ISBN: 978-1-948012-08-9

Contents List available at VOLKSON PRESS

Computer Science and Artificial Intelligence(CSAI)

DOI : http://doi.org/10.26480/iscsai.01.2017.23.25

Research on Buffer Overflow Attack Effect Evaluation Technology

Wang Bing-bing[a]*,Xia Qun-feng [a]

[a]*JiangNan Institute of Science and "Technology" " Shanshui East Road, Wuxi", Jiangsu,China*
**Corresponding Author: 15108948@qq.com*

ARTICLE DETAILS

Article History:

Received 02 october 2017
Accepted 06 october 2017
Available online 11 october 2017

Keywords:

Buffer overflow, Attack effect evaluation, Index system, Gray assessment model

ABSTRACT

Buffer overflow is a very common and serious consequences of security vulnerability. Attack effect evaluation plays an important role in software security assessment. Proceeding from the two aspects of the buffer overflow attack and the bypass of the security mechanism, this paper presents an evaluation method of buffer overflow attack effect. Based mainly on the process of obtaining the authority, the level of the permissions and the stability of the authority, the evaluation index system is proposed and the gray evaluation model is adopted to evaluate the evaluation criteria, then the numerical calculation method of attack effect is given. After experimental analysis, it shows that this method can evaluate the attack effect qualitatively and quantitatively.

1. Introduction

Buffer overflow is a very common and serious consequences of security vulnerability. When the computer operates on data, buffer zone is frequently used to read and write. Since the size of the buffer is usually determined by the program before it is read or written, the contents of the buffer are overwritten if it is filled with data that exceeds the buffer size. If the data is carefully prepared, attacker can even control the flow of programs. Buffer overflow vulnerability has been proposed for nearly 30 years and is still one of the loopholes which is currently widely exist in the network [1].

Attack effect assessment is an important part of cyber security. From the perspective of hackers, you can test and evaluate the system's defensive ability against cyber-attacks, and evaluate the software security qualitatively so as to improve the security management quality of the software system. A group researcher put forward a method of evaluation of the process execution profile monitoring, which can distinguish the attack effect by checking the different system call functions before and after the execution of the buffer attack [2]. Depending on the system call function executed after the overflow attack, the difference between the system privileges obtained can reflect the different attack effects. In a studied, the changes of system authority and proposed a method of assessing the validity of authority [3]. According to the magnitude of the reduction of the system authority's validity when the system encounters buffer overflow attack, the attack effect is evaluated. The studied of buffer overflow attack of network service architecture and set up an index system to obtain the authority, stability and attack time [4]. Using the Apache service architecture as an example, the validity of the network service architecture evaluation was verified.

The general organization is as follows. Section 2 introduces the index system of evaluation process selection is introduces. The gray evaluation model and calculation method are described in Section 3. According to the vulnerability example, the calculation method and the evaluation result is verified in Section 4. In the last Section, the summary and the future work is given.

2. INDEX SYSTEM

2.1 Access rights

Access control is a commonly used technology in the system, which controls the data and information that can be accessed by limiting the user's identity. After an attack, gaining cross-border control permissions is the most intuitive indicator of the effect. There are 5 types of access authority: system authority, service user authority, normal user authority, information leakage authority and authority denied. The information leakage authority refers that when reading data over the buffer size, the additional data in memory is displayed, which may reveal some useful system information and trigger a new attack. Authority denied indicates that the attack did not succeed.

2.2 Authority stability

Authority stability is an indicator of the qualitative determination of access rights. After the buffer overflow, the process space data is destroyed. In order to obtain higher privileges, attackers need to access data and execute system calls in kernel space, which may cause the process to crash. In addition, the program exits may also lead to the system crash. As system crash can cause exploit to fail, stability is one of the important indicators of the attack effect. In this paper, we use the stable length of time as the calculation indicator.

2.3 Local/Remote vulnerability

In cyber security, vulnerabilities that can be exploited remotely are more harmful than those that can only be exploited locally. A prerequisite for a local vulnerability to be exploited is that the attacker needs to have access to the local network and the attack path is relatively long. If the security defense succeeds in blocking one certain point on the attack path, the attack can be invalidated. Remote vulnerabilities score higher than local vulnerabilities.

2.4 Attack Concealment

During the attack process, the execution of the program may cause the system performance to drop or the network traffic may be abnormal, thereby causing the discovery of the security defense mechanism. The more hidden the attack, the longer the intruder controls the system, which is an effective index for assessing the attack effect. As the traffic anomalies are difficult to define in different networks, the decline in system performance is selected as the assessment method in this article.

