AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

A Framework for Analytic Hierarchy Process-Entropy Network Security Situation Assessment and Adaptive Grey Verhulst-Kalman Prediction in Intrusion Prevention System

[1]Leau Yu Beng, [2]Selvakumar Manickam, [3]Tan Soo Fun

[1,2]Universiti Sains Malaysia, National Advanced IPv6 Center, 11800, Bayan Lepas, Penang, Malaysia.
[3] niversiti Malaysia Sabah, Faculty of Computing and Informatics, 88450, Kota Kinabalu, Sabah, Malaysia.

ARTICLE INFO

Article history:
Received 25 June 2014
Received in revised form
8 July 2014
Accepted 10 August May 2014
Available online 30 September 2014

Keywords:
Security Awareness, Current Network Security Situation Assessment, Future Network Security Situation Prediction, Salient Asset Identification

ABSTRACT

Network intrusion attempts have been on the rise. In order to detect the computer misuse and malicious network traffic, Intrusion Detection System (IDS) has become preferred defence mechanism. Nonetheless, almost 99% of the enormous amounts of generated alert are false positive. These poor quality alerts are inadequate to identify ongoing attack rapidly or predict the next likely goal of an intruder. Even though IDS is able to detect malicious activities afterwards, but due to the remedies only can be taken after the suspicious attempts being detected, the damage of the compromised system could have been done. Hence, a more comprehensive Intrusion Prevention System (IPS) with multi-capabilities is greatly desired to complement IDS in securing the network. Our research aimed to present a novel framework to address the network security situation assessment and prediction. To achieve this aim, our specific objectives are to propose a hybrid Analytic Hierarchy Process (AHP)-Entropy network security situation assessment scheme to assess the current network security status, to design an adaptive Grey Verhulst–Kalman prediction mechanism to forecast the incoming network security situation and to introduce a modified Grey Relational Analysis algorithm to identify the salient asset in the network. This proposed framework is expected to minimize the likelihood of success network attack in the future and reduce the possibility of taking reaction on incorrect critical asset. The findings of this research are projected to significantly rise up the network security situation awareness among the network community.

To Cite This Article: Leau Yu Beng, Selvakumar Manickam, Tan Soo Fun., A Framework for Analytic Hierarchy Process-Entropy Network Security Situation Assessment and Adaptive Grey Verhulst-Kalman Prediction in Intrusion Prevention System. ***Aust. J. Basic & Appl. Sci.,*** *8(14): 34-39, 2014*

INTRODUCTION

In this globalization era, Internet has become an important part in our life with offering convenient services and information sharing. The number of Internet users worldwide has mushroomed to reach 2.7 billion which almost 40% of the world population ("The World in 2013 ", February 2013). Unfortunately, the immense popularity of the Internet and prevalent use of online applications has made Internet a breeding ground for malware and cyber criminals.

G Data Software revealed that there were 1,509,934 new malware found in the first half of 2013. It means an average of 8,342 new malware program types was produced every day ("G Data PC Malware Report ", 2013). In 2012, Symantec also encountered a 58% increase in new mobile malware compared to previous year ("Internet Security Threat Report 2013," April 2013). This phenomenon brings serious challenges and problems to network security.

The number of incidents is also rising. In Malaysia, the published incident statistics for year 2013 indicate that 10636 cases were reported to MyCERT with different types of attacks such as denial of service, intrusion attempt, malicious codes, spamming and etc ("MyCERT Incident Statistics ", 2014). An information security breaches survey conducted by PricewaterhouseCoopers on UK business discovered that 93% and 87% of large and small organizations respectively had a security breach in year 2012 and it causes them to lose £450k - £850k in average on the year ("Information Security Breaches Survey," 2013).

Due to the rising number of the threats, it is becoming increasingly difficult to ignore the current security situation assessment and its future situation prediction to the security communities. Both of these situation

Corresponding Author: Leau Yu Beng, Universiti Sains Malaysia, National Advanced IPv6 Center, 11800, Bayan Lepas, Penang, Malaysia.
Tel: (60)16-6552072. E-mail: leauyubeng@gmail.com / beng@nav6.usm.my

assessment and prediction capabilities were considered as the main components in situation awareness by Endsley (Endsley, 1988) when he introduced the concept of situation awareness in 1998. As complement to the aforementioned capabilities, identifying the salient asset in the current network is essential to give the helpful information to administrator in making the decision and taking the remedies against the network threats.

