Overview on Attack Graph Generation and Visualization Technology

Shengwei Yi[1,*], Yong Peng[1,2], Qi Xiong[1], Ting Wang[1], Zhonghua Dai[1], Haihui Gao[1], Junfeng Xu[1], Jiteng Wang[2], Lijuan Xu[2]
[1] China Information Technology Security Evaluation Center, Beijing, China
[2] Information Security Center, Beijing University of Posts and Telecommunications, Beijing, China
Correspondence to Shengwei Yi: yishengwei@foxmail.com

Abstract—**Network vulnerability can be analyzed automatically by attack graph. Attack graph tools can generate attack paths in network and show users the network vulnerabilities analyzing process for network security risk analysis. There are some problems such as state space explosion, the high complexity of algorithms, being difficult to demonstrate graphically, and so on, for attack graph generation and visualization techniques. Therefore, we surveyed and analyzed the attack graph generation and visualization technology. We summarized the open source tools like MulVAL, TVA, Attack Graph Toolkit, NetSPA and so on, and the commercial tools, for example, Cauldron, FireMon, Skybox View. We compared and analyzed these tools from the aspects of the attack graph types, scalability, or complexity of attack graph generation algorithm, the degree of attack graph visualization. Their common denominator was summarized, and their different points were analyzed. The future and applications for attack graph were forecasted, for example its applications in industrial control systems, and in the network security defense and risk assessment.**

Keywords-Attack Graph; Visualization; Attack Paths; Network Vulnerability Analysis

I. INTRODUCTION

Network Vulnerability Scanner can scan the target network by known vulnerabilities. However, all these known vulnerabilities are isolated, independent. While the nodes in the network are interconnected, a single vulnerability is unlikely to cause a great threat to the whole network. When multiple exploitable vulnerabilities are combined, interrelated and formed to be a vulnerability chain, an attacker can successfully reach the target resource according to the vulnerability chain. One or more vulnerability chains constitute an attack graph.

Attack graph can be used in a variety of network security risk analysis due to threats. Different attack graph tools have been developed by researchers for generation and visualization of attack graph. Attack graph tool is a dedicated tool for information technology security risk assessment, and is the basis of proactive defense for information security. It is impossible to deduce manually network security risks in medium-sized or even large-scale network due to the complexity of networks. The challenge can be solved by attack graph automatically. However, there is contradiction between the rapid growth of network size and the poor scalability and slow speed of algorithms for attack graph analysis tools.

Attack graph tool is used in intrusion detection, intrusion prevention, forensic analysis and others in the field of information security. For network operators, the attack graph tools can show users "why the network system is vulnerable to attacks? ", "how many different paths of attack or attack chains on the path from the entrance to targets for attackers?", "which attack path among paths is the most likely to be used by attackers?", "which attack paths or top-k paths are used the highest priority by attackers?".

For network managers, attack graph tools can be used to reduce security risks and intrusion defense. Attack graph tools can show users "what security measures are taken to defense attackers by managers?", "which security configurations can be done to effectively prevent the occurrence of attacking or truncate the attack path?", "does the network configuration comply with corporate security policies?".

Attack graph can be automatically to generate attack paths to analyze the network vulnerability. It can show users the weak point in the network analysis process for network security risk analysis. Once a potential attack path is found, attack graph tools can generate attack graph or attack trees to help system administrators understand how attacks happen, and then take defensive measures. Hypothesis analysis can be used in the attack graph to check the security robustness of the network configuration, and thus to protect unknown threats. However, there are difficulties in the attack graph generation and visualization techniques such as the explosion of state space, the high complexity of algorithms, being difficult to graphically demonstrate.

In the paper, we surveyed and analyzed the attack graph generation and visualization technology. We summarized the open source tools such as MulVAL, TVA, Attack Graph Toolkit, NetSPA and so on, and the commercial tools, for example, Cauldron, FireMon, Skybox View. We compared and analyzed these tools from the aspects of the attack graph types, scalability, or complexity of attack graph generation algorithm, the degree of attack graph visualization. Their common denominator was summarized, and their different points were analyzed. The future and applications for attack graph were forecasted, such as its applications in industrial control systems, and in the network security defense and risk assessment, and so on.

