International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.203-218
http://dx.doi.org/10.14257/ijsia.2017.11.1.17

Multi-step Attack-oriented Assessment of Network Security Situation

Zhang Hengwei[1,2], Yang Haopu[3], Wang Jindong[4] and Li Tao[5]
[1,3,4,5] *Zhengzhou Institute of Information Science and Technology*
Zhengzhou, China
[2]*Science and Technology on Information Assurance Laboratory*
Beijing, China
zhw11qd@126.com, memo_yang@126.com,
restart03wade@163.com,1527105421@qq.com

Abstract

In order to correctly analyze the multi-step attack and comprehensively assess the network security situation, a multistep attack-oriented assessing method of network security situation is proposed. The security events are clustered into different attack scenarios for identifying attackers. Based on the causal correlation between every attack scenario, the attack traces and attack phase can be distinguished. Finally, the quantitative criterion is established to realize the assessment of network security situation. Two network attack and defense experiments are used to verify the correctness and effectiveness, and the result shows the proposed method can truly depict the actual attack.

Keywords*: multi-step attack; network security situation assessment; attack clustering; correlation analysis*

1. Introduction

As the rapid development of computer network as well as telecommunication, Internet has been penetrating in every corner of human society and unconsciously influencing people's lifestyle. It provides great convenience for our life, while it also brings in lots of security problems. The most classic problem is network attack, which always causes severe damages for enterprises, organizations, governments and nations. Based on this, the research of network security situation awareness comes into notices. This research can be used to cognize and predict the security condition as well as the development tendency of network, which provides assistance for managers to timely check for network health and flexibly defense the potential threatens.

The security condition of network can be assessed in accordance with different aspects, such as attack threaten [1, 2] and vulnerability[3, 4]. The existing researches in this field choose only one single factor as the assessing target, which cannot accurately depict the security condition of the whole network. As a novel active defense technology, network security situation awareness fuses various warning information from multiple safety protection equipment (such as IDS, firewall, VDS and et al) and improves the capacity for real-time attack detection. The concept of situation awareness was proposed by Endslesy [5] to merely solve the key difficulties in aerospace, military, traffic monitoring and emergency aid. Until 1999, Tim Bass [6] firstly brought it into the research of network security. Nowadays, network security situation awareness mainly focuses on the assessment of current network situation and the prediction of situation development tendency.

Many assessing methods, which are based on different theories (e.g. Mathematical model [7, 8], information inference [9, 10], pattern recognition [11, 12] or game theory [13, 14]), are proposed. The above methods, ignoring the relation between different security events, are

ISSN: 1738-9976 IJSIA

merely on the basis of single attack. Nevertheless, network attacks are no longer isolate, but large-scale, cooperative and multi-steps. According to the Report of National Computer Network Emergency Response Technical Team/Coordination Center, a large proportion of network attack events, especially those caused huge damages, are multi-step attacks.

Based on the above analysis, some solutions are proposed, such as paper [15] and [16]. The former focuses on the causal relationship between each attack phase on the basis of multi-dimension security information, while the latter assesses the network security situation through mining and restoring the attack paths. However, they both utilize attack-graph into their research, which cannot distinguish attack scenarios or attackers.

In a word, the available network security situation assessment methods can help managers understanding the current network security condition in some certain extent, but they still have severe limitations facing multi-step attacks. (1) Lacking the identification of attack phases, assessing the influence by each attack trace is unavailable. (2) Lacking the identification of attackers, assessing the influence by every attacker is unavailable. (3) The rational and effective quantitative criteria in security situation is absent.

Some related organizations and enterprises focus on the vulnerability in information system and propose different standards, such as Management of Information and Communications Technology Security (ISO13335), Evaluation Criteria for Information Technology Security (ISO15408) and Classified Criteria for Security Protection of Computer Information System (GB17859). Most of those standards are qualitatively analyzing the network security condition, whose intelligibility is limited. The National Infrastructure Adviser Committee proposes Common Vulnerability Scoring System (CVSS) to effectively and commonly grade all security vulnerabilities (including the known as well as those unknown), which is extensively applying in the related researches.

This paper proposes a network security situation assessment method for multi-step attacks based on the view of attackers. Firstly, we distinguish every attacker's traces by clustering attack behaviors into different attack scenarios. Secondly, we establish the attack pattern database and distinguish attack phase by analyzing the causal relationship between attack behaviors. The attack phase is regarded as the crucial factors in assessing network situation. Finally, based on CVSS [17], we quantify the security situation of the whole network through fusing the situation factors and the node situations.

2. The Foundation of Network Security Situation Assessment

The network security situation is always evaluated on the basis of several attack traces and their damage to the information assets. Attackers choose the most suitable attack pattern according to the targeted network environment. Even the same attack pattern can result in different influences due to different environments. The key factors for assessing security situation should both include the attack information and the environment information. In this section, we will illustrate the related definitions. Then we will describe the process of network security situation assessment.

2.1. Definition of Basic Term

Definition1. Host Information, which represents by Host, includes computers and all kinds of network devices, such as firewall. Network devices are usually used as the objects or springboards in network attacks, so the full-scale analysis of them is essential. We use quadruple, (HostIpm, Services, Vuls, Weight), to describe Host information. While, HostIp represents the IP address of the host, Services represents the running services in the host, such as SSHD, SQL, HTTP, MS-Office and et al., Vuls represents the vulnerabilities in the host, and Weight represents the importance of the host.

