International Journal of Security and Its Applications
Vol. 10, No. 11 (2016), pp. 23-32
http://dx.doi.org/10.14257/ijsia.2016.10.11.03

Research on Network Defense Graph Model in Network Security

Feng Qi[1] and Haili Xu[2,*]

[1,2]*Jiamusi College, Heilongjiang University of Chinese Medicine, Jiamusi 154007, China,*
[1]*qifeng0012@hrbeu.edu.cn,* [2]*xuhaili31@126.com*
[2,]**Corresponding author*

Abstract

Security analysis and attack-defense modeling are effective method to identify the vulnerabilities of information systems for proactive defense. The attack graph model reflects only attack actions and system state changes, without considering the perspective of the defenders. To assess the network information system and comprehensively show attack and defense strategies and theirs cost, a defense graph model is proposed. Compared with the attack graph, the model makes some improvements. Defense graph will be mapped to the attack and defense game model, in order to provide a basis for active defense policy decision. What's more, a generation algorithm of defense graph is proposed. A representative example is provided to illustrate our models and generation algorithm.

Keywords*: Network Security, Active Defense, Defense Graph*

1. Introduction

With rapid development and extensive application of of Internet, network security attack emerges one after another. Attacker's motivation is more inclined to economic benefits. Network security has become an increasingly prominent problem to country and various organizations. Statistical researches on lots of network security events reveal that most network attacks made use of weakness of network information system [1-8]. Most of attackers followed a series of steps to realize their objective. The time and space sequence and span of attacking steps are associated with attacker's technique level, utilization of vulnerability, priori knowledge and attacking position. To easily prevent and detect network attack as to make relative counter measures, it's necessary to analyze network safety and describe and model such attack [8-14]. Network security analysis and attack-defense modeling is effective way to know better network security problem and take proactive defense [15-18].

Network security analysis is performed as to create a simple, practical and accomplished model [19-20], thus to detect and discover new vulnerabilities and describe possible permeation of known vulnerabilities utilized by attacker and complete picture of state variations. According to different security analysis purposes, network security analysis method includes two kinds:

(1) Analyze security of network protocol and applications by means of protocol detection and fault injection, of which the purpose is to find new weakness;

(2) Make formalized depiction of known system weakness and modeling and study the connection between vulnerabilities, as to discover and build any attack path possibly taken by attacker.

For network security modeling, it should try to avoid too complicated system states from causing state space explosion [21-22]; otherwise, it can't be used practically. The study on using attack graph method for network security modeling has made big progress

ISSN: 1738-9976 IJSIA

and the method is widely used for network security analysis. Attack graph is collection of attacking routes probably taken by invader for attacking target network. Attack path is sequence of attack actions taken by attacker for its purpose. Network attack graph reflects network attack behaviors possibly taken by attacker and dependence relationship between those behaviors. Such graph analyzes for modeling from the perspective of attacker, which indicates only attack action and changes of system states, not considering defender [23-24]. The essence of network security is game between attacker and defender behind the network, e.g. attacker attempts to utilize vulnerabilities to launch attack; while defender manages to install system patches and formulate defending strategies. So network security modeling should be analyzed from the part of attacker and defender, with defensive strategy and attack-defense strategy cost estimation relating to each attack action included in security analysis and decision to represent fully the essence of offense and defense [25].

At present, active security defense technology based on network security modeling has become research hot, because compared with traditional passive defense technology, the proactive defending technology based on network security modeling can help user recognize beforehand network system weakness and potential security threats. Then, as per security requirements, user can choose active security defensive measures and strategies in line with the optimal cost effect, so as to avoid occurrence of dangerous events and impairment to the system.

By introducing defense graph model in the paper, we improved and extended attack graph, evaluating network information system security and reflecting fully network defense strategy and the cost situation, in order to map defense graph model to attack-defense gambling model and use it as basis of proactive defense decision in network security attack-defense. A defense graph generative model is proposed [26]. Network security modeling method based on that model is experimentally validated. Here we try to make comprehensive assessment and model network security attack-defense situation through defense graph model, providing information foundation and basis for building attack-defense game model and making decision in the following.

2. Defense Graph Model

Attack graph is collection consisted of attack paths possibly taken by attacker when assaulting target network. Attack path is sequence of attack actions taken by attacker. Attack graph reflects attack action and system state changes, without considering defense strategy and attack-defense strategy cost estimation relating to each attack action. To appraise network information system security and fully reflect network attack-defense strategy and the cost, and to create model of attack-defense game model and provide decision-making foundation for active defense, we improved attack graph model and present defense graph model.

