International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.359-368
http://dx.doi.org/10.14257/ijsia.2016.10.12.29

Computer Network Vulnerability Assessment and Safety Evaluation Application based on Bayesian Theory

Xianyou Zhu

Hengyang Normal University, Hengyang, Hunan 421002, China
zxy@hynu.edu.cn

Abstract

Computer network vulnerability analysis is a method of analysis and evaluation of network security beforehand. The attacks method has occurred in the network, the previous network status change as input information, calculated by the model analysis. Forecasting network node may be network attacks given the current security level value network, network security reinforcement measures taken before the danger. Administrators can proactively identify network security issues, to take measures in advance to avoid information leakage, financial losses, ensure the safety of individuals and countries. Therefore, vulnerability analysis computer network is very important. Based on the properties of attack graph shows the method of attack graphs to Bayesian network transformation, using the new algorithm to eliminate loops attribute attack graph optimization, building the Bayesian attribute attack graph model used to evaluate the network itself security situation. In this model, based on Bayes formula for calculating the probability of a new node probability calculation formula and attack paths occur for calculating network vulnerability assessment of the quantitative indicators. The model not only can visually process description of cyber attacks, but also into the Bayesian network probabilistic thinking of possible network attack path prediction and assessment.

Keywords*: Quantitative evaluation; Bayesian network; Exponential distribution; attribute attacks*

1. Introduction

Development of computer networks has accelerated the process of information developments [1, 2]. People on the network can easily access a variety of information to people learning resources, recreation resources of interest [3]. Some of this server sharing information distributed in the network, workstations, some flow between network nodes [5-7]. With the increase of users to share information, the value of these resources is also growing. Internet social progress and national economic development provides an important driving force [8]. With the rapid development of the Internet and the information process, the Internet has penetrated into every aspect of people's lives, shopping from e-commerce, online travel to travel, entertainment, social networking, online education to the network. People's basic needs are inseparable from the computer network. Computer network allows people to work more efficiently [9, 10]. B2B, B2C, C2C, O2O development for people's economic activities provides a richer platform. People's work, life and the Internet have been fused together. Its role in the social development process is growing [11].

With the rapid development of the Internet in recent years, the number of vulnerabilities in the network maintains higher amount of growth, growth in 2014 reached a maximum of 7412 vulnerabilities, mainly high-risk and moderate-risk vulnerabilities [12]. If these network security vulnerabilities being exploited by hackers network, computer network will likely be attacked, leading to information disclosure, network paralysis and other dangerous events [13]. In recent years, network attacks occur

ISSN: 1738-9976 IJSIA

frequently, according to the relevant information in the global Internet, the frequency of network attacks can reach average occur once every 20 seconds.

Computer network vulnerability analysis is a method of analysis and evaluation of network security beforehand, the method of the attacks have occurred in the network, the previous network status change as input information, calculated by the model analysis, forecasting network node may be network attacks given the current security level value network, network security reinforcement measures taken before the danger. Administrators can proactively identify network security issues, to take measures in advance to avoid information leakage, financial losses, ensure the safety of individuals and countries. Therefore, vulnerability analysis computer network is very important. Based on the properties of attack graph shows the method of attack graphs to Bayesian network transformation, using the new algorithm to eliminate loops attribute attack graph optimization, building the Bayesian attribute attack graph model used to evaluate the network itself security situation. In this model, based on Bayes formula formula for calculating the probability of a new node probability calculation formula and attack paths occur for calculating network vulnerability assessment of the quantitative indicators. The model not only can visually process description of cyber attacks, but also into the Bayesian network probabilistic thinking of possible network attack path prediction and assessment. In order to develop an effective defense strategy to provide a reliable basis for the network administrator to get the maximum safety benefits with the least cost.

2. Network Security Evaluation Theory

2.1 Attack Graph Technology

Attack graph model is a mathematical graph theory methods described attacks during the detailed information it contains all possible network attack paths [14]. Use attack graphs can be very intuitive display the details of network attacks, including: the starting point of attack, attack targets, the use of vulnerability information. In an attack graph node can have more than one parent, can represent multiple attackers path to multiple targets simultaneously attack graph model also supports inductive and deductive reasoning. Many scholars of the attack graph depth research, made a lot of types of attack graph, but summed up can be divided into: state diagram attack, attack graph properties, permeability dependency attack graphs, attribute dependency attack graphs, logical attack graphs.

