Wuhan University
Journal of Natural Sciences

2018, Vol.23 No.2, 171-177

Article ID 1007-1202(2018)02-0171-07
DOI https://doi.org/10.1007/s11859-018-1307-0

Exploring Attack Graphs for Security Risk Assessment: A Probabilistic Approach

☐ GAO Ni[1], HE Yiyue[2†]

1. School of Information, Xi'an University of Finance and Economics, Xi'an 710100, Shaanxi, China;

2. School of Economics and Management, Northwest University, Xi'an 710127, Shaanxi, China

Abstract: The attack graph methodology can be used to identify the potential attack paths that an attack can propagate. A risk assessment model based on Bayesian attack graph is presented in this paper. Firstly, attack graphs are generated by the MULVAL (Multi-host, Multistage Vulnerability Analysis) tool according to sufficient information of vulnerabilities, network configurations and host connectivity on networks. Secondly, the probabilistic attack graph is established according to the causal relationships among sophisticated multi-stage attacks by using Bayesian Networks. The probability of successful exploits is calculated by combining index of the Common Vulnerability Scoring System, and the static security risk is assessed by applying local conditional probability distribution tables of the attribute nodes. Finally, the overall security risk in a small network scenario is assessed. Experimental results demonstrate our work can deduce attack intention and potential attack paths effectively, and provide effective guidance on how to choose the optimal security hardening strategy.

Key words: risk assessment; attack graph; Bayesian networks; prior probability

CLC number: TP 393

Received date: 2017-08-26

Foundation item: Supported by the National Natural Science Foundation of China (61373176), the Natural Science Foundation of Shaanxi Province of China (2015JQ7278), and the Scientific Research Plan Projects of Shaanxi Educational Committee (17JK0304, 14JK1693)

Biography: GAO Ni, female, Lecturer, Ph.D., research direction: network security and management. E-mail: gaoni@nwu.edu.cn

† To whom correspondence should be addressed. E-mail: heyiyue@nwu.edu.cn

0 Introduction

Faced with a large number of sophisticated network intrusion events, vulnerabilities are regularly discovered in network systems or software applications which are exploited to stage cyber attacks. In order to carry out security risk assessment, previous researches focused on individual vulnerabilities and ignored interactions among network vulnerabilities. For example, the Common Vulnerability Scoring System (CVSS) is widely accepted in industry standard, and the CVSS metrics are used to assess the actual risk of an organization based on three groups of predefined security metrics[1]. However, attackers can exploit related vulnerabilities to incrementally penetrate network, possibly leading to risk devastating consequences. In order to precisely assess the security risk, the mutual relationship among network vulnerabilities must be taken into account.

The risk assessment of network security is a proactive defense technology and an essential step in any network. In recent years, using attack graphs for cyber security risk assessment has been a well-studied topic. Attack graphs, which capture the interrelationships among vulnerabilities and measure security in the exact way, show us all the possible among multi-stage attacks. The attack graph, which is derived from a network model description, is a collection of attack paths. However, the exiting risk assessment models based on attack graphs have many shortcomings in terms of vulnerabilities analysis ability and evaluation of the emerging threats. In this paper, we aim to develop a model intended for security risk assessment by using Bayesian Networks, and

present a framework for security risk assessment based on attack graphs.

The rest of the paper is structured as follows. Section 1 introduces the related work. Section 2 describes the probabilistic model and the experimental results are analyzed in Section 3. Finally, Section 4 concludes the paper.

1 Related Work

Most previous researches have already been done in analyzing the relationship of network vulnerabilities to build attack graphs. Attack graphs are generated by tools such as TVA (Topological Analysis of Network Attack Vulnerability), NETSPA (Network Security Planning Architecture), and MULVAL (Multi-host, Multistage Vulnerability Analysis). TVA generates attack graphs using a graph search algorithm and utilizes an exploit dependency graphs to create pre and post conditions for vulnerability[2]. MULVAL is a framework for integration of vulnerabilities and network configurations which uses Datalog, and it is open source providing a concrete graph[3]. It consists of a scanner and an analyzer. The reasoning engine which has data-log rules captures system behavior[4].

