The Classification, Design and Placement of Security Sensor for Network Security Situational Awareness System

Wang Hui-qiang, Lai Ji-bao, Liang Ying, Liu Xiao-wu
College of Computer Science & Technology, Harbin Engineering University, Harbin, 150001, China
wanghuiqiang@hrbeu.edu.cn; laijibao@hrbeu.edu.cn; redleaf@hrbeu.edu.cn

Abstract

Network Security Situational Awareness System (NSSAS) is one of the hotspots in information security domain. In order to solve the problem of NSSAS security situation information acquisition, it is highly necessary to study security sensors. On the basis of knowing the information requirement of NSSAS, we put forward a kind of classification method of security sensors, design a general architecture of security sensor, point out some key technologies related to implementing security sensors, give some placement policies, and discuss the management architecture and methods of security sensors finally.

1. Introduction

At present, computer network is developing towards a direction of large-scale and highly distributed, while intrusion attack behaviors are also becoming more and more complicated. For the existing network security devices, such as Intrusion Detection system (IDS) and Firewall, they only collect and process some security data, and can not monitor the global network security situation. In this case, the research on NSSAS gradually becomes more and more important. Situational awareness is derived from Human Factors in aerospace aviation[1]. And it is widely used in the domains of aerospace aviations, military battlefields, nuclear reactor control and air traffic control. In a dynamic and complex environment, decision-makers are eager to have a situational awareness tool that can display consistent changes of environments and supply knowledge for reasonable and precise decisions.

With the wide applications of network, threats and losses made by network viruses and attacks are bigger and bigger. In 1999, Tim Bass et al[2] first proposed the concept of network situational awareness, which is also called network security situational awareness, compared network situational awareness with Air Traffic Control (ATC) situational awareness, and tried to make use of these mature theories and technologies in ATC to the field of network security situational awareness. Meanwhile, he also gave a network security situation awareness model based on multi-sensor data fusion. Jason Shifflet[3] adopted ontology theory to analyze the related concepts of network security situational awareness, and proposed a technique independent fusion model. H.Q. Wang et al[4] gave the definition of network security situational awareness, put forward the architecture of NSSAS, discussed the key technologies and difficulties related to building NSSAS prototype, and described the future development of NSSAS. At the same time, many institutions also began to develop the corresponding network security situation awareness system tools. Lawrence Berkeley National Labs developed a system called “The Spinning cube of potential doom”[5] in 2003. This system used dots to present network traffic information in 3D spaces by which it had better network security situational awareness capabilities than the former tools. In 2005, SILK[6] was developed by CERT/NetSA (Network Situation Awareness) under the lead of CMU/SEI, which could monitor a large-scale network security situation in time, recognize and defend intrusions and attacks, response and early warn potential and malicious network behaviors before they are out of control, and supply appropriate suggestions. NCSA/SIFT (Security Incident Fusion Tools Research Project) was developing an integrated framework of security event fusion tool that made the Internet security visualization. Up to now, some tools for the Internet security situational awareness have been developed by SIFT, such as NVisionIP[7] and VisFlowConnect-IP[8] etc.

Mastering the situation of NSSAS lays the foundation for studying security sensor. Security sensor in cyberspace is different from sensor in nature space, like radar and infrared equipment, here is software or hardware that could offer security situation information. Figure 1 gives the position of security sensor in NSSAS. Security sensor is considered as the hardware base of NSSAS, which missions are to monitor and collect all kinds of security situation data from network, system software, service and other applications, to discover network attack behaviors or other abnormal behaviors,

978-0-7695-3112-0/08 $25.00 © 2008 IEEE
DOI 10.1109/ICICSE.2008.62

and to support network security situational awareness in a large-scale network environment.

The remainder of the paper is organized as follows. In section 2, the information requirement of NSSAS is given. In section 3, a kind of classification method of security sensors is put forward. After that, we propose a general architecture of security sensors in section 4, introduce some placement polices related to security sensors in section 5 and discuss the management methods of security sensors in section 6 respectively. The last section draws a conclusion.