II. EXISTING TECHNICAL OVERVIEW

From the aspects of open source, attack graph type, scalability, or the complexity of attack graph generation algorithm, visualization, the typical attack graph analysis tools were reviewed in this section.

A. MulVAL

MulVAL (Multi-host Multi-stage Vulnerability Analysis), is an open source project in Kansas State University. The network and its security conditions and rules file are described by logic programming language Datalog. The rules file is parsed by the Prolog execution engine [1,2,3].

There is a command-line interface in MulVAL attack graph tool. The complexity of its algorithm is $O(n^2)$~$O(n^3)$. The input files include the vulnerability configuration file (default National Vulnerability Database, NVD), OVAL(Open Vulnerability and Assessment Language)/Nessus vulnerability reports file, the configuration file for host access control list. The attack graphs can be generated according to the logic execution engine.

Figure 1 interprets the framework of MulVAL attack graph tool. The framework includes five parts, i.e. interaction rules, security policies, logical execution engine, analytical database, unauthorized access and attack path tracing. Interaction rules are statements described by Datalog, which to specify the interactions and affect safety by different parts in the network. Given the configuration information in the analysis database, reasoning rules can simulate the behavior of the attacker in the network. Security policy states the attributes of security in the network managed and kept by system administrator. In MulVAL, the security policy is simple data tuples described in Datalog, which list the legal data access rules by system users. Based on the analysis database, interactions rules, security policy, logic execution engine can generate attack graph. Violations and attack path tracing can show users the textual or graphical (in pdf format) display of attack paths.

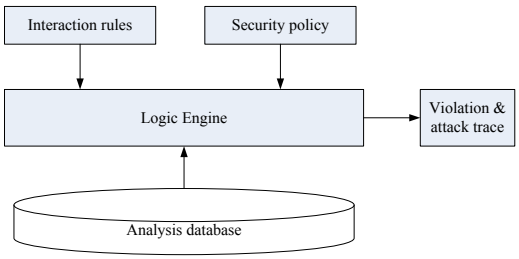

Figure 1. MulVAL Framework[3].

B. TVA

TVA (Topological Vulnerability Analysis) is an attack graph tool developed by George Mason University. It can analyze network vulnerability automatically and mine the weakness to generate the attack graph. TVA can establish the state transition diagram according to attack procedure and attack conditions, which makes network vulnerability analysis good scalability. TVA can generate attack graph according to the network topology to obtain the secure network configuration scheme[4,5] .

TVA relies on the information provided by Nessus vulnerability scanner. While the information may not be accurate and reliable, the further analysis is required. For large-scale network, a huge attack graph can be generated by TVA analysis results. How to manage the huge attack graph is a problem. The vulnerability mining process depends on manual input, an automated, standard knowledge acquisition tool is demanded. Figure 2 illustrates the TVA Architecture.

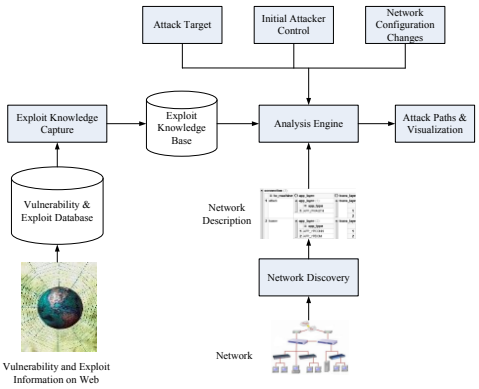

Figure 2. TVA Architecture[5].

C. Cauldron

Cauldron is the commercial version of TVA network topology vulnerability analysis tools developed by George Mason University in the United States[6]. There are three steps of the procedure of the Cauldron, firstly, collect all the information in the target network; secondly, the information is associated with known vulnerabilities data set; thirdly, the analysis of "What-if" rules and attack graphs display can be done by the Cauldron attack graph modeling environment.

Vulnerability scanners including Nessus, FoundScan can be used by Cauldron. The external vulnerability database includes the vulnerability databases, for example, NIST's National Vulnerability Database (NVD), the Open Source Vulnerability Database (OSVDB).

