A Generation Method of Attack Graph Based on Evolutionary Computation

Jiajia Wang [1,a]

[a]wangjiajia_99@163.com

Keywords: evolutionary computation;attack graph;network security

Abstract. In this paper, the static attack graph is combined with the dynamic evolutionary computation, and a method of attack graph generation based on evolutionary computation is proposed. We extend the traditional attack graph to the dynamic attack graph with time and space changes. According to related attributes of network vulnerabilities and the change of the attack, the attack graph of evolutionary computation is given. This method can be combined with the actual adjustment of attribute weights, further simulation of the attack process, and clear the consequences of the attack. The experimental results show that the proposed framework and method can effectively implement attack simulation, and provide more effective defense.

Introduction

In the network security analysis technology, the method of risk assessment was divided to two categories: static assessment and dynamic assessment. Static assessment method includes the attack graph, probabilistic risk assessment and so on; dynamic evaluation methods include game theory, Petri net, etc.. Among them, the attack graph technique has become the network security analysis technology research focus.

Hawrylak[1] used a hybrid attack graph and modeled CPS information attacks, then generated a global attack graph, but there is no quantitative calculation of the risk of information security. The literature [2] is proposed to describe the whole process of the attacker privilege escalation through the privilege graph, to calculate the average attack cost through the attack path from the initial state to the target state with the value of experience, but did not take into account possible changes in the attack process.Fung[3] proposed a quantitative risk assessment method, focused on the calculation of economic losses caused by network attacks on the smart grid, also did not consider the change of possible attack process. In the existing large-scale, long time attack environment, the attack path, the attack strength may be changed with time and space, if the static attack graph and dynamic calculation could be combined , an effective protection could be played to the actual attack environment.

In this paper, the combination of static attack graph and dynamic evolutionary computation proposed an attack graph generation method based on evolutionary computation, the traditional attack graph was expanded to as time, spatial variation and automatic optimization of the dynamic attack graph, through the relevant attributes of network vulnerabilities, combined with changes in the attack process, to be evolutionary computation to generate attack graphs. Particle swarm optimization(PSO) algorithm based on weight can be combined with the actual to adjust attribute weights, to further simulate the attack process, to make clear the attack consequences. The experiment proofed that frame and method proposed in this paper can be effectively simulate the attack, and provide prevention methods.

1. A generation method of attack graph based on eovlutionary computation

In the analysis of attack graphs based on the features of the test of the fragile, a method based on weight of the attack graph was generated. In the evolutionary process, the existing nodes' vulnerabilities in the network were coded and evolved, aimed at local optimal solution in the process of evolution, an open evolutionary strategy was proposed, that is,by the user's flexibility to control the weight of the vulnerabilities, and through to the individual evolution fitness to complete the attack graph generation. This open evolutionary strategy ensures the evolution of fluency and integrity.

Network vulnerabilities mainly includes the following three properties: (1) the extent of vulnerabilities can be exploited, (2) the average degree of exposure to vulnerabilities, (3) the average repair degree of vulnerabilities[4]. The more convenient the use of the vulnerabilities is easier to be used by the attacker, the vulnerabilities that is easy to use attacked the more attention of attackers. Once vulnerabilities were released that can be understood and then used by the attackers, the longer the time vulnerabilities were released the higher the vulnerabilities exposured. Once the vulnerabilities appeared, there could be the possibility of repair, the higher degree of repair the lower success rate of the attack . The attackers' conditions are unpredictable, so the network vulnerabilities' properties were used as the gene of an attack graph, according to the above information to build the attack graph generation system based on evolutionary computation (evolution attack graph design system, EAGDS), as shown in Figure 1.

EAGDS's main function is the application of evolutionary computation and weight adjustment and the method to generate attack graphs based on evolutionary computation. The framework mainly consists of two modules: one is attack graph gene generator module, this module analyzes the vulnerabilities' attribute in the network. The second is the evolutionary design of attack graph, this module completes evolutionary design process, optimize population to obtain the best attack graph.

