Analyzer

Currently, a system is required to provide early warning from security violation intrusion with knowledge based which 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 is executed. This mechanism is activated to terminate or allow process packet data associated with the event. The attack is prevented before entering the network by examining various data record and prevention demeanour of pattern recognition.

Performed work by Shouman in 2010 [20], proposed a system to recognise packet in real time based on host intrusion prevention system (HIPS) for preemptive protection against zero-day attacks and malwares, by applying behavioural analysis techniques. On the contrary, with respect from [51], [52], [53] works, they present new approach for classification to identify threat. Unfortunately working in offline mechanism, collecting data in real capturing but training and identifying threat is offline. In the extension work [45], has combined online and offline mechanism to training data, cluster analysis, also attribute preprocessing.

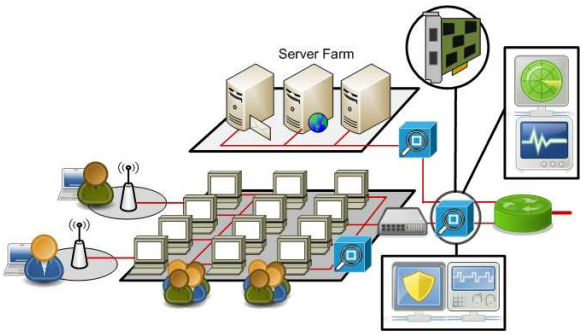

Figure 9. Probe and capturing traffic

One problem faced by all detection in IPS is difficulty to identify and recognise analysis of packet in real-time traffic. To detect suspicious threat, there are two approaches [20], [54], [55], and [56]: (i) Host-based approach: Host-based are currently popular technologies, it is checked for suspicious activity from the host or operating system level, the monitoring location use the agent component, which is useful before the host reaches target of attack. The alarm triggered and provide intrusive this activity, and (ii) Network-based approach, the sniff and identify packet all inbound-outbound in out of the network. The combination of Network-based with other security components provides an active comprehensive network security.

The second problem is accessing traffic can be more difficult then interpreting it as network designer are built often performance, not visibility. They tend to be concerned about how to best path the destination packet,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

when carrying packet is more important than analysing them. On the other hand, as seen in Figure 9, there are issues in traffic data in real network. PCI / interface Ethernet have limited performance, due to network scalability and node of host. The preliminary results, Gigabit Ethernet card with 33 MHz Peripheral Component Interconnect (PCI) slot is a minimum requirement, which its performance has become imperative. Therefore, some vendor's produce they own product based on Gigabit Ethernet. Performed work by [1], presented IPS machine based on Snort with pattern-matching algorithm to identify and recognise threat, previously in 2003 [57], produce DIPS as a separated hardware using field programmable port extender.

3.7 Data Visualisation

The continuous monitoring in graphical information for network operating center is needed. During attack, there is a need for the security operator / officer to depict with visualise the alert from sensor, fully managed and take necessary action respond to them. **Figure 10**, shows a simple visual network management for minimum requirement in network operating center (NOC).

Figure 10. Simple network management

According from [58], they provide sophisticated attack graph visualisations, with high-level overviews and detail drilldown, and work by [59], [60], [61], which became a based literate to develop visualisation and network management in real network. This issue has correlated with **section 3.4** and [62] as a network investigation, incident response and network forensic approach.

Additionally, there are some problems from proposal work by [63]; these include (i) collecting and managing data about networks and their vulnerabilities, (ii) building network attack models in terms of security conditions and attacker exploits, (iii) analysing the models through simulated attacks to produce attack graphs, (iv) aggregating and filtering the attack graphs, (v) drawing the graphs, and (vi) providing interactive controls for attack graph navigation. On the other hand, in some variant of security appliances, standard protocol / system to access and monitoring these devices, such as SNMP, is one of the protocol standards to get traffic information to high level dashboard summary display.

3.8 Unified Integration Solution

According to some reported work by [7], [17], [18], and [64], they declared that IPS has correlated with other security parameters and is more intelligent to ensure the integration with other platform. Network traffic consists of a sequence of packet and produces many packets that must be recognized. Therefore, combination of known and unknown threat prevention within other security parameters to total security coverage is a necessity. As mentioned above, a framework for other associated defence system with IPS is described and it is concluded that there are relationship between IPS, Firewall, network monitoring and policy as in depict in Figure 11.

