ICARFAD: A Novel Framework for Improved Network Security Situation Awareness

Chanchal Sharma
Dept. of CSE
SDBCT Indore
M.P (India)

Vandana Kate
Dept. of CSE
SDBCT Indore
M.P (India)

ABSTRACT

Networking components and technologies is continuously proving their presence in various core areas of business like IT, Health Care, Stocks, and Emergencies with Military systems. It is possible by applying multiple system phenomenons of compatibility, interoperability and integration of different categories of devices and users. As the usage of information is increasing the transaction and data security needs to be provided effectively. It will serve as a critical and important task which assures data protection. This unexpected and frequent changes in the system is measured which gives a direction of vulnerable behaviour and the criticality of affecting the process. Accessing this information through actual network conditions and changes for improving the security is comes under the area of situational awareness system. This work proposes a novel ICARFAD (Information Collection, Assessment and Response, Feedback and Alerts Decisions) based situation awareness mechanism which 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.

General Terms

Network Security Situation Awareness (NSSA)

Keywords

Attack Graphs, Situational Metrics, ICARFAD (Information Collection, Assessment and Response, Feedback and Alerts Decisions);

1. INTRODUCTION

Network situation awareness is used to distinguish network security situations briefly. Based on the separation of monitored network information, it makes a quantitative assessment on the security situations. The system has various components which can be effectively measured by metrics and generates the multiple viewpoints of network. The devices and continuously expanding networking is generating massive amount of information which needs to be processed n time for accurate and preventive detections. Much vulnerability scoring metrics is working to achieve accurate assessments but lacks in generating precise and accurate qualitative alerts. Although various security tools such as firewalls and intrusion detection systems have been deployed in the detection and prevention of attacks, these security tools often generate huge reports as well as numerous false positives and false negatives [1]. It is commonly too difficult for network analysts to understand and manage extremely large amount of network reports. An effective tool on network security situation awareness is highly required to help us fuse all available information properly and comprehend the situations of network security with ease. The current focus is on qualitative aspects rather than a quantitative study of network security [2]. Measuring situation awareness consists of various aspects of network and security behaviour of the system. Initially the current situation is analyzed by recognizing and identifying the kind of security breaches which includes attack vulnerabilities calculation. It is serving more than any intrusion detections which only identifies the intruder. Apart from that the situation awareness system identifies the type of attack, its impact, source, target etc. Impact measurement is further categorized to current analysis and future impact. The system is also capable of understanding the evolution condition which helps the analyst to track the major changes in component configurations. This monitored information identifies the entities behaviour and its effects the network dropping. The system has to be responsible for ensuring availability, integrity and confidentiality of current network situations. Their primary challenge is to maintain situational awareness over thousands of network objects and events [3]. The system totally depends upon the quality of information collected to take the decisions; if the information is poor then the analysis is also weak. Thus, information generation and processing is a vital task for effective situation awareness system and hence it must be updated and complete to derive an intelligent decision.

For measuring the complete and effective security vulnerabilities detection and their attack constructing pattern needs to be identified in real time before damage occurs. Now a day’s most often attack graphs is used for quantitative analysis of security. Detecting the individual effect has no uses today because of multi variant attack combinations striking the network in huge amount. It is used for criticality identification, asset configuration changes detection and location findings in various areas such as military, emergency; IT infrastructure etc depends upon the needs of the system [4]. Thus some mechanism had to be designed which gives precise and accurate information for timely analysis and detection of such attacks. Existing solution is using various metrics to measure the attacks on quantitative and qualitative basis. Usually this involves the prediction based on object, time and space measurement using such derived metrics. In the last few years, some progress is made in standardizing security metrics but still having some issues in their working boundaries. Some of the issues findings are addressed as a part of situational awareness are:

- Design based vulnerabilities identification
- Attack and Response detection
- Interconnectivity and dependencies modifications analysis [5]
- Threat mapping and assessment
- Positive and negative change detections
- Configuration and working boundaries monitoring etc

