ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

A Novel Approach to Network Security Situational Awareness Methods and Models

Chintada Srinivasarao, J UdayKumar
Asst.Prof, Dept of IT, AITAM, Tekkali, Srikakulam, Andhra Pradesh, India
Asst.Prof, Dept of IT, AITAM, Tekkali, Srikakulam, Andhra Pradesh, India

Abstract -- Network is a combination of nodes (a node may be a computer, a mobile, a sensor, and any other communicating devices) in an ordered manner in which they can communicate with each other. Security threats are very often in any kind of network due to many reasons, we developed a system which can detect these threats and provide us hassle free go. But even though by having security systems like intrusion detection system, Firewalls and security scanners etc are give raise to high false positive ratio due to many reasons with them just like malfunctioning of the device, Wrong Event judgment. Due to this network security situation becomes malicious and complete vulnerable and they may rise false to NSSA. We try to solve these kinds of problems by using Knowledge based Discovery to develop an enriched Framework [2],[9],[11,[12].

Index Terms: **Multi-sensor fusion, Security situational awareness, Situation Awareness, security situation, cyber attacks**

I. INTRODUCTION

What Is Network Situational Awareness?

Network situational awareness is the systematic gathering, analysis, and interpretation of data from local and remote networks, regarding structure, applications, traffic, and resources to produce actionable information for decision making in network operations and defense. —Richard Friedberg. Achieving network situational awareness depends on an organization's ability to effectively monitor its networks, ultimately, to analyze that data to detect malicious activity. The CERT Network Situational Awareness (NetSA) group has analyzed hundreds of real-world cases of malicious activity on large, enterprise scale networks to developed tools and approaches that can help organizations defend their networks from potential attacks. The CERT NetSA group works to provide broad quantitative insights on network traffic characteristics relevant to the security of the networks involved.

Network security situational awareness provides the unique high level security view based upon the security alert events. Traditional intrusion detection systems trigger thousands of false positive alarms per minute. This makes the field of NS a very much difficult one to deal with. Multi-sensor fusion coupled with network security situational awareness is a viable solution to the issues that intrusion detection systems encounter. The framework consists of the modeling of network security situation and the generation of network SS. The purpose of modeling is to construct the formal model of NSS measurement based upon the D-S evidence theory, support the general process of fusing and analyzing security alert events collected from security situation sensors. The generation of NSS is to extract the frequent patterns and sequential patterns from the dataset of network security situation based upon knowledge discovery method and transform these patterns to the correlation rules of NSS, and finally to automatically generate the NSS graph. NSSA system aims to get awareness of network, it has to offer intuitionistic data to administrators, such as how dangerous of the device is how serious of an attack is, rather than directly offer alerts to administrators. It is hard for administrators to conclude how serious of the attack is via checking the alerts manually. Application of the Net-SSA shows that the proposed system supports for the accurate modeling and effective generation of NSS. The objective of project is to design a system that will

- Provide unique very high level security view based on the security alert events.
- Detection and notification of infect packets within network.
- Drastically reduce the false positive and false negative rates.

II. RELATED WORK

A. Brief Literature Survey

NSSA is an emerging technique in the field of network security and it helps security analysts to be aware of the actual security situation of their networks. IDSs have received considerable attention as mechanisms for protecting network systems from being compromised the confidentiality, integrity and availability. However, current IDSs trigger thousands of alarms per day, up to 99% of which are false alarms that hinder the automatic deployment and the effectiveness of countermeasures. Security monitor systems can not consider either the attack or the attacker to be the most important in the intrusion detection. What is needed is a situational view and Situation Awareness (SA) tools which may be used to provide an awareness of NSSA.