2.1 Defense Graph Model Definition

Definition1: defense graph (DG), Defense graph is a six triple, $DG = (s, \tau, s_0, s_s, s_a, s_d)$, of which S is collection of picture node; each node refers to one kind of network security state; $\tau \subseteq S \times S$. τ is network security state transition relationship; $S_0 \subseteq S$. S_0 is initial network security initial set; $S_a \subseteq S$ is set of attacker's target states; S_a is set of attacker's strategies; S_d is set of defender's strategies.

Defense graph is directed graph; node stands for one network security state, representing network's resource attribute and user or attacker's accessing ability to the entire network. Directed graph indicates transition relationship of various atomic attack

made by attacker from a network security state to a new one and attack cost for / attack benefit from the transition. The change of such transition can manifest as file modification, system configuration change, executable program running and privilege elevation of attacker. S_a is set of attacker's all attack path from initial node to target node, i.e. set of attack strategies. Each attack path is sequence of one or more atomic attack. Every atomic attack or attack strategy is corresponding to a series of defense strategy. All defense strategies form S_d .

Figure 1 describes defense graph $DG = (s, \tau, s_0, s_s, s_a, s_d)$, $S = \{A, B, C, D, E, F, H, I, J\}$ generated by one network system, circle marked with letter meaning node state set. $S_0 = \{A\}$, use filling green circle to mean initial network security state. $S_s = \{H, I, J\}$, use filling red double circles to mean attacker's attack state. Directed edges noted with atomic attack name and attack benefit refer to state transition relation, as seen in a1: 30 means atomic attack a1 makes network transit from state A to B, attack benefit being 30. $S_a = \{a1, a2, a3\}$, $S_d = \{d1, d2, d3\}$ .Boxes marked with defense strategy name and benefit mean defensive strategy of each attack path; possible defensive strategy of attack path changing from state A to I is respectively d1 and d2. It is shown in Figure1.

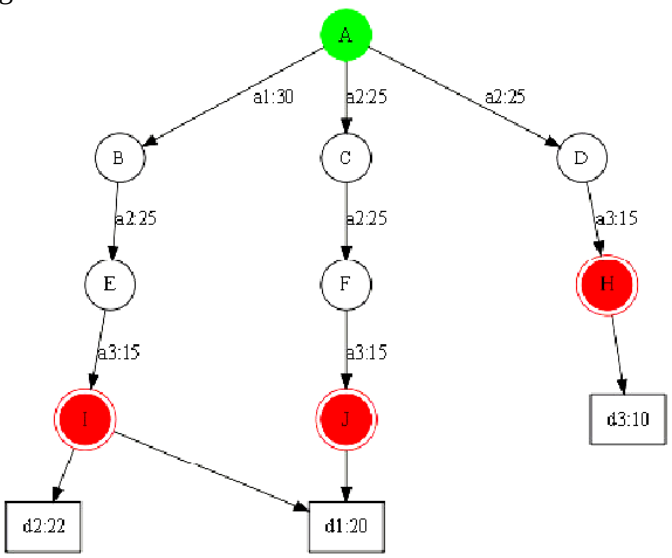

Figure 1. Example of Defense Graph

2.2 Generation of Defense Graph

2.2.1 Network Attack-defense Modeling

One main objective of network security analysis based on attack-defense modeling is to investigate changes of possible permeation into known network vulnerabilities by attacker and how defender defends attack. Attack-defense modeling needs a simple, flexible and perfect model, avoiding too complicated system state space. From the part of attacker's privilege elevation, the paper proposed a network attack-defense modeling method which is consisted of network host-based model, network connection relation model, attack-defense template library and attacker model.

(1) Network host-based model

The network host here includes server and personal computer (PC), without other connecting devices. One host in the network is expressed by a triple (Id, Svcs, Vuls); where Id is host's only identifier; it can be host's IP address and also its name. Svcs is list information of various services which run on the host. Vuls is list information of vulnerabilities existing on the host. The list may contain design weakness of host's hardware and software, implementation or configuration vulnerability. Network host-based model describes mainly PC and server in the network and their open services and vulnerability information.

