

Network Situation Visualization and Alert Generation Using Packet Data Analytics

Author: Bhawin Parmar¹; Mohsin Sheikh²

E-mail: bhawin.parmar@gmail.com¹; er.mohsin.paper@gmail.com²

ABSTRACT

In the present era computer network is taken as the core component of various technology supported areas such as banking sector, emergency systems and communication areas. With this increase in network usage the kind of data protection required to make the system secure is also serving as a challenging task. It includes attack resistant Internet services which results high demand for network analyst which measures the security situations successfully. Existing network analysis tools lacks such capabilities of analysing the network and access situations correctly. Situation awareness mechanism gathers current network condition and clearly defines the boundaries by which security solutions can be designed effectively. It reflects all the changes made in configurations and methods taken as a security measures by maintaining a database which later on used to make the decisions for network security improvements. It also makes the visualization of attack conditions by making the graphs and plots which greatly improves the rate and the quality measures of persons or machines decision making.

This work is going to detect the actual network status by using various metrics of the basis of which accurate decisions can be made. These decisions are used for assessing the current network and status of working devices and let them aware about the network actual conditions. Primarily the work is using four categories of network packet data analysis metrics and Attack Level Analysis.

Keywords:

Situation Awareness, Vulnerability Detection, Attack Graphs, Network Configuration Metrics

1. INTRODUCTION

In today's world information processing and its transferring speed had gone beyond limit. It includes the combined effort of fast networking devices and the nodes which works on certain protocols. The speed and other factors help to improve the current network situations faced by the financial sectors, power generations and other industries such as emergency situations. Once the data is generated by the devices then it is frequently updated by the creator or its user. Though the data is same but now it is having another data to support previous data termed as Meta data. The request made against the data is gone through a wide range of network and IP address. Among them some are trusted but most of them are not trusted. To analyses the behavior and authenticity of networking devices or host from where the request is been transferred or traversed, there must be some mechanism which visualizes the complete real scenarios into some graphs.

The system which performs the above operations is known as network security situation awareness or assessments systems. It aims towards getting the depth monitoring of the packet or the data traversing through or for a particular request or user or node. The system captures all the details from the network communication situations but there must be some factors which can forecast the attack behaviors. All it aims towards getting the correct situation of network after getting all the

nodes or respective nodes in communication. Previously the task is been performed by the network analysis but to capture all the details and analyze them manually is not feasible for limited resources. There must be mechanism which performs all the activities along with accurate analysis. Though there are various tools available with the market such as firewall and IDS but they lack in visualization for the respective data. Visualization always works as easy and effective method for getting the straight forward way of detecting the malicious sources. Also the tool must merge various type of information and shows the output in the form of graph which is quite difficult to understand directly. Thus the visualization tool is the requirement for today's market. Apart from only visualization there are some directed or expert visualization such as attack response, network monitor, spatial vulnerability detector etc.

The primary consent towards getting the network security situational awareness a feasible option is the consolidation of all the information which directs the presence of attack in the system. If the detected factors and the decisions are taken at early stages of the communication then the data drops can be pretended. Normally such system performs a fusion of all the information available at the time of deciding the network conditions. It helps in the attacks detections and other security relevant activities through network fabrication [2]. The situational awareness recognizes the kind of security and network breaches which include various vulnerabilities. Separately from that the situation awareness system identifies the type of attack, its impact, target and source. Impact dimension is further categorized to current analysis and future impact. Network situation assessment is getting high demand from the network analyst.

The existing tool lacks such functionality of analyzing and representing the actual network behavior. For each network and security assumptions, the current focus is on qualitative aspects rather than a quantitative analysis. Thus, to measure the overall security of a network one must first understand the vulnerabilities and how they can be combined to construct an attack which is shows network. Later section of the paper will covers all the details. It gives the background about the approach and then literature covered by the problem and then the solution for the system.