Situation awareness regarding data security comprises information about data security threats targeting the networks and services [7]. The real situation awareness mechanism automatically analyze huge amount of data for useful patterns, unusual behavioral and configuration changes, measuring the dependencies in effective manner. It involves data extraction techniques like spatial index, predictive analytics and machine learning to take the decisions [8]. To measure such awareness security metrics is a very important aspect for information security. These metrics are to facilitate decision making and improves performance accountability. It represents all the parameters in quantifiable and measurable manner [9]. They have to be considered as a reference point which allows the admiration of the systems quality points. This term is very often used to describe the concepts of metric, measure, score, rating, rank or assessment. But for the most important objective of the information security metrics is being developed and specify a useful decision support reporting security system.

Objective of Using Security Metrics:

a) Used to measure performance and to improve protection level.
b) Create a reference level model about monitoring and improvement to contribute to the definition of the security level for evaluation, validation and the optimization of the security necessities;
c) Contribute to the enhancement of the existing security practices and to the integration of information security to its business processes values ;
d) To contribute to the fact that technical problems should be detained on the administration level;

Thus this work identifies such boundaries from which attack resistant system can be separated from actual changes by mapping those parameters on visualization mechanism. It uses metrics based measurement for achieving its goal in timely basis.

2. LITERATURE SURVEY

During the last few years various researchers had worked on analyzing the accurate network conditions for taking the correct decision of changes regarding network improvements. Most of them use security metrics to measure the situations. Such metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data [10]. IT security metrics monitor the accomplishment of the goals and objectives by quantifying the level of implementation of the security controls and the effectiveness and efficiency of the controls, analyzing the adequacy of security activities and identifying possible improvement actions.

In the paper [11], the author gives a new passive network monitoring tool to address these important requirements of current network analysis and assessment, known as Panemoto (Passive Network Monitoring Tool). This tool describes, and characterizes all network components, including devices and connected networks, and delivers an accurate representation of the function of devices and logical connectivity of networks. A real example of Panemoto's output is taken in which the network information is presented in two distinct but related formats: as a clickable network diagram (through the use of NetViz, a commercially available graphical display environment) and as statically linked HTML pages, viewable in any standard web browser. Together, these presentation techniques enable a more complete understanding of the security situation of the network than each does individually.

Network security situational assessment response capacity of the network, to mitigate the harm caused by cyber attacks and found the potentially malicious intrusion attacks [12]. The paper gives a model that has been established combined with gray theory. According to the increasing frequency of current network attacks, the existing network security situational awareness model is unable to meet the network security detection and early warning needs in confrontational environment. The research mainly in establishing unequal time interval sequence model, unequal interval gray model and gray theory-based inverse function model, by the three models, coming out a network security situation awareness model based on gray-theory, and the amendment on the precision of the model based on the multi-stage residuals. At the initial level of work it seems to be providing better results than the existing systems.

In this paper [13], a novel framework is been proposed for attack modeling and security evaluation through SIEM (Security Information and Event Management) Model. The framework measures the behaviour of existing attacks and the generating nodes for accurate evaluation through common attack graph generator. It uses various security metrics for providing accurate risk analysis. Then primary element is key tree generation through attack modeling security component (AMSEC). A prototype model is presented in this for result analysis.

The objective of the research paper [14] is to show an analytical intrusion detection framework (AIDF) using probabilistic determination theory. It comprised of two activities, first, a probability model discovery approach, and second is probabilistic inference mechanism for generating the most probable forensic explanation. It measures the unreported signature rules that are revealed in the probability model. It integrates alert information available from IDS sensors distributed across subnets. It uses the existing open source tool Snort to illustrate its feasibility. Through a preliminary experimental study, illustrates that the applicability of AIDF for information integration and the realization of (i) a distributive IDS environment comprised of multiple sensors, and (ii) a mechanism for selecting and integrating the probabilistic inference results from multiple models for composing the most probable forensic explanation.

The SiLK tool given in [15] is a highly-scalable low-data capture and analysis system developed by the Network Situational Awareness group. Support for network forensics, identifying artifacts of intrusions, vulnerability exploits, worm behaviour, etc. Providing service inventories for large and dynamic networks (on the order of a CIDR/8 block). Generating prowlers of network usage (bandwidth consumption) based on protocols and common communication patterns. It enables non-signature-based scan detection and worm detection, for detection of limited-release malicious software and for identification of precursors.