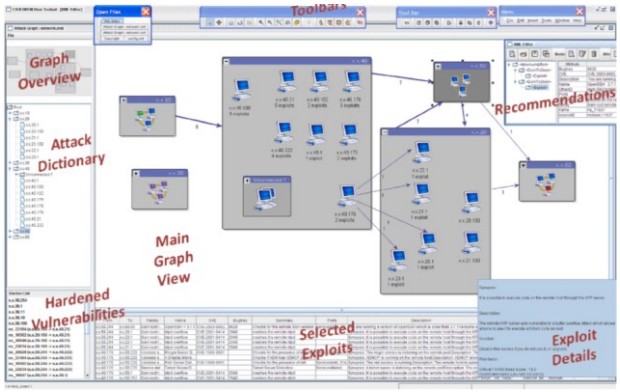

Figure 3. Cauldron attack graph tool's main interface[6].

Formerly, the complexity of the algorithm in the worst case in Cauldron is $O(n^4)$ or $O(n^6)$, where n is the number of hosts in the network. The complexity in the worst case is reduced to $O(n^2)$ after the algorithm improved.

Figure 3 shows the interface of Cauldron attack graph. Protection Domain can make the attack graph output intuitively clear. A Protection Domain is a collection of a group of machines visiting mutually in the network. A Protection Domain is that if an attacker control one machine in the Protection Domain, he can take control of all the machines in the Protection Domain. The main view to show the attack graph, graph overview to navigate the global, toolbars, attack dictionary, reinforced vulnerability database for hypothesis analysis, selected vulnerability and exploitation, recommendations, are included.

D. Attack Graph Toolkit

Attack Graph Toolkit is developed by Oleg in Carnegie Mellon University. The attack graph tool is based on Linux operating system platform, with a graphical interface and open source code[7,8,9]. The source code is no longer updated since 2007.

Attack Graph Toolkit is state diagram, state node represents the global state of network system. Node is state, edge is the state transition.

State graph is poor scalability, a long time to construct, difficult to adapt to large-scale networks, and even not apply to medium-sized networks. The complexity of attack graph generation algorithm in Attack Graph Toolkit is exponential.

Figure 4 shows the architecture of Attack Graph Toolkit. It consists of three main modules, network modeling tools, scene attack graph builder, a graphical user interface(GUI). The input includes network specification, host configuration, network configuration, actions libraries. Scenes attack graph generator builder can generate attack graphs by the results of network modeling tools.

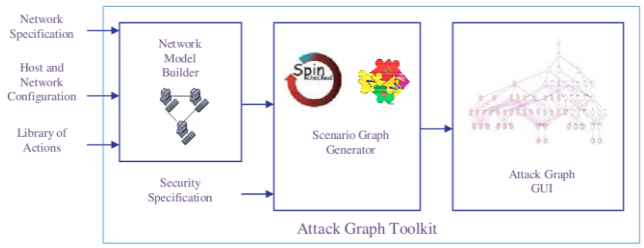

Figure 4. Attack Graph Toolkit architecture[7].

E. NetSPA

NetSPA (A Network Security Planning Architecture) is developed by Ingols and Lippmann in Lincoln Laboratory of MIT to show network attack graph[10,11]. It can identify the most valuable attack path from the network topology. NetSPA can identify the potential attack path to address the long-term threats. NetSPA uses a single host, the running services and network information to create the attack graph, showing how hackers infiltrate path. Network system administrator can check the attack graph visualization and decide what defensive action to be used. NetSPA is able to analyze the attack graph and proposes the suggestions on how to quickly repair the most serious weaknesses in the network.

A network vulnerability scanning analysis tool Nessus scan and get the network connection information and vulnerability information, and generate the attack graph according to the manual modeling infiltration rules and to store the rules into database. NetSPA can analyze the crucial "stepping stone" hosts. The vulnerability of the host become a key node to be attacked in the network compared with other nodes. It provides network administrators with the highest priority to be repaired, reduce the time to patch the host with the vulnerability and reduce the possibility of the host is penetrated by a hacker. Thus, we should defense the network at the first time from the possible network attacks. Figure 5 is the architecture of NetSPA.

The disadvantages of NetSPA are as follows.