For the state explosion problem state attack graph, Shamshirband [15] conducted in-depth research, the properties of attack graphs. It contains two nodes: node atomic attack; attribute node. In attribute attack, the attack represents causality premise atomic properties and results between attributes, and only when all prerequisites are satisfied properties atomic attack, the attack may have occurred and the results obtained control over property. In the Properties attack graph (Figure 1), ellipse attribute node, text represents an atomic attack. By comparison can be found, the relatively small size attribute attack graph, and therefore more suitable for the analysis of complex networks. However, the figure often attribute attack loop, not easy to analyze and understand.

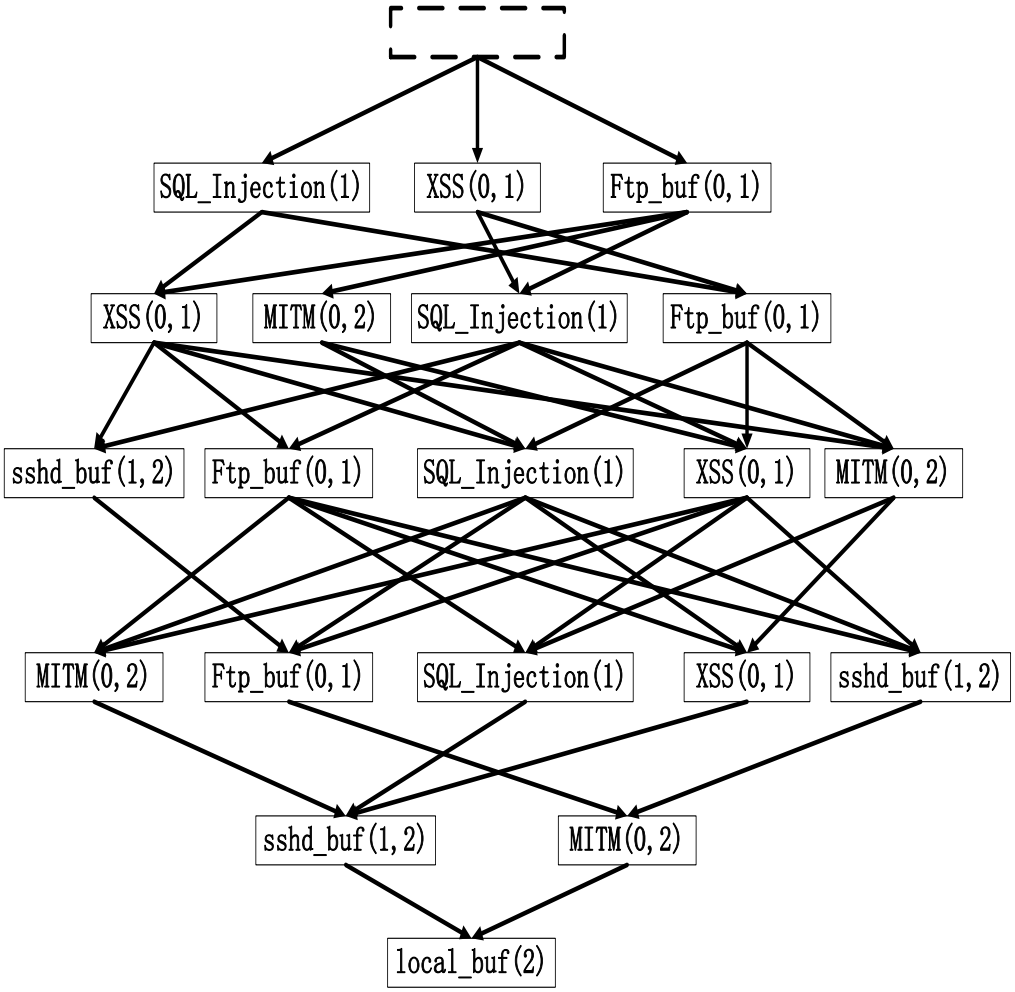

Figure 1. State Attack Graph

2.2 Bayesian Attribute Attack Graph Vulnerability Assessment Method

Attribute attack graph is a directed acyclic graph with GRA = G <A, V, E>, where A represents an attribute node set, ai represents an attribute node; V representatives atomic attack node set, vi represents an atomic attack node; E represents a collection of inter-node edges, ei represents a directed edge.

