Characterizing Network Intrusion Prevention System

Deris Stiawan
Faculty of Computer Science &
Information System
Universiti Teknologi Malaysia
Faculty of Computer Science,
Sriwijaya University Indonesia

Abdul Hanan Abdullah
Faculty of Computer Science &
Information System
Universiti Teknologi Malaysia

Mohd. Yazid Idris
Faculty of Computer Science &
Information System
Universiti Teknologi Malaysia

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, attackers continuously find vulnerabilities at various levels, from the network it self to operating system and applications, exploit the to crack system and services. Defense system and network monitoring has becomes essential component of computer security to predict and prevent attacks. Unlike traditional Intrusion Detection System (IDS), Intrusion Prevention System (IPS) has additional features to secure computer network system. In this paper, we present mapping problem and challenges of IPS. When this study was started in late 2000, there are some models and theories have been developed. Unfortunately, only a few works have done mapping the problem in IPS area, especially in hybrid mechanism. Throughout this paper, we summarize the main current methods and the promising and interesting future directions and challenges research field in IPS.

Keywords

Security Threat, Intrusion Prevention System, Mapping Problem IPS

1. INTRODUCTION

Computer system security has become a major concern over the past few years. Attack, threat or intrusions, against computer system and network have become commonplace events, many system device and other tools are available to help counter the threat of these attack. Analyzed from proposal [1] and [2] highlighted currently countermeasure against from security violation, such as (i) firewall, strengthen in implementing executing rules and policy, but firewall can do nothing about attack from inside network and can not clarify behavior or anomaly attack, (ii) anti virus software. Unfortunately, anti virus very limited ability to pattern recognition of new viruses before the anti-program created by corporate, and (iii) Intrusion Detection, only send the alert to trigger after attacked have entered the network, and do nothing to stop attacks.

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. Ghorbani [3], propose work in IPS filed, describes IPS uses to secure the system, the enterprise uses several technology security systems, and almost 54% of them use intrusion prevention to mitigation and defense from threat and attack.

Recently, intrusion detection system uses to management traffic in real-traffic for increasing the accuracy detection and decreasing false alarm rate. In some instances, IPS adopts techniques from intrusion detection, such as detection approach, monitoring sensor, and alert mechanism.

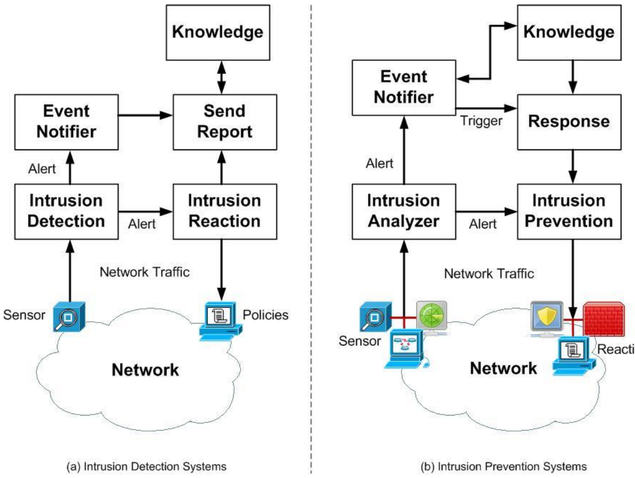

Fig 1: Comparison (a) IDS and (b) IPS

According to some reported work, proposal [4] describes of fundamental IDS and IPS, currently IDS can be seen as a traditional second line of defense system, it is becoming more difficult to apply security access control. On 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. Performed work [5], outline the future trends of IPS is functionality such as: gateway appliance, perimeter defense appliance, all-in-all capability, and network packet inspection/prevent.

We illustrated in **Figure 1**, comparison IPS and IDS. IPS is similar to IDS. It designed and process to identify and recognized potential security violations in stream network. However, the primary intrusion prevention use signature mechanism to identify activity in network traffic and host where perform detect on inbound – outbound packets and would be to block that activity before the damage and access network resources.

An IPS can be defined as an in-line product that focuses on identifying and blocking malicious network activity in real time [4]. IPS combines the technique firewall (data link layer, network layer, transport layer and application layer) with that of the IDS properly with proactive technique, it is a new approach system to defense networking systems and prevents attacks from entering the network by examining various data record and prevention demeanor of pattern recognition sensor. When an attack is identified, intrusion prevention blocks and logs the offending data.

The main contribution this paper is the enhancement of a learning phase, which aims to mapping problem and show the challenge of IPS. The paper is organized as follow. Section 2, we presents mapping of the problem on IPS field research area. Section 3, we present roadmap of hybrid intrusion approach, and conclusion and future work are shown in Section 4.

2. MAPPING AND CHALLENGES IPS

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. An IPS can be defined as an in-line product that focuses on identifying and blocking malicious network activity in real time [4].