Attack graphs have emerged as a mainstream technique to keep the network secure. Sheyner *et al*[5] proposed the probabilistic reliability analysis metric for the first time. While, this algorithm cannot be used to indicate absolute security risks. Xie *et al*[6] proposed the uncertainty model for cyber security, such as uncertainties in attack structure, attacker action, and intrusion alerts. Idika *et al*[7] made a number of crucial observations on the limitations of existing attack graph-based security metrics. Zhang *et al*[8] proposed an approximate Bayesian posterior inference algorithm under the condition of temporal partial ordering relations. Chen *et al*[9] proposed a probabilistic attack graph model to infer the intents under given sequences of observed security events, assuming a one-to-one correspondence between the security events and the attribute nodes. Barik *et al*[10] proposed the attack graph generation and analysis techniques. Kaynar *et al*[11] proposed the parallel computation of attack graphs.

Based on the research done by people in former times, this paper puts forward a more practical risk assessment model based on Bayesian attack graph, which focuses on the likelihoods of potential risk by using the Bayesian inference techniques, combining with observed intrusion evidence such like IDS alerts. In this methods, the probabilities of all nodes in an attack graph are evaluated. The proposed model can deduce attack intention and attack path effectively.

2 Probabilistic Model

2.1 Security Risk Assessment Framework

A holistic design framework is shown in Fig. 1, and static security metrics are appropriately recalculated. The proposed model have the combination of multiple techniques such as vulnerability scanning, intrusion detection, attack graph generation, and risk assessment based on Bayesian networks. Accordingly, the security risk assessment procedure includes the following stages, as shown in Fig. 1.

Phase 1 Risk detection. Firstly, identify network assets such as services available on a network, and connectivity of hosts on the network. Secondly, identify vulnerabilities of network hosts by using Open Vulnerability and Assessment Language (OVAL)-based vulnerability scanner, and the CVSS scores of vulnerability can be given from existing vulnerability databases, such as the National Vulnerability Database (NVD)[12]. Finally, these arguments obtained such as network vulnerability, system configuration and host connectivity on networks are the key inputs of MULVAL tool[3].

Phase 2 Risk assessment. Firstly, attack graphs are generated by the MULVAL tool according to sufficient information of system vulnerability, network configuration and host connectivity on networks. Secondly,

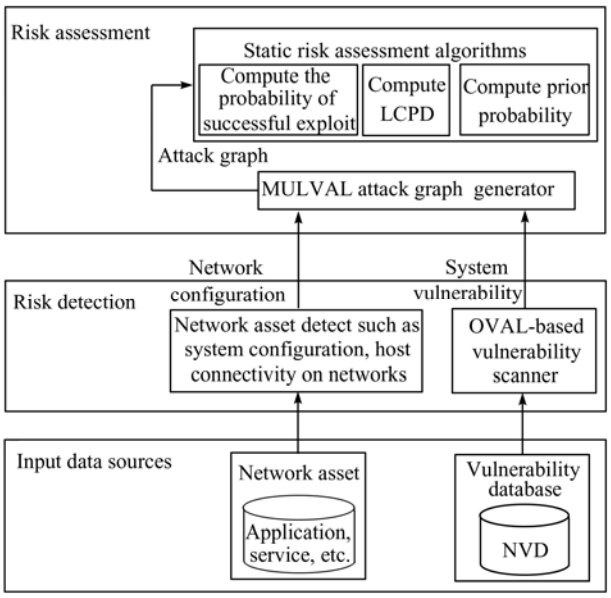

Fig. 1 A framework for the security risk assessment

the probabilistic attack graph is established according to the causal relationships among the multi-stage attacks by using Bayesian networks. Then, compute the probability of successful exploits, which is defined in the CVSS[13].The prior probabilities are given by using the local conditional probability distribution (LCPD) tables of the attribute nodes, and the static security risk is computed by the joint probability at the nodes. Eventually the risk assessment model based on Bayesian attack graph is constructed.

