Network Security Situational Awareness

AHMAD JAKALAN
ahmad@njnet.edu.cn

Jiangsu Key Laboratory of Computer Networking Technology,
China, Nanjing, Southeast University

Abstract: With the different sources of threats to the Networks, from the physical and human threats to the extreme diverse methods used by hackers to exploit networks and disseminate different types of malware from simple kinds of comic, propaganda, ads, and viruses to highly sophisticated with a very advanced levels of Obfuscation Techniques like Packers, Polymorphism, Metamorphism [1] it's becoming more and more difficult the task entrusted to network security scientists and engineers. Many kinds and different names of security monitoring and analysis tools have been used to detect the penetration on the networks and analyze the effectiveness of the network. The list is too long but we may mention Antivirus, firewalls, log audit tools, Host-based and Network-based Intrusion Detection Systems IDS, Low and High interaction based honeypots, general purpose and special purpose honeypots, network flow analysis tools,etc. It is too difficult for network security engineers to be aware of the huge amount of data produced by these different tools, at the same time it has been proved that depending on one kind of these tools is not enough to protect the network from being exploited. In 1999 Bass Tim[2, 3] was the first author who recommended the application of Situational Awareness in the future Network Security. He foresees that next generation cyberspace intrusion detection systems will fuse data from heterogeneous distributed network sensors to create cyberspace situational awareness. In this paper we summarize the state of the art in situational awareness and its application in Network security, we will mention the different efforts done by scientists to apply the concept of Situational Awareness SA in network security.

Keywords: Network Security, Situational Awareness.

1. Introduction

The concept of Situation Awareness (SA) comes from the research on human factors in the realms of aerospace and aviation. The United States Department of Homeland Security defines situational awareness as "the ability to identify, process, and comprehend the critical elements of information about what is happening to the team with regards to the mission [4]". The military term "situational awareness" refers to a commander knowing where his troops are, their readiness and capabilities, and most importantly intelligence on the location of enemy troops, their readiness and capabilities [5]. The knowledge and ability of the analyst to perceive and analyze situations, make sound decisions on how to protect organization's valued assets and offer accurate predictions of future states in a dynamic and complex environment[6]. Situational awareness is a cognitive human factor process that involves a person (security analyst) who observes, analyses, resolves situations in the network, and makes projections about network states. NSSA encompasses security monitoring, security visualization, detection techniques, data fusion, automation, dynamism and complexity to achieve higher levels of situation awareness[6]. **Endsley** defined situation awareness as "the perception of the elements in the environment within a volume of time and space; the comprehension of their meaning and the project of their status in the near future"[7]. In 1999, Tim Bass first proposed the concept of Situational awareness to be used in the field of Network Security NSSA.

2. The evolution of Situational Awareness

In 1988 in her paper Design and evaluation for situation awareness enhancement[7] M. R. Endsley presented a discussion of the SA construct, important considerations facing designers of aircraft systems, and current research in the area of SA measurement. Later in 1995 in her paper Toward a theory of situation awareness in dynamic systems[8] she Proposed a theoretical model of situation awareness based on its role in dynamic human decision making in a variety of domains. In dynamic environments, many decisions are required across a fairly narrow space of time, and tasks are dependent on an ongoing, up-to-date analysis of the environment. She proposed Three levels of SA:

Received July, 22, Reviewed August 24, 2013

1. Level l SA: Perception of the Elements in the Environment to perceive the status, attributes, and dynamics of relevant elements in the environment.
2. Level 2 SA: Comprehension of the Current Situation
3. Level 3 SA: Projection of Future Status: This is achieved through knowledge of the status and dynamics of the elements and comprehension of the situation (both Level I and Level 2 SA).

In 2001, in her article Designing for situation awareness in complex systems[9] M. R. Endsley defined Situation Awareness as The Key to Providing Information because that the problem is no longer lack of information, but finding what is needed when it is needed.

3. Network Security Situational Awareness NSSA

To understand what is the difference between Security monitoring and situation awareness? It is that the Security monitoring is when someone monitors the network and systems for the ongoing phenomenon in which data maybe continuously changing. Whether it is passive or active security monitoring, future projection of the states of the network is neither a mandatory condition nor an optional requirement. Thus, security monitoring is only a part of the perception stage of situation awareness[10].

