Analysing Various Alerts & Evaluating Threat Techniques In NSA

Prof.TambeShital B.,Prof. Sonkar S.K.

.

Abstract-A Network is a connection of many devices, where each node (device) is said to have wired or wireless connection between them. And now a day's most of the threat comes to the network by either from outside or from a sort of situation which arises internally due to many reasons.So the Intrusions or threat which arises due to these situations are generally more damageable than the normal ones. So in this paper it is giving a technique to analyze various types of alerts & also generating attack graph for such alerts. By using algorithms like **Correlation Of IsolatedAlerts to Alert–Pair, Attack Graph Generation.** And after analyzing the threat we are also performing evaluation technique to find the seriousness of the threat. In this paper we mainly focus on alert analysis.It is well-known that current Intrusion Detection Systems produce large volumes of alerts. These overwhelming alerts make it challenging to understand and manage them. Therefore we have to reduce the amount of the alerts and external useful information from them. However, the NSA requires the alert analysis techniques to offer high-level information such as how serious of attacks are and how dangerous of devices are and which attacks or devices need administrator to pay attention to. 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 clearly and efficiently. And a threat evaluation is given to find the most dangerous attack, which further saves administrator's time and energy in processing large amount alerts.

Index Terms-IDS, Alerts, Threats, Security, Algorithms etc.

1 INTRODUCTION

1.1 Fundamental Overview

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 Network Security situation becomes malicious and complete vulnerable and they may raise false Network Security situation awareness. To solve these kinds of problems we use Knowledge based Discovery to develop an enriched Framework.

Network security situation awareness 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 network security situation and the generation of network security situation. The purpose of modeling is to construct the formal model of network security situation 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 network security situation 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 network security situation, and finally to automatically generate the network security situation 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. Application of the integrated Network Security Situation Awareness system (Net-SSA) shows that the proposed system supports for the accurate modeling and effective generation of network security situation.

1.2 How The Existing Problem Works?

Traditional network security devices such as Intrusion Detection Systems (IDS), firewalls, and security scanners operate independently of one another, with virtually no knowledge of the network assets they are defending. This lack of information results in numerous ambiguities when interpreting alerts and making decisions on adequate responses. The general process is to perceive the network security events happened in a certain time period and cyberspace environment, synthetically manipulate the security data, analyze the attack behaviors systems suffered, provide the global view of network security, and assess the whole security situation and predict the future security trends of the network.

1.3 Our Approach To The Existing Problem

The Situation Awareness (SA) pays attention to the information transform technology between the abstract data and the knowledge understood by person. It has three levels to transform the data to the knowledge: perception, comprehension and prediction. Its application in network security is called Network Situation Awareness (NSA).Traditional network security devices such as Intrusion Detection Systems (IDS), firewalls, and security scanners 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 in numerous ambiguities when interpreting alerts and making decisions on appropriate responses. 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 clearly and efficiently. And a threat evaluation is given to find the most dangerous attack, which further saves administrator's time and energy in processing large amount alerts. We propose our own approach to automatically correlate the alerts to generate simple attack graphs based on time and space restriction. In addition, we give an attack evaluation method. We first propose our own alert analysis method to correlate related alerts and offer simple attack graph. Then, we give an evaluation function for possible threats (either from attacks or on devices). Via these proposed methods, administrators can understand the network situation and learn how serious of an attack without checking individual alerts or evaluation values. Here NSA just wants to know where, when and how serious of an attack is, so we only need a small subset of alert fields. Using short alert message also saves time and storage space.

Algorithm 1 shows the method of correlating two isolated alerts to an alert-pair.

Algorithm 1: Correlation of Isolated Alerts to Alert-Pair:

INPUT: individual hyper-alerts a1,a2……an

OUTPUT: set of alert-pairs (ai,aj).denoted APs.

Let TW be the time-window which is set by administrators.

Let HyperAlert be the hyper-alert table.

Let AlertPairs be the alert-pairs table.

1. for all the hyper-alerts in HyperAlert do

2. if Srcip(ai) = Srcip(aj) and Dstip(ai) = Dstip(aj) and

Time(ai) <Time(aj) and Time(aj) – Time(ai) < TW

Then

3. put (ai,aj) into Alert-Pairs.

