ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

A Multi-Stage Analysis Based Framework for Network Security Situational Awareness

[1]R. Mohanraj and [2]S. Anbu

[1]*Research Scholar, Department of Computer Science and Engineering, St.Peter's University, Avadi, Chennai, Tamilnadu, India.*
[2]*Professor, Department of Computer Science and Engineering, St.Peter's College of Engineering and Technology, Avadi, Chennai, Tamilnadu, India.*

ARTICLE INFO

Article history:
Received 23 June 2015
Accepted 25 August 2015
Available online 2 September 2015

Keywords:
Network Security Situation Awareness, Cyber Attacks, Intrusion Detection and Prevention.

ABSTRACT

A Framework for prevention based Network Security Situation Awareness (NSSA) technology has been discussed in the recent research of multi-data analyzing. Real time data transmission, official communication, military information sharing and international political information transmission needs security awareness information as a precaution before real transmission avoid cyber-attacks. In this paper a pre-information about the security is provided to the network peers as precaution information. After the precaution information broadcasting, all the peers can start their communication in the network. All the key points of the network situation are analyzed in situation awareness and the informed to the network peers. An evaluation method is provided for NSS and represent how to apply this method to NSSA. A stage by stage analysis framework for NSSA is presented to demonstrate the advantages and effectiveness by using this precaution method.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: R. Mohanraj and S. Anbu., A Multi-Stage Analysis Based Framework For Network Security Situational Awareness. ***Aust. J. Basic & Appl. Sci.,*** *9(27): 42-47, 2015*

INTRODUCTION

In the present scenario, the threat to the network infrastructure was growing drastically and this leads to the heightened need to implement the security options. Thus the situation awareness it seemed very important in evaluating the situation awareness of security analysts in different phases. The importance lies due to the complexity of all operations in the modern utility system. Situation awareness is the process of being aware of the happenings in the vicinity. This is a major field of study concerned with the perception of the environment for making decisions in the complex fields. Such awareness is required in the networks to ensure the availability, integrity and the confidentiality of the services in the network. The main responsibility lies in the maintenance of situation awareness over the thousands of the objects in the network. In general, the right information was obtained by a systematic process with optimization of time by geographic information system technology. This technology provides enhanced situational awareness. According to the technology, the information should be contextualized. This property provides situational awareness in all phases of management. Then the capability to prevent to the crisis which requires access to the required information was created. And the overloading of information was avoided by prioritizing the data sources based on the mission requirements. The dynamic data will additionally provide support to the mission and the situational awareness was heightened. With these there is an enhancement of accessing, analyzing and presenting information to know in depth about the existing conditions with varying time.

Some traditionally adopted network security devices such as Intrusion Detection System, security scanners and firewalls virtually have no information of the network assets they defend though they have independent operation. This lack of knowledge will lead to numerous uncertainties when the alerts are interpreted and decisions are made on the adequate resource. Due to the threats in the network which includes large scale network attacks and network worms, there needs a security option. Thus network security situation awareness plays an effective way to overcome these threats. Our growing dependency has greatly increased the demand for situation awareness which essentially understands the environment and accurately predicts the potential problems. The topology of the IT infrastructure was very difficult to handle where the network components are located in the logical architecture using references. The simple scenario of the security awareness has web server and file server. This will be protected by the two

Corresponding Author: R. Mohanraj, Research Scholar, Department of Computer Science and Engineering, St.Peter's University, Avadi, Chennai, Tamilnadu, India.
E-mail: mohanresearch254@gmail.com

firewall presented in the demilitarized zone. This could able to separate the external network and the internal network. The firewalls will control the traffic between the DMZ and the internet whereas the next firewall simply allows the access of Network file system protocol between the fileserver and the web server.

The procedure to perceive the security events in the network occurred in a time interval and in the environment involves security data manipulation, analyzing the attack behaviors and in providing a network security in a global view. It also involves assessing the security situation and predicting the future security network trends. Still there exist some difficulties while implementing the network security situation awareness. The difficulty is due to some security sensors which generate tremendous alert events with high false positive rate, the complex relation of the trivial alerts generated by the large scale networks and also due to the abundant alert events form the security sensors, while there is a lack of information needed the alert processes. Rather the difficulty lies in acquiring this information in automated process. In today's demand, there is a necessity of meaningful network situation awareness in order to safeguard the sensitive data, sustain their fundamental operations and protecting their national infrastructure. However the networks will have some vulnerability such as significant risks that occurs in both individual organizations and in national security places. With great expectation about the future of the system, the effective countermeasures have been developed to protect the critical missions.