Definition2. Vulnerability set, which represents by V, contains the existing configuration errors and the vulnerabilities in the network. Every vulnerability, $v \in V$, can be represented by a five-tuple, (id, type, IP, impact, info). While, id represents the unique identification of the vulnerability, type=(C_Error, Vulnerability), C_Error means the type of configuration error, such as insecurity strategy, firewall configuration error and access privilege configuration error, and Vulnerability means the type of vulnerability according to the vulnerability database such as BugTraq or CERT/CC. IP represents the host IP address, impact represents the influence caused by the vulnerability, and info represents the detailed description of the vulnerability.

Definition3. Network Topology, which represents by undirected graph, (N,E), describes the physical connection between the hosts in the network. While, N means the nodes set of the physical hosts, and E means the edges set of physical connection.

Definition4. Network Connection, which represents by $conn \subseteq Host \times Host$, expresses the communicated relationship between hosts. Generally, managers deploy the firewall access strategy list to control the communication privilege between exterior network and interior network. In this paper we use triple (hosti, hostj, protocol/port) to describe the communicated relationship, while hosti and hostj respectively means the connected hosts, and protocol/port represents the essential communication protocol and port.

Definition5. Meta Attack Event means one single attack behavior, which can be represented by a 7-tuple, (id, time, Sip, Dip, Sport, Dport, AttackType, p(a)). While, id represents the unique identification of this attack event, time represents the occurring time, Sip represents the event's source IP address, Dip represents the event's destination IP address, Sport represents the source port, Dport represents the destination port, AttackType represents the attack type in this security event, p(a) represents the probability of occurrence after fusion.

Defition6. Attack Transferring Graph, G, is described by quaternion (S,τ,A,ε).

1)S represents the nodes set of attack status.

2)$\tau \subseteq (Spre, Spost)$, $Spre, Spost \in S$. For $Si \in S$, we use $Pa(Si)=\{Sj \in S|(Sj,Si \in \tau)\}$ to represent the parent node of Si, and use $Ch(Si)=\{Sj \in S|(Si,Sj \in \tau)\}$ to represent the child node of Si.

3) A is represented by a two-tuple $(\tau i,Ati)$, while $\tau i \in \tau$, Ati represents the necessary meta attack event in the status transferring τi.

4) ε, which is represented by a two-tuple (Si, di), describes the dependency relationship between different attack events. If $Si \square true \Rightarrow \forall Si \in Pa(Si), Si \square true$, then $di \square 1$. In this circumstances, only all the parent nodes are successful, this attack status is likely to be successful. If $Si \square true \Rightarrow \exists Si \in Pa(Si), Si \square true$, then $di=0$. This circumstance means that as long as one of the parent nodes is successful, this attack status is likely to succeed. The former relationship is parallel, and the latter is selective.

According to the status transferring model, the network attack pattern set can be established. Figure 1 is an attack status transferring graph of an actual attack case. The status nodes set is S={Address probe, Port scan, ⋯, login}, the meta attack events include fping, nmap ping, strobe, netcat, login and et al. Between the first and the second status, Address probe is the parent node of Port scan, which means that if status Port scan is success, the Address probe is success inevitably. The dependence relationship between them is parallel.

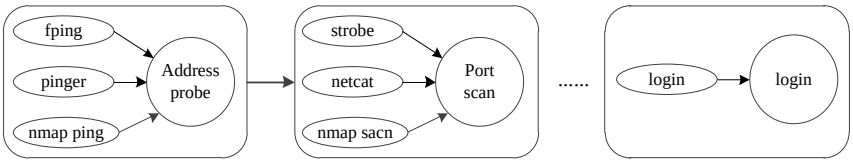


Figure 1. Attack Status Transferring Graph

2.2. Process of Network Security Situation Assessment

Here we will introduce the whole process of network security situation assessment, and the detailed algorithms will explain in the next two sections. The assessing process contains the following three steps.

Step1, collection of network security situation factors. The needed factors are coming from standardizing the warning data and network environment running information. The factors can be divided into attacker information and environment information. The attacker information is obtained from fusing the warnings from IDS, firewall, system logs and et al. The environment information includes host information, system topology and network connection, which is mainly relying on the statistics of network information and the scanning of vulnerabilities. The host information can be gained through the vulnerability scanning as well as the statistics of system and software, the system topology relies on the statistics of network structure, and the network connection relies on the access control lists of firewall.

Step2, identification of network attack phases. According to the standardized information, the attack behaviors are needed causal analysis. Firstly, the attack behaviors are clustered into different attack scenarios. Fuse the attack information into several security events, and then identify the attacker's traces by dividing the security events based on their causal relationship. Secondly, the real-time attack scenarios and attack pattern set are used to identify the attack phase. The detailed algorithms are discussing in section 3.

Step3, quantification of network security situation. Based on identifying the attack phase, the assessment of network security situation can be evaluated through combining the assets' information and CVSS standard. The detailed discussion is shown in section 4.

3. Real-time Identification of Attack Phase

3.1. Attack Scenario Clustering

The targeted information network can be invaded by multi-attackers at the same time, which is much more dangerous than invaded by only one single attacker. It is necessary to identify attackers by fusing the security events and dividing them into different attack scenarios.

Among a multistep attack, the final target is always decided in advance, so all attack behaviors must follow the certain causal relationship. For example, the pre-attack event of vulnerability scanning is IP sweeping, so the source IP and destination IP must be the same in the two events. In the meantime, these two events must occur in time-sequence. In order to identify all attack scenarios, the correlation between warnings is significant.