In 1999 Tim Bass, published a series of papers on the future of intrusion detection in the Internet. These papers, in particular his ACM paper, *Intrusion Detection Systems & Multisensor Data Fusion – Creating Cyberspace Situational Awareness[3]*, helped spark a modern revolution in Internet security, particularly in the area of network-based intrusion detection systems (IDS). Tim Bass in This paper is considered as the first author and network security researcher who has proposed the application of Situational Awareness in Network Security. He proposed that Multisensor data fusion provides an important functional framework for building next generation intrusion detection systems and cyberspace situational awareness. Future design challenges and areas of further research to develop Multisensor data fusion based ID systems are suggested in this article. He discussed the lack of individual Intrusion detection systems to detect the Intrusions combining data from multiple and diverse sensors and sources in order to make inferences about events, activities, and situations. He compared these systems to the human cognitive process where the brain fuses sensory information from the various sensory organs, evaluates situations, makes decisions, and directs the action. The output of data fusion cyberspace ID systems would be estimates of the identity (and possibly the location) of an intruder, the intruder's activity, the observed threats, the attack rates, and an assessment of the severity of the cyber attack.

In another article Multi-sensor Data Fusion for Next Generation Distributed Intrusion Detection Systems[2] 1999, Tim Bass has estimated that “Next generation cyberspace intrusion detection systems will fuse data from heterogeneous distributed network sensors to create cyberspace situational awareness”. This paper provided a few first steps toward developing the engineering requirements using the art and science of Multisensor data fusion as the underlying model. And a functional overview of how the art and science of Multisensor data fusion enhances the performance and reliability of advanced cyberspace management systems, touches on design challenges and suggests areas of further research and development. In addition it suggested that traditional thinking in broad concepts such as network management should evolve to fusion based cyberspace situational awareness.

In 2000 and in his article “Cyberspace Situational Awareness Demands Mimic Traditional Command Requirements” **[11]**, Tim Bass has estimated that Sophisticated computer hardware and software will identify a myriad of objects against a noise-saturated environment. And Cyberspace command and control (CC2) systems will track the objects, calculate the velocity, estimate the projected threats and provide other critical decision support functions. So Cyberspace situational awareness is required to operate and survive in complex global network infrastructures where both friendly and hostile activities coexist.

Cyril Onwubiko in [6] presents the Functional Requirements of Situational Awareness in Computer Network Security. He gives a description of the three levels of situation awareness, *perception*, *comprehension* and *projection* as follows:

- Perception: knowledge of the elements in the network such as alerts reported by intrusion detection systems, firewall logs, scan reports, as well as the time they occurred. Classification of information into meaningful representations that offers the underlying for comprehension, projection and resolution.
- Comprehension: techniques, methodologies, processes and procedures that security analysts use to analyze, synthesize, correlate and aggregate

pieces of evidence data perceived in the network from network elements.
    - Security visualization is the transfer of organized data and information into meaningful patterns or sequence to be visualized. It is part of the comprehension stage of situation awareness.
    - Data fusion is a technique to aggregate sets of evidence regarding a perceived situation;
- Projection: the ability to make future prediction or forecast based on the knowledge extracted from the dynamics of the network elements and comprehension of the situation.

The following figure is adapted from Endsley's SA reference model [8], which presents three levels of situation awareness, *perception*, *comprehension* and *projection*. The fourth level (*resolution*) is as a result of McGuinness and Foy extension of Endsley's SA model[12].

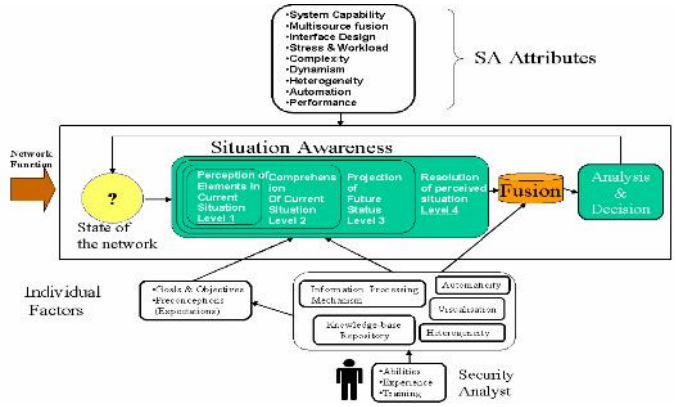

Figure 1 Network Security Situation Awareness Model[6]

Onwubiko[6] proposed the essential attribute to designing and implementing SA in computer network security including: Dynamism and Complexity, Automation, Real time processing, Multisource Data Fusion, Heterogeneity, Security Visualization, Risk Assessment, Resolution, and finally Forecasting and Prediction of how situations may develop over time by predicting or simulating possible scenarios.