2. BACKGROUND

Vulnerability assessment is the art of finding the probability of attack occurrence using pattern analysis. It provides the intended security against the types of threats from which a system can be affected. All it aims towards serving the higher degree of security with minimized cost and information disclosure which we offer towards the protection entity. Recent security controls first analyses the security flaws associated with the system and then develop a strategy to overcome such issues. Thus a mitigation model can only be developed by getting a deep extent of information processing and the correct interpretation for the system. Network security situation assessment requires fixed step wise operations for assessing the performance of the system. It operates on the basis of three steps: Information collector for capturing the entire network and transferring information. Second module is vulnerability assessments which include threat assessment, vulnerability measurer and stability assessment. Last module is visualization of network situations based on the vulnerabilities.

All the above modules are work collaboratively for getting the complete information processing and forecast the nature of information and the network. It fuses the captured details and takes the decision based on the approach. It finally visualize the current network situations and later on used for getting the corrective decisions based on negative conditions or attack preventions. Thus the main component here is the situation visualization module provides multiple level views of situations of network security for helping the analysts to understand the situations of network security in very friendly user interfaces.

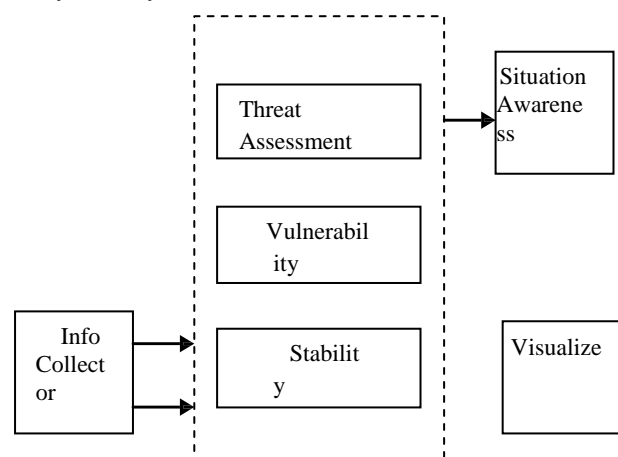


FIGURE 1: NETWORK SECURITIES SITUATIONAL ASSESSMENT PROCESS

The information which is captured during the modules must derive some of the network behaviour and its effects on the various system issues. Security system must have the complete analysis for ensuring the genuine behaviour of the network. Situational awareness means only the way of getting deeper into the system for predicting the attack occurrence probabilities [3]. If the system captures the useful and quality information then the decision based on them will improve the current situations where the performance lags can be prevented. In the preceding few years, various advancement is complete in standardize security metrics but still having some issues in their functioning borders. Some of the issues conclusions are address as a part of situational responsiveness are:

- (i) Design of Dynamic Vulnerability Detection System
- (ii) Attack Measurement and Prediction [4]
- (iii) Interconnection Analysis and Operation dependencies [5]
- (iv) Threat Plotting and Masking
- (v) Change Management
- (vi) Configuration Monitoring etc [6]

Presented approach had situation-awareness consist of susceptibility analysis using assault graphs, intrusion identification and alert relationship, attack investigation, attack collision analysis and forensics and information stream analysis. Thus this effort identifies such limitations from which attack challenging system can be divided from actual changes by map those parameter on visualization method. It use metrics based depth for achieve its objective in appropriate time.

3. LITERATURE SURVEY

During the last few years several authors had worked towards improving the current network analysis situations and take the decision on the basis of that. Now, once the system gets all the information correctly then it is quite easy for the analyst to get the respective decision by which a more secure boundary can be made against the

attacker. The situational awareness or assessment works using the different data fusion based approaches. Some of them are covered here as surveyed literature. The paper [7] covers the visualization primitives for mapping the current network situations using the graph for attack vulnerabilities. The paper uses gray theory model which operates on the basis of the residual error corrections for accuracy in mapping of entities and their behaviour. The experimental evaluation shows the model is performing well in different situations for information fusion. The paper [8] extends the network situational awareness using a newly suggested model SIEM which represents the security information and event management. The system depends upon the Internet based resources for correctly accessing the situations which involves attacks somewhere in their process of information exchanges. The proposed performs the behaviour analysis based on the malicious operations of each nodes and measures their attack nature. It uses several metrics on which the value is plotted for getting the in dept analysis about the nature of the networking entities. Thus it works using interactive decisions for vulnerability analysis. Some of the mechanism works as an intrusion detection system using this vulnerability assessment likewise given in analytical intrusion detection framework (AIDF) [9]. It works using probabilistic inferences rules which detects the patterns and their probability of occurring again using the forecasting behaviour. The behaviour detection is performed using some of the forensic operations and the previously generated alerts against those systems. The suggested system can be considered as a solution for anti-DOS mechanism through IDS. The practical implementation shows the effectiveness of the solution.

