A Process-oriented Evaluation Framework for Cyber-attacker's Capability

Luo Baofeng
Zhengzhou Information Science and Technology Institute
Zhengzhou, China，+86 13526801802
358655618@qq.com

Zhu Junhu
Zhengzhou Information Science and Technology Institute
Zhengzhou, China，+86 15824820935
gn_275@163.com

***Abstract*—Accurately and reasonably evaluating cyber-attacker's capability can help to scientifically forecast following attacks in order to give tailor-made defense tactics. At present, the evaluation measures of cyber-attacker's capability are primarily based on attack effect and the related achievements are few. In this paper, we begin with the study of attack process, and then divide cyber-attacker's capability according to attack stages after analyzing each stage's features within the cyber-attack process. Subsequently, a process-oriented evaluation framework for cyber-attacker's capability is proposed. With the validation of an experiment, it is proved that this evaluation framework can make precise and reasonable evaluations of cyber-attackers' capability.**

***Keywords*-cyber-attack; cyber-attack process; capability; evaluation framework**

I. INTRODUCTION

With the rapid development of computer network technology, the applications of computer network have emerged in every field of our social life. However, many affiliated problems of information security are apparent, cyber-attack has been an effective measure to damage adversarial network and to obtain important intelligence. As is known to all, Attacker is the mastermind of cyber-attacks, thus evaluating cyber-attacker's capability in order to determine the defense tactics has become a new research. To evaluate cyber-attacker's capability, first we must establish an evaluation framework which is able to give an objective and reasonable evaluation of cyber-attacker's capability. Now, the research on evaluation of cyber-attacker's capability is largely based on attack effect and still in its early stage, at the same time, the related achievements are few. These kinds of frameworks evaluate the attack effect so as to give an estimate of cyber-attacker's capability. Due to the various purposes, instruments and methods of current cyber-attack, evaluating cyber-attacker's capability merely with the attack effect is not adequate any more. In reality, There must be only two possible outcomes of a cyber-attack, reaching the attack goal or not. Therefore, two important subjects in this research field should be emphasized, how to evaluate cyber-attacker's capability when he fails to reach the attack goal as well as how to pick out divergence between cyber-attackers' capabilities while they achieve the same goal. Aiming at resolving these two problems, we design an evaluation framework. We begin with the study of attack process, divide attack process into several stages by attack procedures, and analyze each stage's features within the cyber-attack process. According to different attack stages, we disassemble cyber-attacker's capability into several abilities (sub-capabilities), and also define corresponding evaluation indicators for each sub-capability. As a result, a process-oriented evaluation framework for cyber-attacker's capability is established.

II. RELATED WORK

Up to now, the research of cyber-attack mostly comprises two directions: one is evaluation of cyber-attack effect; the other is evaluation of cyber-attacker's capability. The technology of cyber-attack effect evaluation mainly aims at researching the divergence of network security between pre-attacked and post-attacked in order to reflect the status quo of network security and design the defense tactics. Nonetheless, this method has an apparent drawback, i.e., being short of apprehension of attacker's capability and hard to predict the degree and scale of following attacks. To solve this problem, [1] introduces an effect-oriented evaluation framework for cyber-attacker's capability which could evaluate attacker's capability by attack effect. This evaluation framework fulfills the requirement of evaluating cyber-attacker's capability to some extent, and is of certain value.

A. The Effect-Oriented Evaluation Framework For Cyber-Attacker's Capability

Evaluation of cyber-attack refers to the research on how to make quantitative or qualitative evaluations of the cyber-attacks against information systems in a complex network environment, so that we can use these evaluations to measure the effectiveness of cyber-attacks and the security of information systems. The effect-oriented evaluation is to reflect cyber-attacker's capability through the effect of cyber-attacks. With this perspective, [1] divides cyber-attacker's capability into two aspects: ability to collect information and ability to destruct targets.

- Ability to collect information. Within the whole process of a cyber-attack, attacker continuously collects information of the target network or hosts. Information collection represents a procedure in which attackers to obtain relevant information of target network or hosts via a variety of attack means. Getting relevant information of the targets is a prerequisite for the success of cyber-attack. The more information an attacker gets, the more possible he will succeed. The

information mentioned above usually consists of target hosts' IP addresses, usernames, ports opened, running services, existing vulnerabilities, etc.