The concept of SA comes from the research on human factors in the realms of aerospace and aviation. Endsley defined SA as “the perception of the elements in the environment within a volume of time and space; the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

comprehension of their meaning and the project of their status in the near future". In the last fifteen years the application of SA has been revolutionary, particularly in air target control, defence space and cognitive science where SA has been extensively researched. When compared to ATC or defence space, SA in computer network security is still in it searly stages. Cyber attacks are numerous and evolving, code-driven attacks, deliberate malicious software attacks, espionage, distributed denial of service attacks, phishing and insider attacks. Although individual and independent controls exist to protect computer networks from each of these attacks, each control is directed towards addressing a specific attack. Detection of widespread or enterprise-wide attacks is challenging, more so, the way existing controls are deployed makes it extremely difficult to detect a variety of attacks, make broader attacks classifications, assess situations perceived in the enterprise, or quantify associated risks accurately and more swiftly. A known fact is that the capability of any singular security control is limited. It is not possible for organizations to purchase myriad security controls (for every type of attack perceived in the network), especially with the recent credit crunch, it has become ever more important for enterprise to seek alternative, accurate, more reliable and more affordable approaches. A recommended approach is to use existing controls in the organization but to combine their set of evidence to provide better SA of network states, and interdependent risks that may exist in security networks. Integrating evidence of obtainable security controls is the focus of multi-source data fusion [5],[6],[7],[10], where numerous heterogeneous security controls are combined to provide accurate SA in the network. Example, evidence of attacks perceived by firewalls, IDSs, security guards are all combined, such that their independent intelligence are aggregate to provide meaningful and richer inferences than that obtained from any individual security control. To observe (gather evidence), correlate and aggregate data from multiple observing sensors or persons to provide accurate and much improved decision of the observed phenomenon (situation) is the underlying building block of Network security situational awareness. A terminology recently used to describe SA in Computer Network defence (CND), relies on the knowledge and ability of the analyst to perceive and analyze situations, make resonance decisions on how to protect organization's valued assets and offer accurate predictions of future states in a dynamic and complex environment. Security situational awareness has become a hot topic in the area of network security research in topical years, which attracts the interest of more and more domestic and overseas researchers. The offered security situational awareness methods are analyzed and compared in detail. Taking into consideration the characteristics of multi-source information in network security research, a new NSSA model based on information fusion is projected. This model fuses multi-source information from a mass of logs by introducing the modified D-S evidence theory, gets the values of nodes security SA by situational factors fusion using attacks threat and vulnerability information which network nodes have and successful attacks depend on, computes the value of NSSA by nodes situation fusion using service information of the network nodes, and draws the security-situation-graph of network. Then, it analyzes the time series of the computing results by ARMA model to forecast the future threat in network security. In conclusion an example of actual network datasets is given to validate the network security situational awareness model and algorithm. The results show that this model and algorithm is more effective and accurate than the existing security situational awareness methods. [1]

B. Problem Statement

A network is a combination of nodes (a node may be a computer, a sensor, a mobile or any other communicating devices) in a ordered manner in which they can communicate with each other. So the security threats are very often in any kind of network due to many reasons, and we developed many systems which can detect these threats and provide us hassle free go. But even though by having these systems like IDS, Firewalls, security scanners etc are give raise to high false positive ratio due to many reasons with them just like malfunctioning of the device, Wrong Event judgment and many more. Due to this NSS becomes malicious and complete vulnerable and they may raise false NSSA. To solve these kinds of problems we use Knowledge based Discovery to develop an enriched Framework. NSSA provides the unique high level security view based upon the security alert events. Traditional IDS trigger thousands of false positive alarms per day. This makes the field of network security a very difficult one to deal with. Multi-sensor fusion coupled with NSSA is a viable solution to the issues that IDSs encounter. The framework consists of the modeling of NSS and the generation of NSS. The purpose of modeling is to construct the formal model of NSS measurement based upon the D-S evidence theory, and support the general process of fusing and analyzing security alert events collected from security situation sensors. The generation of NSS is to extract the frequent patterns and sequential patterns from the dataset of NSS based upon knowledge discovery method and transform these patterns to the correlation rules of NSS, and finally to automatically generate the NSS graph. NSSA system aims to get awareness of the network, it has to offer intuitionistic information to administrators, such as how serious of an attack is or how dangerous of a device is, rather than directly offer alerts to administrators. Actually, it is hard for administrators to conclude how serious of the attack is via checking the alerts manually.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

Application of the integrated NSSA shows that the proposed system supports for the accurate modeling and effective generation of NSS.

