Research of Attack Model Based on Finite Automaton

ZHANG Zhi-wei
Zhengzhou Information Engineering University
Zhengzhou, China, 13783699684
13783699684@139.com

YUE Yun-Tian
Zhengzhou Information Engineering University
Zhengzhou, China, 13598011803

***Abstract*—According to the unknown of attack behavior in cyberspace, this paper presents an attack modeling method based on system states aggregation. In the model, the basic principle of the finite automaton is researched and attack entities of cyberspace are classified by attack process, it combines finite automaton with the changes of system state caused by attack entity, building the attack model of finite automaton, making an analysis of the model algorithm, and making a quantitative evaluation on attack cost, the success rate, exposure rate and evaluating severity of attack on cyberspace. Finally, through the analysis of typical attack behavior by using network attack modeling, it shows that the model proposed is feasible and effective.**

Keywords; finite automaton; attack model; system states aggregation; attack detection; security early warning

I. INTRODUCTION

Cyberspace, constituted by the Internet, telecommunication networks and other forms of network and physical infrastructure, includes a variety of network forms, throughout the various fields including the land, sea and air and the sky, with increasingly close relationship with human society. With the popularization of network technology in military applications, the new form of warfare has been formed in the network system, namely cyber warfare. The cyber warfare, in order to scramble the right of cyberspace, comprehensively utilizes a variety of cyber-attack and defense to contest. Among them, it is particularly important to have a research on cyberspace attack technology. If there is no further research on it, we will not be able to protect the security of our own networks, to find the vulnerability of the rival network. Through the establishment of the applicable attack model, we can have a formalized and structured description and analysis on cyberspace attack technology, so that we can further improve the efficiency of cyberspace attack detection and security early warning, to provide technical support for security and defense of the cyberspace.

In the process of researching attack model from cyberspace, [1] describes in detail Attack Tree Model, Attack Net Model and attack model based on system states aggregation and other common attack modeling methods. The concept of the attack model based on system states aggregation [2] was first proposed by Koral ILgun and others, who published papers in 1995. The method is mainly a description of the attack to attack detection and security warning. It can distinguish between attack behavior and the impact for the system states. [3] proposes an attack model about system states aggregation; [4] determines the introduction of finite automaton into large-scale intrusion detection; [5], based on the behavioral characteristics of the IP Spoofing attack, puts forward the state analysis. These modeling methods are established on the basis of bulk analysis and research on attack behavior, while the most of attack weapons from cyberspace are controlled by the governments, remaining in the stage of the laboratory simulation, and being not tested in a real network. Therefore, a lot of attack behaviors in cyberspace are unpredictable [6].

Through the above analysis, this paper proposes the Attack Modeling-Finite Automata (AM-FA), taking the attack behavior as the associated process, classifying the attack entity, then studying the state transfer under the attack behavior, proposing model algorithm and evaluation methods, and finally being able to achieve attack detection and safety warning.

II. RELATED KNOWLEDGE

A. Finite Automaton Theory

Finite automaton [7], as a model described through the language, is the regular languages recognizer, which can be a good formal analysis. Finite automaton is a five-tuple:

$$FA = (Q, \Sigma, \delta, q_0, F)$$

Among them:

Q ——non-empty finite set of states, $\forall q \in Q$, q is called a state of Q.

Σ ——input alphabet, the input string is from Σ.

δ ——transition function, sometimes, it can be called the state transition function, $\delta: Q \times \Sigma \to Q$. $\forall (q,a) \in Q \times \Sigma$, $\delta(q,a) = p$ means FA in the state q to read into the character a, and the state becomes p.

q_0 ——initial state of FA, also called the original state.

F——final state collection of FA, $F \subseteq Q$. $\forall q \in F$, q is called the final state of FA.

B. *Classification of Attack Entities*

Because of the unpredictability of attack behavior from cyberspace, we cannot directly make a formal description of attack behavior, and therefore we only give a description of it from the perspective of the attack process. For making an accurate expression of attack process, it defines as follows:

Definition1 The definition of attack entities: An objective or abstract thing attacks on the network system software and data with network vulnerabilities and security flaw.

Definition2 The definition of system state: A series of follow-up action sequences, given attack entity decided for the target system attributes and conditions of this attribute which is used to describe certain characteristics of the target system.