- There are many loops in the MP(Multiple-Prerequisite) graph of NetSPA, it is difficult to understand for network administrators to manage the network effectively;
- There is no vulnerability information in the client;
- There is error for the division of single vulnerability, which may mistake the vulnerability of the client as one of the service to deal with.

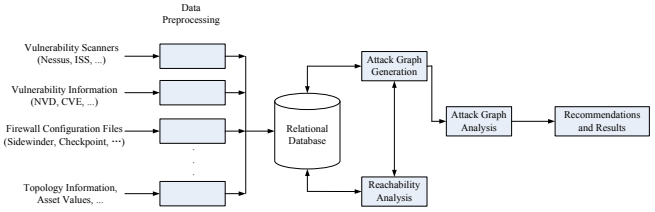

Figure 5. NetSPA System Architecture[10].

F. FireMon

FireMon is the commercial version of network security manager platform tool NetSPA[12].

The features of FireMon are as follows.

- Scenario Definition. The risk scenarios are defined and managed according to the sources of threats and vulnerabilities of assets. The likelihood exposed to the threat sources of the assets with the vulnerability can be assessed by risk analysis.
- Disclosure of Assets. There is a detailed description of the disclosure of a set of assets. For each asset group, it is determined by the severity of its vulnerability.
- Summary of Risk. After the definition of the scene, the network risk analyzer can measure the assets in the network based on the hierarchical division of the network. Generally, the risk is defined by the number of hosts, the total number of vulnerabilities, the total number of root privileges vulnerability.

The process of FireMon is as follows.

- The definition of risk assessment scenarios for the target network.

- After the definition of the scene, FireMon Risk Analyzer can disclose the risk of the assets.
- The summary report of the accessible assets and the potential vulnerabilities is provided.

Figure 6 shows the interface of FireMon attack graph tool.

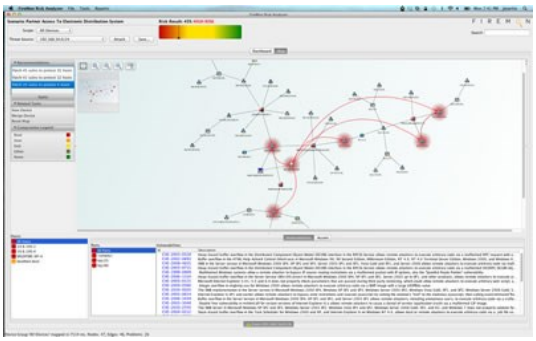

Figure 6. FireMon attack graph tool interface[12].

G. *Skybox View*

Skybox View is a commercial software of network assurance tools developed by Skybox Security Inc.[13,14]. It comprises network modeling, attack simulation, risk analysis reports. Skybox View attack graph tool has a clear and intuitive interface, as shown in Figure 7. Skybox Network Assurance tool can make the enterprise network manager be focus on the management of the equipments in the network, easy to identify the problems in the network, to diagnose the network security incidents, and to provide a detailed report for network security compliance.

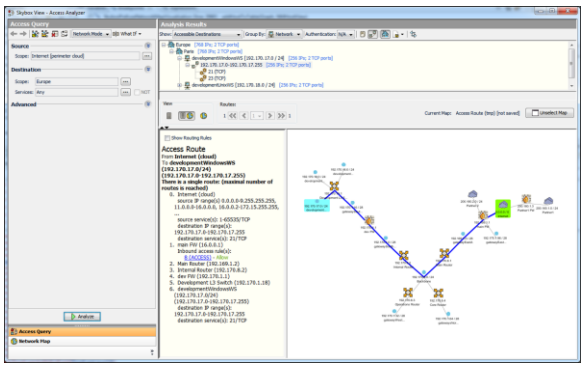

Figure 7. SkyBox View attack graph tool interface[13].

III. COMPARISON AND ANALYSIS

From the aspects of whether open source or not, developers, accessible way, attack graph type, scalability, intuitive and so on, we compared the attack graph tools above mentioned. The comparative results are shown below.

According to the above analysis, from whether open source, the computational complexity of algorithm, attack graph generation, etc., MulVAL has a better advantage compared with several other tools. Network security risk analysis can be developed based on the MulVAL attack graph presentation tool. The specific reasons are as follows.

