International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.217-224
http://dx.doi.org/10.14257/ijsia.2013.7.5.20

Network Security Threats Situation Assessment and Analysis Technology Study

Xiangdong Cai[1], Yang Jingyi[2] and Huanyu Zhang[1]

[1]*Automation College, Harbin University of Science and Technology, Harbin, China*
[2]*Harbin engineering university, Harbin, China*
[1]*82380102@163.com*, [2]*308595109@qq.com*

Abstract

When low level services suffer attacks, the high level services that depend on them will suffer from indirect threats. Most evaluation methods do not consider dependency relationships among services, lack the evaluation upon indirect threats, do not discuss the composition of multiple source threats. Upon these problems, an evaluation method that based on dependency analysis is presented. First, dependency relationships among services are identified from the management information of operating system and the monitoring records of network communication. Afterwards, the direct threats imposed by attacks on services and the indirect threats that transfer along dependency relationships are evaluated, and the threats that come from multiple attacks are composed by means of nonlinear composition. Finally, according to threat degrees and service values, the threat situation of the whole service architecture is evaluated. Experiment shows that the method can evaluate the threat imposed by multiple attacks on network service architecture more comprehensively and deeply.

Keywords: *dependency relationship; network security; situation evaluation; threat situation*

1. Introduction

Network security threat situation assessment is designed to alleviate the pressure of the cognition and response of the management staff, which can make the manager of security situation have a general understanding of the complex security threat to respond quickly. The research has begun in different angles and aims, in general, it started relatively early abroad, but domestic research is even more.

Bass[1] based on the intrusion detection system (IDS) belongs to the early concept of argument using multi-sensor data fusion evaluation security situation. SSARE[2] contains two parts, which are situation assessment and evaluation of response. It uses The Bayesian networks to estimate probability of attack, but it is difficult to adapt to the bigger computer network. Chen Xiuzhen *et al.*, [3] assess the network security threat situation in several levels, such as network, host, service, assess threats, vulnerabilities and attack level, and at the same time, the hierarchy is very clear. Or by means of the theory of fuzzy rough sets[4] can reduce some uncertainty, but the applicable link and scope are very limited. Assessment based on neural network[5] is very simple, but the lack of strict mathematical foundation, and it cannot guarantee that the results of the assessment are monotonicity. Wei Yong *et al.*, [6, 7] proposed a method based on information fusion. Firstly, we can calculate the probability of attack and success according to the test log and vulnerability information. Then synthesize more situation of each node. Network is not a simple stack several hosts, but as an organic whole. The access control discussion by Shahriari *et al.*, The spread of risk discusses by Zhang

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2013 SERSC

Yongzheng *et al.*, the graph theory method used by Chen Tianping *et al.*, are better reflects this idea. The combination of attack-graph and asstes-weight are more in-deep, however, multi-step attack is both rare and difficult to be detected.

Complex dependency relationship exists between the service process, when the low-level service failure occurs due to attack, it often leads to rely on their high-level service failure, which caused by a wider range of collateral damage, but most evaluation methods did not consider this triggered by attacks, indirect threat to spread along the dependencies. The same service may be threatened by multiple attacks, directly or indirectly, when be synthetic, it not reflected in the most of the methods.

In view of the above problem, this paper first to identify dependencies between services. Then before synthetic, assessing each service of direct and indirect threat. Finally using evaluation algorithm and work out the threat value.

2. Safety Factor

2.1. Services

Including from the local area network, for communication subnet interconnection equipment such as hubs, switches, routers attacks (cause network congestion or failures) is rare, and resource subnet in the deployed service is increasingly become the focus of invasion.

Definition 1 s is introduced to replace the service process in the network, while S is introduced to replace its sets, satisfy the relationship of $s \in S$.

Definition 2 $W[s]$ is introduced to indicate the quality of service, satisfy the relationship of $W[s] > 0$, while $F(s)$ is introduced to represent the threat, satisfy the relationship of $0 \le F(s) \le 1$.

$W[s]$ is to measure the importance of service, usually need to manually set. $F(s)$ is to measure the severity, the calculation method is limited.

2.2. Attack

Most of the cyber-attacks is the safety of the service, such as confidentiality, integrity, and availability.

Definition 3 a to refer to s against network attacks have occurred, A represents the collection, satisfy the relationship of $a \in A$.

By analyzing a the characteristic of the communication protocol of the attack of the service, based on TCP/UDP services and attack as an example and also based on a we can locate the attacked s according to the destination IP and port can.

Definition 4 According to the targets, s will be divided A into $|S|$ mutually disjoint subsets, with $A(s)$ represents the set of attack aiming at s.