2.2 Bayesian Attack Graph

The attack graph (AG) model depicts multi-stage network attacks through their preconditions requirements and post-conditions capabilities, and is used to obtain the optimal path and the shortest path for the attacker. The existing Bayesian Attack Graph (BAG) requires the assignment of the likelihoods on AG, so a BAG-based security metrics are probability-based metrics. The BAG is defined by some attributes, attack actions and the cause-consequence relationships between these attributes.

Definition 1 A resource attribute is a Bernoulli random variable representing the state of network properties occupied by the attackers. It includes system vulnerabilities, access privilege on the machine, firewall properties and so on. A state of a resource attribute *S* is set to **True** $(S=1/T)$ or **False** $(S=0/F)$.

$P(S)$ is the probability of the resource attribute being in state $S=1$, and $P(\neg S)=1-P(S)$ is the probability of the resource attribute being in state *S*=0.

Definition 2 An atomic attack is the set of attack actions, and is associated with vulnerability exploitation. The vulnerability exploitation is denoted by v_i. An atomic attack is denoted by $A: S_{\text{pre}} \mapsto S_{\text{post}}$ if

- $S_{\text{pre}} \neq S_{\text{post}}$,
- given $S_{\text{pre}}=1$ and $S_{\text{post}}=1$, and the probability of the attacker from one attribute state S_{pre} to another S_{post} is denoted by $P(S_{\text{pre}}, S_{\text{post}})>0$, and not exiting $S_1, S_2, \cdots, S_i \in S-\{S_{\text{pre}}, S_{\text{post}}\}$ where $P(S_{\text{pre}}, S_1)>0$, $P(S_1, S_2)>0, \cdots,$ and $P(S_i, S_{\text{post}})>0$.

Definition 3 An extended Bayesian Attack Graph is a 5-tuple directed graph $\text{BAG}=(S, A, E, R, T)$.

- $S=N_{\text{external}} \bigcup N_{\text{internal}} \bigcup N_{\text{terminal}}$. N_{external} denotes the set of initial attributes as the external attacker. N_{terminal} denotes the set of final attributes as the attack targets. N_{internal} denotes the set of internal attributes during the attack process.
- $A=\{A_i \mid i=1, \cdots, n\}$ is the set of the atomic attacks. The atomic attack has been occurred being in state $A_i=1$, and the atomic attack hasn't been occurred being in state $A_i=0$.
- $E \in (S_{\text{pre}}, S_{\text{post}})$ is the set of the graph edges if $S_{\text{pre}} \mapsto S_{\text{post}} \in A$. The parent set of S_i is defined by $\text{Pa}[S_i]=\{S_j \in S \mid (S_j, S_i) \in E\}$.
- R denotes the relationship between the attribute and its parent set, and is a set of decomposition 2-tuple of $\langle S_i, d_i \rangle, d_i \in \{\text{AND}, \text{OR}\}$. Given $d_i=\text{AND}, S_i=1 \Rightarrow \forall S_i \in \text{Pa}[S_i], S_i=1$, the attribute S_j is compromised if its parent set is in the true state. Given $d_i=\text{OR}$, $S_j=1 \Rightarrow \exists S_i \in \text{Pa}[S_i], S_i=1$.
- T is the set of discrete LCPD functions, which associate with every attribute node in a BAG.

2.3 Common Vulnerability Scoring System

In order to compute the LCPD tables associated with every attribute node, the administrator needs to assess the probability of success associated with vulnerability exploitation according to the CVSS.

Definition 4 The probability of successful exploits is denoted by $P(v_i)$, which represents the likelihood that a vulnerability exploitation associated with an atomic attack is successfully executed by the attacker.

The CVSS is an open and free risk assessment system that gives quantitative values of individual vulnerabilities based on three metrics: **Base**, **Temporal**, and **Environmental**[12]. The **Base** metrics represent the intrinsic characteristics of individual vulnerability, and the **Base** score is decimal number on a range of 0 to 10. The Access Vector (**AV**) metric, the Access Complexity (**AC**) metric and the Authentication (**Au**) metric are shown in Table 1.