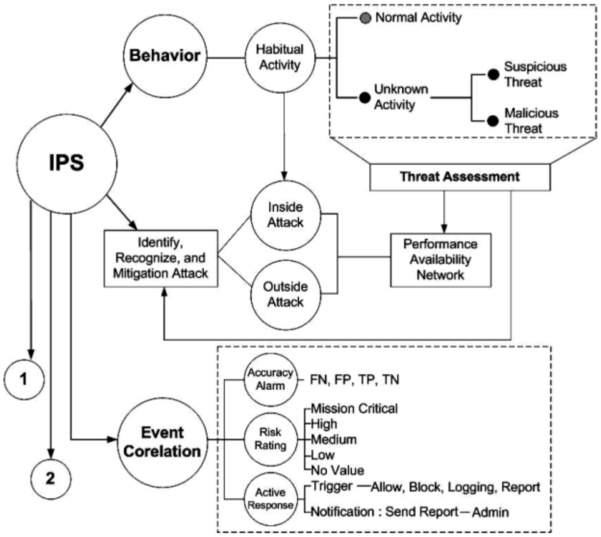

Fig 2: Mapping Problem

IPSs expanded on the functionality provided by IDS by enabling to prevent attack against of network. With respect from proposal [6], they present real-time intrusion prevention and anomaly system, main problem IPS is that can effectively detect only attack they know from signatures, and then Schultz [7], has prediction 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, they prediction concerning intrusion prevention technology is very positive in market.

Various models and frameworks detection have been publication to mitigation from external threat. In some instance, previously researchers focus on the signature system, attack from outside, and taxonomy model attack without discussing how to analyze and recognize normal activity users from inside network. However there is hesitancy to detecting and preventing attack form insider threat. In this section, as in **Figure 2**, we present mapping technique to determine each stage in IPS architecture.

2.1 Behavior

From habit activity of user, we can generate profiles of user behavior, user profiles have to be update periodically to include the most recent changes frequently. According to [8], describes how to deter an individual behavior, which is counterproductive to information security. They use social cognitive theory and explore its viability as a framework for understanding factor influencing and user control-enhancing behavior. Additionally from work [9], they have clustering automatically into cluster that define the access policies, experiment show that the mechanism is effective in detecting attack.

Proposal work [8] study the model and test relationship among self-efficacy in information security, security practice behavior and motivation to strengthen security effort, they conclude self-efficacy in information security does have substantial explanatory power regarding individuals information security practice behavior both in term of technology use and security conscious care behavior. Therefore, we can summarize the behavior is an effective way to identify and detection threat from habitual activity.

In the research by [10], present behavior user to using social website and how to attempt to organize the status, uses, and issues of social web site into comprehensive framework for discussing, understanding, using, building and forecasting the future of social web sites. They was mapping behavior user to uses of social website (behavior user individual, businesses and government).

However, between these two approaches proposal [10] and [11], we can include behavior user for mapping habitual activity, especially interaction behavior and attitude user with the new emergence Web 2.0 applications. Additionally, as a basis, we hold from them for identify the new emergence application have a special characteristic unique that can be used for habitual activity motivation to provides the obviously extended user motivation. Like wise, proposal [12], present taxonomy in which the most relevant features of current solutions are included. Thus, the network feature analyzed, the type of behavior model and the scale of analysis have been proposed as basic criteria to classify current methods as well as key notions to the problem itself. They present the methods based on the analytic traffic flows with divided in case study.

An essential in network security is to monitor and analyzed network traffic for profiling user behavior. A robust defense system has to hold parameters representing both normal and abnormal user behavior patterns, and such parameters require to be recalibrated consistently to adjust for changes in network and user behavior over time. From our observation, we can describe profiles user with convention continuously activity access, it is we called habitual activity [13]. Proposal by Rhee in 2009 [8], present social cognitive theory postulates the reciprocal nature of interaction among behavioral, personal and environmental factors, they uses analysis survey with questioner about security aspect in organization. Therefore, we can summarize that the behavior is an effective way to identify and detect threat from habitual activity. Additionally, as a basis, we have a special characteristic unique that can be used for habitual activity motivation to provide the obviously extended user motivation.

2.2 Threat Assessment

In most of cases, it is very difficult to identify and recognized normal, suspicious or malicious from stream network traffic. All research work listed for divided threat approach. Proposal [14], present with several mechanisms to identify anomaly behavior with pattern of normal behavior. From case environment [15], proposed known activity of malicious threat. Evidently, accurately identified in cases less than 10% of times, being the worst case that was 50% of the peers are malicious. Complementary, analysis by Mark in 2005 [16], present successfully the most basic of malicious insider management requirement. Thus, they have identify that these tools can be used by policy makers, security officers, information technology, human resources, and management to understand the problem and assess risk from insiders based on simulations of policies, cultural, technical, and procedural factor. Thus, they claim to find opportunity to observe individual incidents and/or to detect anomalous behavior from correlated observables.