Some of the authors had also worked on reducing the complexities and requirements of the network vulnerability assessment systems. The paper [10] shows one of such approach which prove itself for smaller system where the resources and the complexities are not measured properly. It mainly analyses the complexity for generating the attack graph which visualizes the situations. The system splits the complete network into multiple zones based on their proprieties and processes their information parallel. Here each fragment represents the combination of the different network entities

which later on abstracted for taking the actions against them. Now once the attack graph is constructed then it can be used for detection of the malfunctioning nodes. The work's authenticity and accuracy is proving its effectiveness. The paper [11] presents a novel tool named as SiLK for capturing the packet level information and then merging them for taking the vulnerability decisions. The paper gives results on the basis of approximation model and network flows for data transmission. The work is on the parameters of active timeout, router exhaustion and cache flush for tracking the malicious behaviour. Thus the major volume of data and its visualization gives the results against the attack vulnerability assessment for network. The paper [12] gives a detailed view of two more visualization tools NvisionIP and the VisFlowConnect-IP. They are capable of getting the actual analysis and representing the situations on real time network. The tool mainly analyses the IP range, processes their massive data, filters their packets and drops the malfunctioning packets.

Another extended tool for VisiFlowConnect and its prototype application is given with the paper [13] and [14] also. It modifies the traffic pattern detection approach for more accuracy. The extended version works on high detection rates with reduced false detection and effective visualizations. It also makes dynamic decisions and multidimensional data. The paper [15] gives an improved WNN based situation assessment model using quantitative prediction for optimizing the result set and its accuracy. It also supports real time detections using preventive intrusion detection mechanism. It also uses genetic parameters and back propagation network for detecting network vulnerabilities. The author works towards getting the improvements in prediction accuracy, functional approximation and convergence speed. At the evaluation analysis the approach is serving its goals. The paper [16] extended the above principle using artificial immune technology. The system provides self learning's and adaptive nature which increases attack immunity. The paper [17] had suggested a novel command vulnerability scoring system for analysing the impact of attacks in the system. The results of an analysis of the scoring system and that of an experiment scoring a large set of vulnerabilities using the standard are presented. Although the scoring system was found to be

useful, it contains a variety of deficiencies that limit its ability to measure the impact of vulnerabilities.

4 PROBLEM STATEMENT

After studying the various approaches of vulnerability assessment the work founds that the current system will work on a defined boundaries which causes static visualizations. Also the impact analysis performed by them will lag somewhere so that the correct analysis and predictions can't be made. As of now the system focuses on qualitative attributes which derives nothing for the attack patterns. It must have various features for quantitative assessments. Also the previous mechanisms have their own scoring mechanism for level of attacks or their impacts. Thus a complete visualization based on the real time network situations against load must be plotted so that the correct preventive measures have been taken. Once the visualization is complete then the network analysts will easily direct the system which protects it from various threats. Also the packet is transmitted from various sources then we must be able to track down all the intermediate entities and their address along with a clear behaviour analysis. Thus the objective of the work is:

“To visualize the real time network packet transmission situations using load analysis for getting the system protected against the various attack vulnerabilities.”