Attribute attack graph GRA meet the following constraints:

(1) $E \in (A \times V) \cup (V \times A)$, that is, the set of edges E contains only A->V and V -> A, attribute nodes to atomic attack directed edge, atomic attack to attribute node directed edges.

(2) Let Pr (Vi) represents the parent node vi atomic attack node set, the attribute node to have a set of edges between nodes v atomic attack as: $E_{av} = P_r(v_i) \times v_i$, set Eav the edge in the relationship "with (and)" between the edge ei..

(3) Let Pr (ai) represents an atomic attack node ia parent node set, the atomic attack directed edge node v to a node between the set of attributes as: $E_{va} = P_r(a_i) \times a_i$, the edge yes "or (or)" in between the collection of Eva edge ei relationship.

Bayesian network exists between the nodes conditional independence relations, that is, for node vi, at a given parent Pre (vi), the conditions, iv and its nonsubtyped point V (vi)

independent of each other, you can use the formula express this relationship, see equation (1):

$$P_r\left(v_i \left| P_{re}\left(v_i\right)\right.\right) = P\left(v_i \left| P_{re}\left(v_i\right)\right.\right) \quad (1)$$

Each node has a conditional probability distribution in a Bayesian network, there is no parent node represents the a priori probability of these probability values are passed causal link between nodes. According to the prior probability of each node and the conditional probability distribution and conditional independence assumption can be derived node joint probability formula, see equation (2):

$$P_r\left(v_1, v_2, \cdots, v_i, \cdots v_k\right) = \prod_{i=1}^{k} P\left(v_i \left| P_{re}\left(v_i\right)\right.\right) \quad (2)$$

2.3 Network Security Elements

Existing common network protocols and services are generally based on TCP / IP protocol suite built. TCP / IP protocol suite is a set of different protocol combinations protocol family together to form a total of four levels, from bottom to top as follows: network interface layer, Internet layer, transport layer and application layer, as shown in Figure 2.

