ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Novel Framework for Composite Network Security Situation Assessment Using HRCAL Approach

Miss. Ankita Patil [*], Mr. Vijay Prakash
[*] Department of CSE, SVITS Sanver Road Indore (M.P.),India
ankitapatil1310@gmail.com

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 analyzing 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 HRCAL work is using four categories of metrics like Host, Route, Configuration and Attack Level Analysis.

Keywords: Situation Awareness, Vulnerability Detection, Attack Graphs, Network Configuration Metrics, HRCAL (Host, Route, Configuration and Attack Level Analysis).

Introduction

At present, the network constitutes as a core component for information processing system in various areas like financial sector, power generations and emergency systems. These systems are continuously using different types of information's from multiple locations. In such situations where data is generating and getting updated regularly from various ends identifying its behaviour and authenticity is a critical area of work for researchers. Security of these networks from malicious intrusions is significant to the economy and of our people. Thus a standard way to measure network security will brings different users together with vendors and researchers. In the last few years there has been some significant improvements over providing standardizing such security measures using: Topological Vulnerability Analysis, Network Hardening and Attack Response. To provide the better security against the tremendous attacks in the Internet, there is developing high demand for network analysts to know about the situations of network security effectively [1]. The existing tool lacks such functionality of analyzing and representing the actual network behaviour. 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 harmful for network. The idea behind the network security situation assessment and awareness is for consolidation of all available information for identification of attack vulnerable to the system. An early finding leads us to develop some countermeasures to avoid such conditions. They process information from various sources and start a proper fusion of information for directing the attacks detections and other security relevant activities through network modifications [2].

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Measuring situation awareness consists of various aspects of network and security behavior 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 behavior 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.

Existing approaches had situation-awareness consist of vulnerability analysis using attack graphs, intrusion recognition and alert association, attack analysis, attack impact analysis and forensics and information flow analysis [4, 5, and 6]. 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.

Background

In the last few years, some progress is made in standardizing security metrics but still having some issues in their working boundaries. For measuring the complete and effective security vulnerabilities detection and their attack constructing pattern needs to be identified in real time before damage occurs. Some of the issues findings are addressed as a part of situational awareness are related to design based vulnerabilities identification for attack and response detection [7]. 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. It is commonly too difficult for network analysts to understand and manage extremely large amount of network reports [8]. 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. It also have various interconnectivity and dependencies modifications analysis, threat mapping and assessment, positive and negative change detections and configuration and working boundaries monitoring etc.

Network Situation Awareness is one of the key requirements for effective management composite devices of complex or geographically dispersed network activities [9]. It opens the area of parallel accessing conditions and attack level analysis for defense activities, such as area surveillance, command and control, network-centric operations and asset protection. Situation awareness may apply, for instance, to the functionality, availability, capacity, data security, and alteration and development of networks and services. To plot the actual visualization of situational assessment some design diagrams needs to be generated. Thus in case of networks best ways is to use the attack graphs that most often used for quantitative analysis of security. Individual attack detections are of no use today because so many variants and attack combinations are hitting market daily. Most of the attack graph analysis toolkits are designed to do deterministic attack consequence estimation. In real time situation-awareness, such consequence estimates could be very misleading due to various uncertainties. Alert correlation techniques cannot handle the inherent uncertainties associated with inaccurate interpretations of intrusion detection sensor reports (such inaccurate interpretations lead to false positives/negatives in determining whether an IDS alert corresponds to an attack). Lack of data or complete knowledge may raise additional uncertainty management issues.

There are so many issues generated with assessing the current network situations:

- The type of alerts and its frequent updations is large in numbers and some time actual changes in network might be detected as an attack causes false alerts generation which misleads the actual aim [10].
- Identification of DDoS is very complex to determine because of their variants nature and lack of knowledge [11].

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

- The uncertainty coming in current tools needs to be handled in a better manner and lacks reasoning capability.
- Attack detection decision has to be more accurate and on time with proper system configuration analysis.

Our vision is that attack graphs can be used to do vulnerability analysis and analyze the damage that can be caused by an attack. It can also be able for calculating the cost of reconfiguration and the amount of resistance to an attack. Thus an optimal solution with metrics can be developed and hence is our prime aim with this paper.