In the year's 1995s intruders from outside network reflected the predominant mode in, the defense system technology solutions focused on outsiders gaining unauthorized access to exposed network resources: Servers Farm (Web, Mail, FTP, Database, DNS, and Application). Furthermore, refers to RFC 1918 (www.faqs.org/qa/rfcc-995) and statistical data from our training data [17],[[18], inside user can also be a serious threat. Moreover, as is well known the security of computer network is support two factors, (i) internal vulnerability: focus on security violations from insider user / insider attack and misuse authentication / authorize user to attack hole internal organizations, and (ii) external vulnerability: refers to attacker from outside organization, which could penetrate find hole of the defense system. Unfortunately, there are no researches that divided and identify threat, in it normal activity or unknown activity. Therefore, what the approach to increasingly accurate and precision threat in stream traffic are the challenges in this field.

2.3 Attack

1) In general, *insider users* have privilege as authentication and authorization access to resources. In this case, to distinguish between insider threat and outsides /external attack as is an insider has greater privilege and knowledge of their organization and can face greater penetration to resources than external attackers (i.e. topology, devices location, mapping network, security control, privilege mechanism and application of assets and targets). Therefore, steps and stages of insider attack to penetrate attack resource can be possibly easy than penetration from outside attacker. Obviously with data from CSI/FBI survey 2008, where in 2008 there occurred 44 % from insider attack. Refers from performed by Schultz [19] in 2002, he has present a framework to promising in that it synthesizes and builds upon critical models and findings concerning insider attacks; unfortunately, however, this framework is also unproven. As well as in 2008, Walker [20] present a case study of the technical counter measures and processes used to deter, detect and mitigate malicious insider threat using non-classified anonymous interview and the analysis of anonymous qualitative field data.

2) *Outside Attack*, they can become or considered insiders through the proxy of a current insider. Analyzed from [21], experience hacker can be expected to continue to try best to evade security mechanism in order to archives their malicious intentions and the evaluate impact of malicious external threat to computer network. From our analysis, attacker has been passed defense system or choke point system. Thus, filtering, screening, blocking, authentication, authorization, and accounting are a standard mechanism of defense system (i.e. probe in layer network, transport and application).

2.4 Event Correlation

1) *Accuracy Alarm.* We observe that the accuracy affects the correctness of deciding whether an attack exists in real-traffic, notifying the logging system of an attack based on the list in the database. Therefore, accuracy performs measuring the percentage of detection and failure as the number of false alarm, to reduce false positive alert is the main focus. Review of proposal literature by [14] and [22], presents consequence of such variability, user profiles are very inaccurate and detection systems raise a large amount of false alarms. In intrusion prevention a positive data is considered to be an attack data, while a negative is considered to be a normal data. Furthermore, evaluation accuracy and speed has been proposed performed work [12], they were measured in terms of FP and FN with timelines activity approaches. Accuracy performs measuring the percentage of detection and failure as the number of false alarm, to reduce false positive alert the main focus in [12]. Review of proposal literature[14] and [22], they present as a consequence of such variability, user profiles are very inaccurate and detection systems raise a large amount of false alarms. Furthermore, As we know, there are four alerts: (i) The true negative (TN), which is normal user traffic and no alarm is generated, (ii) true positive (TP), which is generated alarm after attack traffic, (iii) false negative (FN), which will be silent no alarm is generated at attack traffic. Meanwhile, (iv) the false positive (FP) produces an alert if it identifies normal activity traffic, is means, FP refers to this tend normal event being predicted as attacks, reduce false positive alert the main focus.

2) *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. As in **Figure 2**, 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. For the present RR calculating, we uses the concept of like hood, it can be useful when prioritizing risk and evaluating the effectiveness of potential threat. The like hood estimation is subjective to combination and is typically expressed as a RR of high, medium and low. Additionally, in previous work [21], [23] they depict relations accuracy with RR to increasingly recognized threat.

3) *Active Response*, RR is a quantitative measure for network threat level before active response stages. We assumsed this tends depending on based approach to produce thousand of milions of alert. The active response can be categorized into two approach, (i) reactive response are activated and executed after intrusion have been detected, and (ii) proactive response, aimed to of preempt actions to prevent an intended attack, refer to early prevention system According to some report work [23] and [24], 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. On contrary, proposal work by [12], present timely response with delta interval approach, the suspension of this result is total delay for response timing from attack, detection until response. In passive response they have notify or detect attack instead of stopping the entire help to stop intrusions and network level attack as an after event mechanism.

