2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC) | 978-1-7281-5244-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/ITAIC49862.2020.9339075

Evaluation Methods of WEB Security Threats Based on Situation Change

Tian Fu ,Zhen Wang ,LaiQuan Liu ,ZiQian Xiao
Hainan College Of Software Technology, Hainan, China
fu-tian@163.com, 490345452@QQ.com, 24115571@QQ.com
Corresponding Author: Zhen Wang Email:490345452@qq.com

Abstract—First of all, according to the characteristics of the current Web application service attack, this paper establishes the Web security situation analysis model based on the attack chain, combines the information security level protection 2.0 evaluation control points with the Web security factors extracted from the model, and evaluates the Web service security state by the combination of network analysis and fuzzy theory. Through the combination of quantitative and qualitative methods to solve the shortcomings of the existing vulnerability model and tracking Web application service security specification inspection, to provide a theoretical basis for Web application service security evaluation.

Keywords—Web application services; kill chain; Security evaluation; ANP; Classified protection

I INTRODUCTION

With the rapid development of Internet technology applications, especially driven by the widespread implementation and application of new technologies such as mobile Internet, cloud computing, and big data, network information technology has been deeply integrated into all aspects of the social operation, business operation, and daily life. In the current era of cyberspace, which is highly dependent on network information technology, cyberspace is facing increasingly severe security risks and threats. Therefore, it has become a research hotspot in recent years to study how to make a scientific and accurate risk assessment of the current network or network service timely and make an effective prediction of the possible threats by establishing a credible evaluation model. In the literature [1], based on the vulnerabilities in the software system and their effects on software quality, a new approach was proposed. However, the model only evaluates the security of software quality by the existence of vulnerabilities in ubiquitous software, which lacks pertinence. In the literature[2], a classified protection evaluation model of information security based on a fuzzy comprehensive evaluation of variable weight was established. The model quantifies classified protection and evaluates the security of the system with specific data, but there is no operation designed for Web services. In literature [3], a new evolutionary reasoning model for the uncertainty of system-level evaluation is proposed, where the fault tree is used to decompose the security incidents, and the minimum cut set of the fault tree is transformed into reasoning rules. Then the security state of the system is deduced by reasoning technology. In literature [4], the web security evaluation model based on fuzzy mathematics theory uses the control point of equal guarantee evaluation to evaluate the security. However, the control point involves a wide range, which leads to the poor operability of the model. Based on the kill chain model, this paper proposes a new Web service security situation analysis model, which combines network analysis with fuzzy theory to quantitatively and qualitatively analyze Web security status, to improve the science and accuracy of Web service security assessment.The major contributions of this paper may be summarized as follows:

·Construct the attack chain model based on Web application service.

·Using the analytic network process and the gray fuzzy evaluation method, this paper constructs Web services risk warning model based on ANP-gray fuzzy.

II. CONSTRUCTION OF THE KILL CHAIN MODEL FOR WEB APPLICATION SERVICES

The cyber kill chain was proposed by LM-CIRT (Lockheed Martin Computer Incident Response Team), a term widely used in the field of security. The cyber kill chain(CKC) [5] and the intrusion kill chain(IKC)[6] are the same concepts in this paper. To put it simply, it is a kill chain, an orderly set of paths, and means adopted by intruders to attack the target through the information system with the lapse of time [7]. Such kill chain models and analyzes the intruders' operation and its intended effect.

At present, the existing network kill chain, whether it is the classical kill chain or the extended kill chain, generally describes the network attack process from different aspects, and different application scenarios have their characteristics, and the kill chain for Web application services also has its unique characteristics. For the multi-stage kill chain of Web services, as shown in Fig.1, this paper gives an example of a Web application attack (shown in Fig.2).