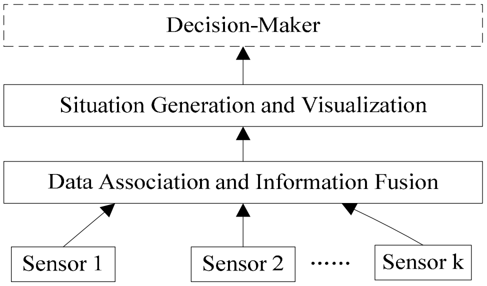
Decision-Maker
Situation Generation and Visualization
Data Association and Information Fusion
Sensor 1
Sensor 2
······
Sensor k

Figure 1. **Position of security sensor in NSSAS**

2. System Information Requirement

The information requirement of NSSAS is the premise for studying security sensor, so it must be clear. When we analyze the information requirement, we should consider the following factors: ①the information type needs to be comprehensive, which can demonstrate the multi-view and multi-scale network security situation; ②the traffic of information must be in control, namely that we can use as little as possible information to reflect the network security situation in time; ③ the complexity of information acquisition must be considered.

Based on the above principles and the functional requirement of NSSAS, we know that NSSAS requires the information as following: ①log data of critical host and system software; ②log data and statistical data of network exchange equipment, like Switch and Router; ③ log data and alarm data of security equipment, for example IDS and Firewall; ④ network management information; ⑤ the security situation of all kinds of services, including service deviation and service invalidation; ⑥other network data.

3. Classification of Security Sensors

Nowadays, there are many different security sensors that mainly classified into four categories in Figure 2.

- According to the level of objects collected by sensors, including network sensor, service sensor, system software sensor and all kinds of application sensors.
- According to the property of objects provided by sensors, including log-oriented sensor, sensor based on flow, sensor based on Agent and other sensors.
- According to the function of sensors, including Firewall, Intrusion Detection System, Virus Detection System and other special systems.
- According to the mode of sensor placement, including sensor based on host and sensor based on network.

In the above classification, each kind of sensor may have some identical character. For the existing security sensor, like IDS and Firewall, we focus on solving the reuse of alarm information and implement the corresponding data collector, for example the acquisition of IDS alarm information. But for the sake of monitoring and collecting security situation data of some software and service, we must design and implement the corresponding sensors.

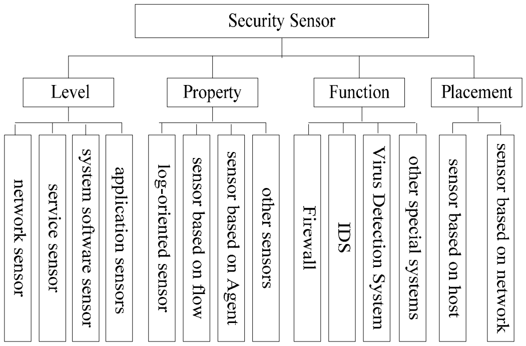

Figure 2. **The classification of security sensor**

4. Security Sensor Design

In order to meet the information demand of NSSAS, we choose some existing security sensors that are used to collect some security situation data, and design the corresponding new security sensors that are used to monitor and to collect security situation data of some software and some service. The new security sensors mainly have the following five functions:

- Be able to collect security situation data of network, service and other applications.
- Be able to implement data filter, data reduction and data format standardization, etc.
- Be able to discover network attack events and the suspicious events preliminarily.
- Be able to load event analysis method and alarm method dynamically.
- Be able to submit detection results to the console and receive the commands from the console.

Figure 3 gives a general architecture of new security sensor which consists of detection component and communication component. The detection component which is one of core components consists of collect engine, analyze engine and alarm engine. The collect engine captures the original data from the network directly, and then supplies the format data to the analyze engine. After the analyze engine receives the format data, it will start the relevant detection model to discover the abnormal event, and the alarm engine makes the alarm to remind administrators to take actions in time. The communication component carries out the interaction between security sensor and upper application, namely that it will send the alarm information of security sensor to the console and receive the command from the console. In order to ensure the secure and reliable communication between security sensor and upper application, all communication data must be transferred by encryption. Now the common encryption methods have the Secure Socket Layer Protocol and RSA algorithm, etc.