Thus, active response analyze and examined inbound-outbound traffic in real-time. In **Figure 2** we shown active response will trigger action (block, allow, logging, report) to mitigation the network connection or the process associated with the event. To summarize the four possible cases. Accordingly, TN as well as TP is to identify operation detector, which is labeled as normal or known activity. On the contrary, FP and FN are the events that undermine the detection performance when unknown or suspicious is not identify. From our review, these high-level alarms can be used as the base to perform further higher-level threat analysis. By using our approach [13], every unknown activity or suspicious threat has labeling. The main problem in sensor are accuracy and timeliness performance identifies threat, as well as sensitivity, and how effective a particular filter was in blocking, knowing and unknown threat response. It was measured in term of FP and FN. In the following, we will refer primarily to relationship accuracy, risk rating and active response, as it is the most widely used type of prevention sensor.

We assume in this approach that accuracy alarm, risk rating and event response allow increasing accuracy. In the other hands, we identified some instances [3], [12], [15], [20], conducted to proposed composite and associate between accuracy and event response or contrary. Unfortunately, elementary correlation can not describe it accurate and clearly. Furthermore, we combine our prevention algorithm to enhance the accurate to identify and recognize the threat. Correlated and interconnection, (a) accuracy (b) risk rating, with equations high (r1), medium (r2), low (r3), and (c) event response, equations allow (e1), block (e2), logging (e3)

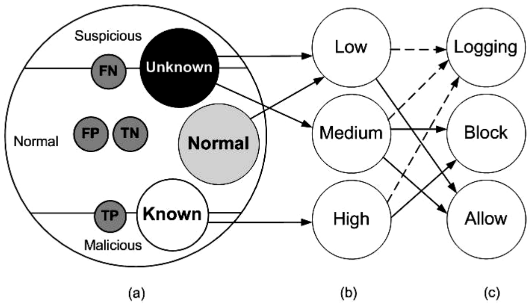

Fig 3: Relationship (a) accuracy alarm, (b) risk rating and (c) active response

2.5 Sensor

The sensor is one of the parts critical in IPSs. Unfortunately, capacity and performance of sensor is limited by amount of network traffic, placement during installation, and choosing the system uses (hardware or module based). Therefore, monitoring network is easy to change control, alert incident response, create notify administrator, or block traffic immediately. Unfortunately, the main issue is that, there are several standard of proprietary vendor between SNMP versions. We evaluate challenges of quota usage, this is due to many log file produce from logging system, which conduce the large storages, logging data transaction, logging attacker traffic, logging victim traffic, logging incident record, logging incident notification, logging summary report, and logging failure report [17]. With respect some reported work [25] and [26], they are introduce the concepts of heterogeneous and distributed sensors for detect normal usages and malicious activities.

The past researcher [27], propose integration and encompassing a security infrastructure where multiple security device from a global security layer, which is defined with respect to the others and interact dynamically and automatically with the different security devices.

1) *Placement*, Security Devices, there are several work : in 2004, Xinyau [28], proposed development intrusion prevention based SNMP, Integrated with other system defense, and [29], propose the implementation load balancing that developed using libpcap library with clustering technique. Unfortunately, there is no one identify to secure intrusion prevention device from attack. Placement, There are two factor that will be affect, *First*, the sensor placement, and *Second*, the number of sensor. The sensor, recognize and identify suspicious data and trigger alert if identify suspicious threat. Furthermore, the situation trigger of alarm (valid or invalid but feasible) from sensor to event response. Previous work performed by Xinyau in 2004 [35], introduce the attempt to develop intrusion sensor with SNMP based. Unfortunately, SNMP based have problem that vulnerability MIB and agent.

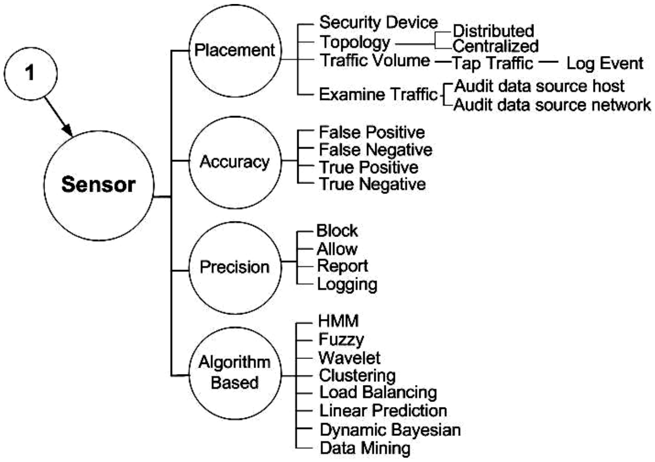

Fig 4: Mapping Problem (*cont*)

2) *Accuracy*, in intrusion prevention a positive alarm is considered to be an attack data, while a negative is considered to be a normal data. Furthermore, evaluation accuracy and speed has been proposed by [12], they 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 Todd in 2007 [23]. The mainly problem in sensor are accuracy and timeliness performance identifies threat, as well as sensitivity, to how effective a particular filter was in blocking knowing and unknown threat response. It was measured in term of FP and FN.