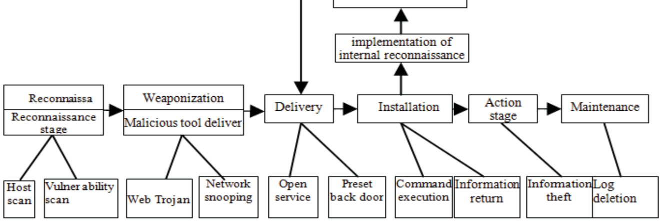

Fig.1 Classic kill chain stages

An example of the kill chain for a Web application is shown in Fig. 2.

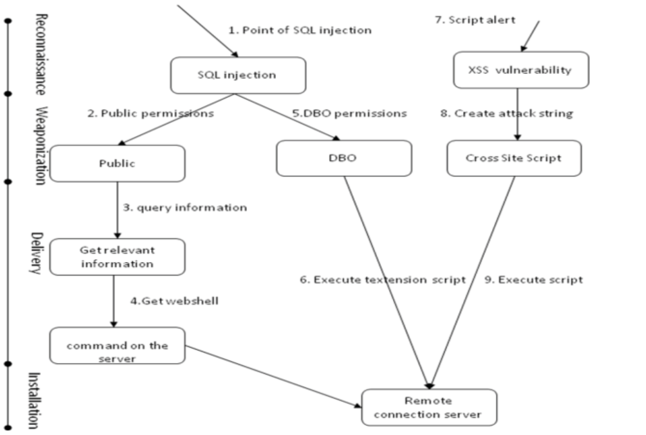

Fig.2. An example of the multi-stage kill chain for Web application

From the above kill chain, there are three ways to control the target server: 1->2->3->4, 1->5->6 or 7->8->9. Through these three kill chains, we can achieve the goal. Combined with the given kill chain model of Web application services, the three kill chains in the example use different vulnerabilities to achieve the target task in the information reconnaissance, weaponization and delivery stages. The specific steps are as follows:

(1)Reconnaissance stage: The intruder collects and analyzes the relevant information of Web application servers, such as service program, application protocol, operating system and other information related to the main body.

(2)Weaponization stage: Intruders select appropriate attack tools according to their own technical level, experience and attack and defense tools.

(3) Delivery stage: Intruders will use the attack points existing in the target Web application services to complete the attack with some appropriate technical means (Sql Injection, analysis of network packets, etc.).

In order to more accurately describe the multi-stage model of the kill chain for Web application services, the model definition of the kill chain state is given here.

$$H(S,V,X)=H(S_1,S_2,\cdots S_l)\prod_{i=1}^{n-l} f\ (S_{i+l})V_iX_i \qquad (1)$$

$$S_{i+1}=A_iS_i+B_iu_i \qquad (2)$$

$$y_{i+1}=Q(S_{i+1}) \qquad (3)$$

It means that the use of some vulnerabilities to achieve the transformation of node state is affected by different attackers' exploit factors, which mainly depend on the attacker's technical level, experience, attack tools, and other factors. The state transition function refers to the state transition algorithm（STA）[8], V_i which is expressed as follows: $V_i=(p,n,o)$, where p is the popularity of vulnerabilities, N is the number of vulnerabilities, O is the severity of vulnerabilities, $o\in\{\text{Mild，General，High，Serious}\}$, and the form of X_i is as follows: $X_i=(t,o)$, where t is the trigger condition of the attack, o the destruction degree of the attack event， $o\in\{\text{Mild，General，Serious}\}$.

According to the above definition, with the help of formulas (1), (2), (3) to calculate the state of the Web application service kill chain, it can be known that the more vulnerabilities that can be exploited in a certain stage of the attack chain, the greater the harm degree, and the more serious the attack event is, then the more kill chains are targeted against Web application services, the easier the attack chain is formed, the lower the security value of Web application services is, and the higher the risk is.