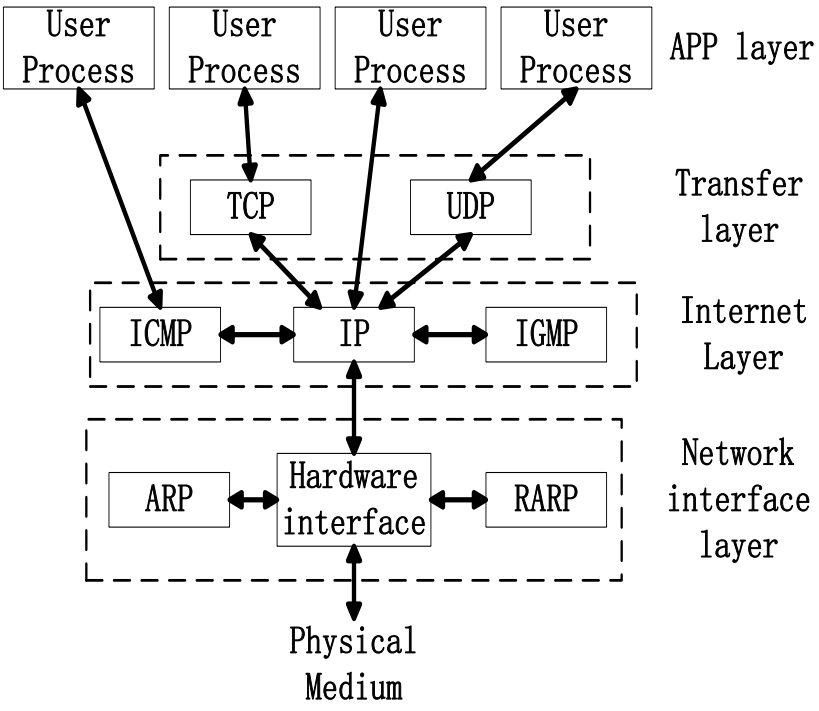

Figure 2. TCP/IP Protocol Family

The underlying network interface layer corresponds include OSI/RM (OSI reference model) physical layer and the data link layer. This layer is responsible for receiving IP packets and sent over the network, or the physical frame received from the network IP packets and sent it to the IP protocol. Network interface by the device driver is usually achieved. The layer of ARP and RARP are two types of network interface layer protocols implement IP address and MAC address conversion between. In the network interface layer to the ARP packets to deceive and take some deep Sniffer attack techniques down.

The application layer includes OSI / RM in the session layer, presentation layer and application layer, it contains the relevant certification, data processing and compression, enables applications to run directly on top of the transport layer to provide users with

services. For example, HTTP, FTP file transfer protocol belonging to the class protocol TELNET protocol is Telnet class protocol, SMTP e-mail protocol is protocol type, SNMP network management protocol belonging to class protocol. Therefore, different application layer corresponds to a different type of service, the network provides file, web, mail and other aspects of services.

3. Bayesian Attribute Attack Graph Model

3.1 Model Definition

Bayesian network, the node status and the probability of occurrence related only with its parent node. In the attack graph network vulnerabilities be exploited only if the attack path parent about this relationship in a Bayesian network node and attack the figure correspond. Bayesian network and attack graph is a kind of directed acyclic graph, and directed edges represent a causal relationship, so you can attack and Bayesian network diagram combining Bayesian attribute attack graph, the network quantitative assessment of the vulnerability.

Conditional independence assumptions: Under the conditions given to the parent node, a node independent of its non-child node setting a parent node of the node (a) Ain, non-descendants node (a) Aout, you can use probability formulas represents, see equation (3):

$$P\left(a\left|A_{in}\left(a\right),\prod_{out}\left(a\right)\right.\right)=P\left(a\left|A_{in}\left(a\right)\right.\right) \tag{3}$$

By definition attribute attack graph shows that between parent node atomic attack "and (and)" the relationship only when an attribute node satisfy all atomic attack will occur. For a multiple conditions and results of atomic attack attribute node properties, the conversion method is as follows: The atomic attack nodes removed, will attribute to each condition there is a directed edge between the results of property connected represents an atomic attack. After transformation in Bayesian network structure, the relationship between the condition of property still is "and (and)" relationship was shown in Figure 3.

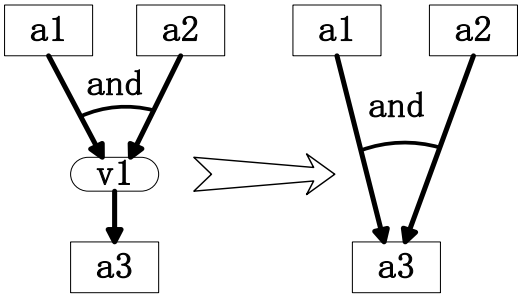

Figure 3. Convert and Structure Into Bayesian network

3.2 Classified Network Security Assessment Technology

Network Security Evaluation based on different technical criteria for the classification of different categories of classification. From a different perspective on the following network security assessment techniques detailed breakdown was shown in Figure 4.

Different agencies for security needs are different, even the same organization, its security needs are also different. For example, web browsing and other focuses availability of sensitive information is focused on privacy. Therefore, the classification includes the following categories of safety requirement category - Confidential assessment class, integrity and availability of assessment category Assessment category. Vulnerability assessment is the weakness of network security impact assessment. Threat assessment is the Index of frequency and severity of cyber attacks occur. Comprehensive

assessment techniques from physical security, security control, security services assess the safety aspects.