3.8.1 Security Policy

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, it is concluded that standard is closely connected with how to regulate user access from the insides and rules on rights of access other outsiders. There are several standard defaults to determine framework requirement security policy: ISO 17799 and ISO 27001, which is to declare, indentify, analyse and describe requirement that must be met to accommodate IPS. The previous researcher declared [65], Information Security Management System (ISMS), it requires regulation standard, in which ISO security standards and government compliance regulations guide and enforce organisations about certain requirements and norm.

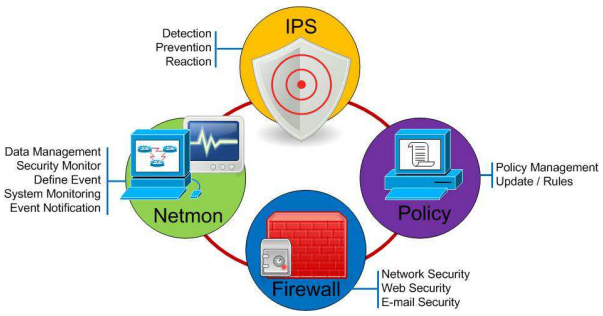

Figure 11. Relationship Security Parameter

3.8.2 Firewall

The primary goal of a firewall is to protect the network behind it, it is essential to every network Firewalls for 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 realise an appropriate security policy for the particular needs of the company [66]. Firewall mechanism (hardware, software and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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).

3.8.3 Network Management

A conceptual gap between intrusion prevention and segment management provide the most security, monitoring and management network segment. In which this integration can do collect all security devices monitoring with one network management. As known from business perspective, enterprise needs to ensure that business-critical application receives proper treatment, defined by a service level agreement (SLA). The most basic function of network management is the collection of the performance utilisation overall network devices. It is observed that there are 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 detection between policy and network monitoring in one control management.

4. CONCLUSION & FUTURE WORK

The basic of identifying and recognising threat with high accuracy, earliness, and active response mainly concerns enabling comprehensive attack coverage available that must exists at present. This paper has provided a comprehensive review of the early detection, response and prevention system features. There are some issues and challenges in this area that can be studied in the future. As mentioned above, it is argued that heterogeneous data has a signature update for predictor dataset, feature extraction, real-time analyser, and unified integration solution are essential issues to be enhancement of learning phase. One integration system for detection, prevention and reaction may still be valid today for network management, countermeasure against, monitoring internal networks and for behavioural analysis.

Furthermore, improvement with one integration system, testing and benchmarking it with others in real-network traffic, will be made in future works. The amount of recognised threat is proposed to rise with correlation accuracy alarm, risk rating and active response. It is believed that this system could be an effective solution for building an integrated system in the industrial world, by combining Firewall and IDS features with Network Management for one integration system in Network Operating Center (NOC).

5. ACKNOWLEDGMENTS

This research is supported by The Ministry of Higher Education and collaboration with Research Management Center (RMC) Universiti Teknologi Malaysia.

REFERENCES

[1] Y. Weinsberg, S. Tzur-David, D. Dolev, and T. Anker, "High Performance String Matching Algorithm for a Network Intrusion Prevention System (NIPS)," *High Performance Switching and Routing*, IEEE, 2006, pp. 147-153.

[2] 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.

[3] 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.

[4] M. Dacier and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Computer Networks*, vol. 31, 1999, pp. 805-822.

[5] M. Apel, J. Biskup, U. Flegel, and M. Meier, "Towards Early Warning Systems – Challenges , Technologies and Architecture," *CRITICAL INFORMATION INFRASTRUCTURES SECURITY, LNCS*, R. Bloomfield, with E. Rome, eds., Springer-Verlag, 2010, pp. 151-164.

[6] N.B. Anuar, M. Papadaki, S. Furnell, and N. Clarke, "An investigation and survey of response options for Intrusion Response Systems (IRSs)," *Information Security for South Africa (ISSA)*, 2010, pp. 1-8.

[7] G. Ollmann, "Intrusion Prevention Systems (IPS) destined to replace legacy routers," *Network Security*, vol. 11, 2003, pp. 18-19.

[8] S.A. Shaikh, H. Chivers, and J.A. Clark, "Towards scalable intrusion," *Network Security*, vol. June, 2009, pp. 12-16.

[9] C. Manikopoulos, "Early statistical anomaly intrusion detection of DOS attacks using MIB traffic parameters," *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.*, 2003, pp. 53-59.