III SAFETY ASSESSMENT MODEL

A. Overall Evaluation of Network Security level Protection 2.0 and stage Defense based on kill chain

At present, the domestic information security level protection 2.0 evaluation is mainly based on the regional boundary security, communication network security, secure computing environment, and security management center as the core of the overall security system [9], as shown in Fig.3 below. From the technical level, at present, the security of the domestic application information system is mainly through the security zone boundary, secure communication network, secure computing environment, security management, and other aspects. through the establishment of boundary protection, access control, intrusion prevention, data security, and other control points, to achieve the purpose of security protection of the application information system. This paper analyzes the control points of Web service penetration attack and equal guarantee evaluation 2.0 evaluation, and sums up the corresponding relationship between Web risk assessment and the requirements related to the application of security indicators in is equal guarantee evaluation 2.0 evalu equal guarantee evaluation ation, as shown in Table 1. below.

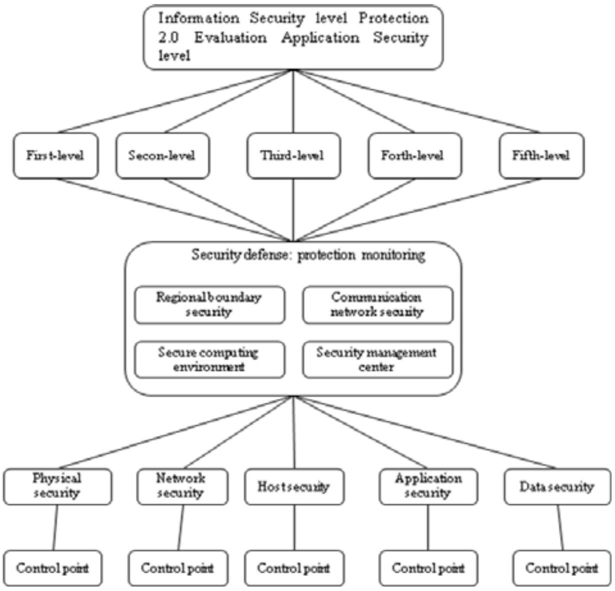
Information Security level Protection 2.0 Evaluation Application Security level
First-level
Secon-level
Third-level
Forth-level
Fifth-level
Security defense: protection monitoring
Regional boundary security
Communication network security
Secure computing environment
Security management center
Physical security
Network security
Host security
Application security
Data security
Control point
Control point
Control point
Control point
Control point

Fig .3. Overall security system for application security

TABLE I. The corresponding relationship between the requirements related to the application of safety indicators in

Web risk assessment and isoinsurance 2.0 assessment (level 3 as an example)

Safety control point	*Requirement items*	*Safety index*
Identification	(1) The logged-in user should be identified and authenticated. The identity is unique, and the authentication information has complexity requirements and is changed regularly. (2) The login failure handling function should be provided and enabled, and necessary protective measures should be taken after multiple login failures. (3) The user should be forced to change the initial password when logging in for the first time. (4) When the user identity authentication information is lost or invalid, technical measures should be taken to ensure the security of the process of resetting authentication information.	Cookie kill Weak password Brute force cracking
Access control	(1) Access control function should be provided to assign accounts and permissions to logged-in users. (2) Account management. Change the default password of the default account. (3) Different accounts should be granted the minimum authority required to complete their respective tasks, and a mutually restrictive relationship should be formed between them. (4) The authorized subject should configure the access control policy, and the access control policy should stipulate the access rules of the subject to the object. (5)The granularity of access control should reach the user level of the subject and the file, database table, record, or field level of the object.	Form bypass Directory ergodic Upload file attack XSS attack CSRF attack Xpath injection attack
Software fault tolerance	(1)The data validity test function should be provided to ensure that the input through the man-machine interface or the communication interface meets the requirements of the system setting. (2)The known vulnerabilities that may exist in the application software components should be found, and the vulnerabilities should be repaired in time after full testing and evaluation.	SQL injection Execute any command Buffer overflow Script code exposure attack Side note attack
Resource control	(1)The maximum or minimum use of system resources by a single user should be limited. (2)It should be possible to limit the maximum number of concurrent session connections in the system. (3)The operation of users to sensitive marked important information resources should be strictly controlled according to the security policy. (4)The service priority setting function should be provided, and after installation, the priority of the access account or request process should be set according to the security policy, and the system resources should be allocated according to the priority.	Denial of service attack Sensitive directory
Data integrity	(1) Check code technology or cryptographic technology should be used to ensure the integrity of important data in the process of transmission, including but not limited to authentication data, important business data, important audit data, important configuration data, important video data, and important personal information, etc. (2) Check code technology or cryptographic technology should be used to ensure the integrity of important data in the process of transmission, including but not limited to authentication data, important business data, important audit data, important configuration data, important video data, and important personal information, etc.	Network sniffing Redirect attack Physical path disclosure
Data confidentiality	(1) Cryptography should be used to ensure the confidentiality of important data in the process of transmission, including but not limited to authentication data, important business data, and important personal information, etc. (2) Cryptography should be used to ensure the confidentiality of important data in the storage process, including but not limited to authentication data, important business data, and important personal information, etc.	Network sniffing XSS attack