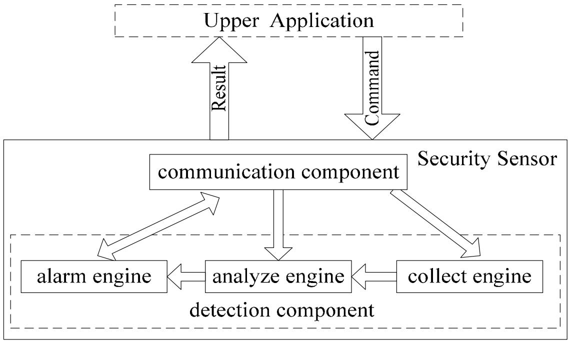

Figure 3. **An architecture of security sensor**

Some key technologies related to implement security sensor must be solved, mainly including high speed network data acquisition technology, network security situation data real time process technology, unified model of security sensor situation information and communication protocol between security sensor and upper application.

5. Security Sensor Placement

The reasonable and effective sensor placement is very important for network security situational awareness system, so we must take into account the following factors comprehensively. ① network topology architecture; ②network entry point, including Internet entry point, Ethernet entry point, Intranet entry point and remote access entry point; ③critical network components, including server, like DNS server and DHCP server, etc, network infrastructure, like Switch and Router, etc, secure components, like IDS and Firewall, etc; ④remote network; ⑤network size and network complexity; ⑥the policy coordination among different secure components in the network.

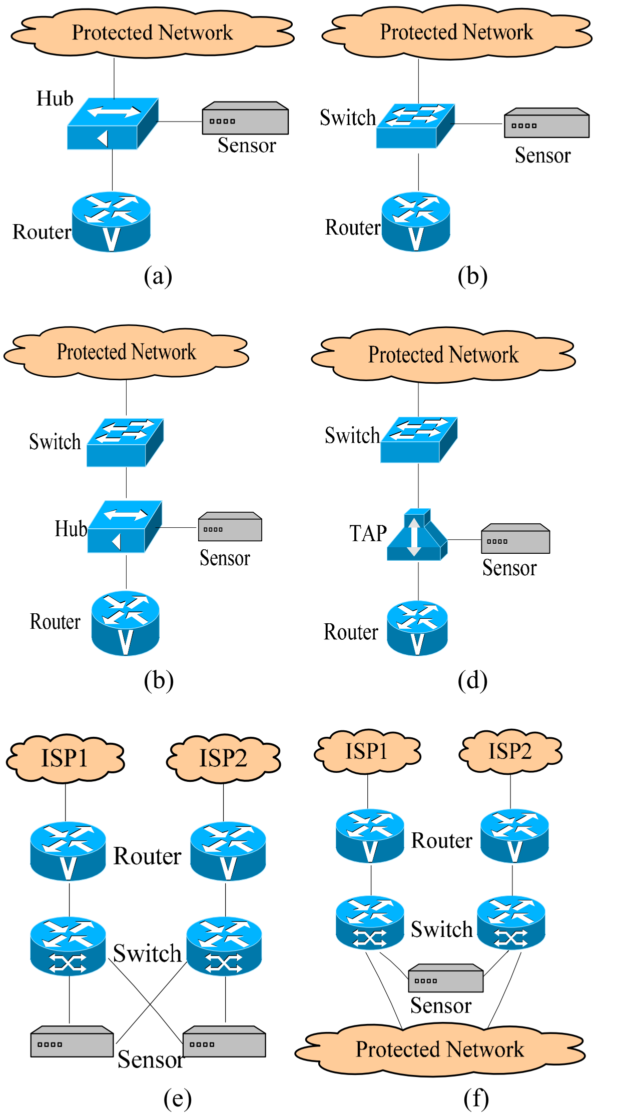

Figure 4. **(a) Sensor placement in shared network; (b) ~ (f) Sensor placement in switch network**