Definition7. Attack Correlation, which is represented by cor(a, b), describes the correlative degree between each two attack events. This value can be used to measure the probability whether two events belong to one same attack scenario. In this paper, we select source IP, destination IP, source port, destination port, time and attack type as the characteristics to calculate the attack correlation. The function is shown in the following.

$$cor(a,b) = \sum_{k=1}^{n} \alpha_k Feature_k(a,b) \Big/ \sum_{k=1}^{n} \alpha_k \quad (1)$$

While, Featurek(a, b) represents the correlation between attack events a and b at characteristic k, and αk represents the weight of k. The characteristics and the weight are valued according to paper [18].

When a new security event is captured, it will be matched with the pre-created attack scenarios and calculated the correlations with them. If the correlations with some attack scenarios are greater than the pre-decided threshold value, this event join into the attack scenario with whose correlation is the maximal. If all of the correlations are less than threshold value, this event will be saved as a new attack scenario.

3.2. Real-time Identifying Attack Phase Algorithm

Definition8. Real-time attack scenario, which is represented by a triple (S,F,Q), is used to save the real-time intrusion traces. While, S represents the nodes set of occurred-attack status, F represents the edges set which express the transferring between status nodes, Q represents the dependency between status, and Qi∈{AND,OR}. If Qi□AND, then Si can possibly succeed when all parent nodes have succeeded. If Qi□OR, then Si can possibly succeed when at least one of its parent nodes have succeeded.

Definition9. Status occurring function, which is represented by bool(s), is used to identify whether the attack status is occurred. If yes, bool(s)=true; Otherwise, bool(s)=false.

Definition10. Transferring window, στ. Usually, the effectiveness of attack behavior is limited by its period of validity. If attacker doesn't launch the post-intrusion before the effective deadline, then we consider that the attacker's capability cannot exploit the newly vulnerabilities. In brief, the intrusion is failed. To improve the identification of effective attack, a transferring window is necessary. According to known information, the period of most network attacks are 2h, so we make στ□2h.

We cluster the real-time security events referring to attack correlation and gain warning-sets in different attack scenarios. Comprehensively analyzing the warning information and the attack pattern, there are four kinds of classical status transferring conditions. Detailed information is shown in Figure 2.

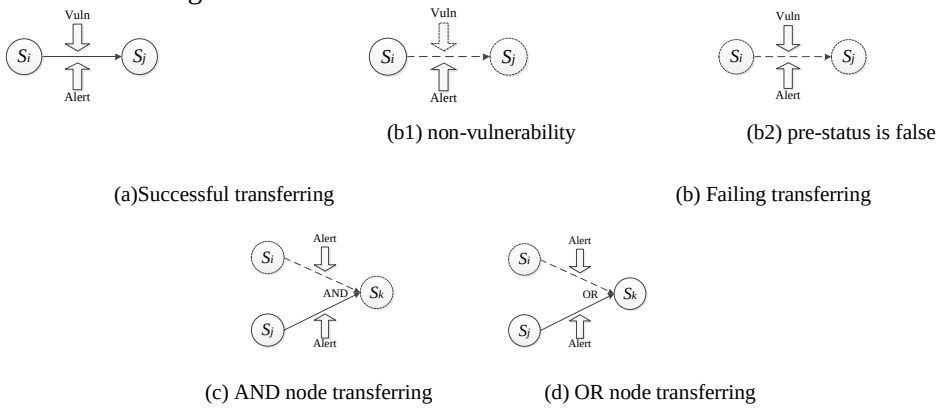


Figure 2. Attack Status Transferring Conditions

Figure 2(a) represents the successful status transferring, in which pre-status of attack is success and the needed vulnerability is existed in targeted host. Figure 2(b) represents the failing status transferring. It can be divided into two parts: the needed vulnerability is lacking in the targeted host (shown in Figure 2(b1)) or the pre-status is false (shown in Figure 2(b2)). Figure 2(c) represents the status transferring in AND nodes, and 2(d) represents the OR nodes. Based on the above analysis, the algorithm of real-time identifying attack phases is described in the following.

Algorithm 1 Algorithm of Real-time Identifying Attack Phases

Input: Fused security events, Alert.

Output: Real-time attack scenarios, ATree.

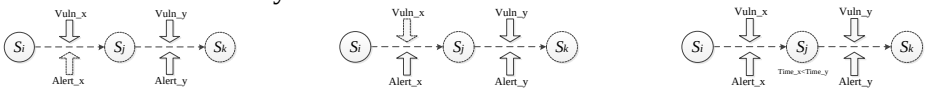
Processing:

1) Keep waiting for the real-time warning information. If a new security event Alert is captured, then calculate its correlations with the pre-created real-time attack scenarios. According to the correlations, the security event is clustered into the suitable attack scenario.
2) Analyzing the warning information and the attack pattern of every attack scenario, the necessary information is obtained, such as the pre-status sx, the post-status sy, the dependency between post-status e, the needed vulnerabilities Vuln and the current time t.
3) If Vuln∉HostInf, which represents the targeted host doesn't have the needed vulnerabilities, then the intrusion is unsuccessful and the status transferring is failed. Under this circumstance, the real-time attack scenario doesn't change anymore and turn to h).
4) If bool(sx)=false, which represents the pre-status doesn't exist, then the intrusion is unsuccessful and the status transferring is failed. Under this circumstance, the real-time attack scenario doesn't change anymore and turn to h).
5) If bool(sx)□□true, bool(sy)□□true, and path(sx→sy)∈F, which represents the attack path is already existed in the pre-created attack scenario, this condition belongs to repeated status transferring. The attack scenario graph doesn't change and turn to h).
6) If e=0, which represents sy belongs to OR node, then join the status node sy and the attack path path(sx→sy) into the real-time attack scenario, set the corresponding parameters Qf=OR, bool(sy)=true and refresh the status occurring time tcurrent=t. Turn to h).
7) If e=1, which represents sy belongs to AND node, then join the status node sy and the attack path path(sx→sy) into the real-time attack scenario, set the corresponding parameters Qf□AND and refresh the status occurring time tcurrent□t. According to the attack pattern, if all of the status sy's pre-conditions are successful, then set the parameter bool(sy)=true. Then turn to h).
8) Check out whether the status transferring time is timeout. If t□tcurrent>στ, then delete the attack scenario and turn back to a).