Network Security Situation Awareness Concept:

Situation awareness is defined as the observation of changing critical factors in complex global network within a time and space interval, the understanding of those factors mean according to the operator's goals and the projection of their status in next interval (Endsley, 1988). In 1999, the concept was first introduced in the cyberspace (Bass & Gruber, 1999) and gradually spread to various areas such as computer network security. In other words, the concept of Network Security Situation (NSS) actually originates from situation awareness (Durso & Gronlund, 1999). Based on Sheng-Hui Chien et al, a security situation can be referred as to which extents of the network devices have been compromised (Chien & Ho, 2012). In computer network, NSS Awareness can be defined as the forecasting of future network security trend by integrating all the captured information regarding the security status in a network.

In general, situation awareness can be divided into three stages which are event detection, current situation assessment and future situation prediction (Endsley, 1995). These stages can be adapted in NSS Awareness and represent the awareness level as Figure 1.

Stage 1: Event Detection is a basic process of situation awareness. This stage mainly to identify the abnormal and malicious activity in the network and translates them into logical format.

Stage 2: Current Situation Assessment is a process to evaluate the security situation of the entire network by using the information obtained from the detected alerts in previous stage.

Stage 3: Future Situation Prediction is aimed to forecast the future network security tendency according to the current and historical network security situation status.

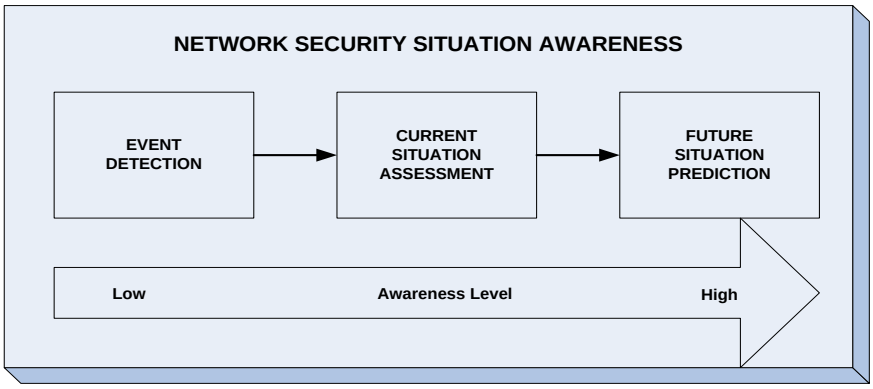

Fig. 1: The Conceptual Model of Network Security Situation Awareness

Problem Statements:

Network intrusion attempts have been on the rise. According to Cisco's 2014 Annual Security Report, there have 50,000 network intrusions are detected and 80 million suspicious web requests are blocked every day ("Cisco 2014 Annual Security Report," 2014). Due to this, Intrusion Detection System (IDS) has become desired security defence mechanism in many companies. They use IDS to analyze the audit log and suspicious packets in order to detect the computer misuse and malicious network traffic. Therefore, Intrusion detection has been studied and grabbed the attention from researchers dating back to the 1980's. Unfortunately, all the remedies only can be taken after the suspicious attempts being detected. It directs the company network to a risky state where they are unable to predict the future security situation of the network.

To date, the research has tended to focus on IDS rather than Intrusion Prevention System (IPS). Despite IDSs may be effective at detecting suspicious activity, but there have a number of problems in use. Literatures have emerged that offer contradictory finding about the reliability and capability of IDS in protecting the organization's network from malicious attempts such as hacking, botnets, worms and etc. Based on Yu and Fricke, almost 99% of the enormous amounts of alert generated by most IDS are false positive and only 1% is corresponding to unique attack (Yu & Frincke, 2007). Even though IDS is able to detect malicious activities afterwards, the damage of the compromised system could have been done. Furthermore, there is no protection provided by IDS against the attacks (Haslum, Abraham, & Knapskog, 2007). The situation has become worse when poor quality alerts of IDS are inadequate to identify ongoing attack rapidly or predict the next likely goal of an intruder. This causes the network to be declared unhealthy and possibly triggering some improper

prevention responses (Sendi, Dagenais, Jabbarifar, & Coulture, 2012). Hence, a more comprehensive IPS with multi-capabilities is greatly desired to complement IDS in advance to ensure the network in healthy.