In the CVSS scoring system, the availability objectives defined vulnerabilities as: Ex = 20 × AV × AC × AU ($0 \leq Ex \leq 10$). The smaller the value of the Ex, indicates the availability of vulnerable points lower, the greater the degree of difficulty based on the atomic attack. Due to availability and inversely proportional to the difficulty of attack, this paper calculated atomic attack based on the three indicators difficulty, PV represents the difficulty of the corresponding atomic attack, attack the greater the difficulty the greater the value, as shown in Equation (4):

$$PV = \frac{1}{2 \times AV \times AC \times AU}; (PV \geq 1) \tag{4}$$

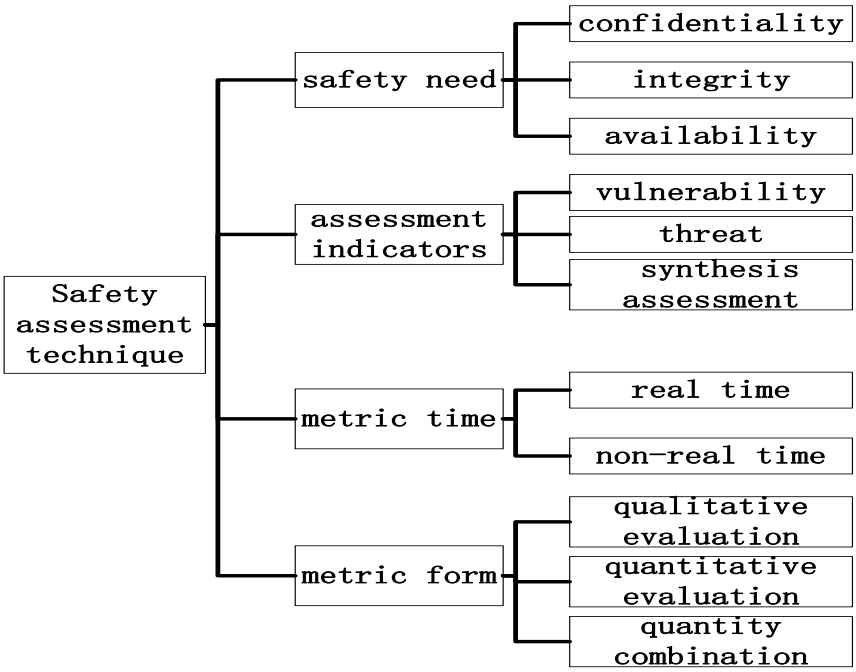

Figure 4. Classified Network Security Assessment Technology

4. Experiment and Analysis

4.1 Automated Network Modeling

Usually attack graph generation requires pretreatment preparation information, including information collection and information. The automated processing of information collection, one hand to facilitate the use of experts and scholars, on the other hand, can improve the efficiency of the safety analysis. In the pre-processing stage information, network threat modeling to automate data extraction and integration is critical and the focus. This paper presents a practical, strong network threats automatic modeling method, shown in Figure 5.

Automatic Modeling vulnerability information, the key lies in the description of vulnerabilities automatically extract and integrate information. Different vulnerability database has details on the vulnerabilities described in text-based form of different levels of detail, the automatic modeling of the vulnerability that is described in the text will be a certain degree of recognition, and the recognition of the results of the corresponding integration. Therefore, the automatic flaw modeling proposed algorithm is based on CVE,

NVD, several vulnerabilities database, indexed by CVE identifier, and then automatically associated scanner plug-in list database to achieve.

The main problem attack graph generation method exists that the state space explosion problem. With the increase of network scale attack graph algorithm state space grows exponentially. All route search network attacks compared with the number of network nodes become very complex, and even lead to infeasibility. Therefore, how to reduce the computational complexity and how to improve the efficiency of the algorithm is the key point of the study.