3.3. Improvement of Real-time Identifying Attack Phases Algorithm

Based on the above algorithm, the attack scenario can be identified from network security events. However, some abnormal conditions can greatly influence the generation of attack scenario, such as false negatives, packet disorder and 0-day vulnerability. Shown in Figure 3, (a) represents the condition of false negatives. Because leaking the security event Alert_x, the status sj is set as FALSE, and the production of status sk is influenced. Due to the difference between theoretical detection policy and real characteristics during intrusion, the intrusion detection devices can easily missing part of warning events. (b) represents the condition of 0-day vulnerability. The security event Alert_x exploits 0-day vulnerability to launch attack, which cannot be detected correctly. So the conclusion in generating status sk is also incorrect. This is the most common condition. Lots of 0-day vulnerabilities exist in network system but still not announced. Skilled attackers are used to digging out 0-day vulnerabilities to intrude into targeted network. (c) represents the condition of disorder. According to the detection, security event Alert_y occurred before Alert_x, resulting in the incorrect conclusion that sk cannot transmit successfully. This

condition always appear when there exist time-delay in the network transmission or the clock in different sensors are asynchronous.



(a)false negatives (b) 0-day vulnerability (c)packet disorder

Figure 3. Abnormal Conditions in Identifying Attack Phases

Based on this, we improve the status occurring function bool(s)∈{true, false, middle}. The new status middle is used to save the possible status and be revised according to the follow up warning events. The improved algorithm is shown in the following.

Step1, setting the middle status.

1) If Vuln∉HostInf, bool(sx)□false, which means there doesn't exist the needed vulnerability in the targeted host and the pre-status is true, then there may exist 0-day vulnerability in this condition. We set the parameter bool(sy)=middle.

2) If Vuln∈HostInf, bool(sx)=false, which means there doesn't exist the needed vulnerability in the targeted host and the pre-status is false, then there can exist false negatives or packet disorder in this condition. Checking out the host which occurred status sx, if the needed vulnerability exist in it, then set the parameter bool(sx)=middle and bool(sy)=middle.

Step2, revising the incorrect status.

1) If Vuln∈HostInf, bool(sx)=middle, which represents there exist the needed vulnerability in the targeted host and the pre-status is middle, then we suppose that attacker can exploit status sx and this status is occurred. Revise the status bool(sx)=true, bool(sy)=true. This condition is suitable for revising the errors resulted by false negatives and 0-day vulnerabilities.

2) If Vuln∈HostInf, bool(sx)=true, bool(sy)=middle, which represents there exist the needed vulnerability in the targeted host and the pre-status is true and the following status is middle, then we consider there exist packet disorder in this condition. Revise the status bool(sy)=true and set all the following nodes as true.

4. Quantitative Analysis of Network Security Situation

4.1. Probability of Successful Attack

In this paper, the probability of successful attack, p(ac), means the possibility that attacker can intrude into the targeted network. Obviously, p(ac) is influenced by the skill of attacker and the environment of the network.

$$p(ac) = \begin{cases} p(a), & vlus_j \in Vuls \\ 0, & otherwise \end{cases} \quad (2)$$

While, p(a) represents the probability that attack occurred, vulsj represents the necessary vulnerabilities in attack, vulsj∈Vuls represents that the necessary vulnerabilities exist in the targeted host.

4.2. Probability of Successful Attack phase

The probability of successful attack phase, p(s), represents the possibility that attack has reached the designated attack phase. The achievement of attack phase depends on multiple single attack behaviors.

$$p(s)=\begin{cases} p_i(ac)+p_j(ac)-p_i(ac)p_j(ac), d=0 \\ p_i(ac)p_j(ac), \qquad\qquad d=1 \end{cases} \quad (3)$$

While, pi(ac) and pj(ac) respectively means the successful intrusion probability of attack Alerti and Alertj, d=0 represents the status s is OR node, d=1 represents that s is AND node.

4.3. Quantification of Network Security Situation

CVSS provides a vulnerability scoring standard based on confidentiality, integrity and availability. This system is appropriate for measuring the influence caused by a single vulnerability. The scoring formula is shown in the following.

$$Impact(v)=10\times(1-(1-C)\times(1-I)\times(1-A)) \quad (4)$$

While, C, I, A respectively represents the confidentiality, integrity and the availability of the vulnerability.

Generally, every attack scenario needs to exploit multiple vulnerabilities, whose contribution to the network security situation can be analyzed by comprehensively assess the p(s), Impact(v) and Weight. This value can also represent the multi-vulnerabilities' influence to security situation.

$$sa(path_i)=\sum_{j=1}^{m} p_j(s)Impact(v)Weight \quad (5)$$

While m represents the occurring attack phase in the attack scenario pathi.