- Both MulVAL and Attack Graph Toolkit are open source, other tools are commercial tools without source code or non-open academic research tools.
- The source code of Attack Graph Toolkit has been no further updated and maintained since 2007.
- From the complexity of attack graph generation algorithm, Attack Graph Toolkit can not support the medium-scale and large-scale network. The complexity of the algorithm of Attack Graph Toolkit is exponential While the complexity of the MulVAL algorithm is close to that of the commercial tool Cauldron algorithm, and better than several other commercial tools.

TABLE I. ATTACK GRAPH GENERATION AND VISUALIZATION TOOLS COMPARISON

Name	Developers	open source	Accessible	Attack Graph Type	Scalability	Intuitive level
Attack Graph Toolkit	Carnegie Mellon University	Yes	Free	State graph	Poor, construction time exponentially	Good. vertices are state node, edges are the state transition.
MulVAL	Kansas State University	Yes	Free	Logical attack graph (attribute attack graph)	Polynomial: $O(N^2) \sim O(N^3)$	Good
TVA	George Mason University	No	not open, difficult to obtain	Penetration dependency graph, aggregation attack graph	Polynomial: $O(N^3)$	Better. Vertex is a host or host group
Cauldron	PROINFO Company, George Mason University	Commercial Software	pay	Penetration dependency graph, aggregation attack graph	Polynomial: $O(N^3)$	Better. Vertex is a host or host group.
NetSPA	Massachusetts Institute of Technology	No	not open, difficult to obtain	MP (Multiple-Prerequisite) graph	O(N lgN)	Good
FireMon	FireMon Corporate, Massachusetts Institute of Technology	Commercial Software	pay	MP (Multiple-Prerequisite) graph	O(N lgN)	Better
Skybox View	Skybox Security, Inc.	Commercial Software	pay	unknown	Polynomial $O(N^3)$	Better. Vertex is the host.

A. *Common Analysis for Attack Graph Techniques*

According to the above attack graph generation and visualization tools, there are similarities on the architecture, interaction with the vulnerability database, visualization.

1) *Common architecture for attack graph tools*

The description of architecture and technical name of existing attack graph tools are different, but these techniques are basically three-tier architecture, as Figure 8, namely, the input layer of configuration information, the layer of attack graph analysis and generation, the layer of attack graph visualization.

The bottom is the layer of configuration information. Users can input the configuration information of network topology, the device, the vulnerability, and others. Some attack graph tools e.g. MulVAL, Cauldron, etc., can interact with the vulnerability scanners e.g. Nessus, Retina, FoundScan, etc., and even can input the vulnerability configuration information automatically.

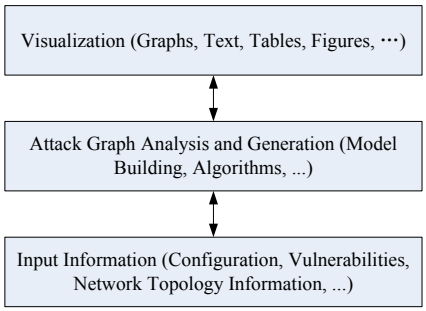

Figure 8. Common Architecture for Attack Graph Tools.

The middle is the layer of attack graph analysis, which includes the differences among the various attack graph tools above mentioned. However, the same point of all the attack graph tools is that they all need an attack graph analysis engine to build the attack graph model. The attack graph generation algorithm of attack graph analysis engine is different, and the requirements of the attack graph developers are different, thus, the attack graph analysis engine in the layer will generate different types of attack graph models, such as the properties attack graph of MulVAL, the state attack graph of Attack Graph Toolkit, the penetration dependency graph of Cauldron, and the multi-prerequisite graph of NetSPA.

The top is the layer of attack graph visualization. It received the result of the attack graph model from the middle layer, to show the attack graph and interact with users.

2) Common vulnerability database for attack graph tools

There are generally consistent vulnerability database interactions for all the attack graph tools, for example, the National Vulnerability Database (NVD) of the National Institute of Standards and Technology in the United States, the Open Source Vulnerability Database(OSVDB).