3) *Precision*, network IPS sensor identifies potentially malicious traffic, it must response to the stream traffic by performing some type of action. Carter in 2006 [30], identified four generate actions: block, allow, report, logging.

4) Algorithm, Algorithm, there are many research efforts have been focused on how to effectively and accurately construct detection models. Combination of expert system and statistical approach was very popular [22]. We identified from past research on using technique method with wavelet by [1] and [31], they present the technique a Hidden Markov Model (HMM) to model

sensor, in 2009, Friaz-Martinez [9] proposed with incremental-learning algorithm, Yaron in 2006 [32], present Pattern-matching algorithm. Additionally proposal [33], they experiment data with artificial immune algorithm, and proposal Myint in 2009 [34] uses incremental learning based solutions.

2.6 Detection Analysis

One problem faced by all detection in IPS is that difficult to identify and recognized analyzing packet in real-time traffic. To detect suspicious threat, there are two approach [3], [35], [36], and [37]: (i) *Host-based approach* : Host-based are currently popular technologies, it is check for suspicious activity from the host or operating system level, the monitoring location use the agent component, which is useful before the host it 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 combining Network-based with other security component, provides a active comprehensive network security

According to some reported work [22], [12], and [14], there are two categories based according to the detection method packet is shown in **Figure 5**: (i) anomaly-based detection, and (ii) misuse-based detection.

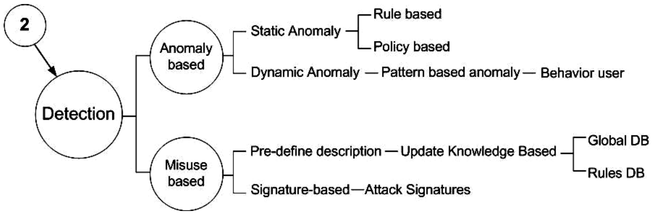
2
Detection
Anomaly based
Static Anomaly
Rule based
Policy based
Dynamic Anomaly — Pattern based anomaly — Behavior user
Misuse based
Pre-define description — Update Knowledge Based
Global DB
Rules DB
Signature-based—Attack Signatures

Fig 5: Mapping Problem (*cont*)

1) *Anomaly-based*, Anomaly-based detection, the key to the application of anomaly detection methods to the field known as threat consists in a simple but critical hypothesis. Hence, anomaly detection has the capability of detecting new types of intrusions and need list of profile data as a normal data, builds model of normal behavior and automatically detect any violation of it to generate alarm.

According to some previous work by [25], they describes to measure and techniques used in anomaly detection, (i) threshold detection, (ii) statistical measures, and (ii) other technology (i.e. data mining, neural network, genetic algorithm and immune system model. According to Wu and Banzhaf in 2010, anomaly detection searches for intrusive activities by comparing network traffic to those established acceptable normal usage patterns learned from training data, and refers from work [38], they divided three classifications of the anomaly detection techniques according to the nature of the processing, such as (i) statistic based, (ii) knowledge based, and machine learning based. Advantage this approach is ability to detect novel attacks for which signatures have not been defined yet. Unfortunately, this approach produces many false alarms and dally time consuming for research intensive to obtain update accurate and comprehensive profiles of normal behavior. This means, it requires a large set of training data with consist network environment system log.

2) *Misuse-based*, Analysis form previously work by [22], misuse detection identifies intrusions by matching observed data with pre-defined description of intrusive behavior. Furthermore, in this approach its find threat by examine the network traffic in search of direct matches to known pattern of packet (signature or rules). Additionally, proposal [39], depicts clearly different between misuse-based and anomaly-based with snort rule structure. Accordingly, a disadvantage of this approach is that it can only detect intrusion that match a pre-defined rule, the set of signature need to be constantly update manually to known the new threat. Fortunately, this method can be highly accurate to increasingly precision identify known attack and their variations. Furthermore, misuse-based produce low false alarm.

3. HYBRID APPROACH

In this section, we introduce the design of hybrid intrusion prevention approach, and describe its basic concepts from previously research work. More recent research explored the deployment of hybrid intrusion detection and prevention to enhancement network security, as in depicted **Figure 6**, there are some hybrid approaches have been proposal to combine this advantage of both misuse-based and anomaly-based. As mentioned above in Section 2.6, there are advantages and disadvantages of both systems. They need for the solution to overcome security violation was recognizes by researcher to provide system, by combining currently approaches.