III. PLAN OF PROPOSED WORK

A. Network Awareness (Today)

- Disciplined asset and configuration management
- Routine vulnerability auditing
- Patch management & compliance reporting
- Recognize and share incident awareness across the organization.

B. Threat Awareness (evolving)

- Identify and track internal incidents and suspicious behavior
- Incorporate knowledge of external threats
- Participate in cross industry or cross-government threat-sharing communities on possible indicators and warnings.

C. Mission Awareness (needed)

- Develop a comprehensive picture of the critical dependencies (and specific components) to operate in cyberspace
- Understanding these critical dependencies to support mission-impact in forensic analysis (after a situation); triage and real time crisis-action response (during a situation); risk/readiness assessments prior to task execution (anticipating and avoiding situations); and informed defence planning (preparing to mitigate the impact of a future situation).

D. Methods for situational awareness

User need: faster development of security, rescuing, and defense applications with enhanced real time situational awareness.

Solution: my method is combining a state-of-the-art sensor network with high-performance computational services.

Benefits: unique in-situ outdoor measurement network, at the training site of Emergency services college. One more is Expertise network for computational methods.

Users: Developers of monitoring services for industrial plants, crisis management, sensor testing, training services..etc

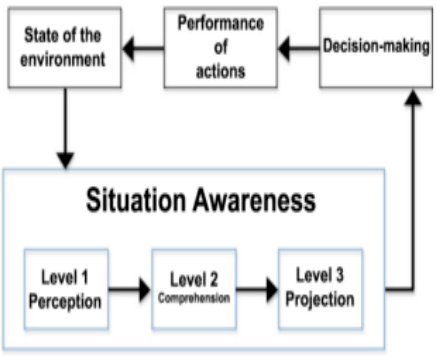

Fig 1: situation awareness

NSSA has been a hot research spot in the NS domain. The existing research situation of NS visualization is analyzed. For the technical issues that the index of security situation is not accurate, and visual effects is not precise, the research designed and implemented the security situation visualization prototype system based on geographic information systems, network topology graph, attack paths. The security situation data show in multiple views, angles, levels, display to the user by visualization technology, the presentation of the security situation will be more accurate and vivid, assessment of NSS become timely and more accurate, laying the foundation for rapid decision-making. NSSA provides the unique high level security view based upon the security alert events. But the complexities and diversities of security alert data on modern networks make such analysis extremely difficult. The research of NSSA is very important because it can improve the network monitoring abilities, tragedy response capacity and predict the development trend of NS. Based on the concept model of SA, This research expound on the situational awareness of the 3 main research information, extraction the factors of NS situational awareness, situation understanding and situation prediction. The focus on the core problem each stage needs to be solved, main algorithm and advantages and disadvantages of these algorithm. The implementation of the development trends of the related theory and application in different stages are analyzed and prospected.

IV. EXPECTED OUTCOME

The Situation Awareness (SA) pays attention to the information transform technology between the abstract data and the information understood by person. It has 3 levels to transform the data to the awareness: perception, comprehension and prediction. Its application in NS is called NSA. Traditional network security devices such as firewalls, security scanners and intrusion detection system [8] work independently and they cannot offer threat evaluation of attacks which make a challenge to administrators to understand how serious of an attack is. This lack of information results innumerous ambiguities

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

when interpreting alerts and making decisions on appropriate responses.

V. CONCLUSION

To address this problem, we propose a time and space based alert analysis technique which can correlate related alerts without background knowledge and offer attack graph to help the administrator understand the attack steps evidently and skillfully. A threat appraisal is given to find the most hazardous attack [3]; this method additional saves administrator's time and energy in processing large amount alerts. We propose routinely correlate the alerts to generate simple attack graphs based on time and space constraint. We propose attentive analysis method to correlate related alerts and offer simple attack graph. We give an attack assessment function for potential threats [4] (either from attacks or on devices). These projected methods, administrators can understand the network situation and learn how serious of an attack without checking individual alerts or assessment values. NS awareness just wants to know where, when and how severe of an attack is, we need a diminutive subset of understanding fields. Using small alert message also saves time and storage space.