Continuing the above key factors based on data sizes and their types multi large volume security issues is resolved by monitoring the performance and behaviour of components. In the paper [16] NSAA has presented a developed suite of tools that solves this problem and is making this software available to the Internet community. Primarily it gives two visualization tools:

(1) NVisionIP and
(2) VisFlowConnect-IP

Both of these tools have been developed based on system administrator requirements, their design peer-reviewed in security research forums, and usability testing is in process. These tools both present large volume complex data transparently to system administrators in simple intuitive visual interfaces that support human cognitive processes. NVisionIP visually represents the state of all IP addresses on large networks on a single screen window (we use a Class B address space as the default) with capabilities to filter and drill-down to subnets and individual machines for details-on-demand. VisFlowConnect-IP [18] visually represents flows between internal network IP hosts and the Internet showing that is connecting with whom with capabilities to filter and drill-down to subnets and individual machines for details-on demand. NVisionIP and VisFlowConnect-IP can be used individually or in unison for correlating events. This work is distinguished from others in that these are the first Internet security visualization tools to be freely available on the Internet and deployed in large production environments.

Multi visualization design is been proposed over the last few years to enhance the ability of an administrator to detect and investigate anomalous traffic between a local network and external domains. Central to the design is a parallel axes view which displays NetFlow [17] records as links between two machines or domains while employing a variety of visual cues to assist the user. The tools have several filtering options that can be employed to hide uninteresting or innocuous traffic such that the user can focus his or her attention on the more unusual network flows. Such effective designing resolves various runtime configuration and management issues through real time administrative controls.

The accurate and real-time prediction of network security situation is the premise and basis of preventing intrusions and attacks in a large-scale network. In order to predict the security situation more accurately, a quantitative prediction method of network security situation based on Wavelet Neural Network with Genetic Algorithm (GAWNN) is proposed in [19]. After analyzing the past and the current network security situation in detail, it builds a network security situation prediction model based on wavelet neural network that is optimized by the improved genetic algorithm and then adopt GAWNN to predict the non-linear time series of network security situation. After analyzing various simulation experiments it proves that the proposed method has advantages over Wavelet Neural Network (WNN) method and Back Propagation Neural Network (BPNN) method with the same architecture in convergence speed, functional approximation and prediction accuracy.

3. PROBLEM STATEMENT

After studying the various approaches of different authors it is found that the current system is used to perceive network security situations expansively. Based on the fusion of network information, they make a preventive assessment on the situations of network security. They are not been able to visualize the situations of network security in its multiple and various views, so that network analysts can’t be able to know about the situations of network security easily and comprehensively. Here are the few identified areas of work for improving the security through accurate and timely assessments:

- The existing system can understand the network security situations through fusing large amount of network information quantitatively.
- The situation assessment provided by existing systems is not quantitative and even not in real time. Measurement metrics and vulnerability affections need to be calculated accurately.
- Out of massive data false alarm has to be driven out without affecting actual identification and assessment mechanism.
- The value used to define network situation and the level of details required for optimal representation.
- The development of prediction function and decision recommendation is not given and the identification of better response plans and actions is also required.

This work is used to measure the overall security of a network one must first understand the vulnerabilities and how they can be combined to construct an attack. Recent advances using attack graphs can be used to measure quantitatively the security of a network. The objective is to develop new algorithms that will greatly enhance the situation assessment by processing such a massive data in real time and also used to make the overall process automation. If successful, the systems being-protected will recognize and learn about evolving situations, generate and reason about situation response plans and actions, and automatically respond to intrusions.

4. PROPOSED SOLUTION

The aim of this proposed domain is to increase the security level of the system through assessing the current situation through situation awareness phenomenon. This work measures the network situation through various assessment metrics and applies the most suitable approach to reduce the vulnerability through various assessed attacks. The proposed work had stored the network state while there is no attack probability and then continuously monitors the current state. Comparison is made regularly to detect the attack probability through the attack graphs. It measures the type of changes occurring in the network and detects potentially anomalous changes to the network configuration. This potential can alert administrators to dynamic changes in the network situation. It detects the devices and networks that are new, missing, or changed, and displays their information depending on their status.