In 2003 [5, 13] present a tool, NVisionIP, that makes a direct contribution to solving the problem of visualizing security events. NVisionIP used NetFlow as a data source. It simultaneously visualizes multidimensional characteristics of individual computers as well as their relationship to network-wide security events in an entire Class B IP address space. NVisionIP utilized Argus NetFlow data to present a visual representation of the traffic of an entire class-B IP network on a single screen. The visualization presented is based upon either the number of bytes transmitted or the number of flows to or from the hosts on the network and can be filtered based upon a number of attributes useful in categorizing security incidents. Flows are recorded at each router in the network and sent over UDP to a central collection point that aggregates the flow data into a single flow file. The galaxy view gives a visual picture of the current state of an entire class-B network. All subnets of the network are listed along the top axis of the galaxy view, while the hosts in each subnet are listed down the vertical axis.

VisFlowConnect[14] looks like an improvement to the previous NVisionIP. It Visualizes by animation the network traffic between an internal network and the Internet (to/from) as well as traffic contained entirely within an internal network. With its filtering capabilities to only show traffic with certain attributes VisFlowConnect is a powerful tool to visualize network traffic flows using points, lines, colors, shapes, and animation. And It allows analysts to focus on abnormal flow behavior signatures.

Another article presenting VisFlowConnect[15] with some improvements to enhance the ability of an administrator to detect and investigate anomalous traffic between a local network and external domains. It displays NetFlow records as links between two machines or domains, Parallel axes view, and an Animation mechanism to display temporal aspects of the data.

In 2005, VisFlowConnect-IP [16] A tool for visualizing IP network traffic flows with a focus on the real-time connectivity between different IP hosts. It Visualizes network traffic both between an internal network and the Internet as well traffic strictly within an internal network. Besides monitoring the overall traffic, VisFlowConnect-IP is also capable of monitoring traffic on specific ports.

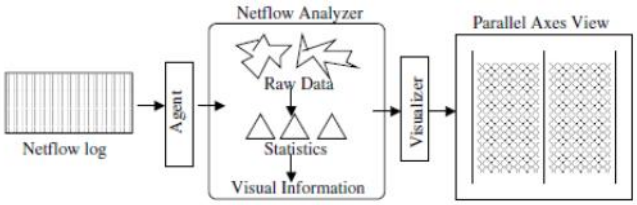

Figure 2 General System Architecture of VisFlowConnect-IP

All previous works could be considered as visualizing IP network traffic flows, but in their article [17] published in 2006 Lai Jibao et al. provide a conceptual model of network security situation awareness consisting of three levels, from bottom to top are network security situation perception, situation evaluation, and situation prediction. Their model of network security situation evaluation uses simple additive weight and established by the threat degree of various services attacked. While the model of future network security situation prediction adopted grey theory and built by past and current network security situation. The starting point of this research is evaluating attacks on services provided by the network.

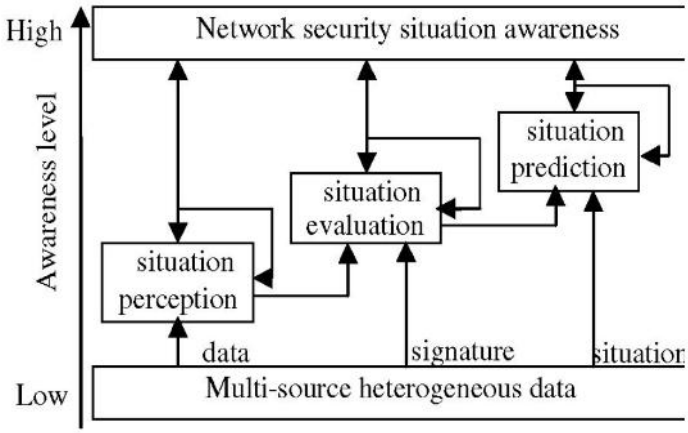

Figure 3 The conceptual model of network security situation awareness[17]