5. PROPOSED WORK

This work suggests a novel mechanism for developing a system for vulnerability assessment and impact analysis using the selected metrics. While measuring the vulnerability for the system against the attacks the real time network situations must be analyzed thoroughly for finding out the patterns or similarity which predicts the attack occurrence. The current system will only give the massive data whose analysis was not present with the tool. All it needs a complete visualization of each and every packet transmission and intermediate entities. Once the vulnerability is analyzed then new decisions can be taken by which some improvements or preventions can be made. The process starts with fetching the network packets and other node details by which some data is generated which is likely to be used for decisions. The collected information is

passes to visualization module which generate the attack graphs using the direct acyclic graphs. The system is configured using various low level details or metrics like network configurations, impact level analysis , energy, load, packet transmitted or received etc. All the details are measured for the different network nodes who somewhere participates in the transmissions. The database generates after the n operation will be used for further detecting the attack vulnerabilities using the previously analyzed factors.

Once the detection is completed then an alert is generated and forwarded to each node in the network. While detecting the attacks the

predictions have to be made based on previously stored patterns. Thus once the attack tries to replicate itself the system get the attack visualize. Now the visualization system mainly deals with the difficulty of plotting the nodes and their transmissions in real time. Visualization using direct acyclic graph phases several challenges like the tree based or cluster representations, their interpretations, decision formation and controls, attack impact analysis etc. The clear view of suggested approach is given in figure 2.

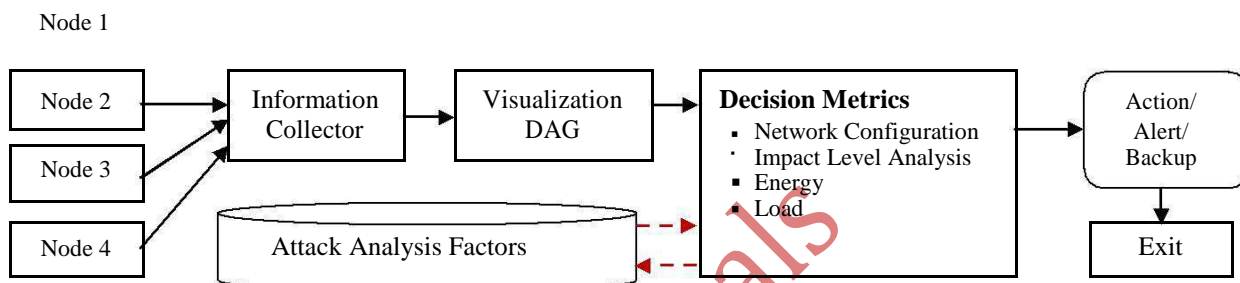


FIGURE 2: PROPOSED NETWORK VISUALIZATION AND ATTACK ANALYSIS SYSTEM

Algorithm:

```

Start Operations
Data Capture Flag== (0); // Initial Flag Status
Vulnerability Assessment==0; // Start Measuring
Information
Assigns Initial Colour;
If (Data Capture Flag==1)
D1, D2, D3...Dn=Capture (Info1, Info2, Info3...Info N);
// Capturing Information Under Multiple Matrices
Where D1=Packet Information;
D2= Transmission Information (Type, Time)
D3= Source Information (SRC_IP, SRC_PORT)
D4=Routing Information;
D5=Destination Load Information (DST_IP, DST_PORT)
D6=Load Information;
Store Value In dataset
Set IP to Nodes; //
Connecting Node as Link based on Packet Transmission
Load
Call DAG (Node, Edge)==SRC_IP & DST_IP;
//Generate Direct Acyclic Graph
Connect Edges According to Source & Destination IP
If Load==Max or Packets Flow==Max
Then Change Node & Edge Colour;
If Request Connect Edges
Calculate Impact Level Analysis (ILI)
If (ILI>=Threshold)
Attacking Node;
Terminate Connection;
  
```

Else
Normal Node;

Exit;

After getting all the above steps correctly the network configuration along with the vulnerability visualization can be performed effectively. The system generates temporary data which can be used for assessment.

APPLICATION AREA

- (i) Dynamic web security
- (ii) Web services monitoring
- (iii) Web performance logger
- (iv) Cloud based web computing
- (v) Blogging
- (vi) Social networking
- (vii) Transaction Systems
- (viii) Online services marketing

6. CONCLUSION

This paper presents an abstract view of all the vulnerability scoring system used for network analysis. The work had found several deficiencies which limit the accuracy and impact detection will high negative detections. For getting the previously

massive text data based system, the work had to integrate some of the decisional recommendation and a graphical visualization mechanism which helps the analyst to increase its capabilities. These changes would improve the accuracy of the scores, which would help organizations and individuals better prioritize their responses to new vulnerabilities. The changes would also be backwards compatible with scoring performed using the original version of the network security situational awareness and vulnerability standard. Existing scoring metric values could simply be entered into a new equation to for getting the correct and accurate analysis. Experimental analysis proves the above theory on the basis of a developed prototype.