From the definition of $A(s)$ visible, $A(s) \subseteq A$, if $s_i \neq s_j$ then $A(s_i) \cap A(s_j) = \varnothing$, $A = \bigcup_{s \in S} A(s)$.

After intrusion detection system detected a is attacked, reference to expand the attack described determine the severity of the list, according to the statistical performance of the detection method used in credibility gives a's credibility of happiness.

Definition 5 $I(a)$ represents the seriousness of a, $C(a)$ represents the happen of a's credibility, $K(a)$ represents the threat degrees of a, according to the formula (1) calculation. Meeting the range $(0,1]$ interval constraint.

 Copyright ⓒ 2013 SERSC

$$K(a) = I(a) \times C(a) \quad (1)$$

Given that most attacks are aimed at service weakness, so first classify in attack description list is a list of all kinds of the seriousness of the attacks, and then classified in BugTraq, CVE, OSVDB vulnerability database and the description of the index segment.

3. Dependencies

In view of the different operating systems, we use different methods to identify dependencies between services within the host. In the Windows SYSTEM, use API function EnumDependentServices enumeration SCM (the Service Control Manager) database (the persistent store is located in the registry key HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services son) stored in the dependencies. In accord with "Linux Standard Base 1.3 ~ 4.0" Standard Linux version, is responsible for the rev. Stop the service script file has a head called "INIT INFO" formatting of the notes, which describes the dependency. Network communication between monitoring service (request/reply) can identify across a host of dependence.

Definition 6 To set $\Psi(s)$ represents s depends on low-level services, satisfy the $\Psi(s) \subset S$ relationship.

If s_i rely on s_k, so when the monitoring to the communication between s_i and s_k the (inter-process communication includes both within the host, such as a named pipe, *etc*, also including network communication across the host), the decision is s_i in the call s_k.

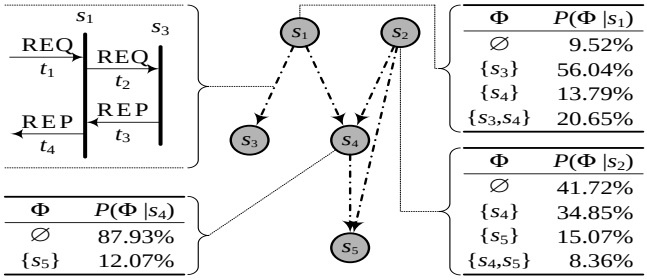

Figure 1. Dependence and Invoke the Sample

In Figure 1 shows the example, from point s_i to point s_k lines directed arc represents s_i depend on the s_k. As s_1, for example, $\Psi(s_1) = \{s_3, s_4\}$ shows that only s_1 when in the period of $[t_1, t_4]$ processing a single business, just think about Φ counting tracking effectively.

When s is dealing with a business request, may has to call some of $\Psi(s)$ the lower-level services, the invoked service form collection Φ, known as the "invocation pattern", meet the relationship $\Phi \subseteq \Psi(s)$. As business request is different, the corresponding Φ also often have changed, by tracking Φ can count statistics the incidence of the patterns $P(\Phi \mid s)$.

If you are not allowed to deploy host level monitoring, and will not be able to statistics some Φ and $P(\Phi \mid s)$ of s, the default s is only 1 kind of invocation pattern, namely, $\Phi = \Psi(s)$, $P(\Phi \mid s) = 100\%$ that steady deterministic dependence, thus to facilitate the implementation.

Strict segmentation of dependencies should be able to constitute a directed acyclic graph, otherwise cause illegal infinite recursion. This section discusses explicit dependent on directly, only implicit indirectly depend on or rely on see later in this article.

Copyright ⓒ 2013 SERSC

4. Assessment Methods

4.1. The Basic Idea

In the collection $A(s)$ against s direct threat toward a service $F_A(s)$ according to the formula (2) calculation, satisfies the constraints $0 \le F_A(s) \le 1$. Regard $(1-K(a))$ as the probability of a attack does not pose a threat, then its successive multiplication said $A(s)$ does not pose s a threaten to the probability of, after eliminating the partial probability $F_A(s)$. After nonlinear superposition, if $a \in A(s)$,then $F_A(s) \ge K(a)$

$$F_A(s) = \begin{cases} 0, & A(s) = \varnothing \\ 1 - \prod_{a \in A(s)} (1-K(a)), & A(s) \ne \varnothing \end{cases} \quad (1)$$