3) Common visualization for attack graph tools

Graphical interface is basically used in all the attack graph tools except MulVAL. No graphical interface is used in MulVAL tool, but its command-line user interface is also able to generate vector attack graph files in .eps and .pdf format to facilitate users to check the vulnerabilities in the network system.

B. Technical Differences for Attack Graph Techniques

In accordance with functions, attack graph tools can be divided into two categories, commercial tools and academic projects. Cauldron, FireMon Security Manager Platform and Skybox View are commercial tools. TVA, MulVAL, Attack Graph Toolkit and NetSPA are academic projects. The academic projects include open source ones and non-open source code ones. MulVAL and Attack Graph Toolkit are open source code projects. TVA and NetSPA are non-open source code projects.

Compared to the academic projects, the commercial tools such as Cauldron, Skybox View, FireMon have better visualization. They are clear and intuitive, easy to use. While, the open source tools are obscure, difficult to understand and use.

It is important that commercial tools are focus on the user experience. The nodes in the attack graph are the hosts. The open source projects are focus on the academic research. In order to show the attacker's invasion route as much detail as possible, the nodes in the attack graph are often the attack steps, for example, to get permission by a defective in the system.

Therefore, one method to enhance the visualization of open source tools is to modify the visualization of attack graph. The nodes in the graph are integrated into the protection domain used in the Cauldron tool.

IV. DIRECTIONS FOR FUTURE RESEARCH

The current mainstream tools on the attack graph generation and visualization are overviewed and analyzed, however there are still some studies can be done for these tools.

- Research on the application of attack graph generation and visualization technology in the industrial control system. Information security for industrial control systems has become a hot topic[15].There are differences between traditional IT networks and industrial control networks. There are the characteristics of real-time, availability in the industrial control network. The existing attack graph generation and visualization tools for IT systems can not be effectively used in risk analysis of industrial control network. It is urgent to research and develop a risk analysis tool for attack graph in the industrial control network. According to the features of real-time and availability, we apply the existing attack graph generation and visualization techniques to the field of industrial control networks, and study the risk analysis tools of attack graph in the industrial control network.
- Research on the challenges of the attack graph generation in the large-scale network. The advancement of computer technology and network communication technology promote large-scale application of networks. The nature of large-scale network has posed challenge to attack graph generation algorithm. The complexity of the attack graph generation algorithm increases dramatically as the network scale. According to the nature of the large-scale network, we should study the algorithm of attack graph generation for large-scale network, reducing the complexity of the algorithm to improve its applicability in large scale networks.
- Research on the information security defense techniques based on attack graph. There are many vulnerabilities in the hosts and network equipments in the network, which the vulnerabilities in the key nodes in the network cause great risk for network security. According to the methods of the attack graph generation and risk analysis, how to quickly find the key nodes in the network, which is the core of the information security defense techniques.
- Research on the risk analysis and risk prediction of attack graph in the big data. The algorithms of the data rules have been studied by mining from uncertain

data[16,17,18] and certain data[19,20,21,22,23]. We have accumulated a large amount of network operation log data as the continuous daily operation of network system. These include normal data of network activity, abnormal data of network activity, or even a network attack data. It is important that how to find the association rules between these undiscovered network attacks behaviors the mined data from the big data. We should do research the data analysis method of the big data and the algorithm of attack graph generation in the big data to generate undiscovered but occurred attack paths, and find the potential attack rules to be against unknown attacks in the network, thereby to prevent the occurrence of attacks of Advanced Persistent Threat(APT).

V. CONCLUSIONS

We have represented and analyzed the risk of networks by attack graph techniques, and have introduced the open source tools such as MulVAL, TVA, NetSPA, Attack Graph Toolkit, and so on, and the commercial tools, for example, Cauldron, FireMon, Skybox View. From the aspects of whether open source, the type of attack graph, scalability, or complexity of algorithms for attack graph generation, intuitive and visualization, etc., these tools are compared and analyzed. The common denominator is summarized, and their different points are analyzed. The future and applications for attack graph are analyzed, for example, applications in the industrial control systems, and applications in the network security risk assessment, and so on. We will focus on the attack graph risk analysis to be used in industrial control systems in the future.