4. if Dstip(ai) = Srcip(aj) and Time(ai) < Time(aj) and

Time(aj) – Time(ai) < TW Then

5. Put (ai,aj) into Alert-Pairs.

Then, we correlate these alert-pairs to an attack graph as Algorithm 2.

Algorithm 2 : Attack Graph Generation:

INPUT: set of alert-pair (ai,aj) - APs.

OUTPUT: attack graph G(N,E)

Put every hyper-alert ai of APs into node set N;

Put every alert-pair (ai,aj) of APs into edge set E;

1. for every edge(ni,nj) do

2. if there is a indirect path ni,…..,nk,….nj then

3. remove the edge (ni, nj) from edge set E

4. return G(N,E)

1.4 System Architecture Of The Project

Following Fig. shows the network/system architecture of the project:

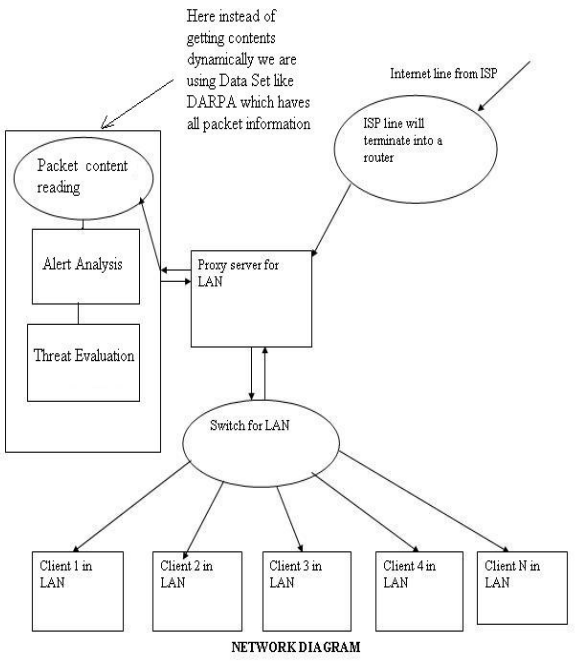


Fig.1: Network/System Diagram

1.5 Problem Definition

The objective of project is to design a system that will:

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

The aim of this project is to develop a network security situation awareness system which will fuse and analyze security alert events collected from security situation sensors and generate the network security situation by extracting 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 network security situation and finally to automatically generate the network security situation graph.

2 SOFTWARE REQUIREMENT SPECIFICATION

2.1 Introduction

Software Requirement Specification states the goals and objectives of the software, describing it in the context of the computer based system. The Software Requirement Specification is produced at the culmination of the analysistask. The function and performance allocated to software as part of system engineering are refined by establishing a complete information description, a detailed functional description, a representation of the system behavior, an indication of performance requirements and design constraints and other information pertinent to requirements.

2.2 Project Scope

The first software project management activity is the determination of software scope. Scope is defined by answering the following questions:

- Context :

How does the software to be built fit into a larger system, product, or business context and what constraints are imposed as result of the context?

- Information objectives:

What user-visible data objects are produced as output from the software? What data objects are required for input?

- Function and performance:

What function does the software perform to transform input data into output? Are any special performance characteristics to be addressed?

The following points describe the scope of Network Security Situation Awareness System:

- Provide Situation awareness

The NSSA system can effectively provide situation awareness which is one of the solutions to current security problems.

- Detect Network Attacks

Alert events are generated by various network security situation sensors and resulted from network intrusions or from themonitored parameters exceeds the threshold value.

- Decrease the false positive and false negative alarm ratesIt uses heterogeneous sensor event fusion techniques to reduce false alert rates and improve the confidence level of event detection.
- Security Situation Visualization by the Administrator

It provides the dynamic generation of network security situation graph that helps the administrator to take decisions.

2.3 Operating Environment

HardWare Specification

For Development we need a machine of following configuration:

- CPU --------→ 2.9 GHz (C2D)
- RAM -------→ DDR 1 GB
- HDD ------→ 100 GB
- Motherboard --------→ Intel 945 GLX
- Monitor, Key Board, Mouse, UPS, DVD Writer etc.