- Ability to destruct targets. Targets destruction refers to summation of attack operations against target network or hosts performed by attacker. With the proceeding of cyber-attack, attacker's ability of targets destruction keeps rising. In the early period of cyber-attack, attacker is unable to manipulate target network or hosts. However with the escalation of attacker's operating authority achieved by a series of attack techniques, attacker becomes able to manipulate or destruct target network or hosts. Generally speaking, ability of targets destruction is always characterized by such respects: artificial congestion among communication links, operations of target hosts' files (e.g. creation, deletion and modification), destruction of registry, modifications of user account's information and hosts' parameters as well as services in the target network, record of target hosts' keyboard input history, remote manipulation of target hosts, etc.

As layered structure of security evaluation[2][3] is taken into account, the effect-oriented evaluation framework for cyber-attacker's capability is carved into three parts in order from top to bottom: evaluation object, evaluation rules and evaluation indicators. Evaluation object is the cyber-attacker's capability to be estimated. Evaluation rules are a succession of criteria to estimate cyber-attacker's capability, which consists of information acquisition and targets destruction. Evaluation indicators are scheme, methods and measures to reach the goal. On the basis of these, this effect-oriented evaluation framework is established in sequence from top to bottom which is showed in Figure 1. In Figure 1, "C" represents attacker's capability; "A_1" represents ability to collect information while $I_{11} \cdots I_{1n}$ are n indicators for this ability; "A_2" represents ability to destruct targets while $I_{21} \cdots I_{2n}$ are n indicators for this ability.

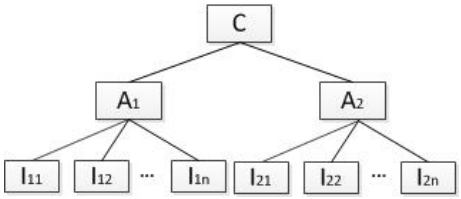

Figure 1. The effect-oriented evaluation framework for cyber-attack's capability

B. Disadvantages

Due to different attack purposes and various attack means, the effect-oriented evaluation framework is not complete. The major disadvantages are the following ones:

- Owing to the incompetence to evaluate all kinds of attack effects, this framework is unable to evaluate attacker's capability. According to attack means and attack purpose, [4] classifies cyber-attacks into congestion attacks, domination attacks, detection attacks, deception attacks, vulnerabilities exploitation attacks, computer virus attacks. For some sorts of attacks, (e.g. congestion attacks and deception attacks) there are too few pertinent evaluation indicators to evaluate attack effect, thus cyber-attacker's capability is much less possible to estimate.
- This evaluation framework is also incompetent to evaluate cyber-attacker's capability when he/she fails to accomplish specific attack missions. It works to evaluate cyber-attacker's capability through the evaluation of attack effect. Because of the unpredictability of attack effect, in case the cyber-attacker fails to achieve specific attack effect, it's impossible for this framework to estimate cyber-attacker's capability.
- This evaluation framework is unable to figure out the differences between cyber-attackers' capabilities while they achieve the same effect. Because of the diversity of cyber-attack method, Attackers would leverage various means to implement assault. In case that cyber-attackers achieve the same attack effect via various means, this evaluation framework would make the same evaluation of these attackers and is incapable to give further analysis of divergence.

III. THE PROCESS-ORIENTED EVALUATION FRAMEWORK FOR CYBER-ATTACKER'S CAPABILITY

In accordance with the effect-oriented evaluation framework's incompetences, we propose a process-oriented evaluation framework for cyber-attacker's capability. Concrete procedures to design it are below: Firstly, we analyze every stage of cyber-attack and pick out purpose and major tasks during each stage; secondly, we divide attack's capability into several sub-capability by each stage's purpose and extract pertinent indicators to evaluate sub-capability from major tasks for each stage; last but not least, we establish a process-oriented evaluation framework for cyber-attacker's capability based on layered structure of security evaluation.