It expresses the value on behalf of two measurable metrics:

a) Qualitative Assessment (Risk analysis).
b) Quantitative Computation Network Security (Bayesian sets and fuzzy theory).

The proposed architecture of the system is shown in figure 1.1. Initially the number of system is monitored to get the current network situation values. Under this monitoring phase various types of network devices and their status is sensed like it will detect the changes occurring in the network configurations, number of host variations, devices working efficiency etc. This measured data is stored in the repository store for current state values. It consists of two stages: security policy detection and network configuration assessment. In the next phase this information can be read by information collector modules from the log details of the individual store and repository for respective data. This data is then passed on to situation assessment modules which work on the bases of five metrics: network configuration, attack impact, policy updates, attack routes and threat risk analysis. This metrics is used for awareness generation regarding the current network situation and for malicious and unwanted activity pattern detection.

This can be achieved by creating various attack graphs from which decision can be taken to detect such activities. Thus an attack graph created from the suggested metrics is going to calculate the types of response and action identification. Later on this response and actions is extracted as a utility entry and stored in vulnerability assessment database store. This store is used as a data access repository for the next step of assessment of network situations. In this phase firstly the useful and malicious pattern is detected from the dataset of existing situation repository. On this extracted dataset the work will apply to decisions for network boundary partitioning. This leads to predict the affects of applied decision; if it improves the condition then the decision is spread through its lower hierarchy or else recalculation is made for accurate assessment. This mechanism will also generate the alert message to aware the system admin or the controlling device to stop such activity. Now feedback of performed action is also measured using response metrics to clarify the usability of proposed mechanism. In this way an improved network awareness can be identify to measure to improve the existing network security situations based on Information Collection, Assessment and Response, Feedback and Alerts Decisions (ICARFAD).

Metrics Used

- *Metrics based on Network Configuration* (Quantity of Hosts, Firewalls, Type of Hosts, Hosts with Antivirus Software Installed, Hosts with Firewalls, Hosts with Host Based Intrusion Detection Systems, etc.);
- *Metrics of Hosts* (Criticality Level, etc.);
- *Metrics of Attack* Actions (Damage Level; Access Complexity; Base Score; Confidentiality Impact; Availability Impact; Access Complexity, etc.);
- *Metrics of Attack Routes* (Route Length in Vulnerable Hosts; Route Average Base Score; Maximum Access Complexity; Damage level of route; Maximum damage level of route, etc.);
- *Metrics of Threats* (Minimum and Maximum Quantity of Different Vulnerable Hosts used for Threat Realization; Quantity of Different Routes; Risk level of threat);

Objective of Using Security Metrics:

a) Used to measure performance and to improves protection level
b) Create a reference level model about monitoring and improvement to contribute to the definition of the security level for evaluation, validation and the optimization of the security necessities;
c) Contribute to the enhancement of the existing security practices and to the integration of information security to its business processes values;
d) To contribute to the fact that technical problems should be detained on the administration level;
e) Measurement can be smoothly calculated with accurate behavior analysis and proceeds to correct awareness.