[10] C.C. Zou and D. Towsley, "The monitoring and early detection of Internet worms," *IEEE/ACM Transactions on Networking*, vol. 13, Oct. 2005, pp. 961-974.

[11] H. Debar, Y. Thomas, F. Cuppens, and N. Cuppens-Boulahia, "Response : bridging the link between intrusion detection alerts and security policies," *Intrusion Detection Systems*, P. Roberto and L.V. Mancini, eds., 2008, pp. 129-170.

[12] C. Mu, B. Shuai, and H. Liu, "Analysis of Response Factors in Intrusion Response Decision-Making," *2010 Third International Joint Conference on Computational Science and Optimization*, 2010, pp. 395-399.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[13] N. Stakhanova, S. Basu, and J. Wong, "A taxonomy of intrusion response systems," *International Journal and Computer Security*, vol. 1, 2007, pp. 169-184.

[14] K. Salah and a Kahtani, "Performance evaluation comparison of Snort NIDS under Linux and Windows Server," *Journal of Network and Computer Applications*, vol. 33, Jan. 2010, pp. 6-15.

[15] H.T. Elshoush and I.M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems—A survey," *Applied Soft Computing*, vol. In Press, , Jan. 2011.

[16] T. Dutkevych, A. Piskozub, and N. Tymoshyk, "Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks," *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems Technology and Application*, 2007, pp. 599-602.

[17] L. Hu, W. Wang, and K. Zhao, "The Design and Implementation of Trusted Communication Protocol for Intrustion Prevention System," *Journal of Convergence Information Technology*, vol. 6, 2011, pp. 55-62.

[18] E.E. Schultz and E. Ray, "Future of Intrusion Prevention," *Computer Fraud & Security*, 2007, pp. 11-13.

[19] E. Schultz, "Intrusion prevention," *Computers & Security*, vol. 23, 2004, pp. 265-266.

[20] M. Shouman, A. Salah, and H.M. Faheem, "Surviving cyber warfare with a hybrid multiagent-based intrusion prevention system," *IEEE Potentials*, 2010, pp. 32-40.

[21] J. Carter, E., Hogue, *Intrusion Prevention Fundamentals : an introduction to network attack mitigation with Intrusion Prevention System*, Cisco press, 2006.

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

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

[24] D. Stiawan, A.H. Abdullah, and M.Y. Idris, "The Trends of Intrusion Prevention System Network," *International Conference Education Technology and Computer (ICETC)*, Shanghai, China: IEEE, 2010, pp. 217-221.

[25] S. Shah, *Web 2.0 Security: Defending Ajax, RIA, and SOA*, Charles River Media, 2008.

[26] R. Dantu, P. Kolan, and C. Joao, "Network risk management using attacker profiling," *Security and Communication*, vol. 2, 2009, pp. 83-96.

[27] A. a Ghorbani, W. Lu, and M. Tavallaee, "Network Intrusion Detection and Prevention," *Network Intrusion Detection and Prevention*, Boston, MA: Springer US, 2010, pp. 129-160.

[28] W. Li and S. Tian, "An ontology-based intrusion alerts correlation system," *Expert Systems with Applications*, vol. 37, Oct. 2010, pp. 7138-7146.

[29] M. Sourour and B. Adel, "Adaptive IDS Alerts Correlation according to the traffic type and the attacks properties," *2009 IEEE International Advance Computing Conference (IACC 2009)*, 2009, pp. 1653-1658.

[30] K. Alsubhi, E. Al-shaer, and R. Boutaba, "Alert Prioritization in Intrusion Detection Systems," *IEEE proceeding Network Operations and Management Symposium*, 2008, pp. 33-40.

[31] 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.

[32] R.A. Martin, "Managing Vulnerabilities in Networked Systems," *Computer*, vol. 34, 2001, pp. 32-38.

[33] R. Vaarandi, "A Data Clustering Algorithm for Mining Patterns From Event Logs," *World Wide Web Internet And Web Information Systems*, 2003, pp. 119-126.

[34] U. Thakar, S. Varma, and A.K. Ramani, "HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot," *The Second International Conference on Innovations in Information Technology (IIT'05)*, 2005.

[35] P.P. Tsang, A. Kapadia, C. Cornelius, and S.W. Smith, "Nymble : Blocking Misbehaving Users in Anonymizing Networks," *IEEE Transaction Dependable and secure computing*, 2009, pp. 1-15.