In equation (5), pj(s)≤1, Impact(v)≤10, ∑Weight=1, sa(pathi)≤10. The implicit meaning of the value is defined according to CVSS. If sa(pathi)∈[0,4], we suppose the attacker has low risk for the network system. If sa(pathi)∈(4,7], we suppose the attacker has middle risk. If sa(pathi)∈(7,10], we suppose the attacker has high risk.

Combined every attack scenario's influence to network, the security situation of whole network can be gained.

$$SA=\sum_{i=1}^{n} sa(path_i) \quad (6)$$

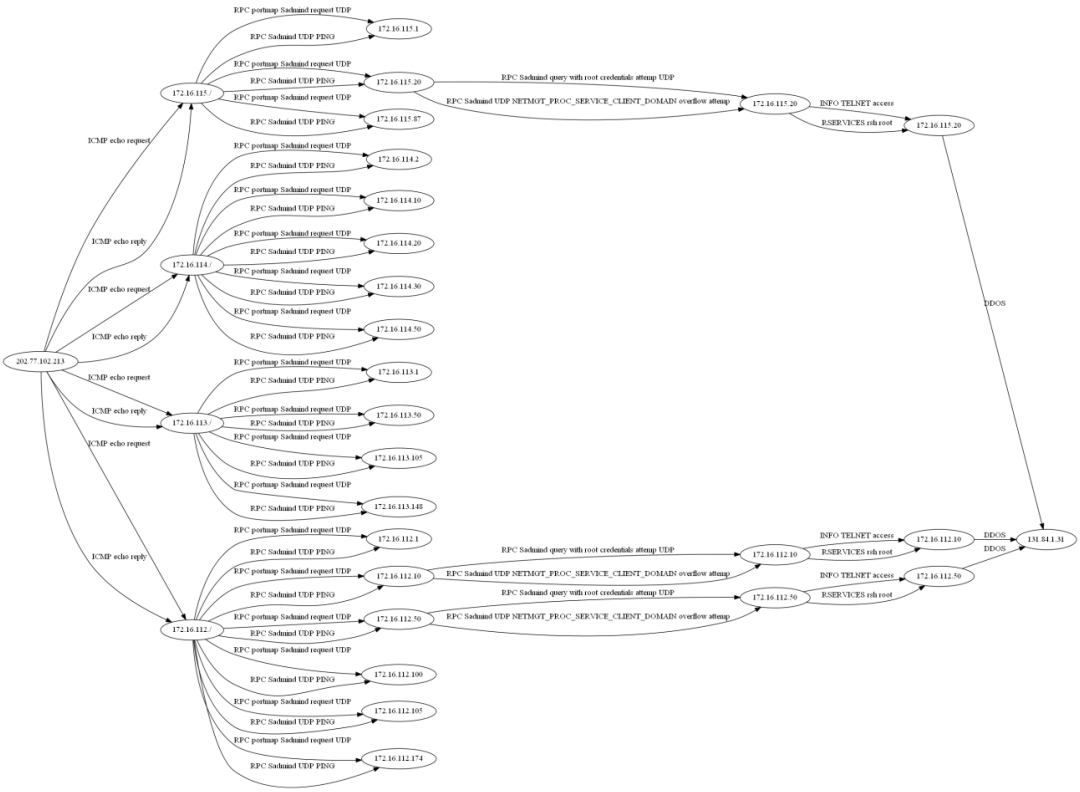
While n represents the amount of the detected attack scenarios.

5. Experimental Analysis

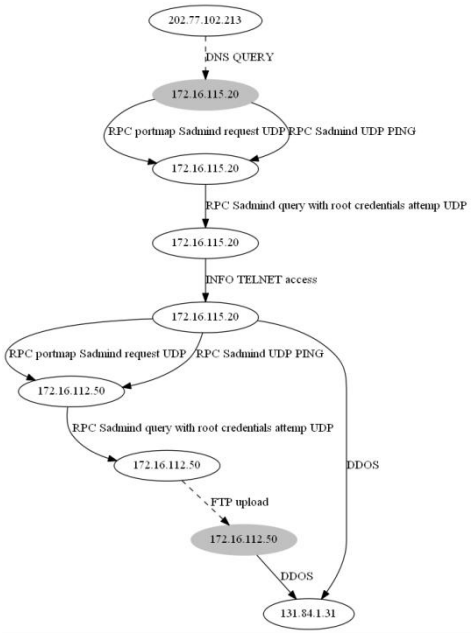
Lincoln Lab provides the specific dataset, DARPA2000[19], for testing the intrusion detection scenario. The Defcon23 CTF[20] dataset used in the 23th hacker competition is suitable for analyzing the competing process during network attack. In this section, we choose these two datasets to verify the feasibility and the effectiveness of the proposed algorithms. Firstly, we replayed the datasets with TCPReplay, and detect the data flow with Snort. The attack phase was identified through fusing the captured flow. We use Graphviz to visualize the status transferring graph. Finally, we assessed the network security situation with the above algorithm.