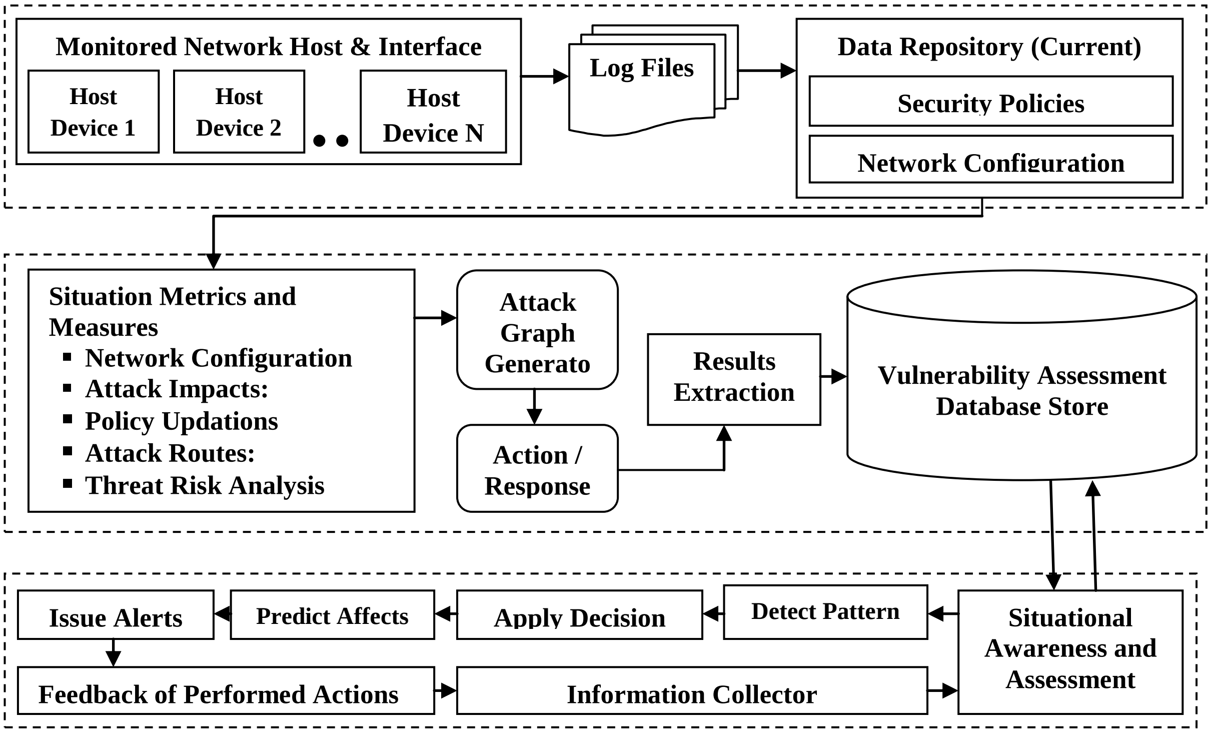

Fig 1: Proposed ICARFAD for Improved Network Situation Awareness

5. EXPECTED OUTCOMES

Situational awareness is essential for decision makers to efficiently manage their resources. Situational awareness has historically been associated with aviation security applications, such as air traffic control (ATC), fighter missions, and missile defense. However, the number of studies in the field of situational awareness for new applications has grown significantly in the past few years. Network security situation awareness system should have the ability to handle information coming from multiple sources, which will include information of network topology, network configuration, vulnerabilities, system logs, network security device alerts, network traffic and etc. Based on proper information fusion, a network security situation awareness system provides network analysts with the insight into security relevant activities occurring within their networks, so as to help them make decisions or modifications on their networks. There are a number of system tools currently used in the field of network security situation awareness, such as NVisionIP and VisFlowConnect-IP. The expected benefits of these systems can be given as:

- Better Security analysis process;
- Easy modification of network configuration and security policy.
- Attacker behavior and intent analysis
- Information combination for network situation-awareness
- Achieving self-awareness for network devices
- Active and passive attack detection
- Transmission intrusion detection
- Deep Packet Inspection

Most of these systems use flow traffic to provide network security situation information. Application of these mechanisms is as follows:

- **Immune Network Security Situation Awareness Technology:** Biological Immune System (BIS) is a complicated system with the ability of self-adapting, self-learning, self-organizing, parallel processing and distributed coordinating, and it also has the basic function to distinguish self and non-self and clean non-self.
- **Situation Forecast:** Situation forecast is the highest level of situation awareness; it is based on historical and present network security situation information and makes quantitative prediction of the network.
- **Analytical Intrusion Detection Framework (AIDF):** It is an underlying structure comprised of a probability model discovery and inference mechanism. The purpose of AIDF is to bridge intrusion detection with forensic analysis based on inferring and integrating alert information from distributive IDS sensors; whereas the outcomes of an inference are referred to as forensic explanations.
- **Other Areas of Application:** This includes awareness of availability, confidentiality, integrity status of the command and control, intelligence, logistics, communications, information technology (IT) etc.