A. Procedures of cyber-attack

A premeditated and complete cyber-attack generally can be divided into 5 stages[5]: information collection, authority acquisition, backdoor programs installation, impact expansion and attack records elimination. The major purpose of the first stage is to collect relevant information of targets as much as possible in order to make following operation more convenient. The purpose of the second stage is to gain target system's authority to read, write and execute, etc. During the third stage, main task represents installing backdoor programs in target system so as to provide a sheltered entrance for attackers to perform operations in the future. The fourth stage aims to expand the attack impact on target network or target hosts. In the fifth stage, attacker attempts to eliminate attack records in order to protect attack source from being identified and traced.

B. The process-oriented evaluation framework for cyber-attacker's capability

The process of cyber-attack is the process of target network or hosts being damaged, at the same time it's also the

demonstrative process for attacker's capability. In the stage of information collection, the amount of target network or hosts' information held by attackers reflects attacker's ability to collect information. In the stage of authority acquisition, whether attacker can pierce into target network and hosts' defense or not has a great influence on the outcome of authority acquisition which represents attacker's ability to penetrate. During the stage of backdoor installation, attacker achieves the goal to control target hosts by installing backdoor programs successfully. This stage represents the ability to control. In the stage of impact expansion, attacker primarily carries out 3 types of activities: acquiring intelligence from target hosts, expanding the scale of dominated hosts in target network and causing severer destruction to target network. These 3 types of activities reflect respectively attacker's ability to acquire intelligence, expand control scale and destruct. Attack records elimination, an ability of self-concealment, is to protect attacker from exposure. With each ability reflected in respective attack stage, attack capability can be divided into 7 following respects:

- Ability to collect information. This represents attacker's ability to collect related information of target network and hosts in the stage of information collection. If an attacker collects a large amount of information about target, he/she would be more familiar with target network or hosts; no doubt it quite increases the possibility of success. Ordinarily, the information about targets consists of network topology, number and names of hosts existing in target network, hosts' opened ports and running services, existing vulnerabilities, hosts' operating system type and version, etc.
- Ability to acquire authority. This is attacker's ability to get target hosts' operating authority via cyber-attack in the stage of authority acquisition. The attacker's operating authority of target hosts escalates with the proceeding of cyber-attack. The level of operating authority owned by the attacker reflects attacker's capability to some extent and can also be demonstrated by the operations (e.g. read, write, deletion and creation, etc.) towards hosts' file system and registry.
- Ability to control. This is attacker's ability to get sustained access to target hosts via installing backdoor programs. It is mainly based on control's stability and comprises times and lasting time of disconnection between attack source and controlled hosts and etc.
- Ability to acquire intelligence. This indicates attacker's ability to acquire intelligence in the stage of impact expansion. After getting control authority of target hosts, the attacker's ability to acquire intelligence stored in target hosts and cause more losses influences attacker's capability to some extent. The ability to acquire intelligence is always composed of quantity of intelligence acquired, accuracy of intelligence and percentage of intelligence missed.
- Ability to expand control scale. It refers to attacker's ability to connect with other hosts through controlled hosts so as to get their control authority during the stage of impact expansion. To propagate more hosts in target network through controlled hosts also proportionately exhibits attacker's capability to some extent. This ability can be evaluated by number of bots, time cost to propagate, scale of bots, etc.
- Ability to destruct. This represents attacker's ability to destroy target network and devastate target hosts via some special attack means in order to cause severer destruction in the stage of impact expansion. It can be conclude that the destruction of target network or hosts caused by attacker determines the attack's impact to a certain extent. It can be exhibited by degree of port occupation, speed of network transport, delay of service response, occupation of network bandwidth, time cost to revitalize network environment.
- Ability to eliminate attack records. This shows attacker's ability to protect himself from being discovered by victims in the stage of attack records elimination. Eliminating attack records is vital for attacker to protect him from being discovered and traced, and it also demonstrates the ability to eliminate attack records. This ability is mainly reflected by deletion or modification of log files, concealment of Trojan processes and communication port, concealment of registry autorun.

