UNIVERSITI PUTRA MALAYSIA

NETWORK SECURITY SITUATION AWARENESS BASED ON INDICATORS EXTRACTED

XIE ZEQIANG

FSKTM 2017 19

Project paper submitted to Faculty of Computer Science and Information Technology, University Putra Malaysia in partial of the requirements for the degree of Master of Computer Science

Network Security Situation Awareness Based On Indicators Extracted

By

Xie Zeqiang

2016

Supervisor : Dr. Kweh Yeah Lun

Faculty : Faculty of Computer Science And Information Technology

Abstract of project paper submitted to Faculty of Computer Science and Information Technology, University Putra Malaysia in partial of the requirements for the degree of Master of Computer Science

Network Security Situation Awareness Based On Indicators Extracted

By

Xie Zeqiang

December 2016

Supervisor : Dr. Kweh Yeah Lun

Faculty : Faculty of Computer Science And Information Technology

Situation awareness refers to collect, process, and extract a variety of factors which can affect network situation awareness in the network environments, then build index system, establish evaluation model to assess the current network security situation awareness index and predict the future trend from the macro.

Based on studying the predecessors' research works, the article regard the security events and network node resource information as the source of extracting index and construct a tree index system, combining with this system, it proposes a hierarchical network security situation assessment model, used fuzzy analytic hierarchy process (FAHP) to solve the problem of weight calculation among the model, designed Index calculation method for calculating network security situation index. Finally, it gives the design and implementation of a network security situation analysis prototype system.

Keywords: Situation awareness, Network security situation, Hierarchical network security situation assessment model

ACKNOWLEDGEMENTS

I want to express my gratitude to all those who helped me during the process of the writing this project.

I am really grateful to my supervisor Dr. Kweh Yeah Lun who gave me valuable advice in academic research. In the preparatory period of the project, he spent a lot of time to read report, gave me suggestions about my proposal and provided me with inspiring advice. Without his patient guidance, insightful criticism and expert guidance, the completion of this project is impossible.

I am also particularly grateful to all the professors in the faculty for their suggestion and to help me better prepare for the project.

Finally, I should express my gratitude to my parents and friends who have always been helping me out of difficulties and uncomplaining support me.

APPROVAL

This project report is submitted to the Department of Professional Development And Continuing Education, Faculty of Educational Studies, University Putra Malaysia, and has been accepted as partial fulfillment of the requirement for the degree of Master of Human Resource Development. The members of the Examination Committee are as follows:

Supervisor:

--

Date:

--

Faculty of Computer Science And Information Technology

University Putra Malaysia

Examiner:

--

Date:

--

Faculty of Computer Science And Information Technology

University Putra Malaysia

DECLARATION

I hereby declare that the project report is my original work except for quotations and citations, which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at University Putra Malaysia or at any other institution.

XIE ZEQIANG
GS43899

Date:

CONTENT

ABSTRACT.....I
ACKNOWLEDGEMENTS.....III
APPROVAL.....IV
DECLARATION.....V
CHAPTER ONE.....1
INTRODUCTION.....1
1.1 Background of the study.....1
1.2 Statement of the Problem.....2
1.3 Objectives of the Study.....3
1.4 Significance of the Study.....3
1.5 Organizational structure of the paper.....4
CHAPTER TWO.....6
REVIEW OF LITERATURE.....6
2.1 Introduction.....6
2.2 The Concept of Situation Awareness and Classical Model.....6
2.2.1 JDL model.....7
2.2.2 Endsley Conceptual model.....8
2.2.3 Tim Bass Functional model.....9
2.3 Network Security Situation Awareness Related Technologies.....11
2.3.1 Event correlation analysis.....12
2.3.2 Index Extraction and Construction of Index System.....15
2.3.3 Index Extraction and Construction of Index System.....21
2.4 Chapter summary.....29
CHAPTER THREE.....30
Research on Index System of Network Security Situation Index Extraction and Construction.....30
3.1 Network security situational awareness of the work process.....30
3.2 Extraction index and construction index system.....33