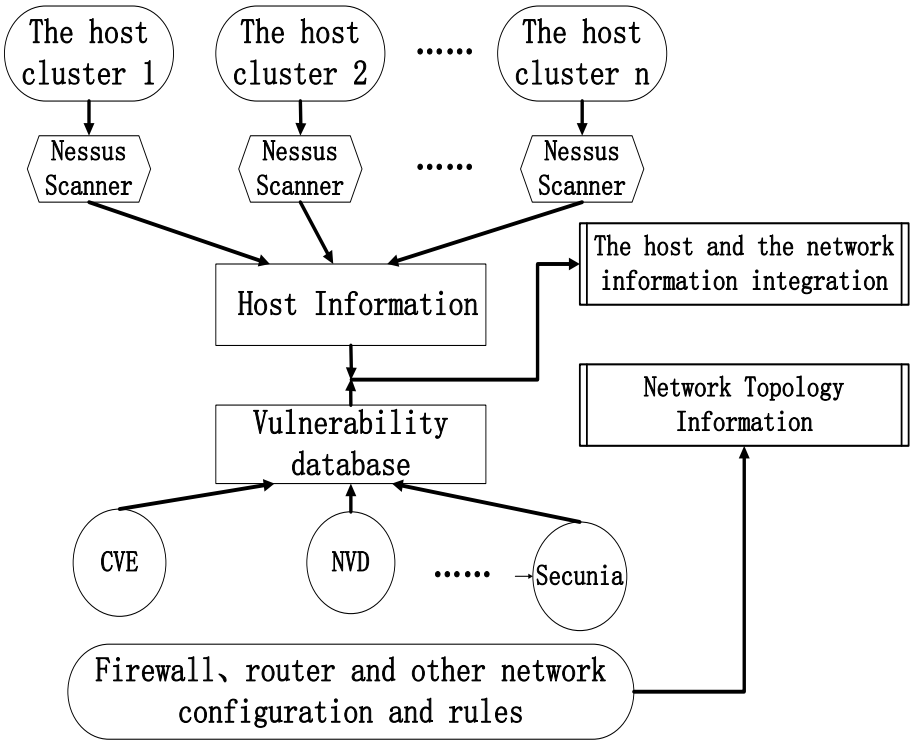

Figure 5. Automatic Modeling of Network Threat

4.2 Experiment Analysis

In order to verify the feasibility of the model's validity, to facilitate comparative analysis, we constructed Figure 6 Figure attribute attack. Attribute attack graph into Bayes attribute attack. FIG attribute nodes representing rectangular, oval nodes represent atomic attack node, there are three hosts, number: 0, 1, 0 wherein the target host is connected to external networks, No. 1, No. 2 hosts within the LAN, the attack is No. 2 host, obtain its root privileges.

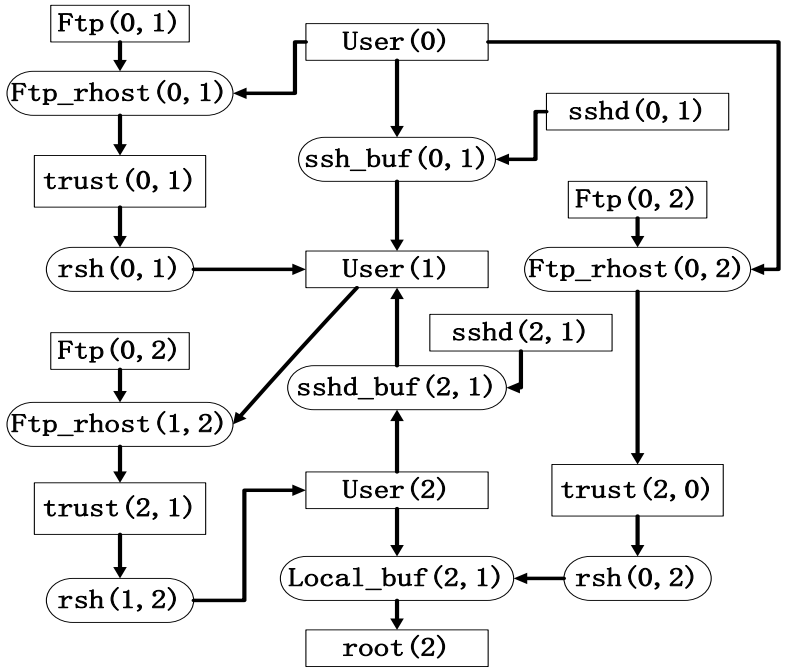

Figure 6. Attribute Attack Graph

As can be seen from the above analysis, when the possibility of increasing evidence of successful attack increases, test data consistent with the actual situation. Therefore, the model based on the current condition of the network, each of the possible attack path calculation of the probability of success, the security status of the network quantitative assessment, and network security status and trends of the correct response. According to the common vulnerabilities now label vulnerability database CVSS scoring system in ratings related attributes give loop three atomic attack vulnerability-related information, as shown in Table 1.