3.1 Roadmap Hybrid Intrusion Prevention

In this section, introduction of design hybrid intrusion prevention approach will be present, and describe its basic concepts from previously research work. More recent research explored the deployment of hybrid intrusion prevention to enhancement network security, as in depicted **Figure 6,** their performed work have been proposed to combine this advantage of both misuse-based and anomaly-based

We identify in 2000, proposal [40], as basis beginning of hybrid intrusion research work, they introduce the earliest method of hybrid, their present architecture of a hybrid intrusion prevention bases on real time user recognition. They combines anomaly and misuse based approach. This approach be adapted and implications to other subsequent researchers. With respect from proposal previously [22], they clearly describe review algorithm approach, such as artificial neural networks, fuzzy sets, evolutionary computation, and artificial immune system. Thus, [41], propose hybrid detection system model combining with immune system and neural network IDS. The idea of this work is a more accurate detection rate of immune system and the powerful learning ability of neural networks. However, they only focused on algorithm approach and improving the detection rate in known and unknown intrusion. Unfortunately, they did not consider reducing the number of false alarm and classifying for identify and recognize behavior user. Therefore, in this work a hybrid intrusion threat using learning behavior-based will be propose.

In 2009, [42] represent their work in optimizing approach by previously work [43], they uses same concept of frequent episode rules (FERs), with dataset KDD99 running on SNORT based machines. While he proposed approach with leverages from previously work in 2007 by Hwang, they equal the same uses the SNORT module detection and FERs are generate from frequent episode with shown frequent episode rule algorithm. In this area field, there are similarities in determining anomaly with proposal [44], uses extract pattern to detect and classify normal or abnormal packet from network. Unfortunately, this paper performs well in the offline detection, but its performance measurement detection in real-time is unanswered and not discussed.

With respect from proposal previously [45], [41], and [46] contribution their work is the enhancement of learning phase and traditional approaches study.

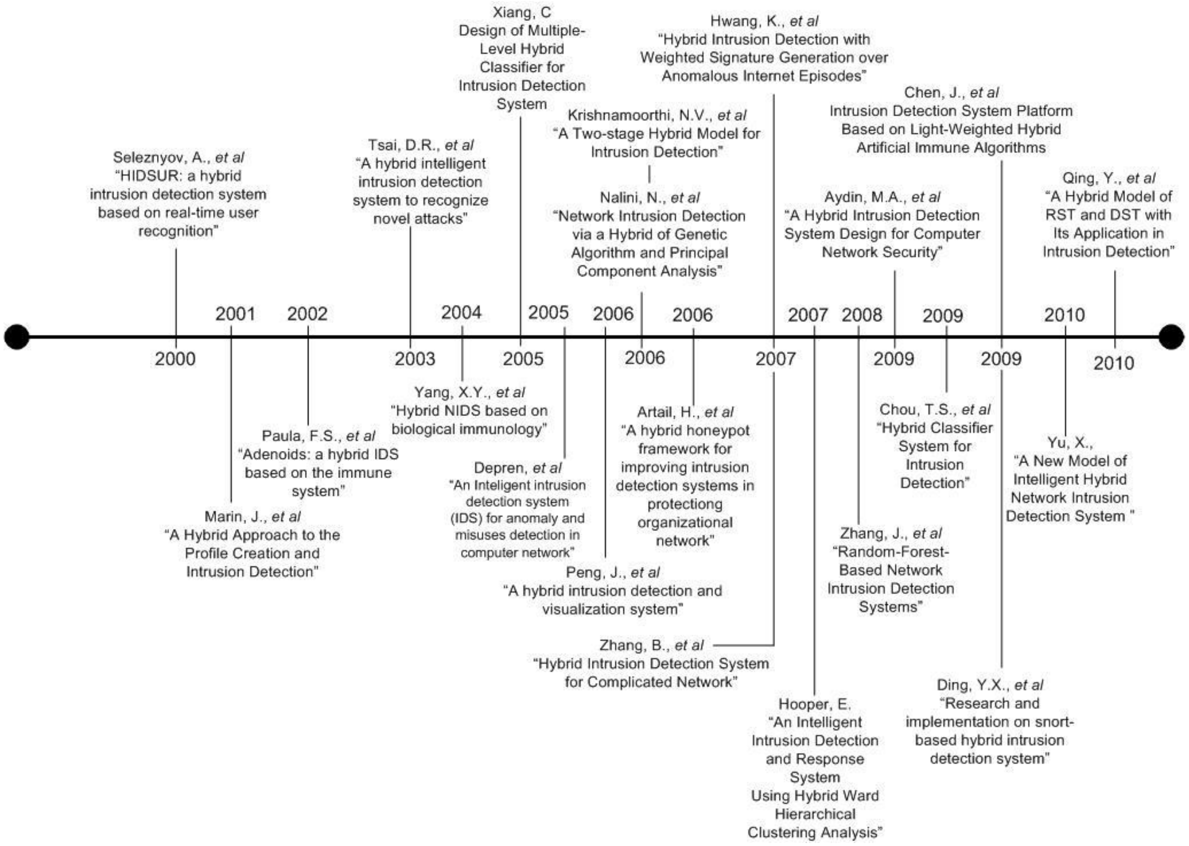
Seleznyov, A., *et al* "HIDSUR: a hybrid intrusion detection system based on real-time user recognition"
Tsai, D.R., *et al* "A hybrid intelligent intrusion detection system to recognize novel attacks"
Xiang, C Design of Multiple-Level Hybrid Classifier for Intrusion Detection System
Krishnamoorthi, N.V., *et al* "A Two-stage Hybrid Model for Intrusion Detection"
Nalini, N., *et al* "Network Intrusion Detection via a Hybrid of Genetic Algorithm and Principal Component Analysis"
Hwang, K., *et al* "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes"
Aydin, M.A., *et al* "A Hybrid Intrusion Detection System Design for Computer Network Security"
Chen, J., *et al* Intrusion Detection System Platform Based on Light-Weighted Hybrid Artificial Immune Algorithms
Qing, Y., *et al* "A Hybrid Model of RST and DST with Its Application in Intrusion Detection"
2001
2002
2004
2005
2006
2006
2007
2008
2009
2010
2000
2003
2005
2006
2007
2009
2009
2010
Yang, X.Y., *et al* "Hybrid NIDS based on biological immunology"
Paula, F.S., *et al* "Adenoids: a hybrid IDS based on the immune system"
Marin, J., *et al* "A Hybrid Approach to the Profile Creation and Intrusion Detection"
Depren, *et al* "An Inteligent intrusion detection system (IDS) for anomaly and misuses detection in computer network"
Artail, H., *et al* "A hybrid honeypot framework for improving intrusion detection systems in protectiong organizational network"
Peng, J., *et al* "A hybrid intrusion detection and visualization system"
Zhang, B., *et al* "Hybrid Intrusion Detection System for Complicated Network"
Hooper, E. "An Intelligent Intrusion Detection and Response System Using Hybrid Ward Hierarchical Clustering Analysis"
Chou, T.S., *et al* "Hybrid Classifier System for Intrusion Detection"
Zhang, J., *et al* "Random-Forest-Based Network Intrusion Detection Systems"
Yu, X., "A New Model of Intelligent Hybrid Network Intrusion Detection System "
Ding, Y.X., *et al* "Research and implementation on snort-based hybrid intrusion detection system"