The **exploitability** metric is defined in CVSS as follows:

$$\textbf{exploitability} = 20 \times \textbf{AV} \times \textbf{AC} \times \textbf{Au} \quad (1)$$

Table 1 Base metrics

Metric name	Rank	Score
Access Vector (**AV**)	requires local access(L)	0.395
	adjacent network accessible(A)	0.646
	network accessible(N)	1.0
Access Complexity (**AC**)	high(H)	0.35
	medium(M)	0.61
	low(L)	0.71
Authentication (**Au**)	requires multiple instances of authentication(M)	0.45
	requires single instances of authentication(S)	0.56
	requires no authentication(N)	0.704

The value of **exploitability** ranges from 0 to 10, and $P(v_i)$ is computed from **exploitability** as follows:

$$P(v_i) = \textbf{exploitability} / 10 = 2 \times \textbf{AV} \times \textbf{AC} \times \textbf{Au} \quad (2)$$

Definition 5 The probability of success associated with an atomic attack is denoted by $P(A_i)$, which is assigned according to certain empirical knowledge.

The probability of successful attacks about three major types is quantized, and defined in this paper, such as the easy attack (0.8), the general attack (0.6) and the hard attack (0.2).

2.4 Static Risk Assessment

2.4.1 Computation of the LCPD function

The LCPD tables represent the likelihood of each state node being compromised, and can be computed by giving the combination of states of the parents.

Definition 6 Given Bayesian Attack Graph BAG= $(S, A, E, R, T), S_j \in N_{\text{internal}} \bigcup N_{\text{terminal}}$, S_i is a parent set of S_j and is denoted by $S_i \in \text{Pa}[S_j]$. In BAG, the LCPD tables T are generated to propagate the probabilities until reaching the target node when multiple exploits has been successfully executed. The LCPD function of the node S_j is denoted by $P(S_j \mid \text{Pa}[S_j])$, which can be calculated as follow:

Case 1 $d_i = \text{AND}$.

$$P(S_j \mid \text{Pa}[S_j]) = \begin{cases} 0, \exists S_i \in \text{Pa}[S_j] \mid S_i = 0 \\ P(\bigcap_{S_i=1} v_i), \text{ otherwise} \end{cases}$$

Case 2 $d_i = \text{OR}$.

$$P(S_j \mid \text{Pa}[S_j]) = \begin{cases} 0, \forall S_i \in \text{Pa}[S_j] \mid S_i = 0 \\ P(\bigcap_{S_i=1} v_i), \text{ otherwise} \end{cases}$$

AND-relationship signifies that compromising the target node S_j depends on all its parent nodes being in true state. Therefore, $P(\bigcap_{S_i=1} v_i))$ is defined as follow:

$$P(\bigcap_{S_i=1} v_i)) = \prod_{S_i=1} P(v_i) \quad (3)$$

Similarly, OR-relationship signifies that compromising the target node S_j depends on at least one parent node being in true state. Therefore, $P(\bigcup_{S_i=1} v_i)$ is defined as follow:

$$P(\bigcup_{S_i=1} v_i) = 1 - \prod_{S_i=1} [1 - P(v_i)] \quad (4)$$

Figure 2 shows a procedure for computing the LCPD tables. The node S_1 is an external attribute node, and the node S_4 is the successor of the nodes S_3, S_2 and S_1.