3.2.1 Working dimension index....36
3.2.2 Vulnerability dimension index.... 38
3.2.3 Risk dimension index....40
3.2.4 Threat dimension index....41
3.3 Chapter summary.... 43
CHAPTER FOUR....44
Research on Evaluation Model of Network Security Situation.... 44
4.1 Network security situation assessment architecture model....44
4.2 Hierarchical Security Situation Assessment Modeling.... 45
4.2.1 Network Security Model.... 45
4.2.2 Hierarchical Security Situation Assessment Model.... 46
4.3 Weight calculation....49
4.4 Calculation of Safety Situation Value.... 54
4.4.1 Evaluate target layer situation calculations....54
4.4.2 Evaluate the target layer situation calculation....54
4.5 Chapter summary.... 58
CHAPTER FIVE....59
Design and Implementation of Network Security Situation Analysis Prototype System 59
5.1 Prototype system design ideas....59
5.1.1 The overall structure of the system.... 59
5.1.2 System Workflow.... 62
5.1.3 Evaluation Model Design....65
5.1.4 Database table design.... 72
5.2 Prototype system implementation.... 75
5.2.1 System implementation platform and environment.... 75
5.2.2 System Architecture and Implementation.... 76
5.2.3 The realization of the situation and display....79
5.3 Result analysis....80
5.4 Chapter summary.... 83

CHAPTER SIX.. 85

SUMMARY.. 85

REFERENCE.. 87

CHAPTER ONE

INTRODUCTION

This introductory chapter provides an overview of the research. The first two parts are the background of the study and statement of the problem that show the explanation of the research and the reasons for doing this study. The third part is the objectives which include the main objective and the specific objectives. It follows by the highlight of the significance of the research. The assumption is briefly presented after the introduction of the significance. The last two parts are the limitations and the definitions of terms, respectively.

1.1 Background of the study

With the rapid development of Internet technology, more and more network services arises increasingly, Internet plays an important role in social development so that it is necessary to maintain the safe operation of the network, in order to deal with this problem, a variety of safety equipment have been introduced, such as firewalls, vulnerability scanning, etc. Initially, these safety equipment can solve the specific issues, but with more types of devices, resulting in more reported incidents, which not only increases the workload of the security administrator, but makes it difficult to control network security situation overall so as to make decisions on time to maintain network security to because lack of interaction between different safety devices. Therefore, network security situation awareness has become increasingly popular perception of the current research.

Situation awareness refers to collect, process, and extract a variety of factors which can affect network situation awareness in the network environments, then build index system, establish evaluation model to assess the current network security situation awareness index and predict the future trend from the macro.

Based on studying the predecessors' research works, the article regard the security events and network node resource information as the source of extracting index and construct a tree index system, combining with this system, it proposes a hierarchical network security situation assessment model, used fuzzy analytic hierarchy process (FAHP) to solve the problem of weight calculation among the model, designed Index calculation method for calculating network security situation index. Finally, it gives the design and implementation of a network security situation analysis prototype system.

1.2 Statement of the Problem

Different devices put into use in order to settle the specific safety issues in the Internet, at beginning, it performed well, however, with the increasing complexity of network structure, more security devices are needed , which lead to two new problems during the maintenance of network security:

1. Many of devices only can resolve the certain problem in one aspect, there is little interaction between different device, which result in safety isolated island and can not reflect the overall situation to help the Internet administrator to make a timely and effective decision during the maintenance of Internet security.

2. Many devices report the information to security administrator so rapidly that the administrator gets large amounts of data, with different event format and so much misdescription and re-description, all of these will bring a huge pressure to Internet management system.

In order to deal with these two problems, this article proposes the topic of technology research based on indicators extracted network security situation awareness, the aim is to conduct a systematical analysis for the heterogeneous data and its overall performance information reported by security devices, extracting index, building index system, creating assessment model to calculate Internet security index to make sure that Internet administrator can understand the situation from the macro and provide basis for making a decision timely and effectively to guarantee the safe operation of Internet.

1.3 Objectives of the Study

1. Collecting, processing, extracting more factors within a wider range of Internet that have an impact on network security situation, constructing a comprehensive indicator system with more safety information more comprehensive index system with more security information so that embodies situation awareness can reflect network security situation from the overall perspective.

2. Conduct a in-depth research for situation assessment model and algorithm to make sure that mathematical theory analysis are included , so that the results of the assessment are more convictive and scientific.

3. Conduct a research on situation forecasting and visualization techniques. Predict the future trend of the situation through a predictive model based on the calculated result of situation assessment to facilitate the future security threats warning for security administrator, and complete the whole process of situation awareness. At the same time, the results of the various stages of situation awareness can be presented to security administrator friendly to make them understand the information of situation efficiently and make decision timely.