Related Study

Network security situational awareness mechanism is very important for military and emergency responses and other than that it is very much required concerning the effective security. In the paper [12], it is calculated with the help of visualization mechanism for correct assessment like that form attack graphs. It provides potential and accurate mechanism using model based on Gray Theory through Residual Error Corrections. It uses three functions Primary residual error correction, secondary residual error correction, and tertiary residual error correction. It resolves the issues related to discrete nature of raw data. Although the proposed method has done some research in achieving network security situational awareness, but many of the key issues needs to be deepen and improved. The experimental evaluation shows that the observation of the model to the network security situation is able to achieve a reasonable getting accuracy, which is full of practical terms.

In the paper [13], author suggested a novel framework for security evaluation with attack modeling using SIEM (Security Information and Event Management) system. It is totally based on internet data for better analysis of security situations and current attack involvements. The proposed management system is based on attack analysis using malefactor behaviour identification and graph generation through various metrics for risk assessment. The paper also presented a prototype for future implementation based on suggested approach. Primarily it is calculating the vulnerability using interactive decisions.

Apart from the above vulnerability identification mechanism there are some mechanism which is designed to identify the intruder's process and their affections. One of that is AIDF (analytical intrusion detection framework) which is proposed in [14]. It uses a probabilistic inference mechanism for generating the most probable forensic clarification based on not only just the practical intrusion detection alerts, but also the unreported signature rules that are exposed in the possibility model. It is quite often for IDs to be opened in full logging mode for the forensic data gathering. It can be considered as practical implementation and solution of anti-DoS strategy in a authentic world deployment.

So many authors had also worked on reducing the complexity so such systems which are too complex to implement for a smaller systems. Among them one is given in [15] for reducing the complexity of generating the attack graph. The suggested approach concludes the work as: First, it splits the network into fragments and does parallel computing for each fragment with subsequent result combinations and second, it gives the aggregation and abstraction for representations of attack actions. Its evaluation is based on comprehensive simulation of malefactor's actions, construction of attack graphs and computation of different security metrics. At the initial level of work, its experimental results show its authenticity and accuracy.

In the paper [16], the author introduces the tools and techniques used to store information about sequences of packets as they are collected on an enterprise network for SiLK. It gives the result approximation based on network flows by generating its own records for data transmission. It analyses multiple flow records for situation assessment. Mainly it identifies active timeout, cache flush and router exhaustion for attack analysis and vulnerability assessment. So by giving both the volume and complexity of this data, it is critical to understand how this data is recorded and that is effectively achieved by above visualization tool.

In the paper [17], some more visualization tool for network situation is proposed by NCSA. These are (1) NVisionIP and (2) VisFlowConnect-IP. The above tools satisfy all the requirements of system administrator for accessing the actual network conditions. They provide IP analysis, huge data processing, and filtration of packets which provides the correlation of events to identify the drops created by malefactor's device. This work is distinguished from others in that these are the first Internet security visualization tools to be freely accessible on the Internet and deployed in large invention environment.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

To get the accurate assessment of network situation, visualization of current devices and host interactions needs to be plotted in correct manner. This can be achieved by network visualization diagrams which satisfy administrator's requirements. It monitors the traffics and will able to control it also. To do this effectively a tool design is implemented in the form of VisFlowConnect as a prototype application. It discovers a variety of interesting network traffic patterns. Some of these were harmless, normal behavior, but some were malicious attacks against machines on the network. This demonstrates that these visualization techniques serve as a powerful tool for situational awareness of network security events.

This paper [19] focuses specifically on the design decisions made during the VisFlowConnect development process so that others may learn from the calculated experiments. Because for the current Tools- the result of these design decisions extensible to processing other high volume multi-dimensional data streams where link connectivity/activity is a focus of study. Thus this paper reports experimental results quantifying the scalability of the underlying algorithms for representing link analysis given continuous high volume traffic flows as input.

WNN-Based network security situation quantitative prediction method and its optimization is given in [20] for accurate and real-time prediction. It provides the basis of preventing intrusions and attacks in a large-scale network. The paper suggests a new model Wavelet Neural Network with Genetic Algorithm (GAWNN) and Back Propagation Neural Network (BPNN) method with the same architecture in convergence speed, functional approximation and prediction accuracy. The tool had some additional predictions for administrator for accurate assessments.