Timely identifying the most affected asset in the network is essential to make a good decision especially in taking preventive measures towards the malicious activities before they exploit to the network. However, to our best knowledge, there is no research has been found that surveyed on recognizing the most salient or possible influential network asset in the future timeline although it is a prerequisite process for administrator before taking any proper precautions to save the network from harm. Lack of this identification function in existing IPS will cause the administrator mistaking the remedies to preserve the security level of the network. In other words, by discovering the most risky asset periodically, administrator is able to identify the hazardous assets and safeguard them in advance. This capability should be included in an IPS.

Besides that, accurately assessing the network security situation before prediction process is vital to provide useful information to IPS for predicting the incoming network security situation and be ready with proper action taken. Unfortunately, most of the existing prevention systems exclude this capability. Although some of them might include the assessment module but consider all the network assets have same importance value in a company network is an inappropriate assumption. The mixing of truly threatening information and the mass of useless information causes the decision making difficult. Consequently, direct response to particular attack without any assessment on alerts itself as well as network in overall will create a lot of false positive and false negative notification (Jawdekar, Richariya, & Richariya, 2012; Sendi et al., 2012; Shi, Hu, Lu, & Xie, 2010). This shortage has become a strong motivation for us to design a current network security situation assessment module for IPS based on the threats assessment on every single asset in the network.

Most studies in IPS have mainly focus on designing an automated response mechanism, and far too little attention has been paid to embed the network security situation prediction into it. As we know, network environment and its security status are changing frequently. Different attack event brings different threat level and context information to the network. In a study done by University of South Wales in 2013 on nine big-brand IPS systems, they found that seven out of them were failed to detect and block 34%-49% of attacks that target vulnerabilities in web-based application (Xynos, Sutherland, & Blyth, April 2013). Thus, countering attacks in an automated IPS is not an easy and simple task. Apart from requiring a complete list of responses, it also needs an accurate assessment of the current and future network security situation. Otherwise, some of the consequences in automated IPS such as degrading the network performance, incorrectly disconnect users from the network, involving high cost for administrator to re-establishing services, possibility of DDOS attack in the network and etc will be happened (Shameli-Sendi, Ezzati-Jivan, Jabbarifar, & Dagenais, 2012). Therefore, develop a network security situation prediction system to forecast the incoming security situation based on current and historical network status is desired to facilitate IPS to be more intelligent in aspect of preventing the problem from growing and in returning the system to a healthy mode.

Research Objectives:

As mentioned earlier, there is a need to develop a novel and comprehensive framework for assessing the current security situation and predicting the incoming situation based on current and previous security situation which obtained from detected intrusion alerts. With this in mind, the specific objectives of this proposal are as follows:

1. To propose a hybrid AHP-Entropy network security situation assessment scheme to assess the current security status of the network.
2. To introduce a modified Grey Relational Analysis algorithm in identifying the most salient asset in the network.
3. To design an adaptive Grey Verhulst-Kalman prediction mechanism to forecast the incoming network security situation.
4. To evaluate the performance of the proposed framework by implementing a novel prototype with real data.

Research Scope:

The present research framework consists of five main modules. There are Data Preparation Module, Data Normalization Module, Network Security Situation Module, Salient Asset Identification Module and Network Security Situation Prediction Module. Figure 2 shows the framework of proposed research.