Background Study:

To study about the network security situation awareness, a historical war story was used to explain the situation awareness concepts and the challenges (Haoliang Zhang, 2013). An evaluation method was provided for the network security situation and to analyze the multi-level framework for its application in NSSA. The complexities and the existing problems of the situational awareness system were studied and a framework was proposed which consists of the network security situation modeling and generation. It also supports accurate modeling and effective generation of the network security. It was shown in their application in the Net-SSA (Fang Lan, 2010). A theoretical model of the situation awareness was presented in the paper. The impact of design features, stress complexity, workload and the automation was addressed based on the model. The model generates the design implications to enhance operator SA and their relation with the future directions for research (Endsley, M., 2005). The network security situation awareness was analyzed all over the world and a model, NSAM based on the simple additive weight and grey theory was presented. The test results proves that the NSAM was very feasible and a reasonable (Lai Jibao, 2006). This approach implies the application of artificial immune technology in the situation awareness. This enables the self-learning and adapting further increasing the immunity and viability. By this accurate and reasonable response was provided for guaranteeing the usability of the system (Sun Jun Liu, Le Yu, Jin Yang, 2011). The survey on the resilience networks and the situation awareness was described in this approach. It was introduced in the development of module in the dynamic adaptation architecture which realizes the resilience control loop. The state transition model was introduced along with a fusion algorithm (Mixia Liu David Hutchison, 2011). Intrusion Detection System is drastically growing mechanism utilized for network protection which can protect all kind of malicious activities occurrence in the network (Deepa U. Mishra, 2013). Present intrusion detection systems provide huge number of false alarms each day which lead to block the network communication through incoming port connections (Goodall, J.R., 2004; Hellman, M.E., W. Diffie, 1999). Security awareness comprises of four levels includes perception, comprehension, projection and resolution (Cyril Onwubiko, 2009). Initially NSSA is a conception pertinent to assessing and showing the global and comprehensive situation of network security (Endsley, M., 1988; Bass, T., 1999; Bass, T., 2000; Ticha, B., T. Ranchin, 2006). So it needs people to gather all types of data and analysis for as many dimensions as possible in order to reflect the macroscopic pictures. After analyzing all the existing approaches, methodologies and techniques, it is concluded that there is essential to have standard network security situation estimation presently (Tadda, G., 2006; Zhuo, Y., 2008; Endsley, M., 1995).

Existing System:

In the existing system the security situation of the network is studied and information passed only to the server. The study phase is carried out by an intelligent approach named PSO which learn the systems with multi-objectives. This approach helps to take a decision about the network by the peer or about the peer by the network. In any network like, military, medical, surveillance it is highly impossible to detect the behavior before connecting in to the network. Also PSO apply a fitness function with an assumed threshold value for all the particles. The fitness function and fitness value may vary for various resources at various times since it is situation awareness study. To overcome these problems and apply a thorough study to decide a peer is good or bad and apply precaution a multi-stage precaution information method is proposed in this paper.

Multi-Stage Analysis:

Various Stage of the network situation should be analyzed such as perception, comprehension and projection. In the perception stage, the basic

information about the peers, neighbors, friend peers and enemy peers are recognized and analyzed to determine the original behavior of the peers while entering in to the network. In the comprehension stage the present situation factors of the peers and the network are analyzed. This analysis can help to find out the future status of the present active peers in the network. In the projection stage, a decision tree based analyzation is applied to all the peers where it can provide the core status of the peers as favor or un-favor to the network. These processes bring out the input assessment of the peers properties, relations derived from each stage in the network. From this assessment an output assessment can be provided to all the peers in the network about the Good and Bad peer in the network. The situation awareness report will be generated only from the comprehension stage and projection stage. In the comprehension stage the analyzation provides what the present situation is, and in the projection stage, it provides what the situation will be in case of the factors changed. This analyzation is applied in a periodic interval to detect and prevent the network from the various attacks. The entire architecture of the proposed Multi-stage precaution broadcasting model is shown in Figure-1. Also, from the above discussion, it is identified that, to assess about the network and peers in the network, the following steps to be followed.