(2) Network connection relation

Network connection relation refers to service accessing relationship which logically appears between two hosts. The relation can be expressed by a triple (SId, Did, Port), where SId means connected source host; Did means connected destination host; Port is port set of source host connecting to destination one. Port=Φ implies no connecting relation between source and destination host; Port=-1 means local connection, i.e. source host same with destination host; (h1, h2,(21,25,80)) means h1 connecting h2 through port 21,25,80 as to access HTTP,FTP,SMTP service.

(3) Offensive-defensive template

Offensive-defensive template lists out rules followed by attacker to launch attack by utilizing network vulnerability and defender to do prevention. Attacker's attack and control of network is manifested on the control of entity components in network, i.e. attacker's acquisition of privilege of entity components. Defense graph expresses network security state as attacker's capability (i.e. privilege) to access each network entity component.

Definition2: a privilege is a (x, m) pair; where x is an object; m is a non-empty accessing model collection of subject to object x; legal authorization must be got before modification of m.

Definition3: privilege function $f(x,m)$ is a monotone increasing function, meeting properties of mathematical monotonic function. Through utilization of weakness, attacker's privilege collection changes from Capability to Capability', i.e. there's an object x' and non-empty accessing model collection m'. Hence it's believed that attack gets privilege elevation.

Attack actions lead to changes of network security states, i.e. changes of attacker's privilege state in each component. In general, attacker's privilege state collection can be defined based on specific network system environment. Here attacker's privilege state is divided into four types: no privilege, remote access privilege, local user privilege and root privilege. It is shown in Table1.

Table 1. Taxonomy of Privilege Level

classification	describe
Without any privilege (None)	No privilege on the system
Remote access privilege (access Remote)	Remote access to the user, you can remote access to network services.
Local user privilege (User)	System for ordinary users, with independent private system resources
Root privilege (Root)	The system administrator user, has a host of resources

The above four privileges sorted from low level to high level are in order: no privilege<remote access privilege<local user privilege<root privilege. Privilege elevation status mirrors the attack evolutionary process of attacker. Complete network security state graph reflects combination of various attack actions possibly taken by attacker as to reach its invasion purpose. Take for instance, if an attacker already has local user privilege for one network entity component, he won't attack again the component as to get privilege lower than local user privilege. Attacker's privilege elevation of entity components includes vertical enhancement on single component and horizontal lift of various components towards attack target.

(4) Attacker model

Attacker property is expressed with following five triple (Id ,Prvl_list,Conn_list ,Target , Max_steps); in it, Id is identifier of attacker's host; Prvl_list is list of attacker's rights being authorized to all hosts in the network in initial state. Generally speaking, remote attacker has root authorization to its local computer. If attacker wants to make attack, it must get certain rights to visit some hosts in the target network; otherwise it can't do assault. Conn_list describes connection relation between attacker's host and others in target network. Target is invader's attack target. The realization of attack target needs several temporal and spatial stages. However, attacker always expects to finish attack in the quickest, most cost-saving and easiest way. We can confine attack steps Max_steps in the hope of reducing defense graph space explosion. User can assign value to Max_steps as per actual needs; Max_steps=0 means no setting of attacker's attack steps.

2.2.2 Generation of Defense Graph

1. Generation of Module Frame Diagram

The modeling and generation of defense graph need information like configuration files of firewall and router, network vulnerability scanner, vulnerability database, attack-defense strategy cost quantification model and attack-defense template rules. The specific module diagram is shown in Figure2.