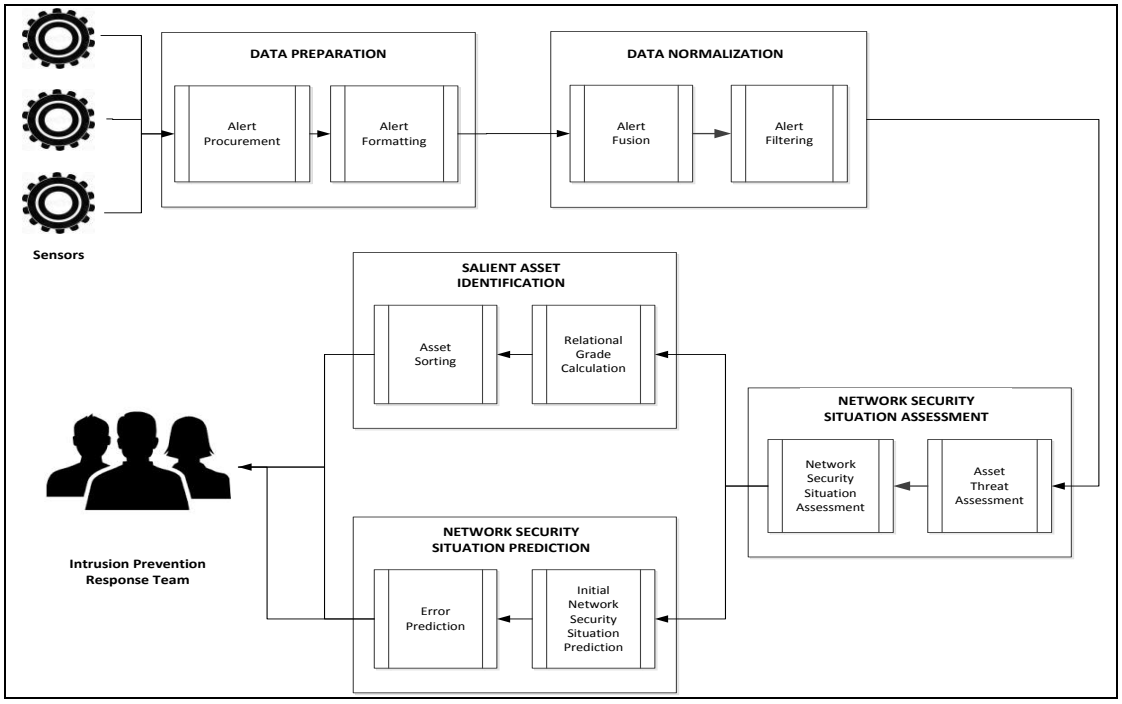

Fig. 2: A Framework for Network Security Situation Assessment and Prediction

Module I: Data Preparation:

The main purpose of this module is to prepare the appropriate data and ensure them are in the proper format before using them in the following processes. There are two components in this module which are Alert Procurement and Alert Standardization. The function of Alert Procurement is to receive the detected alerts from Intrusion Detection System and save them in a text file. In order to smoother the fusion process in next module, Alert Formatting is responsible for extracting the features in each alert from the file and save them in a CSV-type file.

Module II: Data Normalization:

This module is built to categorize the alerts in a particular group based on their similar features. It also aims to eliminate the possibility of using the bunch of redundant alerts which might lengthen the processing time in the process. Alert Fusion and Alert Filtering are the components to accomplish the main function of this module. In Alert Fusion component, with user-defined time-interval and same destination address, the formatted alerts in the file from previous module will be fused accordingly. Then, the redundant alerts in each cluster will be filtered out in the Alert Filtering component. A counter will be used to count the frequency of each type of alert.

Module III: Network Security Situation Assessment:

The function of this module is to assess the overall security situation in the network in order to alert the security administrators with their current network status. Threat on each asset will be evaluated prior to the overall network assessment. The Asset Threat Assessment component in this module will use the Analytic Hierarchy Process (AHP) to derive a ratio scale of each asset from its tangible (e.g. alert severity and frequency) and intangible (e.g. cost and implication) aspects in the network. After calculating the asset threat of each alert type, Alert Network Security Situation Assessment will apply the Entropy concept to measure the uncertainty degree of the network assets. The greater the entropy is, the more serious the security situation of this particular asset is.

Module IV: Salient Asset Identification:

This module is intended to identify the salient asset in a particular time period. The most influential asset in the network will be recognized by using Modified Grey Relational Analysis (MGRA) algorithm. Instead of regression analysis, this relative analysis has been chosen because it requires small sample size and more accurate for comparison of alternatives (Jumaat, February 2012). Depending on duration of time, the relational coefficient and grade of each asset will be calculated in Relational Grade Calculation component. The Asset Sorting component is work for sorting the asset based on its relational grade. Comparison of grade among the assets also will be done to discover the degree of impact between them towards the network in specific time-interval.