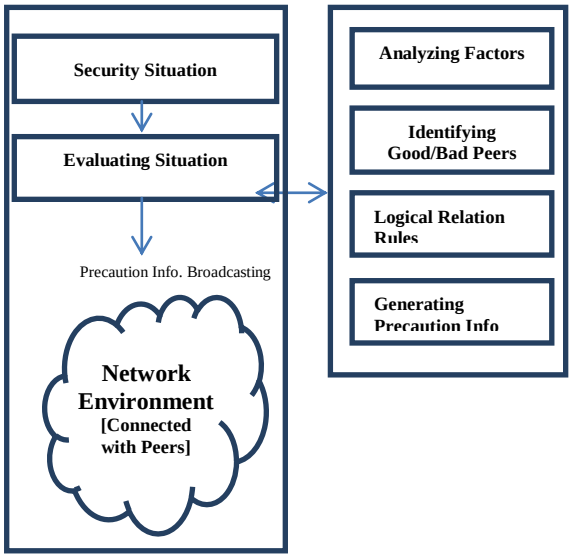

Fig. 1: Multi-Stage Precaution Information Broadcasting Model.

- It is necessary to do evaluation in terms of Good and bad sides of the situation to assess the situation.
- Evaluating the good peers, enemy peers and the environment is more important. Some of them can scale up the power and some of them can restrict the role in the network.
- Main and final step to follow in this paper is applying a threshold value for each factor for accurate evaluation, and import certain rules to increase the network communication as effective and it should be decided after the status of the network specified situation.

The above points are identified and investigated as best to obtain the comprehension of the all kind of situations by evaluating the present situation in terms of present behavior and factors can be calculated. These behavior and factors only can determine the future situation regarding comprehensive and projection.

Precaution Information in Network Security Situation Awareness:

The www has huge amount peers connected to transmit data and information. Various kinds of peers [computer devices and equipment] are connected together by making a virtual space called as cyber space. The security situation of the virtual space is named as cyber situation or NSS. It is dedicated to evaluate the security situation of the virtual space by any typical method more suitable. After evaluation of the security situation the environmental principle will explored to the peers in the cyberspace. During this process, the factors affecting the cyberspace will be noted and the rules for each factor applied within the cyberspace. This security situation exploration is called as pre-caution information.

Proposed Approach:

Since, network environment is more complex in structure due to different kinds of computers, OS, facilities and program installed they should participate in data transmission as the conclusion. Entire network communication and data transmission is simplified by defining the working pattern of the data transmission where the network comprises of houses, workers in MNC, banks and medical industry are working very easily and speedily by sending their letter from one place to another place. If the bankers make mistake then they may lose an amount [money], if they have weakness and their transaction

is noticed by intruders by controlling the network by commands. In our model, it is considered that the LAN is a castle, computers are houses and OS, programs are considered as workers in bank. The network security problems are abstracted as a mission to keep the money safe in their work place.

Whenever the proposed model detects the weakness in a particular banker, it automatically sends an alert message to banker to intimate about their weakness. The alert messages are like "Are you Sure?", "Do u Like to Proceed?", "Think twice before click ok" and so on. It makes the banker to think about their work to be proceeding or not. Making confusion will provide a good decision in most of the time.

Evaluating Network Security Situation:

Let we assume that the NSS is initially studied in a LAN environment. According to our model, the main idea is to measure the NSS is how well it can keep the money safe and on the attacker side it can also be measured how far it is possible to steal the money. Because, it is difficult to measure how to save the money and it is easy to measure how the money be stolen. From this it can be chosen the later approach to do the evaluation. The main factors to be considered to lose the money includes the

- Frequency of banker makes mistake and
- The weakness of the bankers who are easily controlled.

The frequency of banker to make mistake is a statistical data and it is somewhat stable. The weakness of the bankers' means, it is very easy to take control of, and if the new weakness ranked a lower level, then more attackers will have the ability to take control of the bankers, hence it plays a scale up role in the calculation. In this situation, the once the bankers weakness is noticed during the evaluation, it is intimated by precaution message to the network and to the same peers to correct themselves for not making mistakes. In the evaluation of NSS, it is necessary to count the possibilities for lose the money from the internal peer [banker], and integrate the vulnerabilities and historical intruders' quantity scale to speculate on the possibilities of being controlled by attackers. These evaluation methods prevent the bankers from the attackers. To improve the accuracy of the cyberspace prevention, some of the new challenges can also be integrated. During the analyzation, the peer-ID, peer-port, peer-number will be detected for bad peers and informed to the network environment.