When the s_i invocation pattern is Φ for (that is, to deal with a business need to call Φ all the low-level service), if any of the Φ service due to the attack fails, all can lead to s_i failure, this is a kind of by the attacks, along the dependency transfer indirect threat, calculated according to formula (3), to remember $F_\Phi(\Phi)$, satisfies the constraints $0 \le F_\Phi(\Phi) \le 1$. If $F(s)$ will be regarded as attack caused by the failure s , the $(1-F(s))$ LianCheng said not the probability of Φ failure, in the same way can get $F_\Phi(\Phi)$.

$$F_\Phi(\Phi) = \begin{cases} 0, & \Phi = \varnothing \\ 1 - \prod_{s \in \Phi} (1-F(s)), & \Phi \ne \varnothing \end{cases} \quad (2)$$

From a statistical point of view, when s is dealing with all kinds of business, $P(\Phi \mid s)$ is depending on the collection Φ in probability, so the indirect s threats $F_D(s)$ should be various $F_\Phi(\Phi)$ according to the $P(\Phi \mid s)$ weighted sum, as shown in formula (4) and satisfy the constraints $0 \le F_D(s) \le 1$.

$$F_D(s) = \sum_{\Phi \subseteq \Psi(s)} \left(F_\Phi(\Phi) \times P(\Phi \mid s) \right) \quad (3)$$

Direct $F_A(s)$ and indirect $F_D(s)$ threat to according to the formula (5) synthesis $F(s)$, satisfies the constraints $0 \le F(s) \le 1$.

$$F(s) = 1 - (1 - F_A(s)) \times (1 - F_D(s)) \quad (4)$$

Used $(W[s] \times F(s))$ to measure s the threat situation, when the service is more important, the more serious the threat is, the threat of the value is greater. The whole S set of threats situational value U according to the formula (6) calculation.

$$U = \sum_{s \in S} (W[s] \times F(s)) \quad (5)$$

In order to facilitate the comparison between different network, according to formula (7) will return U one becomes u , satisfies the constraints $0 \le u \le 1$.

$$u = U \Big/ \sum_{s \in S} W[s] \quad (6)$$

Further generalization can be more "security",which is divided into three parts in accordance, they are confidentiality, integrity, availability. Respectively defined on each

 Copyright ⓒ 2013 SERSC

side $I(a)$, $K(a)$, $F_A(s)$, $F_\Phi(\Phi)$, $F_D(s)$, $F(s)$, $W(s)$, U, u, according to the principle mentioned above assess all aspects of the threat, so as to expand to three groups of the definition and evaluation of sui generis, further discusses escapes.

4.2. Describe Algorithm

From formula (3) ~ (4), to calculate $F_D(s)$, need to find out $\Psi(s)$ in the various services (x) in $F(x)$, the on-demand computing embodied in the form of depth-first recursive call in algorithm 1. The Boolean scalar $Updated[s]$ called "update tag", when it is true that $F(s)$ value has been updated and is effective, or that have not been updated, and it is invalid.

Compose1 calculate $F(s)$
Input: s
Output: $F(s)$

1. IF $Updated[s] = \text{false}$ THEN
2. FOR EACH $x \in \Psi(s)$ DO
3. CALL $Compose(x)$
4. ENDFOR
5. $F(s) \leftarrow 1-(1-F_A(s))\times(1-F_D(s))$
6. $Updated[s] \leftarrow \text{true}$
7. ENDIF

Line 1 and 7 check if not calculated $F(s)$, if the calculated no longer double counting, or find out $F(s)$ later on line 6 will set $Updated[s]$ to true. In dependency graph, the path between two vertices may be more than one, for example, in Figure 1 from s_2 to s_5 have $s_2 \to s_4 \to s_5$ and $s_2 \to s_5$ two paths, in order to avoid double counting $F(s_5)$, it is necessary to check before computing (line 1, 7), mark (line 6) after calculation.

2 ~ 4 lines cycle $\Psi(s)$ to list each item in the low-level services x, and the recursive call algorithm 1to get $F(x)$. According to the formula (2) ~ (5), line 5 gives the value of $F(s)$.

Dependency graph may contain a number of mutually connected subgraph, each graph contains at least one of degrees of 0 vertex (not rely on any services). In algorithm 2, line 1 $Updated[s]$ is set to false. An enumerated set 2 ~ 6 line cycle, find out vertex degree is 0, called algorithm 1 the threat of s and rely on the service; Line 7 according to the formula (6) ~ (7) calculate u.