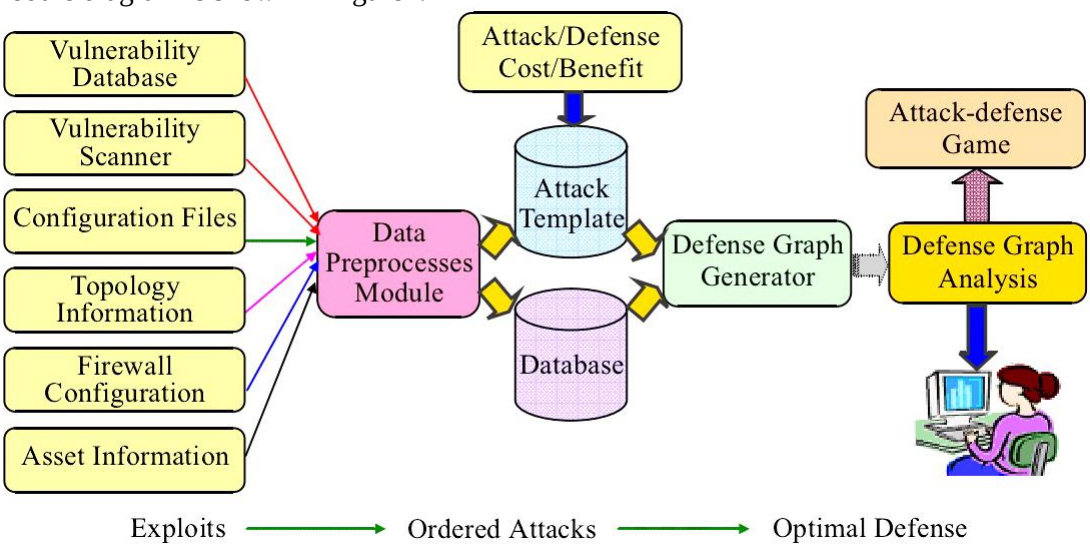

Figure 2. Architecture of Defense Graph Generation System

2 Generative Algorithm and Ideas

The algorithm and ideas are generated with reference to existing attack graph. We

analyze the procedure of attacker's attacking on network system form the part of attacker. At first, attacker scans target network from available computer, collecting information like network system topology and vulnerabilities; then it launches attack of weak hosts. After attack action is finished, attacker's privilege for the computer is raised and it gains certain root, thus able to acquire system information without authorized access, or with it as springboard, it can other hosts which the host can visit and which have vulnerabilities, and so on, till attacker achieves its final attack goal. Attacker's attack is characteristic of complexity, intelligence and temporal and spatial multi-stages.

Researches show that in attack graph generative algorithm, monotonicity hypothesis is made about attack, which helps reduce greatly the number of attack graph nodes and edges. Suppose CMU researchers do testing on five hosts with eight vulnerabilities. By means of NuSMV tool without monotonic hypothesis, they spent around two hours in producing the attack graph which contains 5948 nodes and 68364 edges [27]. But Amann et al. [28] used attack monotonicity hypothesis to produce an attack graph containing 229 nodes. Attack monotonicity hypothesis accords to most network analysis environment, suggesting it has rationality.

3 Algorithm Descriptions

Based on the above defense graph generative algorithm and ideas, we present an attack-defense path generative algorithm which bases on attacker-oriented privilege monotonic increase and breadth-first. Algorithm described in detail as shown in algorithm 1.

Defense graph generation algorithm1

Input: Host, Connection, Attack_template and related parameters
Output: Defense map DG
1 .Initial host Id and permission to join the queue;
2. Generate the initial network state node;
3.While (network host queue host_queue is not empty)
4 Take host_queue 1 host;
5 If (input specifies the target to achieve full & &target)
6 Continue
7 While (permission queue prvl_queue is not null)
8 Take prvl_queue 1 user rights;
9 Generates a new connection host queue con_host_queue;
10 According to the current host ID Query the host connection, will connect with the host all the host Id to join.
11 If (host Id is not in host_queue)
12 Be connected to the host Id join host_queue;
13 While (con_host_queue is not empty)
14 Take con_host_queue in the 1 host, construct the current attack host can access the host port queue port_queue;
15 While (port_queue is not empty)
16 Take port_queue 1 port;
17Structure and port related offensive and defensive template queue attack_template_queue
18 While (attack_template_queue is not empty)
19 If (attack elevated permissions not in prvl_queue.)
20 Permission to join prvl_queue;
21 Output attack path;
22 Uusing graphical tools Graphviz the output of the generated defense graph DG;
23 DG return

4. Experimental Analysis and Results

We use attack graph to generate typical network topology. Attacker's host is IP0; target network is switching network; IP1, IP2 are both Linux host. It is shown in Table2.

4.1 Connection Information

Firewall separates target network and external network, allowing external hosts only to access IP1's FTP, SSH service and IP2's FTP service. In initial state, we assume attacker has root authorization to access host IP0 and remote accessing privilege for host IP1 and IP2. It is shown in Table3.

Table 2. Host Information Descriptions

Id	Svcs	Vuls
ip1	ftp, ssh	sshd buffer overflow(CVE-1999-1455),ftp .rhost overwrite
ip2	ftp, database	ftp .rhost overwrite, local buffer overflow

Table 3. Connection Relation

Id	ip0	ip1	ip2
ip0	-2	23,24	21
ip1	Φ	-2	21
ip2	Φ	23,24	21

4.2 Offensive and Defensive Template Rule Construction

Suppose attacker's target is to get root privilege of IP2. Although attacker's host IP0 can't visit IP2, due to existence of host vulnerability and dependence relation, attacker can realize attack by taking actions as shown in Table 4. The table lists other cost quantifying information as well like attack type, criticality and attack benefit.