5.1. LLDOS Dataset

The DAPRA2000 dataset has two subsets: LLDOS1.0 and LLDOS2.0.2. Each of the two subsets contains an integrated DDOS attack procedure. The skill level of the former attacker is novice, while the latter is more stealthy. In LLDOS1.0, attacker firstly launched IPSweeping in four network segments (172.16.115/, 172.16.114/, 172.16.113/,172.16.112/) to look for the targeted host running Sadmind service. The effective hosts are 172.16.115.20, 172.16.112.50 and 172.16.112.20. Then attacker utilizes the common vulnerability in these three hosts, Sadmind Buffer Overflow existing in Solaris OS, to launch Daemon Installed attack. The Sadmind Exploit helps attacker to get the root privilege. Finally, attacker launched DDOS attack in the targeted network based on the three hosts. During the final attack, the random IP address was used to hide the true information. So we choose the fixed mac address in our subsequent analysis. The attack status transferring graph (shown in Figure 4(a)) is generated in accordance with the Real-time Attack Phase Identifying Algorithm. In LLDOS2.0.2, the attack process is much stealthier than LLDOS1.0. Attacker gave up the easy-shielded behavior, ICMP Ping, but selected the normal behavior DNS Query to look for DNS server 172.16.115.20. The root privilege of DNS was obtained through the vulnerability Sadmind. Then attacker regarded the DNS as the footstep to control the privilege of host 172.16.112.50. Finally the DDOS attack was launched. The attack status transferring graph is shown in Figure 4(b).



(a) LLDOS1.0



(b) LLDOS2.0.2

Figure 4. Attack Status Transferring Graph of LLDOS

Referring to the above attack status transferring graphs, the inner connection between every independent attack event can be clearly described. Comparing with the method which associates the warning events, this graph concisely shows the causal relationship between attack behaviors. In figure 4(b), the DNS QUERY and FTP Upload are normal accessing methods, which cannot be regarded as anomalous behaviors. In fact, these two behaviors are meta attack events, which means the regular security defense device leaks the attack warning information. The improved algorithm can predict the concealed attack status referring to the following events, which effectively solve the leakage problem and truly reappear the process of status transferring in real attack.

We analyze the attack events as well as the running services to obtain the key vulnerabilities in the attacked hosts. Detailed information is shown in table 1.

Tabe 1. Key Vulnerabilities in Attacked Hosts

Vulnerability	Mil l	Pascal	Locke	www.af.mil
ICMP Incorrectly Configured	√	√	√	
SunRPC Incorrectly Configured	√	√	√	
Sadmind Buffer Overflow (CVE-1999-0977)	√	√	√	
RCP Incorrectly Configured	√	√	√	
SYN Flood (CVE-1999-0116)				√
HINFO Query Incorrectly Configured	√			
FTP Incorrectly Configured	√	√	√	

Then we analyze the exploitation between all vulnerabilities during the attack and calculate the Impact value based on CVSS. The result is shown in table 2.

Table 2. Exploitation between Vulnerabilities

Attack Events	Exploited Vulnerability	Impact
IPsweep	ICMP Incorrectly Configured	1
Sadmind Ping	SunRPC Incorrectly Configured	2
Daemon Installed	Sadmind Buffer Overflow (CVE-1999-0977)	10
Sadmind Exploit	RCP Incorrectly Configured	4
DDOS	SYN Flood (CVE-1999-0116)	10

This network can be divided into DMZ area and INSIDE area. DMZ area occupies one segment, while INSIDE area occupies six. The whole weight of DMZ is 0.1, and all hosts in this area equally assign the weight. In INSIDE area, the weight of segment 172.16.113/, 172.16.116/, 172.16.117/, 172.16.118/ are all 0.1 and hosts in each segment equally assign the weight. The weight of segment 172.16.115/ is 0.1, and Mill’s weight is 0.05 while the rest of hosts equally assign the weight. The weight of 172.16.112/ is 0.2, and Pascal and Locke’s weight are all 0.05 while the rest are equally assigned.

In the following, we verify the correctness of network security situation assessment in LLDOS1.0. Combined with the IDS warning as well as the auditing log, we evaluate the real-time network security situation by fusing the attack events, identifying the attack phase and assessing the security situation value sequentially. We choose the host MILL as an example. In 10:08:07, the host is attacked by SadmindPing attack. Fusing the auditing logs from DMZ, INSIDE and BSM, the probability of attack occurring is p2(s)=0.918. And it is easily to know that p2(ac)=0.918 because the needed vulnerability is existed in this host. Comprehensively analyzing the impact of attack and the weight of every host, the influence to network security situation by the current attack path is

$$sa(path)=p_1(s)\times impact_1(v)\times weight_1+p_2(s)\times impact_2(v)\times weight_2$$

$$=0.917\times 1\times 0.5+0.918\times 2\times 0.15=0.7339$$

At that moment, the network is intruded by one attack path, which means the network’s security situation is equal with the attack path’s influence. SA=sa(path)=0.7339. The detailed information is shown in Table 3.

Table 3. Network Security Situation Result

Time	Attack status	Mill	Locke	Pascal	www.af.mil	SA
09:51~09:52	A1_status1	0.917	0.917	0.917	0	0.4585
10:07~10:17	A1_status2	0.918	0.918	0.918	0	0.7339
10:33~10:35	A1_status3	0.95	0.95	0.96	0	2.1639
10:50	A1_status4	0.94	0.94	0.94	0	2.7279
11:27	A1_status5	0	0	0	0.96	3.6879

With gradually realizing the attack intension, the security situation is growing up. In fact, the network is always in the low risk status. This is because for the whole network, the attacked hosts only occupy a small part. So the situation value can correctly fit the actual condition.

5.2. CTF Dataset

Defcon is the biggest hacker organization in the world. In the annual competition, Capture The Flag, 20 high-skilled network attack and defense teams will compete by intruding other's network and defensing their own network. The organizer collect all the network flow with capture tool. The dataset is almost several hundreds of gigabytes. We choose the attack data from Blue Lotus group in Defcon CTF 23 for this experiment. This dataset includes three days' attack information, we assess the first day's network security situation.