Compose2 evaluate
Input: a, $K(a)$
Output: u

1. $(\forall s \in S)(Updated[s] \leftarrow \text{false})$
2. FOR EACH $s \in S$ DO
3. IF $InDegree(s) = 0$ THEN
4. CALL $Compose(s)$
5. ENDIF
6. ENDFOR
7. $u \leftarrow \sum_{s\in S}(W[s]\times F(s)) \Big/ \sum_{s\in S} W[s]$

Copyright ⓒ 2013 SERSC

Next regard algorithm 1 ~ 2 as a whole, use λ to describe $\max_{s \in S}(|\Psi(s)|)$, analysis of time and space complexity.

Time complexity analysis are as follows: (1) each has not been calculated s up to check in λ algorithm 1,2 ~ 4 line update tag; (2) the synthesis of $F_A(s)$ up to need $|A|$ calculations; (3) synthetic $F_\Phi(\Phi)$ need λ at most times operation, calculated $F_D(s)$ up to use 2^λ value $F_\Phi(\Phi)$, therefore, synthetic $F_D(s)$ need at most $\lambda \times 2^\lambda$ times. For a total of a $|S|$ service, so the comprehensive complexity is $O(|S| \times (|A| + \lambda \times 2^\lambda))$.

Space complexity analysis are as follows: (1) the dependencies, invocation pattern, and the statistical probability of storage cost $O(|S| \times \lambda \times 2^\lambda)$ for the level; (2) against a collection of storage overhead for $O(|A|)$ class. Therefore, for the comprehensive complexity $O(|S| \times \lambda \times 2^\lambda + |A|)$.

In terms of statistics, the vast majority of $|\Psi(s)|$ no more than 3, many invocation pattern also had ever seen. Given neither storage, also do not calculate Φ which is not be seen and $P(\Phi | s)$, therefore, the level of complexity 2^λ is far less than usually. Taken together, the actual cost is far less than the theoretical analysis.

5. Experimental Analysis

5.1. Test Environment

Using 4 computer, install Windows 2000 operating system. According to table 1 to deploy five services, dependencies, invocation pattern and statistical probability, as already shown in Figure 1.

Table 1. Service Deployment

Host	s	Service name	$W[s]$
1	s_1	MIS Server	2.00
2	s_2	OA Server	1.30
3	s_3	SQL Server 2000	1.50
4	s_4	IIS 5.0	0.80
4	s_5	RPC	0.30

Listed in Table 2 attack, a_1 is not for a specific weaknesses of password cracking, a_2 is similar to the Slammer worm attack means, a_3 is HTTP can lead to denial of service (DoS) attack, a_4 is similar to Blaster worm attack means.

Table 2. Description

a	Target	Exploited vulnerability	$I(a)$	$C(a)$
a_1	s_3	None(crack password)	0.03	0.96
a_2	s_3	CVE-2002-0649	0.64	0.91
a_3	s_4	CVE-2001-0337	0.29	0.74
a_4	s_5	CVE-2003-0352	0.64	0.87

According to the target, A will be divided into five $A(s)$ subsets, for example $A(s_1) = \varnothing$, $A(s_3) = \{a_1, a_2\}$.

 Copyright ⓒ 2013 SERSC

5.2. The Result Analysis

In Figure 2, respectively, with a solid line and dotted line has a direct and indirect threat to the arc labels, with ring number labeled *s* nodes and directed arcs belonging to the spread of the diagram, threatened the a_i services were spread into the figure ⓘ, the same service may be threatened by multiple attacks.

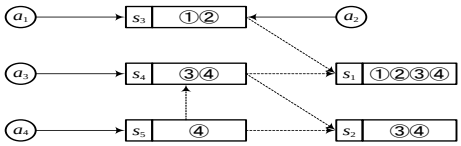

Figure 2. Threat of Diffusion and Stack

From the point of dependencies, s_4 directly dependence s_5, s_1 through s_4 indirectly dependence s_5, s_2 dependence s_5 in two ways. Accordingly, when the threat to a_4 direct s_5 spread along the dependencies, will spread to rely on s_5, s_4, s_1 and s_2 make them under threat, the indirect a_4 spread of embodied in the Figure 2 .

When the above four kinds of attack concurrent, based on the evaluation algorithm and the direct, indirect, synthetic threat as shown in Table 3.

Table 3. The Threat Assessment Result

	s_1	s_2	s_3	s_4	s_5
$F_A(s_i)$	0.00	0.00	0.59	0.21	0.56
$F_D(s_i)$	0.52	0.23	0.00	0.07	0.00
$F(s_i)$	0.52	0.23	0.59	0.27	0.56

For example with s_3, the paper expounds direct threat. When a_1, a_2 concurrent attacks s_3, according to the formula (2), the superposition of the threat of the $F_A(s_3) = 1-(1-0.03\times 0.96)\times(1-0.64\times 0.91)$, more than a_1, a_2, separate $K(a_1)$, $K(a_2)$ occurs.