In fact, we use different security sensor placement policies in a different network environment. But to sum up, there are mainly two categories that one is security sensor placement policy in a shared network environment shown in Figure 4 (a) and the other one is sensor placement policy in a switched network environment shown in Figure 4 (b)~(f). In Figure 4 (a), the observing-port of sensor is in promiscuous mode, so it can monitor the communication content among all network equipments. But in Figure 4 (c), the Hub between Switch and Router would convert switched network environment to shared network environment. By this way, we can place the sensor easily with the low cost. In Figure 4 (b), Switch port mirroring is the premise of placement policy. We can place security sensors without changing the existing network topology architecture and interrupting the network simply and conveniently. However, if the Switch doesn't support the port mirroring, or the function will turn off because of the performance requirement. We are able to use the policy in Figure 4 (d) to place security sensors in full-duplex 100Mbps or 1000Mbps mode. In Figure 4 (e), the placement policy of security sensor can avoids the fail of security sensor and the fail of link, and ensures network unblocked effectively. In Figure 4 (f), the security sensor is able to merge the traffic information among different network cards, and then analyzes and judges the network security situation.

On the basis of knowing the network environment and the placement policy, we place the corresponding security sensor by the actual requirement of network security situational awareness system.

6. Security Sensor Management

In order to manage and coordinate the resources of security sensor well, it is very necessary to strengthen security sensor management to improve data acquisition and the process of awareness. In fact, security sensor management is a system or a process that can control a group of sensors automatically. Now there are mainly two management architectures. One is central management architecture, and the other is distributed management architecture. In a large-scale network environment, network security situational awareness system generally adopts the distributed management architecture that could enhance the processing efficiency enormously.

Sensor management is a cross-discipline research domain, including mathematical programming, computer science, expert system and artificial neural network, etc[9]. The common methods mainly have sensor management based on mathematical programming and optimizing technology, sensor management based on fuzzy reasoning and neural network, and sensor management based on expert system[10].

7. Conclusion

It is highly necessary to study security sensors for solving the problem of NSSAS security situation information acquisition. The paper discussed and solved the problem of security sensor classification, design, placement and management preliminarily. Along with going deep into researching, many problems must be further resolved.

8. References

[1] M.R. Endsley, *Situation awareness in aviation systems*, In Garland D J, Wise J A, Hopkin V D.: Handbook of aviation human factors, Mahwah, NJ Erlbaum, 1999, pp.257–276.

[2] T. Bass, Intrusion Detection Systems and Multi-sensor Data Fusion: Creating Cyberspace Situational Awareness, *Communications of the ACM*, USA, 2000, Vol.43, pp.99-105.

[3] J. Shifflet, A Technique Independent Fusion Model For Network Intrusion Detection, Proceedings of the Midstates Conference on Undergraduate Research in Computer Science and Mathematics, Wooster, 2005, Vol.3, pp.13–19.

[4] H.Q. Wang, J.B. Lai, L. Zhu (ed.), Survey of Network Situation Awareness System, *Computer Science*, ChongQing, China, 2006, Vol.33, pp.5-10.

[5] S. Lau, The spinning cube of potential doom, *Communications of the ACM*, USA, 2004, pp.25-26.

[6] C. Gates, M. Collins, M. Duggan (eds.), More Netflow tools: for performance and security, In Proceedings of the 18th Large Installation Systems Administration Conference. Atlanta, Georgia, 2004, pp.121-132.

[7] R. Bearavolu, K. Lakkaraju, W. Yurcik, NVisionIP: An Animated State Analysis Tool for Visualizing NetFlows, FLOCON Network Flow Analysis Workshop (Network Flow Analysis for Security Situational Awareness), Pittsburgh, Pennsylvania, 2005.

[8] X.X. Yin, W. Yurcik, A. Slagell, The Design of VisFlowConnect-IP: a Link Analysis System for IP Security Situational Awareness, The third IEEE International Workshop on Information Assurance (IWIA). Maryland, USA, 2005, pp.141-153.

[9] S. Blackman, R. Popoli, *Design and Analysis of Modern Tracking Systems*, Boston London, Artech House, 1999, pp.967-1065.

[10] X.X. Liu, S.L. Shen, Q. Pan, A Survey of Sensor Management and Methods, *Acta Electronica Sinica*, Beijing, China, 2002, Vol.30, 394-398.