As layered structure of security evaluation is taken into account, like the effect-oriented evaluation framework for cyber-attacker's capability, the process-oriented evaluation framework is also carved into three parts in order from top to bottom: evaluation object, evaluation rules and evaluation indicators. Evaluation object is the cyber-attacker's capability to be estimated. Evaluation rules are a succession of criteria known as 7 types of abilities mentioned above. Evaluation indicators with characteristics of rationality and scalability are the elements to reflect these abilities. On the basis of these, this effect-oriented evaluation framework is established in sequence from top to bottom which is shown in Figure 2.In Figure 2, "C" represents attacker's capability; "$A_1 \cdots A_2$" represent 7 abilities mentioned above while $I_{k1} \cdots I_{kn}$ are n indicators for the corresponding kth ability.

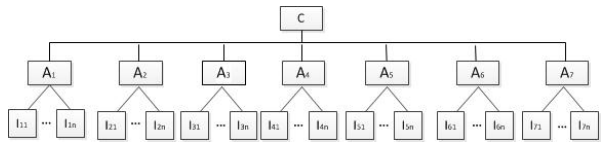

Figure 2. The process-oriented evaluation framework for cyber-attack's capability

IV. EXPERIMENT

The objective of this experiment is to validate rationality of this framework via taking advantage of existing evaluation measures. During this experiment, the attacker is to carry out destructive assaults to the target network. The experiment is separated into group A and group B. Group A adopts the effect-oriented evaluation framework for cyber-attacker's

capability while the comparative one, group B, adopts the process-oriented evaluation framework for cyber-attacker's capability. Both groups aim at acquiring intelligence from target host and then utilize UDP/TCP flood attack to destruct target network. The experiment is in a 100M/s network environment which consists of 2 routers, 2 exchangers and 10 PCs. Experimental network topology is showed in Figure 3.

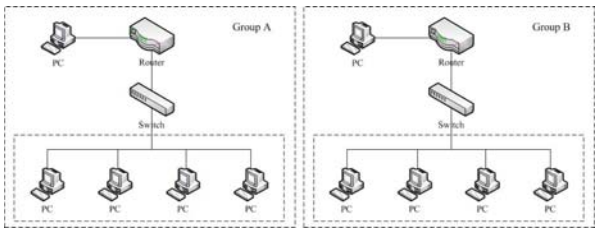

Figure 3. Experimental network topology

The result of this experiment indicates that in the same circumstances of network environment and attack effect, the effect-oriented evaluation framework fails to estimate the capability due to the lack of pertinent evaluation indicators. However, the process-oriented evaluation framework could make use of evaluation indicators for relevant abilities to give a relatively reasonable and comprehensive evaluation for the attacker's capability.

V. CONCLUSION

The evaluation for cyber-attacker's capability is an emerging field in information security research. In this paper, a process-oriented evaluation framework for cyber-attacker's capability is proposed. Through experimental validation, we are reaffirmed that this evaluation framework can make a reasonable evaluation for cyber-attacker's capability and also bring a significant expansion of application range. This framework is of a more comprehensive range for the indicators in comparison with previous ones, nevertheless the indicators of some evaluation rules are still rude and improper. Thus measures to enhance the framework's completeness may be one of our research directions in the future.

REFERENCES

[1] Bo-fu ZHAO, Xiao-chuan YIN, and Chuan-zhi WU, "Attack Ability Evaluation of Attackers Based on Grey Theory," Computer Engineering vol. 37, pp. 114–117, July 2011.

[2] Dong-mei ZHAO,Jing-hong WANG,Fuzzy Risk Assessment of Network Security.Proceeding of 2006 International Conference on Machine Learning and Cybernetics.Dalian,Chaina,August 2006.

[3] David M. Nicol, "Modeling and simulation in security evaluation," IEEE Security and Privacy , pp. 33–37,2005.

[4] Hao CHEN,Jian-qing QI, "Method of network attack taxonomy based on effect,"Electronic Test vol.5,pp.82-84,May 2009.

[5] Hao WU.Network Security:Attack and Defense[M].Beijing:China Machine Press.2009