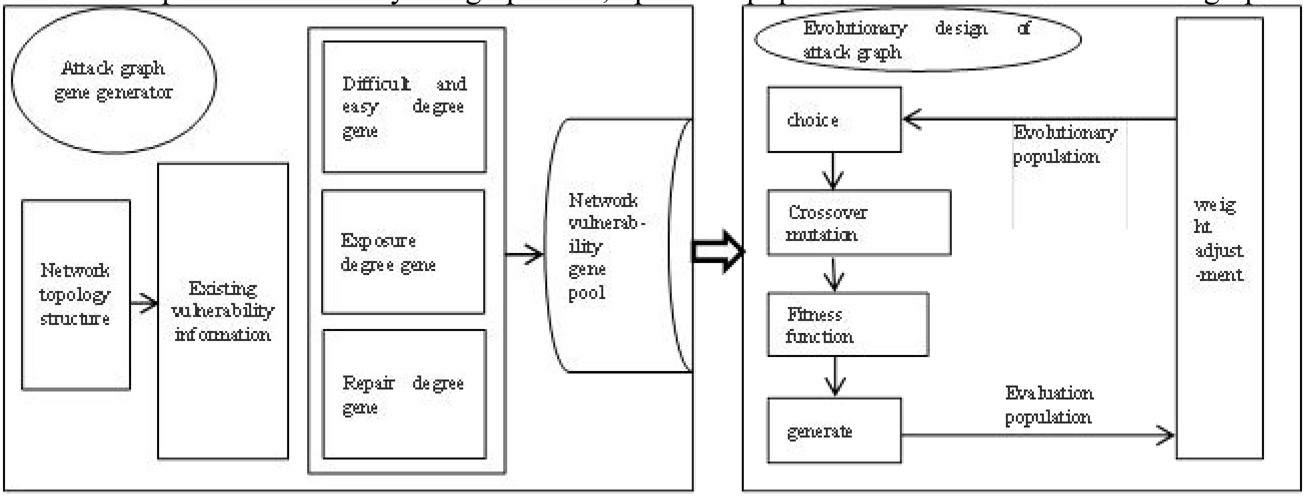
Attack graph gene generator
Network topology structure
Existing vulnerability information
Difficult and easy degree gene
Exposure degree gene
Repair degree gene
Network vulnerab-ility gene pool
Evolutionary design of attack graph
choice
Evolutionary population
Crossover mutation
Fitness function
generate
Evaluation population
weig ht adjust -ment

Figure. 1 EAGDS framework

2. Design of particle swarm optimization algorithm based on weight

According to the attributes of vulnerabilities analysed on the problems of the network shows that with the change of time, the attacker would chose different vulnerabilities to implement attack. Therefore, the weights of different vulnerabilities should change over time but not fixed. In this paper, a Particle Swarm Optimization Algorithm based on Weight is adopted. The description of standard PSO algorithm is as follows:

At some point, the solution of a group containing N particles, each particle contains M individual gene number (the extent of vulnerabilities can be exploited, the average degree of exposure to vulnerabilities, the average repair degree of vulnerabilities),M=3, the position of the i-th particle that Xi=(Xi1，Xi2，Xi3)，i=1, 2, ⋯,N. The initial position is regarded as a set of coordinates of the point of the three-dimensional space, in each iteration of the algorithm, the current position Xi is evaluated as the problem solution. Assuming the initial velocity Vi= (Vi1, Vi2, Vi3), the historical best position Pi= (Pi1, Pi2, Pi3).

For each particle, its d(1<=d<=3)- dimensional attributes can be updated according to the velocity displacement formula:

$$Vi+1,d=W*Vid+C1*(Pid-Xid)+C2*(Pgd-Xid) \quad (1)$$

$$Xi+1,d=Xid+Vi+1,d \quad (2)$$

Among them, W is the inertia weight, C1, C2 is constant, usually between 0 to 2. In the literature [6] proposed an adaptive adjustment strategy, its weight is calculated as follows:

$$W=Wmin+(Wmax-Wmin)*(Tmax-T)/Tmax \quad (3)$$

Among them, Wmax is the initial weight and Wmin is the weight of last calculation, Tmax is the maximum number of iterations, T is the number of iterations, the weight is W. According to literature [7], the weight, W, which is between 0 to 1 can fast convergence, so the value of W should meet the corresponding conditions. In this paper, the inertia weight value depended on the known attack. Assuming there is A vulnerabilities totally, the probability of the ith vulnerability was used in the attack is Pi, meet the following condition: $\sum_{i=1}^{A} p_i = 1$， 0<pi<1. With the increase of vulnerability exposure, the degree of restoration would also increase, the difficulty level of vulnerabilities to be exploited would also increase, these three properties would cause pi decreases continuously with the passage of time. Therefore, Pi as the initial weights of the vulnerabilities accorded with the decreasing convergence condition of algorithm. Attack consequence was strictly related to the importance of vulnerabilities to be attacked in the host, mainly include economic losses, environmental damage and so on. In this paper,the product of the current weight of vulnerabilities and probability was a measure value of the consequences of the attack.

3. Case and analysis

In order to verify the algorithm proposed in this paper, a small and medium enterprises was as the experimental object.

The enterprise is connected with Internet through the Mobile Corporation line. The enterprise cloud server ip address is 211.65.186.1, stored in a large number of experimental data, and installed a virtual machine tool, operating system and so on; the enterprise web server ip address is 211.65.186.2, to provide publicity to the inside and outside of the enterprise; the enterprise database server ip address is 211.65.186.3, running SQL server and Oracle database; the enterprise server which can be accessed by the network, ip address is 211.65.186.4, is convenient for staff to visit the headquarters of the company at any time.

According to business needs, the server which ip address was 211.65.186.2 completely opened to the Internet, IIS components and the Tomcat components on the server that ip address was 211.65.186.1 and 211.65.186.2 needed to access in database which ip address was 211.65.186.3. By the vulnerability scanning tools we can find the vulnerabilities information in the network, as shown in Table 1, and we can generate the initial attack graph, as shown in Figure 2.