Software Specification

- Coding Language ---------→ Java.
- Development Kit ---------→ JDK 1.6, JRE 6.
- Front End ----------→ Java Swings
- Development IDE-→Netbeans 6.9.1
- Database ---------→ My SQL 5.0
- Protocols ----------→ Java networking
- External Softwares---→Snort
- External Jar ----------→ jxl.jar, sql.jar,jpcap.jar
- Operating System--------→ Windows xp,Windows 7

2.4 Design and Implementation Constraints (OOD) Mathematical Model

NSSA system uses the Mathematical Model described as follows:

Set Theory Of Project:-

1. PACKET DATASET READER:

Set P:

P0= Get Excel Datasets

P1=Read Rows And Columns

P2=Allocation in Queue

2. ALERT OBJECT CREATOR:

Set C:

C0=Get Data Packet

C1=Read Packet Info

C2=Create Alert Object

3. TIME AND SPACE RESTRICTION ANALYSER:

Set T:

T0=Get Alerts

T1=Check for Hyper Alerts

T2=Calculate the Space Restriction

T3=Time Calculator

T4=Create Alert Pairs

2.5 System Features (Modules)

We are implementing the following modules in our project:

2.5.1 System Feature 1

Reading Packet Dataset: First we maintain the database of alerts in excel. And in 1st module we read this packet dataset.After reading all the rows and columns we put it in array.so that we can easily get information about alerts.

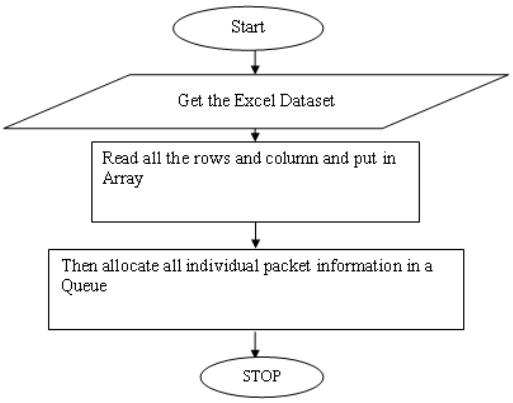
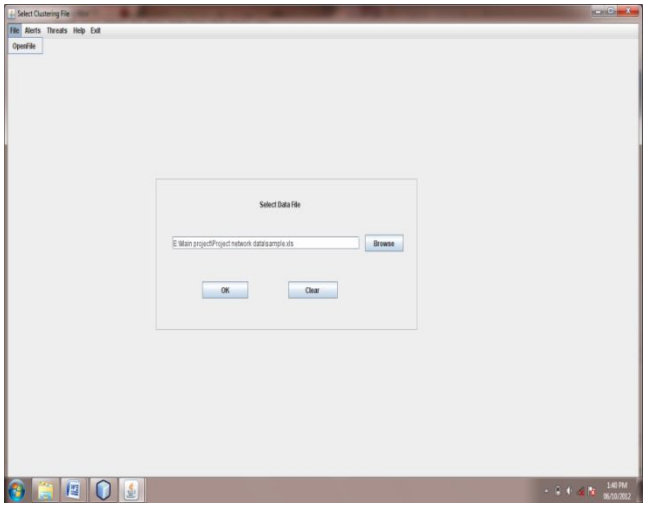


Figure 2: Module 1: Reading Packet Dataset

Fig below shows the snapshot for output window of module 1



2.5.2 System Feature 2

Creating Alert object: In 2nd module we read the information about each alert such as, sourceip, sourceport, destip, destport,time for each packet. And after reading all this information creates the object of each alert.