Table 4. Description of Attack Action

Symbol	Name	Category	AL	Att_return
a1	Ftp .rhost attack on Ftp Sever	User	8	420
a2	Sshd Buffer overflow	Root	11	600
a3	Local Buffer Overflow	Root	11	1500

Through analysis of host weakness and attack actions, selecting available defensive strategy from the strategy base, considering when there's no defensive measures, and quantifying defense cost, we can complete offensive-defensive template construction. It is shown in Table5.

Table 5. Description of Defense Action

Symbol	Name	Ocost	Ncost
d1	Patch Ftp .rhost on Ftp Sever	50	0
d2	Close rsh on Ftp Sever	10	120
d3	Close Sshd on Ftp Sever	10	120
d4	Patch Sshd on Ftp Sever	50	0
d5	Patch the Database	50	0
d6	No action	0	0

Using the information of the host, the network connection, the attack and defense movement and so on. The construction of offensive and defensive templates, rules are as follows:

Rule1=（a1, Root, Remote access, ftp .rhost overwrite, 21, User, 420, ｛（d1, 50）, （d2, 130）, （d6, 0）｝）；

Rule2=（a2, Root, Remote access, Sshd Buffer overflow, 22, Root, 600, ｛（d3, 130）, （d4, 50）, （d6, 0）｝）；

Rule3=（a3, User, User, Sshd Buffer overflow, -1, Root, 1500, ｛（d5, 50）, （d6, 0）｝）.

4.3. Defense Graph Generation

Based on the algorithm1, the network defense map obtained by the automatic analysis of the above model was analyzed by Graphviz. It is shown in Figure3.

State S1 said the attacker's initial state, filled with red double circle node S5, S10, S11 said the attack on the IP2 to obtain Root privileges, to achieve the target. A box attached to the destination node indicates the defense strategy of the attack action on the path.

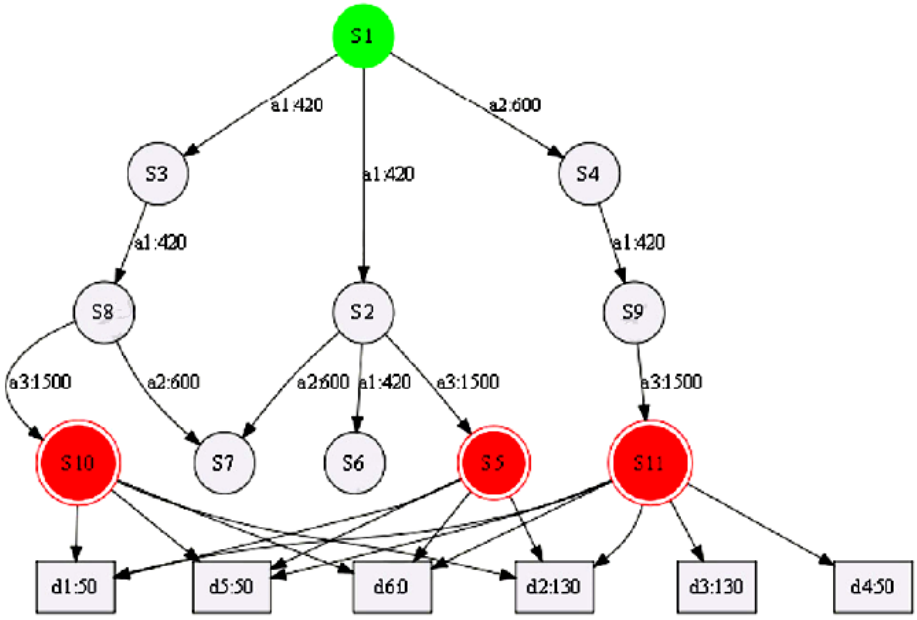

Figure 3. Defense Graph of Network Example

5. Conclusion

In this paper, Attack graph considers attack actions and system state changes only from the part of attacker without defender. To address the problem, we introduced network defense graph model to have improved and extended the attack graph. Defensive strategy and relative cost estimation of each attack action are altogether included in security analysis, to reflect comprehensively the nature of attack and defense. Firstly, we profiled network security modeling method; then introduced defense graph model and gave definition; next we described formally host information model, network connection and attack-defense template. On that basis, we proposed a defense graph generative algorithm and experimentally demonstrated the network security modeling method based on that model.