[36] Z. Zhou, T. Song, and Y. Jia, "A High-Performance URL Lookup Engine for URL Filtering Systems," *IEEE ICC 2010*, 2010, pp. 1-5.

[37] D. Stiawan, M.Y. Idris, and A.H. Abdullah, "Survey on Heterogeneous Data for Recognizing Threat," *Journal of Computational Information Systems (JCIS)*, vol. 4, 2011.

[38] A.C. David Nguyen, Gokhan Memik, Seda OgrenciMemik, "REAL-TIME FEATURE EXTRACTION FOR HIGH SPEED NETWORKS," *Field Programmable Logic and Applications*, IEEE, 2005, pp. 438-443.

[39] S.R.G. Gopi K. Kuchimanchi, Vir V. Phoha, Kiran S. Balagani, "Dimension Reduction Using Feature Extraction Methods for Real-time Misuse Detection Systems," *Analysis*, 2004, pp. 10-11.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[40] Q. Ye, X. Wu, and B. Yan, "An Intrusion Detection Approach Based on System Call Sequences and Rules Extraction," *2010 2nd International Conference on E-business and Information System Security*, Ieee, 2010, pp. 1-4.

[41] J.J. Davis, "Data Preprocessing For Anomaly Based Network Intrusion Detection: A Review," *Computers & Security*, vol. In Press, Jun. 2011.

[42] 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.

[43] 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.

[44] Y. Ding, L.E.I. Li, and H.-qi Luo, "A novel signature searching for intrusion detection system using data mining," *Proceedings of the Eighth International Conference on Machine Learning and Cybernetics*, 2009, pp. 12-15.

[45] K. Hwang, M. Cai, Y. Chen, S. Member, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, 2007, pp. 41-55.

[46] K. Kumar, "Securing communication using function extraction technology for malicious code behavior analysis," *Computers & Security*, vol. 28, Feb. 2009, pp. 77-84.

[47] 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.

[48] 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.

[49] H. Artail, H. Safa, M. Sraj, I. Kuwatly, and Z. Al-masri, "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks," *Computer & Security*, vol. 25, 2006, pp. 274-288.

[50] P. Garcıa-Teodoro, J. Dian-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection : Techniques , systems and challenges," *Computer & Security*, vol. 28, 2009, pp. 18-28.

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

[52] 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.

[53] O. Depren, M. Topallar, E. Anarim, and M.K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert Systems with," *Expert System with Application*, vol. 29, 2005, pp. 713-722.

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

[55] 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.

[56] Ghorbani A.A, *Network Intrusion Detection and Prevention : Concepts and Technique*, Springer, 2009.

[57] Q. Zhang and R. Janakiraman, "Indra : A Distributed Approach to Network Intrusion Detection and Prevention," *Access*, vol. WUCS-01-30, 2003, pp. 1-6.

[58] S. Noel, M. Elder, S. Jajodia, P. Kalapa, S. O'Hare, and K. Prole, "Advances in Topological Vulnerability Analysis," *2009 Cybersecurity Applications & Technology Conference for Homeland Security*, Mar. 2009, pp. 124-129.

[59] P. Ren, Y. Gao, Z. Li, Y. Chen, and B. Watson, "IDGraphs: intrusion detection and analysis using stream compositing.," *IEEE computer graphics and applications*, vol. 26, 2007, pp. 28-39.

[60] M. Alsaleh, D. Barrera, and P.C.V. Oorschot, "Improving Security Visualization with Exposure Map Filtering," *2008 Annual Computer Security Applications Conference (ACSAC)*, Dec. 2008, pp. 205-214.

[61] H. Read, a Blyth, and I. Sutherland, "A Unified Approach to Network Traffic and Network Security Visualisation," *2009 IEEE International Conference on Communications*, Jun. 2009, pp. 1-6.

[62] A. Johnston and J. Reust, "Network intrusion investigation – Preparation and challenges," *Digital Investigation*, vol. 3, Sep. 2006, pp. 118-126.

[63] S. Noel, M. Jacobs, P. Kalapa, and S. Jajodia, "Multiple coordinated views for network attack graphs," *IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05).*, 2005, pp. 99-106.

[64] W.Z. Xinyou Zhang, Chengzhong Li, "Intrusion Prevention System Design," *Computer and Information Technology, 2004. CIT '04*, 2004, pp. 386-390.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[65] 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.

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