REFERENCES

[1] http://people.cis.ksu.edu/~xou/mulval/

[2] Xinming Ou, Wayne F. Boyer, and Miles A. McQueen. “A scalable approach to attack graph generation”. Proceedings of the 13th ACM conference on Computer and Communications Security, 2006.

[3] Xinming Ou. A Logic-programming Approach to Network Security Analysis. PhD dissertation, Princeton University, 2005.

[4] http://csis.gmu.edu/TVA/

[5] Sushil Jajodia, Steven Noel, Brian O’Berry. “Topological analysis of network attack vulnerability”. Managing Cyber Threats: Issues, Approaches and Challenges. 2005.

[6] http://www.proinfomd.com/

[7] http://www.cs.cmu.edu/~scenariograph/

[8] Jeannette M. Wing. “Scenario graphs applied to security”. Proceedings of the NATO Advanced Research Workshop of Verification of Infinite State Systems with Applications to Security (VISSAS 2005), Timisoara, Romania, 2005, pp. 229-234.

[9] Jeannette M. Wing. “Attack graph generation and analysis”. Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2006, Taipei, Taiwan.

[10] http://www.ll.mit.edu/publications/labnotes/pluggingtherightholes.html

[11] Kyle Ingols, Richard Lippmann, and Keith Piwowarski. “Practical attack graph generation for network defense”. IEEE 22nd Annual Computer Security Applications Conference, 2006. ACSAC2006.

[12] http://www.firemon.com/products/riskanalyzer

[13] http://www.skyboxsecurity.com/products/network-assurance

[14] Gidi Cohen, “Proactive Security for a Mega-Merger”, http://www.skyboxsecurity.com/sites/default/files/Skybox_ProactiveSecurityForAMegaMerger_July2010_0.pdf, 2010.

[15] Yong Peng, Changqing Jiang, Feng Xie, Zhonghua Dai, Qi Xiong, Yang Gao. “Industrial control system cybersecurity research”. Journal of Tsinghua University(Science and Technology), 2012, Vol.52, No. 10, pp. 1396-1408. (in Chinese).

[16] Yongxin Tong, Lei Chen, Yurong Cheng, Philip S. Yu. “Mining frequent itemsets over uncertain databases”, in PVLDB 5(11), pp. 1650-1661, 2012.

[17] Yongxin Tong, Lei Chen, Bolin Ding. “Discovering threshold-based frequent closed itemsets over probabilistic data”, in Proceedings of the 28th International Conference on Data Engineering, (ICDE 2012), pp. 270-281, 2012.

[18] Yongxin Tong, Lei Chen, Philip S. Yu. “UFIMT: An uncertain frequent itemset mining toolbox”, in Proceedings of the 18th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, (KDD 2012), pp. 1508-1511, 2012.

[19] Yongxin Tong, Li Zhao, Dan Yu, Shilong Ma, Zhiyuan Cheng, Ke Xu, “Mining compressed repetitive gapped sequential patterns efficiently”. in Proceedings of 5th International Conference on Advanced Data Mining and Applications, (ADMA 2009), pp. 652-660, 2009.

[20] Yongxin Tong, Shilong Ma, Dan Yu, Yuanyuan Zhang, Li Zhao, Ke Xu, “Discovering compatible Top-K theme patterns from text based on users' preferences”. Pacific Asia Workshop on Intelligence and Security Informatics, (PAISI 2009), pp. 130-142, April 27, 2009.

[21] Shengwei Yi, Yuanyuan Zhang, Tianheng Zhao, Shilong Ma, Jie Yin. “Efficient sequential generator discovery over stream sliding windows”. Advanced Science Letters, 2012,11(1), pp. 437-442.

[22] Shengwei Yi, Tianheng Zhao, Yuanyuan Zhang, Shilong Ma, Jie Yin. “SeqGen: Mining sequential generator patterns from sequence databases”. Advanced Science Letters, 2012,11(1), pp. 340-345.

[23] Shengwei Yi, Jize Xu, Yong Peng, Qi Xiong, Ting Wang, Shilong Ma. “Mining frequent rooted ordered tree generators efficiently”. 2013 IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2013).