REFERENCES

- [1] R. Xi, S. Jin, X. Yun and Y. Zhang, "CNSSA: A Comprehensive Network Security Situation Awareness System", in International Joint Conference of IEEE TrustCom, ISSN: 978-0-7695-4600-1/11, doi: 10.1109/TrustCom.2011.62, 2011.
- [2] W., C. Yao, A. Singhal and S. Jajodia, "Network Security Analysis Using Attack Graphs :Interactive Analysis of Attack Graphs using Relational Queries", in proceedings of IFIP WG Working Conference on Data and Application Security (DBSEC), 11.3 pages 119-132, 2006.
- [3] M. Grégoire and L. Beaudoin, "Visualisation for Network Situational Awareness in Computer Network Defence", in proceedings of visualisation and the common operational picture meeting RTO-MP-IST-043, Paper 20. 2008.
- [4] White Paper on, "Public Safety and Homeland Security Situational Awareness", in ESRI, February 2008.
- [5] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, "Cyber SA: Situational Awareness", in Cyber Defense University of Wisconsin, 2009.
- [6] R. Barabanov, S. Kowalski and L. Yngström, "Information Security Metrics", DSV Report series No 11-007, Mar 25, 2011
- [7] R. FAN, M. ZHOU, "Network Security Awareness and Tracking Method by GT", in Journal of Computational Information Systems, Binary Information Press, ISSN: 1043-1050, Vol. 9: Issue 3, 2013.
- [8] I. Kotenko and A. Chechulim, "Attack Modelling and Security Evaluation in SIEM System", in International Transaction of System Science and Application, SIWN Press,, ISSN:2051-5642, Vol. 8, Dec 2012.
- [9] Bon K. Sy, "Integrating intrusion alert information to aid forensic explanation: An analytical intrusion detection framework for distributive IDS", in Elsevier Journal of Information Fusion, ISSN: 1566-2535, doi:10.1016/j.inffus.2009.01.001, 2009.
- [10] I. Kotenko and M. Stepashkin, "Attack Graph Based Evaluation of Network Security", in International Federation for Information Processing, in LNCS 4237, 2006. Pp:216-227
- [11] T. Shimeall, S. Faber, M. DeShon and A. Kompanek, "Using SiLK for Network Traffic Analysis", in CERT R Network Situational Awareness Group, Carnegie Mellon University. September 2010.
- [12] W. Yurcik, "Visualizing NetFlows for Security at Line Speed: The SIFT Tool Suite", in 19th Large Installation System Administration Conference (LISA '05), 2005.
- [13] X. xin Yin, W. Yurcik and M. Treaster, "VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness", in ACM, doi: 1581139748/04/0010, Oct 2004.
- [14] X. Yin, W. Yurcik and A. Slagell, "The Design of VisFlowConnect-IP: a Link Analysis System for IP Security", in National Center for Advanced Secure Systems Research (NCASSR), 2010.
- [15] Ji-Bao Lai, Hui-Qiang Wang, Xiao-Wu Liu and Ying Liang, "WNN-Based Network Security Situation Quantitative Prediction Method and Its Optimization", in Journal of computer science and technology, Vol. 23, Issue 3, ISSN: 0222:0230, Mar 2008.
- [16] S. Jun Liu, Le Yu and J. Yang, "Research on Network Security Situation Awareness Technology based on AIS", in International Journal of Knowledge and Language Processing, ISSN: 2191-2734, Volume 2, Number 2, April 2011.
- [17] P. Mell and K. Scarfone, "Improving the Common Vulnerability Scoring System", in proceedings of IET Information Security, doi:10.1049/iet-ifs:20060055