According to the kill chain model constructed in this paper, when carrying out security defense based on the kill chain, we first need to clarify the position of the current security problems in the kill chain. Secondly, analyze the threats and defense measures faced by the target system in the pre-order and post-order stages of the kill chain, and see whether other security measures can block the kill chain as a whole, or whether other security vulnerabilities can be exploited by attackers. Bypass the current defense measures. Based on the information security level protection 2.0 evaluation, when conducting the overall evaluation, we first longitudinally analyze whether there is a security hidden danger at each preorder control point in the secure computing environment, that is, whether it is possible to block the attack behavior in the links such as target reconnaissance, weaponization, vulnerability exploitation, delivery, etc., that is, the overall evaluation between the security control points. Secondly, it analyzes whether the corresponding security measures such as security communication network, security zone boundary, security management center, security management, and so on can block the attack behavior, that is, the overall interregional evaluation. Combining the two core ideas of security defense, the security index and kill technology based on the kill chain is essentially the same as the control points evaluated by equal protection 2.0.

B. Security Evaluation Metrics of WEB Application Services based on hierarchical Defense

According to the analysis of Fig.1 and Fig.3, the key to the security evaluation of Web application services lies in the technical test indicators. as the technical means for Web service attacks become more and more advanced, especially for APT (Advanced Persistent Threat), which has the characteristics of difficult detection, long duration, and clear attack target, how to analyze whether there are security risks at the preorder control points in the Web service environment through vertical security analysis. And by blocking the attack behavior in the links of target reconnaissance, weaponization, vulnerability exploitation, and delivery to effectively improve the Web service security defense. Through the research and analysis of the existing Web service security evaluation system, this paper combines the Web application service kill chain multi-stage model established in this paper with the Web security evaluation model in the information security level protection 2.0 evaluation architecture to build a secondary index system for Web service security evaluation, as shown in Table 2. below.

TABLE II. Web service security evaluation index system

Target	*First-level index*	*Secondary index*
Web security index system	Environmental safety	Network sniffing Sensitive information disclosure
	Communication network security	Exchange protocol Denial of service attack Cookie attack Weak password attack
	System and service security	XSS attack CSRF attack SQL injection Brute force cracking Buffer overflow Xpath injection attack Script code exposure attack Redirect attack Http heads attack Side note attack XML external entity
	Safety management	Physical path disclosure Unsafe deserialization Sensitive directory Upload file attack Security configuration error

Analytic Network Process [10-11] is a decision-making method adapted to a non-independent hierarchical structure proposed by Professor T.L.S in 1996. The model consists of two parts: the control factor layer and the network layer. The risk factors are not completely independent but interrelated and constitute an interdependent and feedback network structure as a whole. This method fully takes into account the interaction and influence of various factors in the system and is very consistent with the actual characteristics of Web service security risk.

First of all, according to the Web service security evaluation index system established in this paper, according to the CVSS 3.0 vulnerability rating standard and combined with the latest 2017 OWASP top 10 Web service risk analysis, determine the risk factors, as shown in Table 2, establish the evaluation object factor set U = {environment security, communication network security, system, and service security, security management}, that is $U=\{u_1,u_2,u_3,\cdots u_i\}$, factor evaluation index $U=\{u_{i1},u_{i2},u_{i3},\cdots u_{ij}\}$, among $1\le i\le n, 1\le j\le n$.