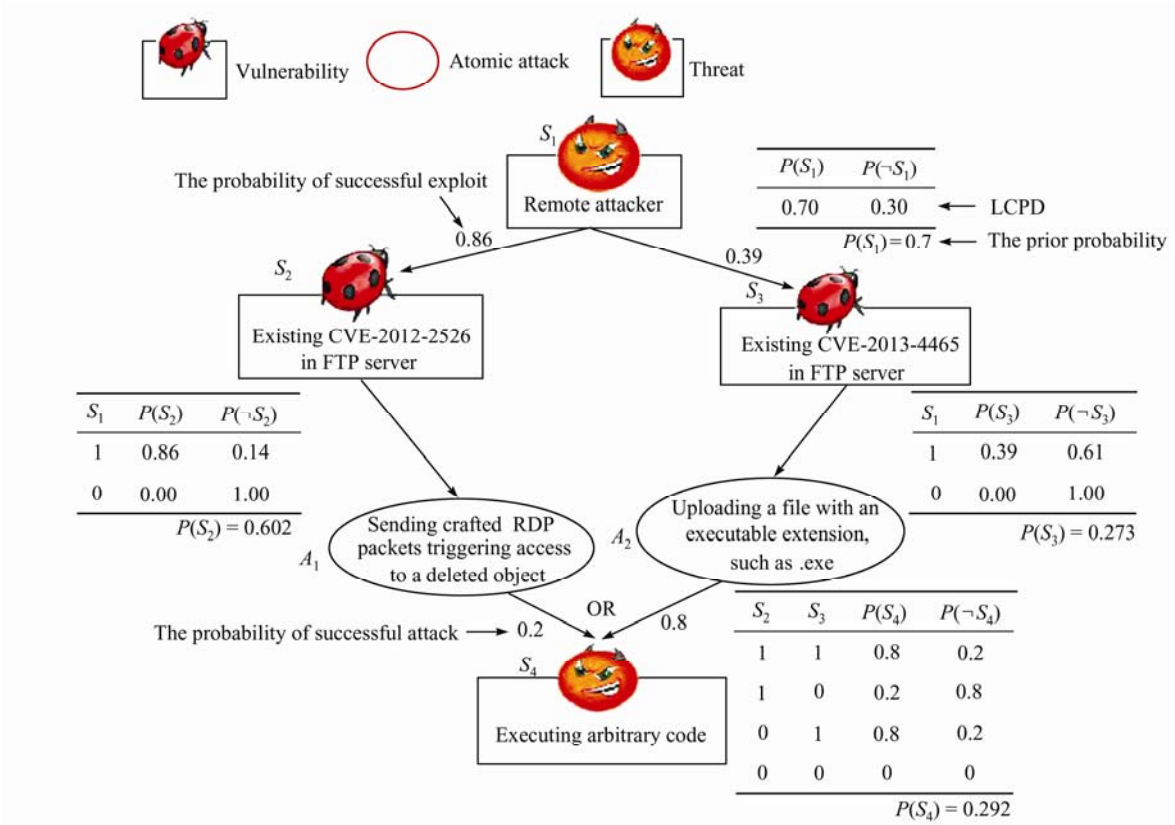

Fig. 2 A procedure for computing probability in a BAG

The probability of successful attacks $P(A_1)$ and $P(A_2)$ is assigned by the empirical knowledge, and a prior probability $P(S_1)$ is similarly assigned to 0.7. The probability of successful exploits is computed according to Eq. (2), and the LCPDs of the nodes S_2, S_3 and S_4 is calculated by the equations defined in Definition 6.

2.4.2 Computation of the prior probability

Definition 7 The prior probability is the joint probability of all the attribute nodes, is defined as follows:

$$P(S_1,\cdots,S_n)=\prod_{i=1}^{n}P(S_i\mid \mathrm{Pa}[S_i]) \tag{5}$$

Once the LCPDs of all nodes are obtained in the BAG, the prior probability of each node is derived as the joint probability of this node and its all ancestors by using the Bayesian Theorem. For example, in Fig. 2, the prior probability of S_2, S_3 and S_4 is computed as follows according to Eq. (5).

$$\begin{aligned}P(S_2)&=P(S_2,S_1)=P(S_2=1\mid S_1=1)\cdot P(S_1)\\&=0.86\times 0.7=0.602\\P(S_3)&=P(S_3,S_1)=P(S_3=1\mid S_4=1)\cdot P(S_1)\\&=0.39\times 0.7=0.273\\P(S_4)&=P(S_4,S_3,S_2,S_1)\\&=\sum_{\exists S_2,S_3=1}P(S_4\mid S_3,S_2)\cdot P(S_3\mid S_1)\cdot P(S_2\mid S_1)\cdot P(S_1)\\&=P(S_4\mid S_3=1,S_2=1)\cdot P(S_3=1\mid S_1=1)\cdot P(S_2=1\mid S_1=1)\\&\cdot P(S_1)+P(S_4\mid S_3=1,S_2=0)\cdot P(S_3=1\mid S_1=1)\\&\cdot P(S_2=0\mid S_1=1)\cdot P(S_1)+P(S_4\mid S_3=0,S_2=1)\\&\cdot P(S_3=0\mid S_1=1)\cdot P(S_2=1\mid S_1=1)\cdot P(S_1)\\&=0.8\times 0.86\times 0.39\times 0.7+0.8\times 0.14\times 0.39\times 0.7\\&+0.2\times 0.86\times 0.61\times 0.7=0.292\end{aligned}$$