2.5 Time Consumption

Attack time consumption refers to the duration from the beginning of the attack to the gaining of access rights. It is a cost index to evaluate the attack effect. The shorter the attack time, the better the representation. A long time, usually indicates the failure of attack.

2.6 Breakthrough in safety mechanisms

Aiming at the buffer overflow vulnerability, there are many security defense mechanisms in the system at present, which can prevent most overflow utilization and put forward higher requirements for the intruder. The Canary mechanism adds a random number before the return address to verify the return address of the stack space. After the NX mechanism is enabled, the user program stack space is not executable, which prevents the system call operation on the stack space. The ASLR mechanism distributes the address space of the stack Randomize, making the key program address uncertain to prevent illegal use. RELRO mechanism set the symbol redirection form read-only to reduce the attack on the GOT table. The system may exist a variety of defense mechanisms at the same time. While the system is more secure, it also means that the performance of the system is degraded. There are already many breakthrough methods for these security mechanisms [5-7]. The more security mechanisms that can be breached through, the better the attack effect. We use the number of security mechanisms which been breached through as the assessment indicator.

3 GRAY ASSESSMENT MODEL

The gray system is a model to study the problem of “little data and uncertainty”, which is suitable for the system of incomplete observation data. There is no strict requirement on the sample observation, and the calculation is convenient. While interacting with the system kernel, the process of buffer overflow utilization is not transparent, so the gray evaluation model is suitable for the attack effect assessment.

3.1 Determining the indicator weight

The weight represents the importance of the indicator. Corresponding to each indicator T_i, the weight is named as W_i, and $\sum_{1}^{n} W_{i}$ =1. The weights of all the indicators constitute the weight set W.

Judgment matrix method is a widely used subjective weight calculation method, which is usually calculated by 9-scale method [8]. According to the scores of experts, we summarize the importance degree between two indexes and construct the judgment matrix D_{nn}, in which the element d_{ij} represents the importance of index d_i relative to d_j.

Normalize the element d_{ij} in the judgment matrix:

$$\overline{d_{ij}} = \frac{d_{ij}}{\sum_{k=1}^{n} d_{kj}} \quad (i,j\in[1,n]) \qquad (3\text{-}1)$$

Operate the row sum on judgment matrix, that is:

$$\overline{W_i} = \sum_{j=1}^{n} \overline{d_{ij}} \text{, while } (i,j\in[1,n]). \qquad (3\text{-}2)$$

The weight value can be obtained by the following formula:

$$W_i = \frac{\overline{W_i}}{\sum_{j=1}^{n} \overline{W_j}} \quad (i,j\in[1,n]) \qquad (3\text{-}3)$$

3.2 Determining the whitening weight function

The evaluation number of gray assessment model is called the gray number, and whitening weight function is the function expression of the gray value. That is the quantitative value of judgment matrix element r_{ij}, denoted as $\overline{r_{ij}}$. For the comment set V, the whitening weight function is shown in the following figure [8]:

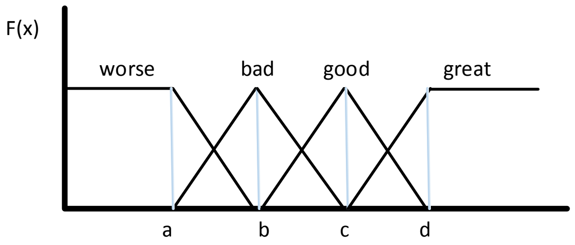

Figure 1: Whitening weight function

The specific form of expression is as follows:

(1) worse：$f_1(x)=\begin{cases} 1 & x < a \\ (b-x)/(b-a) & a < x < b \\ 0 & x > b \end{cases}$ (3-4)

(2) bad：$f_2(x)=\begin{cases} 0 & x < a, x > c \\ (x-a)/(b-a) & a < x < b \\ (c-x)/(c-b) & b < x < c \end{cases}$ (3-5)

(3) good：$f_3(x)=\begin{cases} 0 & x < b, x > d \\ (x-b)/(c-b) & b < x < c \\ (d-x)/(d-c) & c < x < d \end{cases}$ (3-6)

(4) great：$f_4(x)=\begin{cases} 0 & x < c \\ (x-c)/(d-c) & c < x < d \\ 1 & d > d \end{cases}$ (3-7)

For different indicators, the expected value of the whitening weight function (a-d) takes different values, depending on the actual indicators.