To illustrate the indirect threat in this paper with an example of s_1.According to the formula (3) shows that, $F_\Phi(\{s_3, s_4\}) = 1-(1-0.59)\times(1-0.27)$, the rest of the models in the same way. According to the formula (4), the four kinds of value $F_\Phi(\Phi)$ according to the obtained after the weighting $P(\Phi \mid s_1)$ and summation $F_D(s_1)$ in Figure 1.

To illustrate the synthetic threat in this paper with an example of s_4.According to the formula (5) shows that, $F(s_4) = 1-(1-0.21)\times(1-0.07)$.

In figure 3 shows the sequence of situational, $u(t)$ said the value u of the t moment the call number at the top of the assessment period $(t-1, t]$ marked attack combination, for example, (3,4]the time mark only, " ①③ " means the period of a_1, a_3 time.

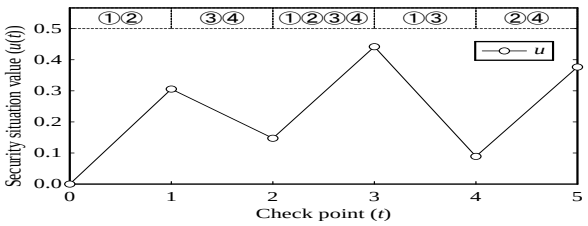

Figure 3. Threat Sequence of Situation Assessment

Copyright ⓒ 2013 SERSC

The research direction has not yet established a quantitative evaluation criterion, only qualitative comparison with the similar work. Most of traditional methods only evaluate the direct threat, but not along the dependency transfer indirect threat assessment. When, for example, s_1 rely on the service failure occurs due to attack, and s_1 is likely to result in failure, but it thinks in traditional methods, since s_1 is not directly attack, so it is not threatened by attack, and when the threat of s_1 potential evolution as a result of actual infringement fails, it is difficult to explain the failure is caused by what kind of reason, if not attack and rely on, there would be no this kind of failure mode. In addition, how to overlay or synthetic from multiple also shouldn't ignore the threat of attack. Traditional method in this article has got a good solution to these problems.

6. Conclusion

In this paper, from the perspective of dependence analysis, along the veins assessed threat situation as follows: identifying dependencies, in directed acyclic graph; Invocation pattern monitoring communication between the service process, statistics and their probability of occurrence; Each service of direct and indirect threat assessment, synthesized from multiple attacks, via multiple paths of multi-source threats; Based on threat degree, and service value to assess the threat of individual service situation; Use assessment algorithm the threat situation of the whole service system.

Traditional methods mostly isolated individual service deployment, in view of the local area network (LAN) dissever the relationship of service process, whereas in this paper, as an organic whole, which contain the dependencies, evaluate the diffusion along the dependency relationship of indirect threat, probes into the superposition of multiple source of threat, can a more comprehensive, in-depth threat revealed the whole service system.

In view of the invocation pattern tracking monitoring remains to be further improved. In addition, the field is still a lack of evaluation criterion, greatly restricted the peer comparison of workshop.

References

[1] T. Bass, “Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness”, Communications of the ACM, vol. 43, no. 4, **(2000)**, pp. 99-105.
[2] B. D’Ambrosio and M. Takikawa, “Upper D, *et al*. Security situaion assessment and response evaluation(SSARE)”, Proceedings of the DARPA Information Survivability Conference & Exposition II, Los Alamitos, America: IEEE Computer Society, **(2001)**, pp. 387-394.
[3] C. Xiuzhen, Z. Qinghua and G. X. Hong, “A hierarchical network security threat situation of quantitative evaluation method”, Journal of software, vol. 17, no. 4, **(2006)**, pp. 885-897.
[4] L. Ying Wang Huijiang and L. Jibao, “A method of network security situational awareness based on rough set theory”, Journal of computer science, vol. 34, no. 8, **(2007)**, pp. 95-97.
[5] X. Haidong, “Network security situation assessment and trend analysis of perception research”, Shanghai: Shanghai jiaotong university institute of electronic engineering, **(2007)**, pp. 89-98.
[6] W. Yong, Even other Feng Dengguo, “Network security situation assessment model based on information fusion”, Journal of computer research and development, vol. 46, no. 3, **(2009)**, pp. 353-362.
[7] W. Yong, “Based on log audit and performance correction algorithm of network security situation assessment model”, Journal of computers, vol. 32, no. 4, **(2009)**, pp. 763-772.

 Copyright ⓒ 2013 SERSC