Carrying forward the above research and accurate analysis of network situations few of the authors had also applied the artificial immune technology as in [21]. It enables self-learning and self-adapting of network system, and increases its immunity and viability. When network is under attack, it can find out the current network security situation and future trend in an all-around way, provide grounds for reasonable and accurate response to guarantee the usability of system. Situation forecast makes prediction of future network security trend based on historical and present network security situation information. When network information system is under attack, network security situation awareness model based on immunity has all-around and whole knowledge of current network security situation and its future trend and can provide grounds for reasonable and accurate response to guarantee the availability of system.

Some of the authors had developed a unique standard for correct and unified network conditions and behaviour accuracy detections. This system is Common Vulnerability Scoring System, which is an emerging standard for scoring the impact of vulnerabilities [22]. 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.

The above study on various research articles demonstrates here that how actual assessment of network is required to be for removal of deficiencies of existing systems. So the derived results shows that using common vulnerability standards is not sufficient apart form that some more data mapping metrics needs to be used and a new model needs to be proposed for effective detections.

Problem Identification

Network situation security assessment and awareness is mechanism which requires frequent modifications in attack databases and must give real time vulnerability calculations and alerts. It is used to perceive network security situations comprehensively. Based on the fusion of network information, the current tools make a qualitative assessment on the situations of network security. The existing system can recognize the network security situations through fusing large amount of network information. The existing system which is taken as a base for this work CNSSA [1] adopts the measurement metrics of the Common Vulnerability Scoring System (CVSS) to make quantitative assessment on the situations of network security which needs to be modified for frequent updates processing. It should also implements filter function in its information collection process. 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.

After studying various research works carried out during the last few years following are the key

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

requirements or problems identified as a baseline for our proposed work;

- The current focus is on qualitative aspects rather than a quantitative study of network security.
- Current situation has to be understood deeply for better understanding of the system and attack vulnerability identifications.
- The development of prediction function and decision recommendation is not given and hence more accurate filter and prediction function needs to be designed for accurate and early analysis of vulnerability and attack impacts.
- Situation perception needs to be plot in multi-view so as system administrator gets deeps access of analysis and affects for particular attacks.
- False alarm has to be filtered out for improved performance and situation tracking

Thus by this research work our objective is to develop new algorithm and architecture for enhancing the machine intelligence against the attack detection and network security situation assessment and awareness. The successful deployment of such system will lead the network to self protections from evolving network attacks situations.

Proposed Work

This work proposes a novel HRCAL model for accessing the actual network situations and providing the attack resistant decisions on time. It increases the security views which are available with current networks. The work measures the actual network conditions by accessing the data from all the connected devices. It identifies the changes made in the network which are positive and which are making the network down. Hence making the system as anti-attack resistance, it needs to get better analysis of their behaviour and impacts levels. Thus it uses 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.

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 measurement 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. This mechanism will also generate the alert message to aware the system admin or the controlling device to stop such activity. In this way an improved network awareness can be identify to measure to improve the existing network security situations based on Host, Route, Configuration and Attack level analysis (HRCAL).

Use of Security Metrics:

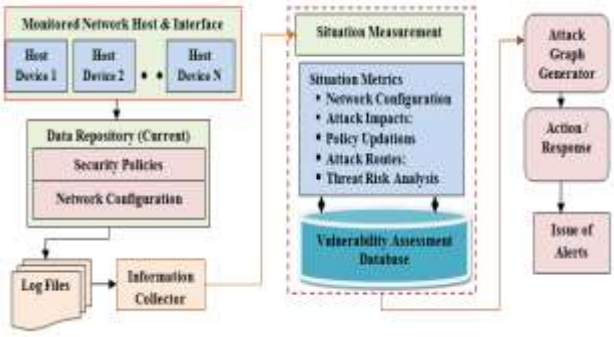
It involves data extraction techniques like spatial index, predictive analytics and machine learning to take the decisions. To measure such awareness security metrics is a very important aspect for information security. These metrics are to facilitate decision making and improves performance accountability. It represents all the parameters in quantifiable and measurable manner. 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.

