A Real-Time Risk Detection Method for Network Security based on Static Analysis

Jiajia He
Department of network data information The First Affliated Hospital of Guangdong University of Chinese Medicine
Guangzhou, 510405, China

Abstract: Traditional network security risk detection methods can only evaluate and detect the long-term security state of the network, but cannot accurately and real-time detect the network risk. Therefore, the real-time risk detection method of network security based on static analysis is studied. After analyzing the state of network security using the static constraint analysis theory, the qualitative network attack and defense using the game theory. Based on the calculation of network security risks, the artificial immune principle is used to realize the real-time risk detection. Experimental results show that the detection accuracy of this method is higher than 93.5%, which is better than the traditional method to achieve better network protection effect.

Keywords: Static analysis; Network security; Network security risks; Real-time risk detection; Artificial immunity

1. Introduction

At present most of the network security risk assessment method is static evaluation method, only a rough estimate network risk of state for a long time, not when the attack in real time detection of network security risk, so when you meet the network intrusion can real-time adjust their defensive measures, thus the most the earth to reduce the loss of the system. Therefore, real-time network security risk detection is of great significance to the study of dynamic network security [1]. At present, the traditional network security technology carries out risk detection under the control and guidance of the overall security policy. However, it is based on a static assessment method, which can only make a rough static assessment of the long-term risk state of the network, and the risk detection accuracy is poor [2].

Static analysis is a method to obtain endogenous variables according to the established exogenous variables. At present, static analysis gradually develops to be able to find more defects that can only be found by dynamic testing, so as to achieve the purpose of reducing false positives and increasing efficiency. According to the above analysis content, this paper will study the real-time risk detection method of network security based on static analysis.

2 Research on Real-Time Risk Detection Method of Network Security based on Static Analysis

2.1. Static analysis of network security state

Taking abstract interpretation as a sufficient condition for static analysis, this paper chooses to use static constraint analysis to analyze the real-time properties of network security state. Static constraint analysis is developed on the basis of type inference and data flow analysis, both of which determine program attributes by maintaining variable types or analyzing constraints between states. The constraint analysis method divides the analysis process into two stages: constraint generation and constraint solving. The former uses constraint generation rules to establish the constraint system between variable types or analysis states, namely the attribute attack graph of network security. The latter solves these constrained systems [3].

The static analysis method needs to verify that each activity in the path satisfies the security policy, that is, it repeatedly transforms an initial constraint until the constraint becomes a solved form from which the solution can be derived directly. This paper adopts the following form of minimum solution constraint solving algorithm for safety analysis and solution [4]:

$$\begin{cases} \wedge_{i=1}^{k} L_i \subseteq R_i \\ L_i = L \cup L \left| c\left(L, \cdots, L\right) \right| a \left| \perp \right. \\ R_i = R \cup R \left| c\left(R, \cdots, R\right) \right| a \left| \mathrm{T} \right. \end{cases} \tag{1}$$

In formula (1), a is set variable; c is the set constructor. $\perp$ and T represent the bottom and top elements of the range, respectively. In this set constraint solving method, the constraint is first transformed into a constraint graph: in the constraint graph, each node represents a subexpression of the constraint system, and each directed edge from node L to node R represents a set constraint $L \subseteq R$. Then the dynamic transmission closure algorithm is used to solve the problem. Therefore, when the static analysis of network security state is carried out, the attribute attack graph of network security, namely the network security constraint graph, needs to be established first [5].

The attribute attack graph of network security contains two kinds of nodes: attribute node and atomic attack node. The attribute node represents the attribute of the target network and the attacker, and the atomic attack node represents an attack by the attacker using a single vulnerability. Among them, the set of reachable attribute nodes shows all the attack targets that an attacker can reach after carrying out a network attack based on the initial attack capability. Multi-target construction algorithm is adopted to obtain all or most of the approaches that an attacker can attack the target network, so as to improve the detection accuracy of network security risks [6]. After the static analysis of the network security state, the offense and defense in the network are defined according to the game theory.