3 Experimental Results

3.1 Experiment Scenrio

In order to examine the feasibility of the proposed models, we generated an attack graph for three subnets in our experiment. Figure 3 indicates the network topology of the given network configurations. The Web Server (WS), the DNS Server (DS) and the Mail Server (MS) are in the DMZ network, which protect the trusted network. The machines in the DMZ have limited connectivity to specific machines in the trusted network, for example, the WS is executed SQL queries to the Database Server (DBS), which may not be publicly accessible and may contain sensitive information. The DBS, FTP Server (FS), the Gateway Server (GS) and the Administrative Server (AS) are located in the trusted network.

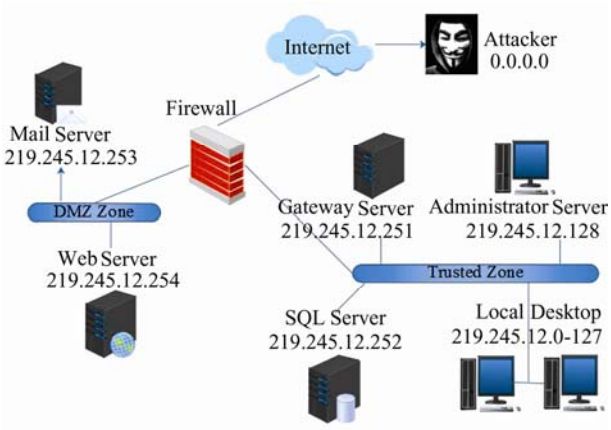

Fig. 3 Network topology

3.2 Attack Graph Generation

The OVAL scanner is used to recognize vulnerabilities of the hosts, and host vulnerabilities are listed in Table 2. MulVAL tool is used for generating attack graphs[3]. The file input.P contains information of network vulnerability, system configuration and host connectivity on networks, and output files, including the vertex file VERTICES.CSV and the edge file ARCS.CSV, represent the main attack graph information. A visual representation of the attack graph will be produced in AttackGraph.pdf through GraphViz[14], and experiment scenario is used to generate the attack graph shown in Fig. 4.

Table 2 Host vulnerabilities

Host	Threat description	CVE identifier	Probability of successful exploit
Administrator Server(219.245.12.128)	RPC Marshalling Engine Vulnerability	CVE-2009-0568	1
Local Desktop(219.245.12.0-127)	Microsoft Video ActiveX Control Vulnerability	CVE-2008-0015	0.86
Gateway Server(219.245.12.251)	FreeSSHd Authentication Bypass	CVE-2012-6066	0.86
Mail Server(219.245.12.253)	MiniSMTP Server Remote Stack BOF	CVE-2011-4040	1
SQL Server(219.245.12.252)	Remote Code Execution Vulnerability	CVE-2015-1762	0.39
Web Server(219.245.12.254)	IIS FTP Service Heap BOF	CVE-2010-3972	1