Table 1. The Conditional Probability of Exploited Vulnerability

Atomic attack code	vulnerability	AV	AC	AU	Ps
ftp_rhost(0,1)	CVE-2014-1443	1.0	0.72	0.56	0.7952
rsh(0,1)	CVE-2012-0814	1.0	0.72	0.56	0.6888
ssh_buf(0,1)	CVE-2014-1692	1.0	0.72	0.70	0.9999
ftp_rhost(0,2)	CVE-2014-4800	1.0	0.72	0.56	0.7955
ftp_rhost(1,2)	CVE-2011-7167	1.0	0.72	0.56	0.7955
rsh(1,2)	CVE-2012-0814	1.0	0.64	0.70	0.9999
rsh(0,2)	CVE-2013-1443	1.0	0.72	0.56	0.6832
local_buff(2)	CVE-2014-1763	0.415	0.72	0..71	0.394454

Figure 7 can be drawn from the attacks more difficult sshd_buf (2,1) point of maximum vulnerability, therefore, according to FIG attack ring elimination algorithm, the weak point off the edge, eliminating the loop to give acyclic attribute attack graphs. In this figure acyclic attack, reserved atomic attack is most likely to occur, in line with the

actual situation of the attack, which likely to be successful atomic attack is most likely to be exploited by attackers.

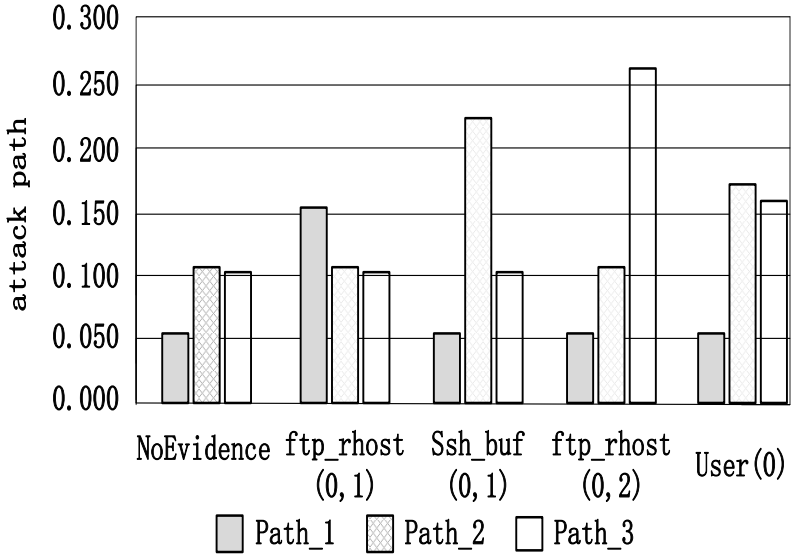

Figure 7. Difficulty Value of Atomic Attack in Loop

This paper established a Bayesian attribute attack graph model, a method to attribute attack graph Bayesian network transformation, loop algorithm attribute attack diagram eliminated. On the basis of Bayesian attribute attack graph, the calculated probability of success of each attack path for vulnerability assessment of the network. Through experimental analysis, the use of Bayesian network conversion method in this paper can be simple Bayesian attribute attack graph, simplifying the node probability calculations.

With the development of the Internet, people's daily lives more and more closely bound to the Internet, the network of people's social life has brought great convenience to enhance the level of information society, and promote the development of society. However, there are many security risks, such as cyber attacks, information theft and other security issues in the network. In this paper, the use of loop elimination algorithm can reduce the loss of important information about the attack path and improve the accuracy of the assessment. Based on this evaluation, the network administrator can design targeted, efficient network reinforcement case. However, after working there for improvement, to study how to use the Internet own historical data obtained conditional probability training nodes so that the probability of deriving more accurate.