According to the Attack Phase Identifying Algorithm, the attack status transferring graph is shown in figure 5. In this graph, 19 attackers launched attack to the targeted network. Because the vulnerability in the network is the same for every attacker, all the attack paths are similar.

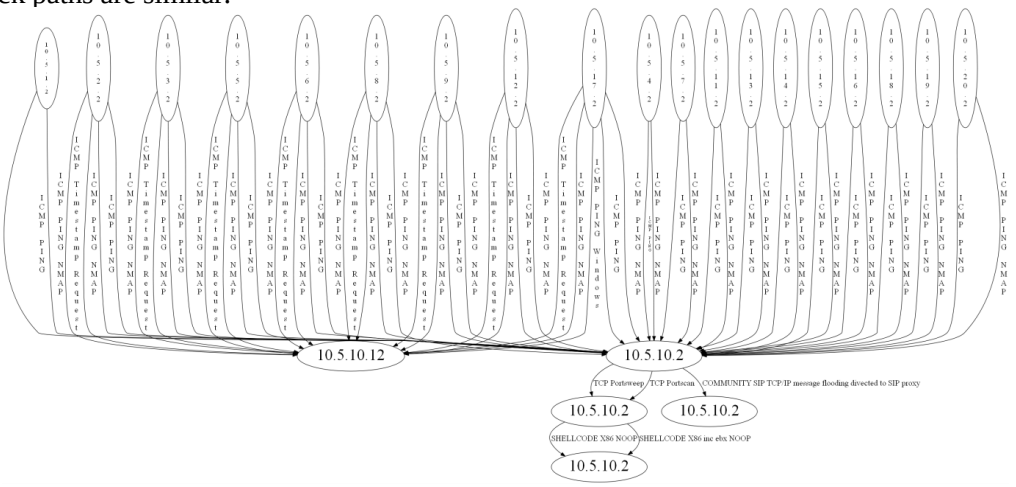


Figure 5. Attack Status Transferring Graph

The vulnerability information of this network is unknown. So we suppose that all needed vulnerabilities can be exploited in this network. The assessing result of security situation is shown in figure 6.

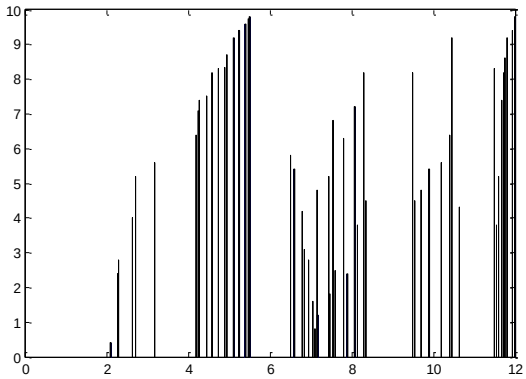


Figure 6. Network Security Situation Assessment Graph

In figure 6, the horizontal axis represents time and the vertical axis represents the security situation value. During the period 2 to 4, attackers focus on scanning the network. Attack event SHELLCODE X86 NOOP is launched in period 4 to 6. The situation value is growing in this period. In period 6 to 7, attackers just wait and don't launch any attack. Because of the limitation of transferring waiting window, the attack scenario will be deleted. So the situation value is decreasing. During the period 8 to 11, several attackers

take actions and others still keep waiting. The situation value is changing without regular pattern. In period 11 to 12, all attackers intrude the network with SHELLCODE X86NOOP or SHELLCODE X86 in ebx NOOP, and the situation value suddenly increase. Consequently, the network security situation graph can correctly depict the actual attack.

5.3. Analyzing of Algorithm Efficiency

Aiming at identifying attack phase and attacker, the proposed algorithm provides a more effective method for quantitatively assessing the network security situation. The security defense device may result in many problems such as repetition, disorder, false positives, missing and et al., which seriously disturb the identification of network attack. In the following, the efficiency of the proposed algorithm is going to analyze in accordance with these four aspects.

(1) This algorithm can deal with the repetition of warnings. Two steps are utilized in this paper to handle this problem. The first step is to cluster the warning events according to their characteristics, which can aggregate the repeated events into one single event. The second step is to discard the repeated events based on the status transferring, which reduce the repeated events' influence for evaluating the security situation.

(2) This algorithm can deal with the disorder of warnings. The following status which is captured earlier is temporarily saved as the new status, middle. After the pre-status is captured, the post-status is refreshed and turned to happened status. This method can obviously improve the identification of attack phase.

(3) This algorithm can deal with the false positives. Because of the inherent drawbacks of security system, plenty of wrong warnings are generated. Two methods are applied in this algorithm. Firstly, fusing the warning information from different multiple sensors, the incorrect influence by false positives can be reduce because of the low probability that different sensors generate the same wrong warning. Secondly, this algorithm restores the attack scenario. Wrong warning is usually a single attack, so it can hardly effect the identification of real attack scenario.

(4) This algorithm can partly distinguish the false negatives. The middle status can deal with this problem in some extent. However, if the following status is unsuccessful, this algorithm in identifying the false positives is invalid.

(5) This algorithm preliminarily analyzes 0-day vulnerability and 0-day attack. The middle status saves the unsuccessful attack, which can predict possibility of 0-day vulnerability. This method greatly rely on the captured of post-status and is hard to verify the correctness through experiment, which can discuss only in theoretical aspect.