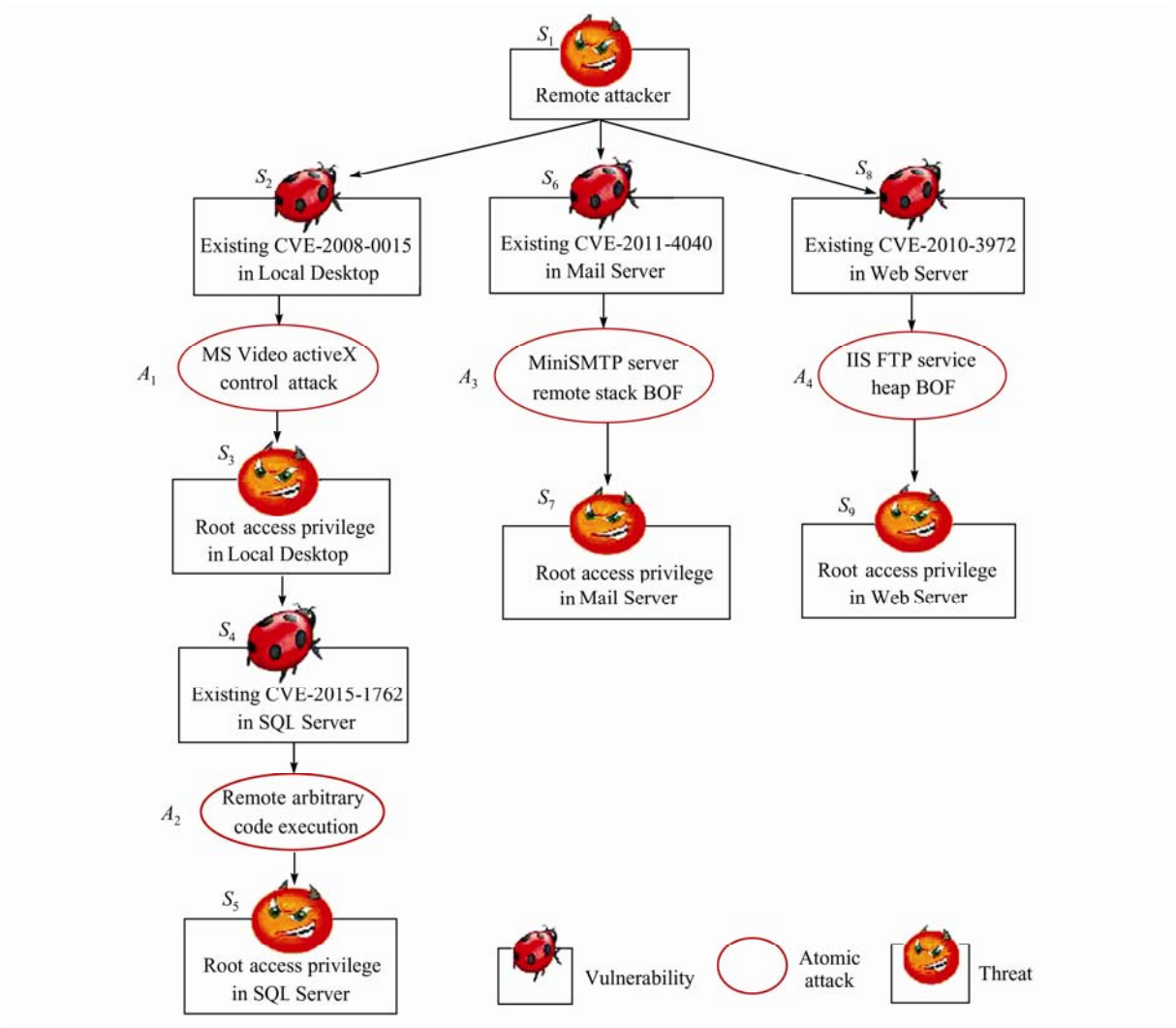

Fig. 4 The attack graph of our experiment network

3.3 Computing Security Risk

3.3.1 Computation of the probabilities of successful attacks

In order to avoid complicated calculations, the LCPDs of all nodes are omitted in Fig. 4. The probabilities of successful exploits are calculated according to Eq. (2), and the probabilities of successful attacks are assigned according to certain empirical knowledge. The results are listed in Table 3.

Table 3 Probability of each edge in the attack graph

Edge	Probability	Edge	Probability
(S_1, S_2)	0.86	(S_1, S_6)	1
(S_2, S_3)	0.60	(S_6, S_7)	0.6
(S_3, S_4)	0.39	(S_1, S_8)	1
(S_4, S_5)	0.80	(S_8, S_9)	0.2

3.3.2 Computation of the risk probability

The LCPDs of the all nodes are calculated by the equations defined in Definition 6, combining with the probability of each edge in Table 3. The prior probability of $P(S_1) = 0.7$ to the external attribute S_1 is assigned in our experiment, the prior probabilities of the rest nodes are computed according to the procedure described in Section 2.3.2. The result is listed in Table 4.