Challenges of Precaution Information:

Most of the theoretical information is gathered in comprehensive stage only. It is used to emphasize the logical relation among the present situation and the future situation in terms of various factors in the analyzation method. From the analyzation, it easy to identify the weakness bankers, weak environment, attackers ready for compromising, situation factors in the virtual objects. So it is essential to provide a specific identification method for every kind of low-level data to assign speculative value to the right risk factors. To avoid weakness, attacks the environment can be studied by implementing certain rules physically [by deploying sensing devices] or by logically the present behavior of the peers can be studied. This evaluation method is shown in Figure-2. According to the irregular, irrespective behavior, the precaution information will be broadcast to all other peers and to the network environment speedily.

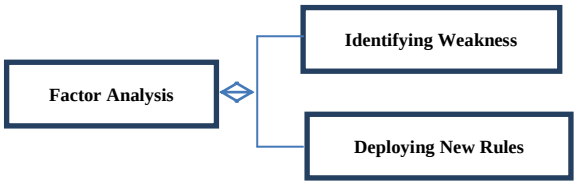

Fig. 2: Evaluation Method.

Simulation and Result:

The Multi-stage precaution information methodology is simulated in a college Laboratory having more than 250 computer systems. Lab is installed with Windows-7 operating system; Airtel based WiFi internet connection and more hardware and software resources. It is noticed that all kind of secured transactions is happening in the internet like bank transaction in the office, student data transaction between the college and the university and so on. All the transactions make in the college is more important and need more security. To do simulation about the proposed approach, a system monitoring software is installed and analyzed about the systems and the system behavior. According to our evaluation strategy, and the constraints applied some of the systems are identified as bad systems due their request applied in the internet as well as in the intranet. The entire details of the simulation data and the identification of bad system are given in Table-1.

Table 1: Simulation Results.

No. of Systems	Normal	Denial of Service	Probe	Sybil	Selective Forward
250 [R1]	250	12	9	7	3
250 [R2]	200	8	6	3	3
250 [R3]	100	4	4	1	1

Table-1, depicts that there are 250 systems are connected in the LAB and all the systems are assumed as normal [Good-behavior] systems. A LAN and System monitoring software is installed in the server as well as in each system respectively for monitoring the behavior in the network. According to the factors analyzed it is detected that 12 systems are identified under DoS behavior, 9 systems are detected under Probe behavior, 7 systems are detected under Sybil behavior and 3 systems are detected under selective forwarding attack. After detecting the abnormal system behavior it is broadcasted to the entire peers connected in the network about them with the peer information. The following Figure-3 illustrates the above process is simulated three rounds and the results obtained in each round. From this it is clear that the number of attack created in a network is less for less number of resources, and number of attacks is more for more number of resources connected in the internet.

But in the existing system the data are taken from the benchmark dataset and it is simulated. The results are given in the following Table-2 and in Figure-4.

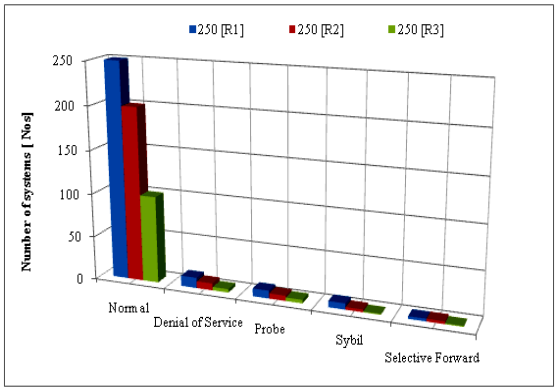

Fig. 3: Analyzation of Network and Identifying the Abnormal Peers.

Table 2: Classification of Network and Attacks.

No. of Network Connection	No. of Attack	Category	Types of Attack	Correctly Identified	InCor. Ident.
20	4	Back	DOS	4	0
40	7	IPSweep	Probe	6	1
20	2	Perl	U2r	2	0
10	3	ftp_write	R2l	1	2

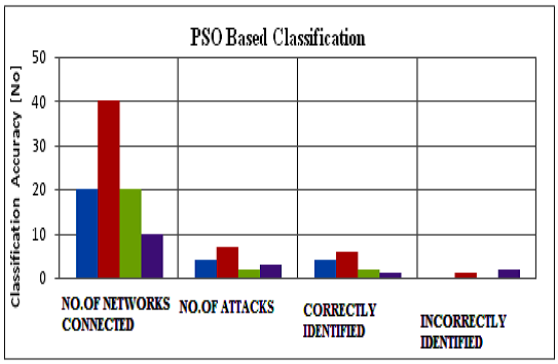

Fig. 4: PSO Based Classification on NSSA.