6. Conclusion

In order to correctly analyze the influence by multi-step attack and comprehensively evaluate the network security situation, a multi-step attack-oriented assessment method of network security situation is proposed. Firstly, the security events are clustered according to attack scenario to identify the attackers. Secondly, attack trace and attack phase are distinguished by association analysis of all attack scenarios. Finally, a situation quantification method is proposed on the basis of CVSS. The experimental result indicates that the proposed method can effectively deal with the repetition, disorder of warnings, false positives and false negatives. Network security situation assessment includes the assessment of current status and the prediction of future status. This paper mainly focuses on the assessment of current attack status. The next research will enhance the study on predicting the future status and improve the comprehensiveness in security situation assessment.

Acknowledgment

This research is supported by The National Natural Science Foundation of China (No.61303074, 61309013). The authors also like to acknowledge contributions made by State Key Laboratory of Mathematical Engineering and Advanced Computing for experimental data and environment.

References

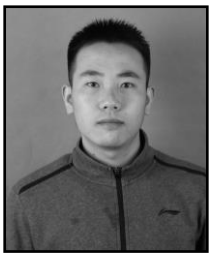
[1] Wu Di, Lian Yifeng, Chen Kai, et al. A Security Threats Identification and Analysis Method Based on Attack Graph [J]. Chinese Journal of Computers, 2012, 35(6): 1938-1950.
[2] Tian Zhihong, Yu Xiangzhan, Zhang Hongli, et al. A Real-Time Intrusion Forensics Method Based on Evidence Reasoning Network [J]. Chinese Journal of Computer. 2014, 37(5): 1184-1194.
[3] Alhazmi O H, Malaiya Y K, Ray I. Measuring, analyzing and predicting security vulnerabilities in software systems [J]. Computers & Security, 2013, 26(3): 219-228.
[4] Hannes Holm, Mathias Ekstedt, Dennis Andersson. Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks [J]. IEEE Transactions on dependable and secure computing, 2015, 9(6): 825-837.
[5] Endsley MR. Design and evaluation for situation awareness enhancement [C]//Pro. of the Human Factors Society 32nd Annual Meeting. Santa Monica, CA: Human Factors Society, 1988: 97-101.
[6] Bass T. Intrusion detection systems & multisensory data fusion: Creating Cyberspace Situational Awareness [J]. Communications of the ACM, 2015, 43(4): 99-105.
[7] Chen Xiuzhen, Zheng Qinhua, Guan Xiaohong et al. Quantitative hierarchical threat evaluation model for network security [J]. Journal of Software, 2014, 17(4): 885-997.
[8] Wei Yong, Lian Yifeng, Feng Dengguo. A network security situation awareness model based on information fusiom[J]. Journal of Computer Research and Development, 2013, 46(3):353-362.
[9] Mirmoeini F, Krishnamurthy V. Reconfigurable Bayesian networks for hierarchical multi-stage situation assessment in battlespace [C]//Proc. of the 39th Asilomar Conf. on Signals, Systems and Computers, 2015, 104-108
[10] Xu XH, Liu ZL. A method for situation assessment based on D-S evidence theory [J]. Electronics Optics & Control, 2015, 12(5): 36-37
[11] Zhuo Y, Zhang Q, Gong ZH. Network situation assessment based on RST [C]//Pro. Of the PACIIC, Wuhan, 2012, 502-506.
[12] Zhou Y, Zhang Q, Gong ZH. Research and implementation of network transmission situation awareness [C]// Pro. Of the CSIE, Los Angeles, 2013, 210-214
[13] Zhang Yong, Tan Xiaobin, Cui Xiaolin, et al. Network Security Situation Awareness Approach Based on Markov Game Model [J]. Journal of Software. 2015, 22(3): 495-508
[14] Yee Weilaw, Tansu Alpcan, Marimuthu Palaniswami. Security Games for Risk Minization in Automatic Generation Control [J]. IEEE Transactions on Power Systems. 2015, 30(1): 223-232.
[15] Lv Huiying, Peng Wu, Wang Ruimei, et al. A Real-time Network Threat Recognition and Assessment Method Based on Association Analysis of Time and Space [J]. Journal of Computer Research and Development, 2014, 51(5): 1039-1049.
[16] Cyril Onwubiko, Thomas Owens. Situational Awareness in Computer Network Defense Principles, Methods and Applications [M]. Hershey: IGI Global Snippet, 2012:125-137.
[17] M Schiffman. Common Vulnerability Scoring System Version 2.0 [EB/OL]. [2013-7-8]. http://www.first.org/cvss/cvss-guide. html.
[18] Fatemeh Kavousi, Behzad Akbari. Automatic learning of attack behavior patterns using Bayesian networks [C]. 6'th International Symposium on Telecommunications (IST'2012), 2012:999-1004.
[19] 2000 DARPA Intrusion Detection Scenario Specific Data Sets [OL]. http://ll.mit.edu/IST/ideval/data/2000/2000_data_index.html.
[20] Capture the flag traffic dump [OL]. http://www.defcon.org/html/links/dc-cft.html.

Authors

Zhang Hengwei, He received the Ph.D. degree in the Zhengzhou Institute of Information Science and Technology. His research interests include risk assessment and game theory.

Yang Haopu, She is currently pursuing the master's degree in the Zhengzhou Institute of Information Science and Technology. Her research interests include APT attack and game theory.

Wang Jindong, He received the Ph.D. degree in the Zhengzhou Institute of Information Science and Technology. His research interests include information security and cloud model.



Li Tao, He is currently pursuing the master's degree in the Zhengzhou Institute of Information Science and Technology. His research interests include risk assessment and game theory.