Secondly, establish the evaluation set V, according to the type and requirement of the evaluation result, take the threat risk of this factor to the system as the evaluation basis, establish the evaluation set as follows: v = {low risk, medium risk, high risk, high risk}. Abbreviated as V = {low, medium, high, very high}.

Thirdly, according to the ANP method, the index system of the "control layer-network layer" is constructed, combined with the defined first-level index and second-level index. According to the indirect dominance comparison method, the judgment matrix U is established by analyzing and comparing the importance of the pairwise indexes of the same level, and the maximum eigenvalue and the corresponding eigenvector of the matrix are calculated. The weight of the index is represented by the components of the feature vector. The weight vector W of the first-level index set of Web service security assessment is determined, and the weight of the first-level index is set as $W=\{w_1,w_2,w_3,\cdots w_i\}$, among $1\le i\le 4$. By calculating the eigenvalues and Eigenvectors of $WU=\lambda_{\max}U$, the eigenvalues and Eigenvectors can be approximately solved by the square root method. The calculation process is as follows:

$$A_i=\prod_{j=1}^{n}u_{ij} \qquad (4)$$

Where $1\le i\le 4$, $1\le j\le n$, A_i , W represent the product of each row of elements of the matrix.

$$\overline{\alpha}=\sqrt[n]{A_i} \qquad (5)$$

Where， $1\le i\le n$ and $\overline{\alpha}$ represent A_i the power root of n.

$$W_i=\frac{\overline{a_i}}{\sum_{j}^{n}\overline{a_i}} \qquad (6)$$

Among them, $1\le i,j\le n$ normalizes $\overline{\alpha}$. Then the maximum characteristic of the matrix is calculated by $\lambda_{\max}=\frac{1}{n}\sum_{i=1}^{n}\frac{(WU)_i}{nW_i}$, where $(WU)_i$ represents the I component of the vector WU . Through the k experts and the network to obtain the relevant data calculation, and finally calculate the first-level index weight, as shown in Table 3 below. The weight of type I factors is calculated by $U=\{u_{i1},u_{i2},u_{i3},\cdots u_{ij}\}$ and so on.

Table III. Indicator weight %

First-level index	*Wight*
Environmental safety	9.8
Communication network security	15.3
System and service security	61.2
Safety management	13.7

Finally, according to the previously defined judgment set V, set V={1, 2, 3, 4}. Take the corresponding threshold values of each evaluation grey class as 4,3,2,1, and when between two adjacent grades, the corresponding scores are 3.5, 2.5, and 1.5, respectively.The corresponding whitenization weight function is classified as follows:Where, C_{ij} is the score result of the index。

(1) The first grey class is " very high " (V =1). Set the grey number $V1 \in [4, \infty]$, and the whitenization weight function is:

$$f_1(c_{ij}) = \begin{cases} c_{ij}/4 & c_{ij} \in [0,4] \\ 1 & c_{ij} \in [4,\infty] \\ 0 & c_{ij} \notin [0,\infty] \end{cases} \quad (7)$$

(2) The second grey class is " high " (V =2). Set the grey number $V2 \in [0,3,6]$,and the whitenization weight function is:

$$f_2(c_{ij}) = \begin{cases} c_{ij}/3 & c_{ij} \in [0,3] \\ 6-c_{ij}/3 & c_{ij} \in [3,6] \\ 0 & c_{ij} \notin [0,6] \end{cases} \quad (8)$$

(3) The third grey class is " medium " (V =3). Set the grey number $V3 \in [0,2,4]$,and the whitenization weight function is:

$$f_3(c_{ij}) = \begin{cases} c_{ij}/2 & c_{ij} \in [0,2] \\ 4-c_{ij}/2 & c_{ij} \in [2,4] \\ 0 & c_{ij} \notin [0,4] \end{cases} \quad (9)$$