3.3 Evaluation result

For each of the evaluation indexes Ti, the values will be different due to the different expectation values selected by the whitening weight function. In order to facilitate the comparison between different assessment objectives, the quantification values need to be normalized as well:

$$r_{ij} = \frac{\overline{r_{ij}}}{\sum_{j=1}^{4} \overline{r_{ij}}} \qquad (3\text{-}8)$$

In (3-8) , $r_{ij} \in [0,1]$, which is the proportion of a single indicator. Finally, r_{ij} forms the entire decision matrix R. Evaluation results is recorded as:

E=W*R （3-9）

4 EXPERIMENTAL VERIFICATION

4.1 Experimental environment

For a buffer overflow vulnerability, there may be a variety of ways to attack. As an example, this article selects “DNSTracer 1.9 buffer overflow vulnerability” as the test target, vulnerability number is CVE-2017-9430. The vulnerability validation system environment is Ubuntu 12.04, exploit code is open source.

4.2 Determining the indicator weight and the expected value

After calculated with the expert rating method, the indicator weight judgment matrix is:

$$D = \begin{bmatrix} 1 & 5 & 3 & 6 & 9 & 8 \\ 1/5 & 1 & 1/2 & 3 & 5 & 4 \\ 1/3 & 2 & 1 & 4 & 6 & 5 \\ 1/6 & 1/3 & 1/4 & 1 & 3 & 2 \\ 1/9 & 1/5 & 1/6 & 1/3 & 1 & 1/2 \\ 1/8 & 1/4 & 1/5 & 1/2 & 2 & 1 \end{bmatrix}$$

According to the formula (3-1) to (3-3), the index weight vectors are obtained as W = (0.4688, 0.1507, 0.2233, 0.0756, 0.033, 0.0486).

For the six evaluation indicators selected in this paper, according to the actual situation and the characteristics of cyber-attacks, the expected value of the whitening right is as follows:

Table 1: Expected value of the whitening right

Indicator	**Expectation value set (worse, bad, good, great)**
Access rights	Authority (information leakage, normal user, service user, system)
Authority stability	Duration of stable permissions (20s, 40s, 60s, 80s)
Attack Concealment	Performance decline (%80, %60, %40, %20)
Time Consumption	Time needed (60s, 30s, 15s, 5s)
Breakthroughs	The number of breakthroughs (0,1,2,3)

The indicator “remote / local vulnerability” has only two kinds of results in the evaluation. In this paper, we use 0.5 for the value of the local vulnerability and 1 for that of the remote vulnerability to calculate the evaluation result.

4.3 Assessment Results

After the test, the result set of the six indicators is (system authority, > 80s, local, 7%, 2s, 0). According to Equation 3-4 through Equation 3-8, the judgment matrix can be calculated as:

$$R = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

According to the formula 3-9, the evaluation result is E = W * R = (0.0486, 0.1117, 0.1117, 0.7281). It can be seen from the results that the results of this utilization are between good and great gray intervals, more likely to be great [9]. The experimental results demonstrate the effectiveness of the gray scale evaluation model.

5 CONCLUSION

In order to meet the needs of network security analysis, this paper presents an effect evaluation method based on the general buffer overflow vulnerability attack process. Through the specific exploit example, the effectiveness of the assessment method is verified using the evaluation model proposed in this paper.

The future work is to reduce subjective judgments among different modes of utilization, to establish a more comprehensive assessment index, and increase the relevance analysis and judgment of different utilization modes.

REFERENCES

[1] Yi-chao, L., Dan, L. 2008. Research and Development of Buffer Overflow. Computer Science, 35 (1), 87-89.

[2] Peng, S., Xing-yuan, C. 2009. Buffer Overflow Attack Impact Detection Based on Process Execution Profile. Computer Engineering, 35 (6), 156-158.

[3] Xiu-zhen, C., Jian-hua, L. 2009. Quantitative assessment of privilege validity for security situation awareness. Journal of Southeast University, 39 (4), 742-746.

[4] Song, W., Yong-xin, F. 2015. Research on Effect Evaluation Technology of Network Attack Oriented Web Service. ShenYang Ligong University, 9 (2), 44-46.

[5] Yinan, M., Lihe, Z. 2014. Buffer Overflow Protection Mechanism and Bypass Technology Under Windows. Computer Engineering, 9 (36), 147-151.

[6] Zhuo, H., Xiao-ming, R. 2011. Research on Security Mechanisms Evasion of Windows 7 Based on reverse Analysis. Information Engineering University, 17-26.

[7] Hu-sheng, Z., Wei-ping, W. 2011. Research on Key Memory Attack Windows 7 Operating System. Netinfo Security, 7 (1), 38-41.

[8] Yong-jie, W., Liang, J. 2007. Research of Online Evaluation Model and Algorithm for Network Attack Effect [J]. Computer Science, 34 (5), 72-74.

[9] Bo-fu, Z., Xiao-chuan, Y. 2011. Attack Ability Evaluation of Attackers based on Grey Theory. Computer Engineering, 37, 114-117.