Table 4 Security risk assessment with the attack graph

Attribute node	Prior probability	Attribute node	Prior probability
S_1	0.700	S_6	0.70
S_2	0.602	S_7	0.42
S_3	0.361	S_8	0.70
S_4	0.141	S_9	0.14
S_5	0.113		

3.3.3 Computation of the optimal attack paths

In Fig. 4, the attacker can get the ROOT privilege of SQL Server in the trusted network. Attack path, which represents the each stage vulnerability exploited, is the trace of an attack from the source to the compromised host. The optimal path or the shortest path algorithm in Ref.[13] is used in our experiment, and potential attack paths can be easily identified. Therefore, to compromise the target host such as SQL Server, the attacker can choose path, including $S_1 \rightarrow S_2 \rightarrow A_1 \rightarrow S_3 \rightarrow S_4 \rightarrow A_2 \rightarrow S_5$. Finally, the experimental results show that the model proposed can analyze potential attack paths and deduce ways an attack may propagate.

4 Conclusion

As the attack graph methodology is widely utilized in security risk assessment, we aim to develop a model intended for security risk assessment by using the attack graph, which is established according to the causal relationships among the multi-stage in one attack progress by using Bayesian Networks. A framework for network security risk assessment is presented by combining multiple techniques, such as vulnerability scanning, attack graph generation and risk assessment. Finally, the experimental results demonstrate that our model can generate the attack graph successfully and deduce attack paths effectively. This model can help to take hardening measures in network security.

References

[1] Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system [J]. *IEEE Security & Privacy*, 2006, **4**(6): 85-89.

[2] Ou X, Homer J, Zhang S, *et al*. MulVal project at Kansas State University[EB/OL]. [2013-11-20]. *http://people.cs.ksu.edu/~xou/mulval/*.

[3] Jajodia S, Noel S. *Topological Vulnerability Analysis*: *A Powerful New Approach for Network Attack Prevention*, *Detection*, *and Response* [M]. Singapore: World Scientific Publishing Company, 2008.

[4] Ou X, Boyer W F, McQueen M A. A scalable approach to attack graph generation[C]// *Proc* 13*th ACM Conference on Computer and Communications Security* (*CCS* 2006). New York: ACM, 2006: 336-345.

[5] Sheyner O, Haines J, Jha S, *et al*. Automated generation and analysis of attack graphs[C]// *Pro of the* 2002 *IEEE Symposium on Security and Privacy*(*S&P*). Washington D C: IEEE, 2002: 273-284.

[6] Xie P, Li J, Ou X, *et al*. Using Bayesian networks for cyber security analysis[C] // *Proc* 43*rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (*DSN*). Washington D C: IEEE, 2010: 211-220.

[7] Idika N, Bhargava B. Extending attack graph-based security metrics and aggregating their application [J]. *IEEE Transactions on Dependable and Secure Computing*, 2012, **9**(1): 75-85.

[8] Zhang S J, Song S S. A novel attack graph posterior inference model based on Bayesian network [J]. *Journal of Information Security*, 2011, **2**:8-27(Ch).

[9] Chen X J, Fang B X, Tan Q F, *et al*. Inferring attack intent of malicious insider based on probabilistic attack graph model [J]. *Chinese Journal of Computers*, 2014, 37(1):62-72(Ch).

[10] Barik M S, Sengupta A, Mazumdar C. Attack graph generation and analysis techniques[J]. *Defence Science Journal*, 2016, **66**(6): 559-567.

[11] Kaynar K, Sivrikaya F. Distributed attack graph generation[J]. *IEEE Transactions on Dependable & Secure Computing*, 2016, **13**(5):519-532.

[12] National Institute of Standards and Technology (NIST). National vulnerability database(NVD)[EB/OL]. [2017-03-20]. *https://nvd.nist. gov/*.

[13] The Forum of Incident Response and Security Teams (FIRST). Common vulnerability scoring system (CVSS) [EB/OL]. [2017-07-24]. *https://www.first.org/cvss/*.

[14] AT&T Labs Research. GraphViz-graph visualization software[EB/OL]. [2017-08-06]. *http://www.graphviz.org/*.

□