Another approach is provided by using HoneyNet dataset and adopts statistical analysis to find the vulnerabilities of the services which the hosts provide the network system. According to the network topology, the host layout and the relations among services, the **[18]** presents a novel time-divided and hierarchical approach to achieve the current situation of network security. The evaluation of the security situation depends on first classifying services depending on importance as high level, medium level, and low level services. And Damage degree of the attacks on five levels: Ultra-High, High, Medium, Low, and None. A hierarchical structure of situational awareness is used starting from each host in the network and situational awareness of the total system is obtained from combining the calculated values on different hosts.

A novel NSSA model, based on multi-sensor data fusion and multi-class support vector machines, is presented in [19] and [20] and [21] which Adopts Snort and NetFlow as the two sensors to gather data from network traffic. It employed multi-class support vector machines as fusion engine of their model in combination with an efficient feature reduction approach to fuse the gathered data from heterogeneous sensors. Multi-source provides more integrated and robust data which can be analyzed and a more accurate result can be gained. The authors discussed the alert aggregation algorithm and the security situation awareness generation techniques. The model has proven to be feasible and effectively through a series of experiments.

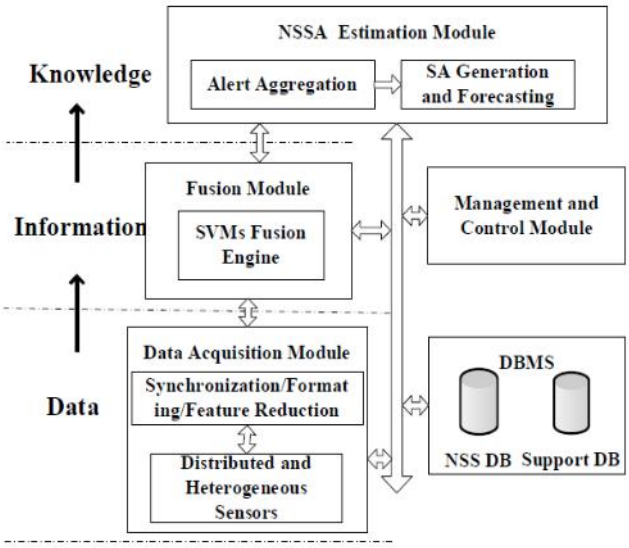

Figure 4 The NSSA model [20]

By adopting a multi-perspective analysis, In [22] Yong, Z. et al. use the description of security attacks, vulnerabilities and security services to evaluate the current network security situation. The situation prediction model adopts time series analysis. It uses past and current situation map to forecast future network security situation. The data collection module includes: Malware Detection, IDS, Firewall, Vulnerability Scan, Penetration Testing, Online Testing, and Security Service Detection. According to the security situation of each host, they adopted additive weight method to compute the security situation of the entire network (N hosts). Situation Prediction based on probability and statistics, time series analysis.

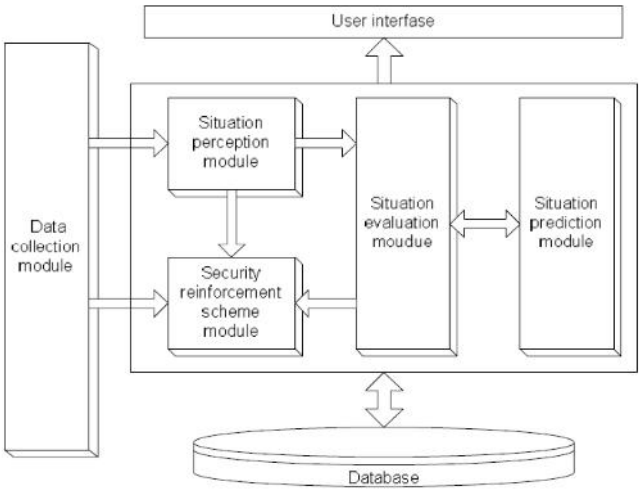

Figure 5 The framework of NSSA[22]