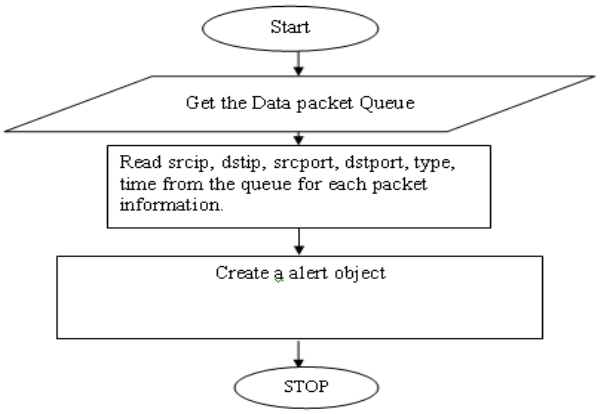
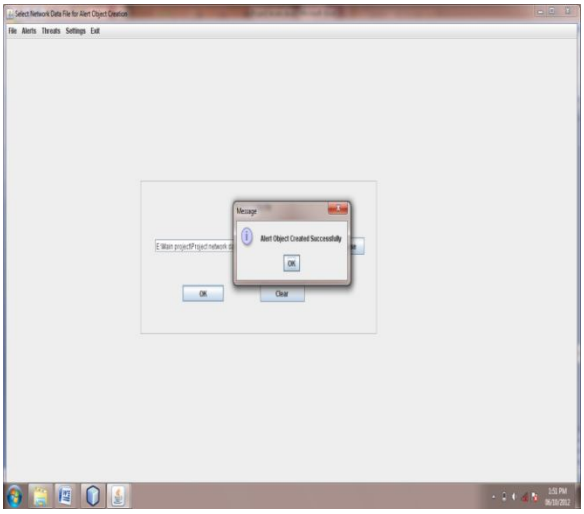


Figure 3: Module 2: Creating Alert object

Fig below shows the snapshot for output window of module 2



2.5.3 System Feature 3

Time and Space Restriction Analysis (TSRA): In third module our 1st algorithm is actually implemented .i.e.here comparison between various alert objects is done.i.e.we find which alert comes from which location & also incoming time of that object For this we use the following steps of algorithm.

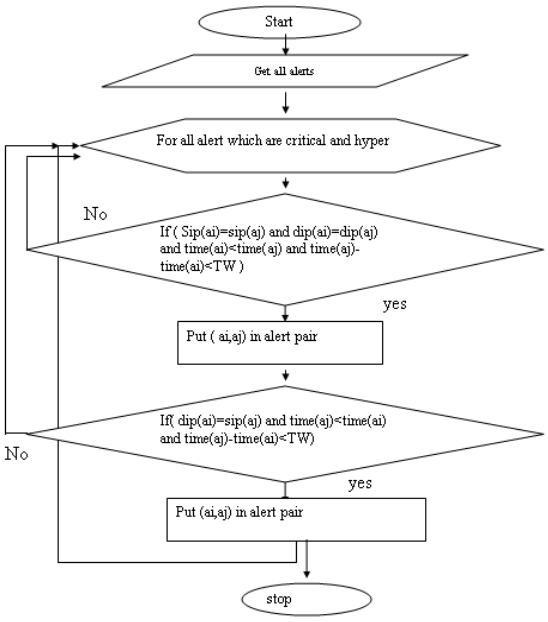
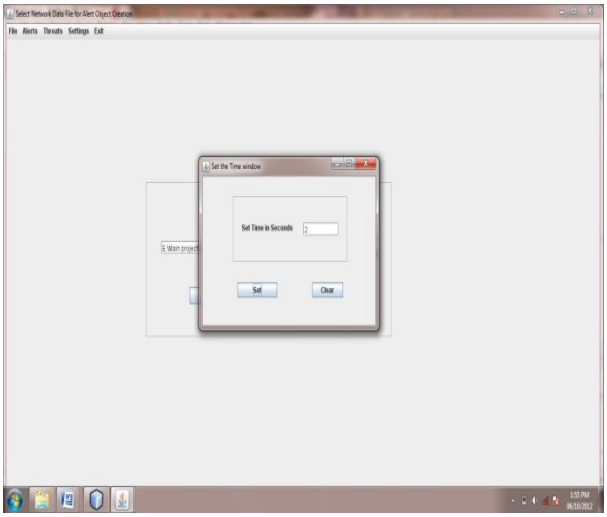


Figure 4:Module 3:Time & Space Restriction Analysis



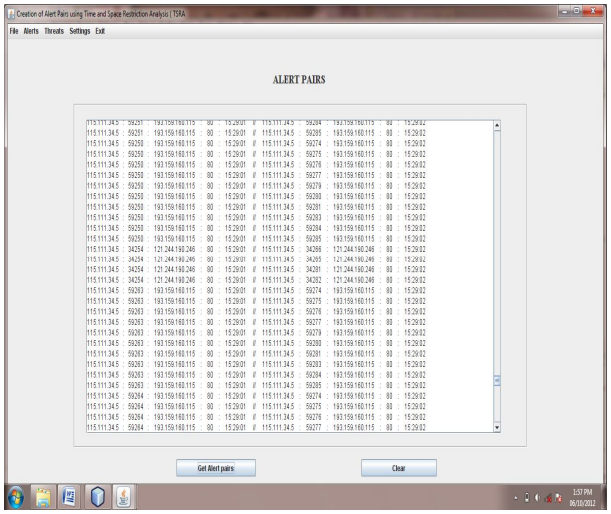


Fig.above shows the snapshot of output window.For this administrator have to set the time window first,and after that alert pairs are generated.