2.2. Network offense and defense qualitative

The qualitative game process of network offense and defense can be represented by the eight-tuple model, that is $NSDG=(N,B,S,t,X,P,f,G)$, each variable is defined as follows:

$N=(N_D,N_A)$ represents the participant space of the qualitative differential game of network offense and defense, N_D represents the defender, and N_A represents the attacker. $B=(DS,AS)$ represents the action space for offense and defense, and $DS=\{DS_j|1\le j\le n\}$ represents the optional defense strategy of the defense side. $AS=\{AS_j|1\le j\le m\}$ represents an optional attack strategy for an attacker. $S=\{S_k|k=1,\cdots,K\}$ represents a collection of subnet works divided by function and topology. K is the number of subnet works; S_k is the k th subnet work. $t\in[t_{bin},t_{end}]$ represents the moment of qualitative differential game of network offense and defense [7]. $X(t)=\{(\rho_1(t),\cdots,\rho_k(t),\cdots,\rho_K(t))|0\le\rho_k(t)\le1\}$ represents the network security state variable at time t, and is a K-dimensional state space composed of each sub-network infection node density $\rho_k(t)$. Since $\rho_k(t)$ is determined by the number of infected nodes in the network, the security state is discretized in the K-dimensional state space. $P=\{P_D(t),P_A(t)\}$ represents the control strategy of both offense and defense at time t, which is the control trajectory with time as the variable. $P_D(t)=\{p_D^j(t)|1\le j\le n\}$ represents the mixed strategy selected by the defender at time t, $\sum_{j=1}^{n}p_D^j(t)=1$; $P_A(t)=\{p_A^j(t)|1\le j\le m\}$ represents the mixed strategy selected by the attacker at time t, $\sum_{j=1}^{n}p_A^j(t)=1$ 。 $f=\{f_k|k=1,\cdots,K\}$ represents the network security state migration function, which is a function of the change in the density of each sub network infected node over time, in which $f_k=\frac{d\rho_k(t)}{dt}$. G Represents the set of attack targets and is also a high-risk area of network security risks.

Based on the analysis of the actual situation of offense and defense, it can be seen that the transformation of node security state is jointly determined by the interaction of offense and defense strategies. The above qualitative eight-tuple model of offense and defense game is solved, and the multi-dimensional state space of network security is divided into capture zone and escape zone [8]. If the current network security state is in the capture zone, the attacker can always make the security state reach the target set and achieve the expected target by adopting appropriate attack strategies. If it is located in the zone of evasion, the defensive side can always take appropriate defensive measures to resist the further spread of the threat and prevent the security state from migrating into the target set. Therefore, both sides of offense and defense will adopt the optimal strategy for continuous confrontation to avoid falling into the dominant region of the other side, so as to make the network security state constantly migrate at the interface of the two regions. After defining the network offense and defense, the network security risk is calculated to realize the risk detection.

2.3. Calculate network security risks

Based on the qualitative relationship of network offense and defense as determined above and static analysis results of network security, a network security risk calculation frame diagram is established as shown in the figure below.

The network security risk calculation framework includes two parts: threat identification and risk calculation. There is a correlation between vulnerabilities in the network, and the attack graph can combine vulnerability information, network topology information, host configuration information, etc., to show all attack paths of the attacker against the target network [9]. The vulnerability scanner can scan the vulnerabilities in the target network and the service information running on each host. The host information scanning tool can automatically obtain the host configuration information in the target network and network services running on the host. The topology information of the target network can be obtained by the network topology discovery tool, and the connection information of each host in the target network at the network transport layer can be calculated. Vulnerability information, service information running on each host, and connection information between each host constitute the target environment. The attack graph auto-build engine uses target environment and vulnerability knowledge base to build attack graph. The automatic building process of attack graph is actually the process of instantiating local variables in attack mode according to the target environment, and then visualizing the attack graph as nodes and directed edges. In view of the specific attack behavior of some different vulnerabilities, the common points of the current vulnerability attack methods are extracted to form an attack pattern. According to the calculated network security risk, the basic principle of artificial immunity is used to detect the risk in real time.

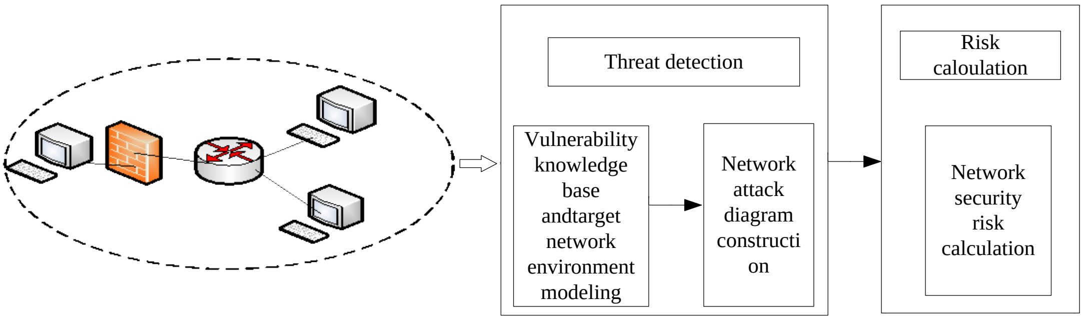
Threat detection
Vulnerability knowledge base andtarget network environment modeling
Network attack diagram constructi on
Risk caloulation
Network security risk calculation