Module V: Network Security Situation Prediction:

This module is aimed to forecast the incoming network security situation which able to alert the network administrator before the attack intruded into the network. For better precision rate, the predicted value of network situation is combined with its predicted error as well. Initial Network Security Situation Prediction component utilize a novel Adaptive Grey Verhulst algorithm to compute the predicted assessment of the network on next time-interval. Meanwhile, Error Prediction component will apply Recurring Kalman Filtering algorithm to calculate the predicted error based on the previous prediction errors. Grey Verhulst and Kalman Filtering algorithms are chosen due to their few input samples needed and less training required respectively. The combinations of them are able to form a new dynamic prediction model in finding more accurate projected security situation value in the network.

Conclusion:

In the nutshell, a more intelligent and multi-functional intrusion prevention system which embedded with capabilities of assessing current network security situation, forecasting future network security situation and identifying salient asset in the network is desired to complement IDS to secure the network. Our proposed framework is expected to minimize the likelihood of success network attack in the future and reduce the possibility of taking reaction on incorrect critical asset. With the predicted value of incoming security situation and identified most influential asset, it will acknowledge the security analyst with a significant confidence level of the prediction to have a comprehensive plan in taking a more proper action against the incoming event. The findings of this research are also projected to significantly rise up the network security situation awareness among the network community.

REFERENCES

Bass, T., and D. Gruber, 1999. A glimpse into the future of id login: Special Issue Intrusion Detection. *The USENIX Association Magazine*.

Chien, S.-H., and C.-S. Ho, 2012. A Novel Threat Prediction Framework for Network Security *Advances in Information Technology and Industry Applications* pp: 1-9: Springer.

Cisco, 2014 Annual Security Report. pp: 1-81. United States: Cisco.

Durso, F.T., and S.D. Gronlund, 1999. Situation awareness.

Endsley, M.R., 1988. *Design and evaluation for situation awareness enhancement.* Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting.

Endsley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. The Journal of the Human Factors and Ergonomics Society, 37(1): 32-64.

Data, G., P.C. Malware Report, 2013. *Half-yearly Report (January - June 2013)* pp: 1-12. Germany: G Data SecurityLabs.

Haslum, K., A. Abraham and S. Knapskog, 2007. *Dips: A framework for distributed intrusion prediction and prevention using hidden markov models and online fuzzy risk assessment.* Paper presented at the Third International Symposium on Information Assurance and Security (IAS 2007).

Information Security Breaches Survey. (2013) pp: 1-22). London, United Kingdom: Department for Business Innovation & Skills, PwC.

Internet Security Threat Report 2013. (April 2013) (Vol. 18, pp. 1-58). United States: Symantec Corporation.

Jawdekar, A., V. Richariya and V. Richariya, 2012. Minimization of False Alarm Prediction in IDS Based On Frequent Pattern Mining. International Journal of Emerging Technology and Advanced Engineering, 2(4): 511-514.

Jumaat, N.B.A., 2012. *Incident Prioritisation for Intrusion Response Systems.* Doctor of Philosophy, Plymouth University, United Kingdom.

MyCERT Incident Statistics, 2014. *Year 2013* Retrieved 28 February 2014, 2014, from http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html

Sendi, A.S., M. Dagenais, M. Jabbarifar and M. Coulture, 2012. Real Time Intrusion Prediction based on Optimized Alerts with Hidden Markov Model. Journal of Networks, 7(2): 311-321.

Shameli-Sendi, A., N. Ezzati-Jivan, M. Jabbarifar and M. Dagenais, 2012. Intrusion response systems: survey and taxonomy. International Journal Computer Science and Network Security (IJCSNS), 12(1): 1-14.

Shi, J., G. Hu, M. Lu and L. Xie, 2010. Intrusion alerts correlation based assessment of network security. Paper presented at the 2010 International Conference of Information Science and Management Engineering (ISME).

The World in 2013 (February 2013). *ICT Facts and Figures*, 1-8. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Xynos, K., L. Sutherland and A. Blyth, 2013. Effectiveness of Blocking Evasions in Intrusion Prevention System (pp. 1-6): University of South Wales.

Yu, D., and D. Frincke, 2007. Improving the quality of alerts and predicting intruder's next goal with Hidden Colored Petri-Net. Journal of Computer Networks, 51(3): 632-654.