5. Conclusions

This paper presents a prototype network security assessment system based on attack graph model, given the system design flow and overall system function module design, divided into information collection and pre-processing module, attack graph generation and visualization module, multi-target attack graph Safety Assessment module three modules, and each module detailed design and implementation of its sub-module functions. It gives the network security concepts, defined to include network security, security requirements and security elements and the like. Next, the proposed steps, levels and methods of cyber attacks. Then, the concept of network security assessment, classification of indicators to assess, evaluate, and network security assessment methods of technical analysis concludes for the establishment of attack graph model basis.

References

[1] Roy N K, Potter W D, Landau D P. Polymer property prediction and optimization using neural networks. IEEE Transactions on Neural Networks, 17 (4): 1001-1014**(2016)**
[2] Kornecki A J, Subramanian N, Zalewski J. Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on bayesian belief networks[C]//Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on. IEEE, 393-1399**(2013)**
[3] Liau L C-K, Yang T C-K, Tsai M-T. Expert system of a crude oil distillation unit for process optimization using neural networks. Expert System with Applications, 2004, 26 (2): 247-255.
[4] Li S, Tryfonas T, Russell G. Risk Assessment for Mobile Systems Through a Multilayered Hierarchical Bayesian Network**(2016)**
[5] Shin J S, Son H S, Heo G. Application of Bayesian network methodology for evaluating industrial control system, Advanced Science and Technology Letters, 42: 157-161**(2013)**
[6] Y. Zhao, W. Wei, P.H. Mei, Y.S. Pei, M.L. Zhao, W. Wang, An Effective Secure Routing Way to Reduce Energy Consumption in Wireless Sensor Networks, AISS. 4(2012)277-283**(2012)**
[7] W. Wustmann, S. Helduser, W. Wimmer. CFD-simulation of the reversing process in external gear pump. 6thinternational fluid power conference, TU Dresden, Apr. 1-2, 2008(2): 455-468**(2008)**
[8] Y. Zhao, W. Wei, B.S. Hou, L. Wei, The hardware design of intelligent circuit breaker, Energy Education Science and Technology Part A: Energy Science and Research., 1:695-702**(2014)**
[9] Wang L, Jajodia S, Singhal A, et al. k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities, IEEE Transactions on Dependable and Secure Computing, 11(1): 30-44**(2014)**
[10] Han G, Jiang J, Shu L. Management and applications of trust in Wireless Sensor Networks: A survey[J]. Journal of Computer and System Sciences, 80(3): 602-617**(2014)**
[11] Y. Zhao, Y. Chen, G. Zhang, W. Wei, Research on the VXI fault diagnosis for computer network based on immune genetic algorithm in process of data transfer, Computer Modelling & New Technologies. 5B (2013) 71-75**(2013)**
[12] Patel A, Taghavi M, Bakhtiyari K, et al. An intrusion detection and prevention system in cloud computing: A systematic review, Journal of network and computer applications, 36(1): 25-41**(2013)**
[13] James Dhinakaran, C. Maharaja Ganapathy, T. Kodeswaran, et al. Quality Improvement of Lubricating Oil Pump Shaft through Statistical Process Control Used in Automobile Industry. Procedia Engineering, 38: 2053-2062**(2012)**
[14] Marcus Vinicius C. Alves, Jader R. Barbosa Jr, Alvaro T. Prata. Analytical and CFD modeling of the fluid flow in an eccentric-tube centrifugal oil pump for hermetic compressors. International Journal of Refrigeration, August 11**(2012)**
[15] Shamshirband S, Anuar N B, Kiah M L M, et al. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique[J]. Engineering Applications of Artificial Intelligence, 26(9): 2105-2127**(2013)**

Author

Xianyou Zhu. Male, born in 1982.He received his Bachelor Degree from School of Computer science and technology, Hengyang Normal University, Hengyang, China in 2004, and his Master Degree from School of Software engineering, Hunan University, Changsha, China in 2010. Currently, He is a lecture working in School of Computer science and technology at Hengyang Normal University. He has published more than 10 academic papers, his current research interests include Applied of Computer and Software Engineering.