Figure 1. Network security risk calculation frame diagram

2.4. Realize the real-time detection of network security risks

Artificial immunity is to realize the defense of computer network security detection by simulating the defense process of biological immune system. In this paper, the state mode and attribute parameters of the computer network are defined as self-data, so as to realize network security risk detection by using artificial immunity. In morphological space, the recognition between immune cells and antigens is quantitatively described. If a certain number of antibodies are placed appropriately in a morph space and given the appropriate threshold for cross-reaction, then these antibodies can cover the entire morph space and the molecular morphology presented by the immune system can be recognized. The recognition between an antibody and an antigen can be calculated using the following affinity formula:

$$D=\sqrt{\sum_{i=1}^{L}\left(Ab_i-Ag_i\right)^2} \tag{2}$$

In formula (2), Ab_i is the antibody of artificial immunity; Ag_i is an antigen for artificial immunity. When the principle of artificial immunity is used for real-time risk detection, the autologous mutation can be eliminated at any time to avoid the autologous tolerance of immature immune cells to the mutation, so as to reduce the error denial. By dynamically increasing the self element, the description scope of self is expanded and the false affirmation is reduced. Mature immune cells evolve from newly generated immature immune cells that are self-tolerant. Mature immune cells have a certain life cycle. If the mature immune cells match a certain number of antigens during the life cycle, they will be activated and evolve into memory cells, otherwise they will die. In addition, mature immune cells will also die if they develop new autoimmune intolerance. Therefore, the evolutionary process of mature immune cells is as follows [10]:

$$T_b\left(t\right)=\begin{cases}\phi,t=0\\ T_b^{'}\left(t\right)\cup T_{new}\left(t\right)-T_a\left(t\right),t>1\end{cases} \tag{3}$$

In the above equation, $T_b^{'}\left(t\right)$ is the evolutionary process of mature immune cells. T_a were mature immune cells. $T_{new}\left(t\right)$ is the process of generating new mature immune cells. ϕ is an empty set. Memory antibody concentration of immune cells can accurately assess the current risk of the network. Let μ_i be the risk of i th type attack type A_i^g in k th network host, then at time T, the host is exposed to the risk $r_{k,t}\left(t\right)$ of attack A_i^g and the overall network risk A_i^g are respectively:

$$\begin{cases}r_{k,t}\left(t\right)=\dfrac{2}{1+e^{-\mu_i\sum x,p}}-1\\ r_k\left(t\right)=\dfrac{2}{1+e^{-\sum\left(\mu_i\cdot\sum x,p\right)}}-1\end{cases} \tag{4}$$

When the value of $r_{k,t}\left(t\right)$ is 0, it indicates that attack A_i^g poses no threat to the host. When the value of $r_{k,t}\left(t\right)$ is 1, it indicates that an attack of A_i^g is extremely dangerous to the host. The greater the value of $r_{k,t}\left(t\right)$, the greater the risk to the host. Similarly, the value of $r_k\left(t\right)$ indicates the degree of security risk in the overall network. At this point, the research on the real-time risk detection method of network security based on static analysis is completed, and the effectiveness of this method will be studied in the following part.

3. Experiment

3.1. Experiment content

In this experiment, the traditional network security risk detection method is compared with the real-time network security risk detection method based on static analysis proposed in this paper, and the actual detection accuracy of the two methods is compared from the aspect of missing rate and accuracy rate of risk detection. DRAP200 data set was selected for the simulation experiment. Record experimental data of network vulnerabilities detected by the two detection methods under the attack. After processing by data software, the data of omission rate and accuracy rate of risk detection are obtained. Analyze the data of omission rate and accuracy rate, and draw the final conclusion of this experiment.

3.2. Cyber attack process

The DRAP200 attack scenario test data set contains a series of attacks, the whole attack process is the implementation of the DDoS attack. The attacker first detects the active host via IPSweep; Then port scanning is carried out to find the host with security vulnerability, and then the network host with the vulnerability is attacked to make it a puppet machine. Then install the Trojan horse software of DDoS attack on the accused host, login the victim host remotely through RSH, and launch DDoS attack on the attacked target by using the accused host.