The above metrics will create a reference level model about monitoring and improvement to contribute to the definition of the security level for

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

evaluation, validation and the optimization of the security necessities. It will also contribute to the enhancement of the existing security practices and to the integration of information security to its business processes values.

Figure:



HRCAL based network situation awareness

Tables:

Table 1. Matrics used in proposed HRCAL

S. No	Metrics Tag	Name	Data Sources	Functionality/ Type Metrics
1	H	Host Behaviour	Scan Information	Type, Specification; Criticality Level;
2	R	Attack Routes	Network Traffic	Response Time Delay; Route length, Max and Min Damage Route;
3	C	Network Configuration	Network Traffic	Network Bandwidth Consumption; Type, Number, Category with IDS Installed or Not
4	A	Attack Impact	IDS Alerts	Packet Drop Rate; Damage Level, Vulnerability Score etc;
5	L	Threat Level	IDS Alerts	Min and Max Quantity of Different Vulnerable, Risk level of threat

Expected Benefits

The presented approach differs from the former work in that it focuses on achieving comprehensive and accurate threat evaluation. 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. Instead of emphasizing particularly the impact of isolated incidents, the current mechanism of HRCAL filters out some network packets corresponding to irrelevant or invalid intrusions by fusing information (service, application software and vulnerability) generated by a scanner, and some packets corresponding to unsuccessful intrusions by use of intrusion response rules that serve as the standard for determining whether or not it is to succeed in achieving user privilege. Once a decision is reached, planning and execution (of the response actions) occur.

- 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

Evalution Parameter

On the basis of above proposed mechanism there is a need to prove the performance and authenticity of proposed approach and hence few performance analysis parameters is needs to be given so as to evaluate the approach correctly. These are network bandwidth consumption, packet drop rate and response time delay which serve as security evidences that are used to represent the running state of the target host. These are defined as follows:

- *Network Bandwidth Consumption:* It is defined as the ratio between the increased in transmission data bytes by intrusion and the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

maximum increase in transmission data bytes up to some operation level of system which is unacceptable state; Similarly for decrease can also be calculated.

- *Packet Drop Rate*: It is defined as the percentage of total number of non replied requests over total number of issued request. It gives the details about the total packet sent and total packet received.
- *Response Time Delay:* It is defined as the increase in response time of packet sent to destination due to intrusion upon the maximum increase in response time due to updations in level of data transmission.

The fusion of the three evidences results in a more accurate measure of system security than does relying on single evidence.

Conclusion

Situational awareness is essential for improving the security of network having large number of devices continuously interacting with each others. It is associated with various applications like military, healthcare, air traffic control or aviations etc. 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. Thus as its usage is increasing the trust for more accurate attack analysis is also creating pressure. Thus for providing a pivot in the area of security assessments, this work proposes a novel HRCAL security situation awareness mechanism based on five set of metrics. The unique feature of the proposed system is real time analysis and behaviour plotting through attack graphs. It can also process different types of information simultaneously. At the initial level of research it proves as a better option for network and security administrator. Future results and implementation prototype will definitely makes the way open for various researchers.

Future Work

Some problems and concepts that remain unaddressed can be performed in future as a theoretical background, but the first thing is to develop a prototype so as to prove the results. Such as with the help of pre-emptive approach more information can be added for exact timely analysis of network situations & its successful assessment with high accuracy. It can also be used for quantitative & qualitative analysis.

Acknowledgements

This research work is self financed but recommended from the institute so as to improve the security situations and breaches with current techniques. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. The authors also wish to acknowledge SVITS administration for their support & motivation during this research. They also like to give thanks to Mr. Vijay Prakash & Dr. Rajeev Vishwakarmafor discussion regarding the situational awareness system & for producing the approach adapted for this paper.

References example:

[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.*

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

[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] *Igor Kotenko and Mikhail Stepashkin, "Attack Graph Based Evaluation of Network Security", in International Federation for Information Processing, in LNCS 4237, 2006. Pp:216-227*

[16] *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.*

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

[18] *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.*

[19] *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.*

[20] *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.*

[21] *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.*

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

Author Biblography

Athor Name Ankita Patil
Research Scholar,
Department of CSE
SVITS, Sanver Road
Indore (M.P), India
Email:
ankitapatil1310@gmail.com