1.4 Significance of the Study

In this paper, we present a research topic of network security situation awareness technology based on index extraction. The purpose of this paper is to analyze the heterogeneous data and its performance information get Security situation index, so that network managers can understand the situation from the macro-network security and network security to ensure timely operation of decision-making basis.

In order to provide the basis for the network security administrator to make decisions in time to ensure the safe operation of the network, this paper focuses on the problems encountered in network security research, such as the isolation of security devices, the escalation of security information, the isomerize, With theoretical research and practical application of the dual value.

1.5 Organizational structure of the paper

The content of the thesis is divided into six chapters. The main points of each chapter are discussed as follows:

Chapter One:The research background and significance of this paper are introduced, the results of research on situational awareness at home and abroad are analyzed, and the content of the research in the future is clarified. Finally, the basic content and innovation of the thesis are discussed and chapter arrangement.

Chapter Two:At the beginning of this chapter, discuss the process of proposing situational awareness and describe the descriptive concept of situational awareness. And then through the study of three classic framework models of foreign situational awareness,understand the characteristics of each framework. Then, the paper discusses and compares the research results of the previous researches on incident correlation analysis, index extraction and index system construction, and situation assessment method in network security situational awareness.

Chapter Three:Mainly on index extraction and construction of the situation index system has been studied. First of all, through the study and research of relevant literatures domestic and overseas, the whole process of situational awareness is given, and the position and importance of the index system and situation assessment in network security situational awareness are clarified; the methods of constructing index system are compared with previous research workers Finally, combining the structure of the network system and the data source of the safety assessment, the situation evaluation of the paper is established on the operational status, the fragile dimension, the risk dimension and the threat dimension of the network, and then, Index system.

Chapter Four:Mainly discusses the establishment process of the network security situation assessment model based on fuzzy analytic hierarchy process (AHP). Based on the results of the previous chapter, builds up the situation assessment model based on the network architecture and relevant theories of fuzzy analytic hierarchy process. Fuzzy mathematics and fuzzy analytic hierarchy process (AHP) are combined to solve the problems of weight calculation, index quantification and situation calculation.

Chapter Five:The NSSAS prototype system is designed and implemented. The overall structure and work flow of the NSSAS system are given. The evaluation model and the evaluation model are designed. The situation evaluation of the prototype system is given, and the evaluation result is reasonable of the experimental verification.

Chapter Six:Summary and Prospect. Summarizes the research work done in this paper, discusses the achievements of this research work, and points out the areas to be improved and the direction of future research.

REFERENCE

[1] ENDSLEY MR.Design and evaluation for situation awareness enhancement[A]//Proceeding of the 32nd Human Factors Annual Meeting[C].Santa Monica:Human Factors and Ergonomics Society,1988:97-101.

[2] Bass T.Intrusion detection systems & multisensor data fusion,Creating Cyberspace Situational Awareness[J].Communication of the ACM,2000,43(4):99-105.

[3] D'Ambrosio B.Security situation assessment and response evaluation (SSARE)DISCEX'01[A]//.Proceedings:DARPA Information Survivability Conference & Expossition II.Los Alamitos[C]:IEEE Computer Socity,2001:387-394.

[4] Yegneswaran V,Barford P,Paxson V.Using Honeynets for Internet situational awareness [C/OL]//Proc of ACM/USENIX Hotnets IV.2005[2008-01-12].

[5] Srihari R K. Situation awareness through concept-based information extraction[EB/OL].(2012-05-20)

[6] Stephen L.The spinning cube of potential doom [j] communication of the ACM,2004,47(6):25-26Srihari R K. Situation awareness through concept-based information extraction[EB/OL].(2012-05-20)

[7] Stephen L.The spinning cube of potential doom [j] communication of the ACM,2004,47(6):25-26

[8] Yong, Z., Xiaobin, T., & Hongsheng, X. (2007, December). A novel approach to network security situation awareness based on multi-perspective analysis. In Computational Intelligence and Security, 2007 International Conference on (pp. 768-772). IEEE.

[9]Jibao L, Huiqiang W, Liang Z. Study of network security situation awareness mode l based on simple additive weight and grey theory[C]//2006 International Conference on Computational Intelligence and Security. IEEE, 2006, 2: 1545-1548.

[10]JAKALAN A. Network security situational awareness[J]. Interna-tional Journal o f Computer Science and Communication Security, 2013, 3: 61-67.