A portion of the data taken from [18], input to PSO algorithm. The PSO algorithm investigate and evaluate the network parameters and classify the networks is Secured or unsecured. According to the classification PSO proves that it can evaluate the network security situation awareness in a better manner than the other existing approaches. From Figure-3 and Figure-4, Table-1 and Table-2 comparatively the Multi-stage precaution information is suitable for NSSA analyzation for making a good decision about the peers or about the network environment. Also identifying the bad resources is more accurate for more number of resources in proposed approach than the existing approach. From the results it can be noticed that our proposed multi-stage precaution information is a better approach for NSSA analyzation in real time network.

Conclusion:

The main objective of this paper is to provide a challenging NSSA by providing precaution information broadcasting. Precaution information is generated by analyzing the risk factors in various stages. The factors belong to all the peers in the network and the environment where the peers are going to connected. By identifying the factors and applying rules in various stages can improve the prevention method in this paper. Identification of the factors is obtained while analyzing the logical relation among the peers and the environment in each continuous stage. These identification, rule applying, analyzation are the steps integrated in the multi-stage framework to provide a precaution information about the attacker and the bad environment in the internet. Preventing the data loss from the malicious activity is obtained highly here by deploying the proposed multi-stage precaution information broadcasting method on the whole. From the results and discussion it is clear that providing prevention from Intruder safe the data more than loss the data.

REFERENCES

Bass, T., 1999. "Multisensor data fusion for next generation distributed intrusion detection systems", IRIS National Symposium on Sensor and Data Fusion.

Bass, T., 2000. "Intrusion systems and multisensor data fusion", Communications of the ACM., 43(4): 99-105.

Bode Moyinoluwa, A., Alese K. Boniface, Thompson F. Aderonke and Iyare Otasowie, 2014. A Bayesian Network Model for Risk Management in Cyber Situation", WCECS, 22-24.

Cyril Onwubiko, 2009. "Functional Requirements of Situational Awareness in Computer Network Security", Conference on Intelligence and Security Informatics, IEEE, pp: 209-213.

Deepa U. Mishra, 2013. "Knowledge Based Context Awareness Network Security For Wireless Networks", International Journal of Computer Trends and Technology, 4(10).

Endsley, M., 1988. "Situation awareness global assessment technique (SAGAT)", In Proceedings of the IEEE 1988 National Aerospace and Electronics Conference, 3: 789-795.

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

Endsley, M., 2005. "Toward a theory of situation awareness in dynamic systems, " Human Factors, 37(1): 32-64.

Fang Lan, Wang Chunlei, MaGuoqing, 2010. "A Framework for Network Security Situation Awareness Based on Knowledge Discovery, International Conference on Computer Engineering and Technology, IEEE.

Goodall, J.R., W.G. Lutters and K. Anita, 2004. "The work of intrusion detection: rethinking the role of security analysts," Proceeding of the Tenth Americas Conference on Information System, New York, pp: 1421-1427.

Haoliang Zhang, Jinqiao Shi, Xiaojun Chen, 2013. "A Multi-Level Analysis Framework in Network Security Situation Awareness", Elsevier B.V.

Hellman, M.E., W. Diffie, 1999. "An Introduction to Cryptography", Proceedings of IEEE, 67: 397-427.

Lai Jibao, Wang Huiqiang and Zhu Liang, 2006. "Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory", Computational Intelligence and Security, IEEE.

Mixia Liu David Hutchison, 2011. "Towards Resilient Networks Using Situation Awareness", ISPEC, Springer.

Sun Jun Liu, Le Yu, Jin Yang, 2011. **"**Research on Network Security Situation Awareness Technology based on AIS" International Journal of Knowledge and Language Processing.

Tadda, G., J. Salerno, D. Boulwarea, M. Hinmana, S. Gorton, 2006. "Realizing situation awareness in a cyber environment", In: Dasarathy, BV., editor. Proceedings of SPIE, 6242.

Ticha, B., T. Ranchin, 2006. "A case based reasoning data fusion scheme: Application to offshore wind energy resource mapping", 9thInternational Conference on Information Fusion" Florence, Italy, pp: 206.

Zhuo, Y., Q. Zhang, Z.H. Gong, 2008. "Cyberspace situation representation based on niche theory", International Conference on Information and Automation. Zhangjiajie, China, pp: 1400-1405.