Fig 6: Roadmap intrusion early detection / prevention

We analyzed from proposal [44], has connectivity and contribute some researchers uses same dataset and soft computing approaches.

Currently in 2010, [45], proposes hybrid approach based on data mining & machine learning techniques and [47], Unfortunately, they just started to do combine hybrid data mining and data fusion. In the other hands, work by [48] approach strengthen to continue this hybrid mechanism with uses random forest algorithm in misuse and anomaly, we observed their approach based on work [40] uses online learning mechanism in order to catch, encode and then update variation of user behavior.

Performed work [49], 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 [50], 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.

Refers from some previous work in hybrid systems, [51] describes architecture utilizing both anomaly and misuse detection, this architecture using Self –organizing maps (SOM) consists in an anomaly detection module and misuse detection modules. This tends using traditional preprocessing based on decision support system, the preprocessing using six basic features.

In 2008, [52] using multiple-level hybrids classifier to have high detection and low false alarms rates. They describes multiple-level hybrid using Bayesian clustering for tree classifier design and clustering analysis. Unfortunately, this approach is not relevant with currently behavior access in web technology.

We should cites and compare to the hybrid approach [44], [50], [49] and [43] to our approach [18]. Furthermore, this propose a new hybrid approach with composite: (i) parallel mechanism anomaly-misuse detection, (ii) anomaly detection sustain and support of misuse detection, (iii) Conversely, misuses detection sustain and support of anomaly detection, and (iv) combine with database record (Regex, Global, Signature and Archive) to update list knowledge-based.

4. CONCLUSION & FUTURE WORKS

IPS has additional features to secure computer network system. The additional features identifying and recognizing suspicious threat trigger alarm, event notification, through responsible response. In this preliminary observation from previously researcher, hybrid techniques is one of solution for classification and detection intrusion threat. Proposed hybrid IPS takes the advantages to increase accuracy and precision normal or suspicious threat. There are some researchers combine misuse-based and anomaly-based to solve this problem. In this work we present approaches are state-of-the-art, considers and addresses several aspect of IPS, and also provide effort to summarizes the main current status and the promising and interesting future directions and challenges. In this paper, we present a mapping problem and challenges in IPS with others related work. There are some issues can be researched, i.e. heterogeneous sensor, distributed sensor, and combine hybrid early detection/ prevention mechanism with other approaches. Future work will focus on accuracy and precision with our algorithm based on behavior-based prevention, which is an experiment with our data set of real-traffic network.