6. CONCLUSION

This work is used to analyze the existing problem of accurate network situation awareness in real time. The size of information generated by any monitoring tool is very large and hence required complex processing. Fusion of this information is used to derive a decision for vulnerability detection. In this work a novel ICARFAD based assessment mechanism is proposed for improved detection of security situations and taking timely response. It consist of three phase; information collection, assessment and response and feedback. All the data passes through a repository to hold the decisions. Pattern is also extracted for better measurement of situations. This work uses various metrics to calculate the correct behavior of the system. At the initial level of this work approach seems to provide effective results in near future.

7. ACKNOWLEDGMENTS

The authors wish to acknowledge SDBCT administration for their support & motivation during this research. The authors would also like to thank anonymous referees for their many helpful comments, which have strengthened the paper. They also like to give thanks to Mrs. Vandana Kate & Dr. Suresh Jain for discussion regarding the intrusion systems & for producing the approach adapted for this paper.

8. REFERENCES

[1] Rongrong Xi, Shuyuan Jin, Xiaochun Yun and Yongzheng 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] Wang, 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] Mr. Marc Grégoire and Mr. Luc 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] Rostyslav Barabanov, Stewart Kowalski and Louise Yngström, "*Information Security Metrics*", DSV Report series No 11-007, Mar 25, 2011

[7] Pallavi Vaidya and S. K. Shinde, "*Application for Network Security Situation Awareness*", in International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012), IJCA, ISSN: 0975 – 8887, 2012.

[8] Xiu-Zhen Chena, Qing-Hua Zhenga, Xiao-Hong Guana,b, Chen-Guang Lina, Jie Sun, "*Multiple behavior information fusion based quantitative threat evaluation*", in Elsevier Journal of Computers & Security , ISSN: 0167-4048 ,doi:10.1016/j.cose.2004.08.009,2005. pp 218-231

[9] Lingyu Wang, Tania Islam, Tao Long, Anoop Singhal, and Sushil Jajodia, "*An Attack Graph-Based Probabilistic Security Metric*", in National Institute of Standards and Technology Computer Security Division; Concordia Institute for Information Systems Engineering, Montreal, Canada.

[10] Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo, "*Security Metrics Guide for Information Technology Systems*", in NIST Special Publication 800-55, July 2003.

[11] William Streilein, Kendra Kratkiewicz, Michael Sikorski, Keith Piwowarski, Seth Webster, "*PANEMOTO: Network Visualization of Security*

Situational Awareness through Passive Analysis“, in Workshop on Information Assurance United States Military Academy, Proceedings of the IEEE, 2007.

[12] Rongzhen FAN, Mingkuai 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.

[13] Igor Kotenko and Andrew 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.

[14] 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.

[15] Timothy Shimeall, Sidney Faber, Markus DeShon and Andrew Kompanek, “*Using SiLK for Network Traffic Analysis*”, in CERT R Network Situational Awareness Group, Carnegie Mellon University. September 2010.

[16] William Yurcik, “*Visualizing NetFlows for Security at Line Speed: The SIFT Tool Suite*”, in 19th Large Installation System Administration Conference (LISA ’05), 2005.

[17] Xiaoxin Yin, William Yurcik and Michael Treaster, “*VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness*”, in ACM, doi: 1-58113-974-8/04/0010, Oct 2004.

[18] Xiaoxin Yin, William Yurcik and Adam Slagell, “*The Design of VisFlowConnect-IP: a Link Analysis System for IP Security*”, in National Center for Advanced Secure Systems Research (NCASSR), 2010.

[19] 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.

[20] SunJun Liu, Le Yu and Jin 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.

[21] P. Mell and K. Scarfone, “*Improving the Common Vulnerability Scoring System*”, in proceedings of IET Information Security, doi:10.1049/iet-ifs:20060055, 2007.