VI. FUTURE WORK

Based on this work anybody can implement network security situational awareness algorithms and countenance challenges in network security situational awareness and improve effectiveness in network security situational awareness. This work may focus on how you can face new challenges in network security environment.

ACKNOWLEDGEMENT

1) The work of chintada srinivasarao and j uday Kumar are partially supported by AITAM college TEQIP grants. The work of chintada srinivasararo and j uday kumar are partially supported by AITAM management and Department of IT grants..

2) The authors would like to thank Wei Yong, Lian Yifeng, and Feng Dengguo (Department of Electronic Engineering and Information Science, University of Science and Technology of China, Fang Lan, Wang Chunlei, and MaGuoqing, Juan Wang, Feng-li Zhang, Jing Jin,Wei Chen, Cyril Onwubiko, Liu Mixi, Yu Dongmei and Zhang Qiuyu et aI, Wang Huiqiang, Lai Jibao, and Ying Liang, Mr. Marc Grégoire, Yu Dong and Frincke, D, J Hall, J Pei, Y Yin., Bass. T, Jia Han, Micheline Kamber, Mika Klemettinen

REFERENCES

[1] Wei Yong, Lian Yifeng, and Feng Dengguo (Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027)(State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190).

[2] Fang Lan, Wang Chunlei, and MaGuoqing, "A Framework for Network Security Situation Awareness Based on Knowledge Discovery" 2010 2nd International Conference on Computer Engineering and Technology 2010 IEEE.

[3] Juan Wang,Feng-li Zhang,Jing Jin,Wei Chen, "Alert Analysis and Threat Evaluation in Network Situation Awareness" 2010 IEEE

[4] Cyril Onwubiko, "Functional Requirements of Situational Awareness in Computer Network Security" 2009 IEEE.

[5] Liu Mixi, Yu Dongmei and Zhang Qiuyu et aI., "Network Security Situation Assessment Based on Data Fusion, " 2008 Workshop on Knowledge Discovery and Data Mining, 2008.

[6] Wang Huiqiang, Lai Jibao, and Ying Liang, "Network Security Situation Awareness Based on Heterogeneous Multi-Sensor Data Fusion and Neural Network," Second International Multisymposium on Computer and Computational Sciences, 2007 IEEE.

[7] Mr. Marc Grégoire ,"Visualization for Network Situational Awareness in Computer Network Defence" (2005). In Visualisation and the Common Operational Picture (pp. 20-1– 20-6). Meeting Proceedings RTO MP-IST-043, Paper 20. Neuilly-sur-Seine, France: RTO. Avalable from:http://www.rto.nato.int/abstracts.asp

[8] Yu Dong and Frincke, D., "Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory, " 43rd ACM Southeast Conference, March 18-20, 2005.

[9] J Hall, J Pei, Y Yin. Mining frequent patterns without candidate generation. 2000ACM. SIGMOD int'I Conf on Management of Data (SIGMOD'OO), DallaS, TX,2000

[10] Bass, T., "Intrusion Detection Systems and Multisensor Data Fusion, Communications of the ACM, Vol. 43, No. 4, April 2000.

[11] Jia Han, Micheline Kamber., "Data Mining concepts and techniques", second edition 2006, Elsevier Inc.

[12] Mika Klemettinen, A Knowledge Discovery Methodology for Telecommunication Network Alarm Databases. Report A-1999-1 (PhD Thesis), University of Helsinki, Department of Computer Science, January 1999. See electronic version at http://www.cs.helsinki.fi/u/mklemett/THESIS/,especially pages 27-49

AUTHOR BIOGRAPHY

CHINTADA SRINIVASARAO received B. Tech degree from SISTAM (JNTU, Hyderabad, India). He was received M. Tech degree in Computer Science & Engineering from Nova College of engineering (JNTU, Kakinada). His area of interests includes Network Security, Image Processing, Data Mining cloud computing.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

J UDAY KUMAR received B. Tech degree from SISTAM (JNTU, Hyderabad, India). He was received M. Tech degree in Computer Science & Engineering from AIET college of engineering (JNTU, Kakinada). His area of interests includes mobile computing Network Security, Image Processing, Data Mining cloud computing.