(4) The fourth grey class is " low " (V =4). Set the grey number $V4 \in [0,1,2]$,and the whitenization weight function is:

$$f_4(c_{ij}) = \begin{cases} 1 & c_{ij} \in [0,1] \\ 2-c_{ij} & c_{ij} \in [1,2] \\ 0 & c_{ij} \notin [0,2] \end{cases} \quad (10)$$

Using the gray statistical method, according to the whitenization weight function of formula(7)-(10), for any evaluation index c_{ij} , the gray evaluation coefficient belonging to the V evaluation gray category is solved, and then the total gray statistics are further calculated, thereby the Web services security risk early warning index of the gray fuzzy comprehensive evaluation matrix R, according to the comprehensive evaluation model $B = W \circ R$, finally calculated the Web services security level.

IV. Conclusions

In this paper, Aiming at the attack of current Web application service, this paper constructs a new Web service security situation analysis model, calculates the weight of web security index through network analytic hierarchy process, uses a fuzzy evaluation matrix and fuzzy comprehensive evaluation method to calculate the security state value of Web service, to make an accurate security assessment of Web service security state.

Acknowledgment

This project was supported The High-level Talents Project Fund of Hainan Basic and Applied Basic Research Plan (Natural Science) in 2019 (No.2019RC253). And supported by the natural science foundation of Hainan Province (No. 618ms078) .

References

[1] Du zhenyu, liu fangzheng. A new method based on vulnerabilities in software systems and their impact on software quality[J], Computer application research, 2018 36(7).

[2] XU Yang, XIE Xiao-yao, ZHANG Huan-guo.Information aecurity testing model based on variable weights fuzzy comprehensive valuation[J].China Communication,2011,8(4) : 76-83.

[3] Liu Zen Lian, Yu Da Tai. New Uncertainty Evolution Inference Model for Classified Evaluation of Information System,2010,5:537-542.

[4] QI Fu-min,XIE Xiao-yao,XU Yang.Web security assessment model based on fuzzy theory.Application R esearch of Computers.2014,6(31):1883-1888.

[5] HUTCHINS EM, CLOPPERT MJ, AMIN RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[C]//The 6th Annual International Conference on Information Warfare and Security. 2011.

[6] YADAV T, RAO AM. Technical aspects of cyber kill chain[J].Security in Computing and Communications, 2016,536:438-452.

[7] Xiaomei Li. Research on prevention solution of advanced persistent threat[C]// Proc of the 2nd International Conference on Software Engineering,Knowledge Engineering and Information Engineering. Singapore: Springer,2014: 1-4.

[8] Feng Xiao Tao, Zheng Zi Zhan,Hu Peng Fei,et al.stealthy attacks meets insider threats: A three-player game model[C]//proc of the 34th Military Communications conf(IEEE Milcom2015).piscataway,NJ:IEEE 2015:25-30.

[9] Zhang Ming, Zheng Zi Zhan,shroff NB.A game thepretic model for defending against stealthy attacks with limited resources[C]//proc of the 6th Decision and game theory for security.berlin:springer,2015:93-112.

[10] Tim Bass, Dave Gruber.a glimpse into the future of id,Special Issue Intrusion Detection,The USENIX AssociationMagazine,September 2005.http://www.usenix.org/publications/login/1999-9/features/future.html.

[11] BODMER S, KILGER M, CARPENTER G, et al. Reverse Deception:Organized Cyber Threat Counter-Exploitation[M]. McGraw-Hill Educationand Post & Telecom Press,2014.

[12] Neura l netw ork toolbox user 's Guide. Th e Mathw orks Inc, 2000.

[13] Tian Fu, YiQin Lu, Wang Zhen. APT Attack Situation Assessment Model Based on Optimized BP Neural Network[C]. Proceedings of 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2019, p 2108-2111.

[14] Liang Hao,Li xiaobo,Xu xuyu.array optimization for mimo radar based on improved adaptive genetic algorithm[J].journal of Micowaves. 2013.29(4):12-19(in chinese).