On the basis of the initial attack graph, according to the framework of EAGDS, we would generate the evolutionary attack graph and each step of attack consequences. Assuming that the target is 211.65.186.1, cloud server data, according to the principle of maximization the consequences of the attack, through the Particle Swarm Optimization Algorithm based on Weight, we can get results analysis as shown in Figure 3, the number in the circle is the consequence of the attack.

Can be seen from the figure 3, the attacker via the host, which ip address was 211.65.186.4, operating system vulnerabilities then got user permission for access to the host 211.65.186.2, and finally obtained the host 211.65.186.1 access, we could see the attacker's path clearly. For the above attack patterns, we only need to reduce the risk of vulnerabilities of Windows operating system, that can greatly improve the security of data on cloud server.

Table. 1. Vulnerabilities information

Host	Vulnerabilities type	Use pattern
211.65.186.1	Remote login	Promotion Authority
211.65.186.1	Not encrypted login request	Information leakage
211.65.186.2	HTML Code execution	Promotion Authority
211.65.186.2	XSS vulnerabilities	Promotion Authority
211.65.186.3	SQL injection	Promotion Authority
211.65.186.3	Sensitive information leakage vulnerability	Information leakage
211.65.186.4	Weak password vulnerability	Promotion Authority
211.65.186.4	Remote buffer overflow	Modified control algorithm

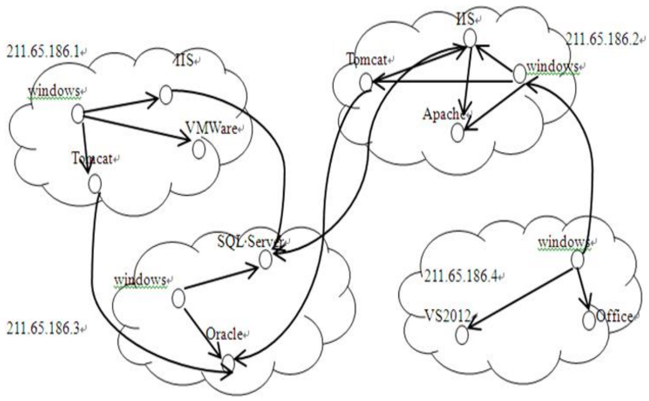

Figure 2. Initial attack graph of experimental network

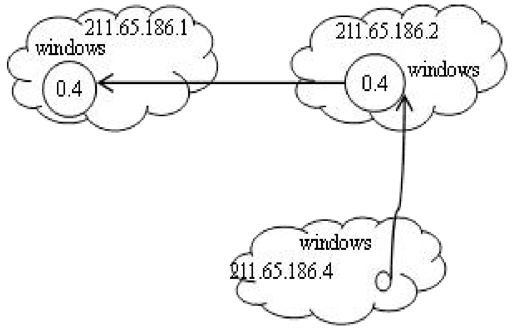

Figure 3. Attack graph based on evolutionary computation

4. Conclusion

At present, vulnerability analysis technology based on attack graph has been the focus of research in the field of network security. However the traditional vulnerability analysis technology is only for atomic attack, and is not satisfied for multi-step attack complex. How to combine the static attack graph and the changing of the attack with practice is the focus of the study.

This paper presented a generation method of attack graph based on evolutionary computation, combined the attack attribute with the continuous evolution of the algorithm to generate dynamic attack graph, correlation algorithm could determine the attacker's path that is the most easy choosed and then defense. Experiments showed that the method proposed in this paper can effectively simulate the attack, and targeted select the most likely, most efficient, most effective nodes to defense in order to achieve the ideal effect. Study on dynamic attack graph still in initial stage, henceforth we will verified the rationality and validity of the algorithm in the actual.

References

[1] HAWRYIAK P J, HARTNEY c， PAPA M， et a1. Using hybrid attack graphs to model and analyze attacks against the critical information infrastnlcture[J].Critical infomation infrastructure protection and resilience in the ICT sector, 2013, 11(3): 173-179.

[2] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with quantitative evaluation tools for monitoring operational security[J], IEEE Trans on Software Engineering, 1999, 25(5): 633-650.

[3] FUNG C C, ROUMANI M A, WONG K P. A proposed study on economic impacts due to cyber attacks in smart grid: a risk based assessment[C]//Proceedings of the 2013 IEEE Power and Energy Society General Meeting. Piscataway, NJ：IEEE, 2013: l-5。

[4] WU Wenbo, KANG Rui, LI Zi. Attack graph based risk asessment method for cyber security of cyber—physical system[J], Joumal of Computer Applications, 2016, 36(1):203-206.

[5] Kirkpatriek S, Gelatt C D, Veechi M P. Optimization by simulated annealing[J],Science, 1983, 220: 671 – 680.

[6] LIU Jian-hua, ZHANG Yong-hui, ZHOU Li, HE Wen-wu. Particle Swarm Optimization with Weight Increasing[J], Computer Science, 2014, 41(3), 59-65, 84.