In [23], Juan, W., et al. adopted **Alert Analysis and Threat Evaluation in Network Situation Awareness where** the NSA system gets alerts from IDS deployed in the network (SNORT, REALSECURE). NSA just wants to know where, when and how serious of an attack is. The main idea of correlation in their work is that a successful attack usually has several steps. The attacker may use scan tools to get the target network information firstly. After finding weakness of the network, the attacker will focuses on certain devices, and start certain attack steps. These attack steps are related, thus their corresponding alerts are also related. We correlate the related alerts to an attack scenario based on time and space relations. From this definition, Two alerts *ai; aj* , if they are related, they usually have certain time and space relations as follows:

1. Srcip(*ai*)=Srcip(*aj*), Dstip(*ai*)=Dstip(*aj*), Time(*ai*) <Time(*aj*).
2. Dstip(*ai*)= Srcip(*aj*), Time(*ai*) <Time(*aj*).

They give different threat levels for different snort alert classes,

Alert Classes	Attack Describe	Severe Level
Root-attempted	attempting to get administrators privileges	high
Attempted-dos	attempting to denial of service attack	medium
Network-scan	network scan was detected	low

Also devices have different importance too. For example the servers are usually more important than the individual hosts. Because individual hosts only store personal information, intrusion of them can only hurt individuals. An Alert Device Evaluation Matrix (ADEM) for *n* alerts and *m* devices is a *n X m* matrix, in which the element contains an evaluation value of a device suffering from an attack.

Published in 2011 Towards Situational Awareness of Large-Scale Botnet Probing Events [24] the authors investigated ways to analyze collections of malicious probing traffic in order to understand the significance of large-scale "botnet probes." In such events, an entire collection of remote hosts together probes the address space monitored by a sensor in some sort of coordinated fashion. The analysis draws upon extensive Honeynet data to explore the prevalence of different types of scanning, including properties, such as trend, uniformity, coordination, and Darknet avoidance. They developed techniques for recognizing botnet scanning strategies and inferring the global properties of botnet events. The approach holds for contributing to a site's "situational awareness"—including the crucial question of whether a large probing event detected by the site simply reflects broader, indiscriminate activity, or instead reflects an attacker who has explicitly targeted the site.

The article in [25] "Situation awareness for networked systems" presents the concepts of forming situational information templates and hierarchies based on data available from a distributed monitoring system where the temporal and spatial properties of situational information are taken into account. A case study is presented that shows the feasibility of the concepts in a real world monitoring scenario.

Conclusion

From the previous article we can summarize the needs and techniques related issues (Problems) for situational awareness application in network security as the following:

- Three levels of situation awareness:
  - *Perception*: IDS alerts, firewall logs, Netflow, Honeynet [26],…
  - *Comprehension:*
    - Techniques used to analyze, correlate and aggregate pieces of perceived data.
    - Visualization, Data fusion are parts of this stage.
  - *Projection*: make future prediction
- Classification

    - Threats[23], resources, services, alerts, sensors, vulnerabilities,…
- Data Reduction: Selecting useful parts of the collected data
- Data Fusion (Which theoretical model will be used?)
    - multi-class support vector machines
    - Additive-weights
- Prediction and Estimation (Which Prediction model will be used? And What is the meaning of the achieved results?)
    - Time series analysis
    - Probability and statistics
    - Artificial neural networks,
    - Fuzzy mathematics,
    - The Grey theory [27, 28]
- Scope: Protect What? Is there any Critical area should be protected. LAN or Cyberspace?