5. REFERENCES

[1] E. Guillen, D. Padilla, and Y. Colorado, "based Intrusion Detection and Prevention Systems," *Latin-American Conference Communications*, 2009, pp. 0-4.

[2] B. Cao, Z. Zhihong, L. Tie, Y. Zhongde, and L. Jiren, "A Study on Performance Improvement of Gateway Anti-Virus System Based on File Scanning," *Control and Decision Conference 09*, 2009, pp. 2293-2295.

[3] T. Ghorbani, A.A., Lu, W., *Network Intrusion Detection and Prevention : Concepts and Technique*, Springer, 2009.

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

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

[6] 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.

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

[8] H.S. Rhee, C. Kim, and Y.U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Journal Computer & Security*, vol. 28, 2009, pp. 816-826.

[9] V. Frias-martinez, J. Sherrick, S.J. Stolfo, and A.D. Keromytis, "A Network Access Control Mechanism Based on Behavior Profiles," *Annual Computer Security Applications Conference*, 2009, pp. 3-12.

[10] W. Kim, O.K. Jeong, and S.W. Lee, "On social Web sites," *Journal of Information Systems*, vol. 35, 2010, pp. 215-236.

[11] C.Y. Wang, S.-cho T. Chou, and H.-ching Chang, "Emotion and Motivation : Understanding User Behavior of Web 2 . 0 Application," *IEEE Computer Society Seventh Annual Commnucation Networks and Services Research Conference*, 2009, pp. 1341-1346.

[12] 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.

[13] 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.

[14] J.M. Estevez-Tapiador, P. Garcia-Teodoro, and J.E. Diaz-verdejo, "Anomaly detection methods in wired networks : a survey and taxonomy," *Computer Communications*, vol. 27, 2004, pp. 1569-1584.

[15] F.G. Marmol and G.M. Perez, "Security threats scenarios in trust and reputation models for distributed systems," *Computers & Security*, vol. 28, 2009, pp. 545-556.

[16] M. Maybury, P. Chase, B. Cheikes, D. Brackney, F.G.G. Meade, T. Hetherington, C. Sibley, J. Marin, T. Longstaff, J. Haile, J. Copeland, and S. Lewandowski, "Analysis and Detection of Malicious Insiders Sara Matzner," *International Conference on Intelligence Analysis*, 2005.

[17] D. Stiawan, A.H. Abdullah, and M.Y. Idris, "The Trends of Intrusion Prevention System Network," *IEEE, ICETC 2010*, vol. 4, 2010, pp. 217-221.

[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] E.E. Schultz, "A framework for understanding and predicting insider attacks," *Computer & Security*, 2002, pp. 526-531.

[20] T. Walker, "Practical management of malicious insider threat – An enterprise CSIRT perspective," *Information Security Technical Report*, vol. 13, 2008, pp. 225-234.

[21] T. Abbes, A. Bouhoula, M. Rusinowitch, and L. Inria-lorraine, "A Traffic Classification Algorithm for Intrusion Detection," *IEEE 21st International Conference on Advanced Information Networking and Application Workshops (AINAW'07)*, 2007, pp. 0-5.

[22] 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.

[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] 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.

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

[26] 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.

[27] M. Sourour, B. Adel, and A. Tarek, "Collaboration between Security Devices toward improving Network Defense," *Seventh IEEE/ACIS International Conference on Computer and Information Science (icis 2008)*, May. 2008, pp. 13-18.

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

[29] A. Le, E. Al-shaer, and R. Boutaba, "On Optimizing Load Balancing of Intrusion Detection and Prevention Systems," *IEEE, INFOCOM Workshops*, 2008.

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

[31] C.M. Akujuobi, N.K. Ampah, and M.N.O. Sadiku, "Application of Wavelets and Self-similarity to Enterprise Network Intrusion Detection and Prevention Systems.," *IEEE International Symposium on Digital Consumer Electronics*, 2007, pp. 1-6.

[32] 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*, 2006, pp. 147-153.

[33] Y. Jiang, Y. Gan, J. Zhou, and Z. Cai, “A Model of Intrusion Prevention Base on Immune,” *2009 Fifth International Conference on Information Assurance and Security*, 2009.

[34] H.O. Myint and P. Meesad, “Incremental Learning Algorithm based on Support Vector Machine with Mahalanobis distance (ISVMM) for Intrusion Prevention,” *Second International Conference on Intelligent Computation Technology and Automation*, 2009, pp. 25-28.

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

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] A. Foroughifar, M.S. Abadeh, A. Momenzaideh, and M.B. Pouyyan, “Misuse Detection via a Novel Hybrid System,” *2009 Third UKSim European Symposium on Computer Modeling and Simulation*, 2009, pp. 11-16.

[47] 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.

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

[49] 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.

[50] 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.

[51] 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.

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