2.5.4 System Feature 4

Attack Graph Generation: After getting the alert pairs,we can generate the attack graph which is very useful to the administrator for taking decision. Fig, below shows the flowchart for attack graph generation. Here we implement second algorithm.

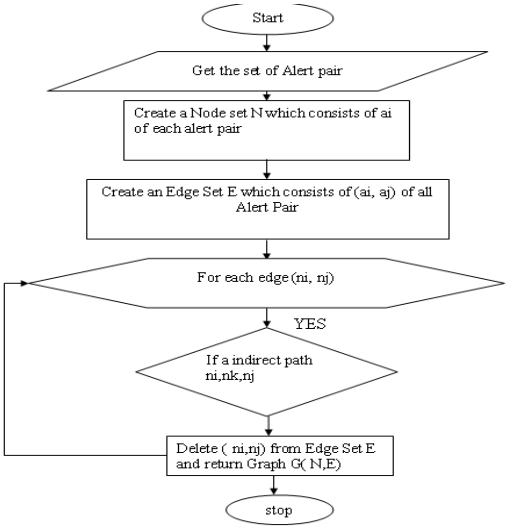
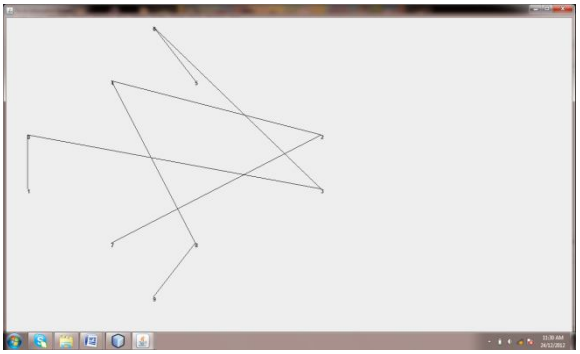


Figure 5:Module 4:Attack Graph Generation

Suppose we consider the first 10 alert pairs,then we can design the attack graph by using Kruskal's algorithm.The snapshot for attack graph is as follows:



3 PROPOSED WORK

After implementing this algorithms our proposed work is as follows:

Creation of evaluation function:-Then, we give an evaluation function for possible threats (either from attacks or on devices). Via these proposed methods, administrators can understand the network situation and learn how serious of an attack without checking individual alerts or evaluation values. Here NSA just wants to know where, when and how serious of an attack is, so we only need a small subset of alert fields. Using short alert message also saves time and storage space.

4 ACKNOWLEDGMENTS

Our sincere thanks go to Amrutvahini College of Engineering for providing a strong platform to develop our skill and capabilities. We would like to thanks to our friends,& relatives for their constant support and motivation for us. We are also very greatful to IJSER Author for giving an opportunity for presenting this paper. Last but not least, we would like to thanks all those who directly or indirectly help us in presenting the paper.

5 REFERENCES

1. 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.

2. Juan Wang,Feng-li Zhang,JingJin,Wei Chen, “Alert Analysis and Threat Evaluation in Network Situation Awareness” 2010 IEEE.

3. Cyril Onwubiko ,“Functional Requirements of Situational Awareness in Computer Network Security” 2009 IEEE.

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

5. 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.

6. Mr. Marc Grégoire ,“Visualisation 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. Availablefrom: http://www.rto.nato.int/abstracts.asp

7. 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.

8. J Hall, J Pei, Y Yin. Mining frequent patterns without candidate generation. 2000 ACM. SIGMOD int'IConf on Management of Data (SIGMOD'OO), DallaS, TX, 2000

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

10. Jia Han, MichelineKamber., “Data Mining concepts and techniques” , second edition 2006, Elsevier Inc.

11. 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