References

1. O'Kane, P., S. Sezer, and K. McLaughlin, *Obfuscation: The Hidden Malware.* Ieee Security & Privacy, 2011. **9**(5): p. 41-47.
2. Bass, T., *Multisensor data fusion for next generation distributed intrusion detection systems.* 1999.
3. Bass, T., *Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness.* Communications of the ACM, 1999. **43**(4): p. 99-105.
4. *United States Department of Homeland Security. Team Coordination Training, Student Guide, .*
5. Bearavolu, R., et al. *A visualization tool for situational awareness of tactical and strategic security events on large and complex computer networks*. 2003. IEEE.
6. Onwubiko, C. *Functional requirements of situational awareness in computer network security*. in *Intelligence and Security Informatics, 2009. ISI '09. IEEE International Conference on*. 2009.
7. ENDSLEY, M. *Design and evaluation for situation awareness enhancement*. 1988.
8. Endsley, M.R., *Toward a theory of situation awareness in dynamic systems.* Human Factors: The Journal of the Human Factors and Ergonomics Society, 1995. **37**(1): p. 32-64.
9. Endsley, M.R. *Designing for situation awareness in complex systems*. 2001.
10. D'Amico, A. and M. Kocka. *Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned*. in *Visualization for Computer Security, 2005.(VizSEC 05). IEEE Workshop on*. 2005. IEEE.
11. Bass, T., *Cyberspace situational awareness demands mimic traditional command requirements.* SIGNAL-FALLS CHURCH VIRGINIA THEN FAIRFAX--, 2000. **54**(6): p. 83-84.
12. McGuinness, B. and L. Foy. *A subjective measure of SA: the Crew Awareness Rating Scale (CARS)*. in *Proc. of Human Performance, Situation Awareness and Automation: User-Centered Design for the New Millenium*. 2000.
13. Lakkaraju, K., W. Yurcik, and A.J. Lee, *NVisionIP: netflow visualizations of system state for security situational awareness,* in *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*. 2004, ACM: Washington DC, USA. p. 65-72.
14. Xiaoxin, Y., et al. *VisFlowConnect: providing security situational awareness by visualizing network traffic flows*. in *Performance, Computing, and Communications, 2004 IEEE International Conference on*. 2004.
15. Yin, X., et al., *VisFlowConnect: netflow visualizations of link relationships for security situational awareness,* in *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*. 2004, ACM: Washington DC, USA. p. 26-34.
16. Xiaoxin, Y., W. Yurcik, and A. Slagell. *The design of VisFlowConnect-IP: a link analysis system for IP security situational awareness*. in *Information Assurance, 2005. Proceedings. Third IEEE International Workshop on*. 2005.
17. Lai, J., H. Wang, and L. Zhu. *Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory*. in *Computational Intelligence and Security, 2006 International Conference on*. 2006.
18. Wei, H., L. Jianhua, and S. Jianjun. *A Novel Approach to Cyberspace Security Situation Based on the Vulnerabilities Analysis*. in *Intelligent Control and Automation, 2006. WCICA 2006. The Sixth World Congress on*. 2006.
19. Xiaowu, L., et al. *Network security situation awareness model based on heterogeneous multi-sensor data fusion*. in *Computer and information sciences, 2007. iscis 2007. 22nd international symposium on*. 2007.
20. Xiaowu, L., et al. *Multiclass Support Vector Machines Theory and Its Data Fusion Application in Network Security Situation Awareness*. in *Wireless Communications, Networking and Mobile*

Computing, 2007. WiCom 2007. International Conference on. 2007.
21. Liu, X., J. Yu, and M. Wang. *Network Security Situation Generation and Evaluation Based on Heterogeneous Sensor Fusion*. in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on*. 2009.
22. Yong, Z., T. Xiaobin, and X. Hongsheng. *A Novel Approach to Network Security Situation Awareness Based on Multi-Perspective Analysis*. in *Computational Intelligence and Security, 2007 International Conference on*. 2007.
23. Juan, W., et al. *Alert analysis and threat evaluation in Network Situation Awareness*. in *Communications, Circuits and Systems (ICCCAS), 2010 International Conference on*. 2010.
24. Li, Z., et al., *Towards Situational Awareness of Large-Scale Botnet Probing Events.* IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2011. **6**(1).
25. Preden, J., et al. *Situation awareness for networked systems*. in *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2011 IEEE First International Multi-Disciplinary Conference on*. 2011.
26. Barford, P., et al., *Employing Honeynets For Network Situational Awareness Cyber Situational Awareness*, S. Jajodia, et al., Editors. 2010, Springer US. p. 71-102.
27. Jiaquan, S., et al. *Study of Index Weight in Network Threat Evaluation Based on Improved Grey Theory*. in *Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on*. 2008.
28. Rongzhen, F. and Z. Mingkuai, *Network Security Awareness and Tracking Method by GT*. Journal of Computational Information Systems, 2013. **9**(3): p. 1043-1050.