References

[1] Jiang Weixin, Fang Binxing, Tian Zhihong, Zhang Hongli. Based on attack defense game model of network security evaluation and optimal active defense. Chinese Journal of computers, 2009,04:817-827.
[2] Liuxin, Tiancheng, Mari, Jing Jun double. A kind of improved information network security defense graph model and method for generating research. Shandong Electric Power Technology,2014,01:7-10
[3] Li Qianmu, Liu Gang, Zhang Hong. A method for the generation of network security defense strategy based on state attack defense graph model. Computer application, 2013, S1:121-125.
[4] The research and experiment of network attack and defense strategy and active defense based on game theory. Computer application and software, 2013,09:312-315.
[5] Zhang Dehong. Research on offensive and defensive strategies and active defense in network security. Journal of natural science of Harbin Normal University, 2012,02:49-53.
[6] Li Qun. Network security decision making based on attack graph. Jiangnan University, 2015
[7] Jia Wei. Research on the evaluation method of computer network vulnerability. University of Science & Technology China, 2012
[8] Wang Chunzi. Research on Modeling and security evaluation of complex network attacks. Xi'an University Of Architecture And Technology, 2011
[9] Zhao Zhenguo. Network security evaluation and optimal active defense based on offensive and defensive game model. Electronic test, 2015,02:62-64.
[10] Cai Jianqiang. Research on network vulnerability assessment based on game model. North China Electric Power University, 2011
[11] Li Xuezhen. Network system security analysis and decision technology research based on game theory. Harbin Engineering University, 2011
[12] Jiang Weixin, Fang Binxing, Tian Zhihong, Zhang Hongli. Based on attack defense stochastic game model of defense strategy selection of. Computer research and development, 2010,10:1714-1723.
[13] Wang Huimei, sharp, Wang Guoyu. An algorithm for network attack strategy based on extended network attack graph. Journal of electronics and information, 2011,12:3015-3021.
[14] Jiang Weixin, Fang Binxing, Tian Zhihong, Zhang Hongli. Based on attack defense game model of network security evaluation and optimal active defense. Chinese Journal of computers, 2009,04:817-827.
[15] Liuxin, Tiancheng, Mari, Jing Jun double. A kind of improved information network security defense graph model and method for generating research. Shandong Electric Power Technology, 2014,01:7-10
[16] Li Qianmu, Liu Gang, Zhang Hong. A method for the generation of network security defense strategy based on state attack defense graph model. Computer application, 2013, S1:121-125.
[17] Ruan tiquan. The research and experiment of network attack and defense strategy and active defense based on game theory. Computer application and software, 2013,09:312-315.
[18] Liu Liu. Safety evaluation of power communication transmission network for SCADA service. North China Electric Power University, 2013
[19] Li Qun. Network security decision making based on attack graph. Jiangnan University, 2015
[20] Liu Liu, Gao Huisheng, Li Cheng. Evaluation model of electric power SCADA system transmission network security. Electronic Science and technology, 2012,12:116-119.
[21] Zhang Dehong. Research on offensive and defensive strategies and active defense in network security. Journal of natural science of Harbin Normal University, 2012,02:49-53.
[22] Li Yan. Research on network attack and evaluation model based on T-G protection system. Xi'an University Of Architecture And Technology, 2010
[23] Wang Yongjie, bright, Liu Jin, Wang Guoyu. Research on network security evaluation based on attack graph model. Journal of communication, 2007,03:29-34.

[24] Zhao Zhenguo. Network security evaluation and optimal active defense based on offensive and defensive game model. Electronic test, 2015,02:62-64.
[25] Wu Renzhi. Analysis on the status quo of computer network security and defense technology research. Henan science and technology,2016,04:4-18
[26] Wang Wang. Research on computer network security and defense. Computer knowledge and technology, 2016,16:83-84.
[27] Sheyner, J Haines, S Jha, et al. Automated Generation and Analysis of Attack Graphs. Proceedings of IEEE Symposium on Security and Privacy, 2002. 273-284
[28] Paul Ammann, Duminda Wijesekera, Saket Kaushik. Scalable, graphbased network vulnerability analysis. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA. 2002: 217-224

Authors

Feng Qi, He received his B.S degree from Qiqihar University and received his M.S degree from Harbin Engineering University. He is a Teaching Assistant from Jiamusi College, Heilongjiang University of Chinese Medicine. He is in the research of Network security, Opportunistic network, Network coding.