The attack steps corresponding to the DRAP200 dataset are described as follows:

Step 1: The attacker scans the target network to search for active hosts.

Step 2: Detect the active hosts found in Step 1, and detect which hosts are executing the Sad mind remote manager tool, and then lock the attack target.

Step 3: Attack the network host. For the network host locked in Step 2, try to exploit the vulnerability of Sad mind until the invasion is successful.

Step 4: Install the DDoS attack tool on the dummy machine. The attacker logs into the dummy machine remotely through the RSH service and installs the attack tools that generate the real DDoS attack package, while installing an attack agent on one of the victim hosts that provides a user interface and controls the attack tools installed on the other victim hosts.

Step 5: Start the DDoS attack. The attacker remotely logs on to the host with the attack agent installed, controls all the controlled machines with the attack tools to forge IP addresses and together conduct DDoS attacks on the remote server.

3.3. Experimental results

The data of omission rate and accuracy rate of the two methods for real-time detection of network security risks are shown in the table below, and the data in the table are analyzed.

Table 1. Comparison of omission rate and accuracy rate /%

Attack power level	Hole density /%	Method of this paper		Traditional method	
		Non-response rates	Accuracy rate	Non-response rates	Accuracy rate
1	0.471	1.30	95.88	4.74	76.08
1	1.258	1.42	94.76	4.78	77.02
1	3.682	1.44	95.10	4.85	71.67
2	0.471	1.33	93.62	4.73	77.11
2	1.258	1.42	95.45	4.93	75.53
2	3.682	1.24	97.44	5.02	76.49
2	4.539	1.19	96.16	5.69	76.98
3	0.471	1.46	93.82	4.84	77.69
3	1.258	1.43	97.37	5.25	74.72
3	3.682	1.37	96.35	6.02	76.05

It can be seen from the above table that the alarm failure rate is similar when applying this method to risk detection under the condition of different attack intensity and the same density of network security vulnerability. However, the alarm failure rate increases with the increase of network attack intensity. Under the condition of the same attack intensity and different density of network security vulnerability, the missing rate of traditional method is also proportional to the security vulnerability density. Overall analysis of the data in the above table shows that the accuracy of this method is higher than 93.5%, which is far higher than the detection accuracy of the traditional method. It shows that in practical application, the real-time risk detection method based on static analysis proposed in this paper has higher detection accuracy and better protection effect for network security.

4. Conclusion

There are some problems in the traditional network security risk calculation methods, which often ignore the propagation of threats and fail to identify the potential threats in the network. Therefore, this paper studies the real-time risk detection method of network security based on static analysis. The validity of the proposed method is verified by relevant experiments. In the future, the knowledge base of vulnerability will be continuously improved and maintained, and the practical application effect of detection method will be improved through a large number of practices.

Reference

[1] Wang Ying. Network information security risk prediction based on information mining technology. Journal of LanZhou University of Arts And Science (Natural Sciences Edition). 2020, 34(04), 57-61.

[2] Zhang Junfei, Shi Hongyu. Network security risk assessment method based on analysis of internet behavior characteristics. Digital Technology and Application. 2020, 38(04), 50+52.

[3] Huang Ke. A remote network video education information intrusion risk detection method based on cloud computing. Journal of Inner Mongolia University for Nationalities(Natural Sciences). 2019, 34(04), 286-290.

[4] Wen Jiachao, Yang Hongzhang. Optimization analysis of network security risk quantification parameters based on numerical simulation. Science Technology and Engineering. 2019, 19(07), 183-188.

[5] Li Xin. A real-time prediction method of network security risk based on predictive model. Journal of Chongqing Institute of Technology. 2019, 33(02), 132-137.

[6] Yan Jishan. Analysis on network security risk assessment based on attack graph behavior pattern. Microcontrollers & Embedded Systems. 2018, 18(10), 1-3+7.

[7] Wang Zengguang, Lu Yu, Li Jindong. Network security risk assessment method based on bayesian attack graph. Journal of Academy of Armored Force Engineering. 2018, 32(03), 81-86.

[8] Li Yonghu. Network security risk analysis method based on attack detection and node vulnerability. China Computer & Communication. 2018, (05), 218-219.

[9] Tan Yubo, Zhao Meng, Deng Miaolei. Research and simulation of optimal assessment of network security situation. Computer Simulation. 2018, 35(03), 210-215.

[10] Zhang Haocheng, Wu xiaojie, Tang Xiang, et al. System detecting network anomaly with visualization techniques. Chinese Journal of Network and Information Security. 2018, 4(02), 40-54+9-16.