By the definitions, the process of the attack is formed by triggering from the corresponding attack entities, which can cause the change of system state, each of which is caused by a class of corresponding attack entities, which contains a variety of attack behaviors. Reference [6] on the division of the attack entities, which are divided into: reconnaissance entities, scanning entities, access and escalation entities, exfiltration entities, assault entities, sustainment entities, and obfuscation entities, the first six parts can be combined as an attack process. Obfuscation entities also called supportive entities, has an important role on supporting the attack process. There into:

- Reconnaissance entities: also called Intelligence-gathering, the first step of network attack, by which to realize the basic outline of the target system.
- Scanning entities: Mainly used for collecting more detailed information for the target environment and systems, such as the port number of the target host, IP address and other information.
- Access and escalation entities: Through cracking passwords and modifying permissions, to obtain the target system and further improve the access permissions.
- Exfiltration entities: By means of encryption or using the communication protocol of the target system to steal data in the target system for interest.
- Assault entities: To attack on the target system, and destroy its confidentiality, integrity and availability.
- Sustainment entities: To ensure that the next attack can smoothly access the target system, sustainment entities added access permission and a back door.
- Obfuscation entities: To attack process with the hidden, confused, traps and others, so that the target system administrator could not track, identify attack source and attack purpose. It may exist in the each stage of the process, or before the attack, or after the attack, so it supports the whole attack process.

During the actual attack process, with being not completely in accordance with the established order of the first six attack entities, there may be jumping and iteration.

Comprehensive analysis on the finite automaton theory and the relationship between the attack entities and system states: the target system can be divided into different states, which are limited. System states can transfer under the action of the attack entities, and the transferred entities are limited, with the system showing the state behaviors. It can bring cyberspace attack behavior into state transfer behavior of finite automaton.

III. ATTACK MODEL BASED ON FINITE AUTOMATON ITS ALGORITHM

Through the above analysis, we put forward an attack model based on finite automaton. This section first presents the definition the system states as symbolic representation, second establishes of attack model, studies its analysis method and algorithm description, and finally evaluates the attack model.

A. *Definitions of the System State Symbols*

To express succinctly, we will take the obfuscation entities and the six attack entities as h and a_n, n=1,2, ... ,6; the effects of the six attack entities to the target system and the state before the attack, after the attack as S_m, m=0,1,2, ... ,6,7, such as S_2 expressing the state of the target system after the scanning entities (a_2) attacking, specific conditions as shown in TABLE Ⅰ:

TABLE I. DEFINITIONS OF THE SYSTEM STATE SYMBOLS

attack stages	attack entities	the system state
Before the attack		S_0
Reconnaissance	a_1	S_1
Scanning	a_2	S_2
Access & escalation	a_3	S_3
Exfiltration	a_4	S_4
Assault	a_5	S_5
Sustainment	a_6	S_6
attack end		S_7
Obfuscation	h	

Visibly, when the system is in a certain state, an entity attack will cause the system state to change. Therefore, the research on attack process can be converted to the study on the system state transfer. Based on the graphical rules of the finite automaton, attack process built through finite automation can be expressed with transition diagram. With the arrow S pointing out the start state of FA, with the vertex of acceptable state set S_7 marked with a double circle; $\delta(q,a)=p$ in the diagram represents a arc marked as a from the vertex q to vertex p. The state transition diagram with the attack process (τ as the support for the action hidden entities to attack-hidden) as shown in Figure 1:

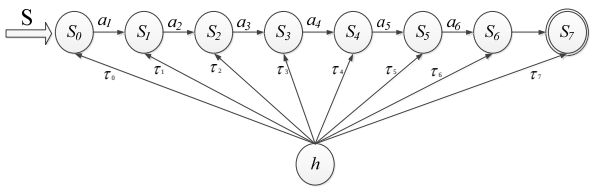

Figure 1. Attack process state transition diagram

Definition3 An attack entity makes the system transfer from one state to another state (including its own state), which is named single-step attack.

Definition4 Multiple single-step attacks forming an attack sequences is called Multi-Step attack.

The preconditions when single-step attack occurs: the effective use of the system vulnerabilities and defects that means static configuration; the information and resources that the attack entities obtain from the last step, whether they meet the needs of the attack; the current system state, if the current system state does not meet what the attack behavior requires, the attack behavior cannot occur. When single-step attack successfully attack on the target system, the target system state will transfer for the next state; if not success , it still return to itself state, as shown below:

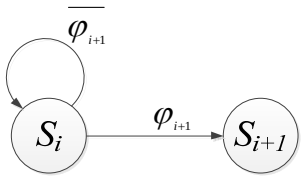

Figure 2. Single-step attack diagram

B. Construction of the Attack Model

By the above analysis, the attack process of cyberspace can meet the basic principles of the finite automaton. Therefore, we build our attack model through the finite automaton.

Definition5 A finite automaton M with output, expressed with six-tuple: $M=(Q,\Sigma,\delta,\Omega,S_0,S_7)$, there into:

Q is a state collection, one of its elements on behalf of a state node. As shown in TABLE Ⅰ, before the attack, the end of the attack, the attacked system states are set to the nodes, $Q=\{S_0,S_1,\cdots,S_7\}$.

Σ is the input alphabet $\{0,1\}$. 0 means attack unsuccessfully, 1 means attack successfully.

δ is a transfer function, $\delta:Q\times\Sigma\rightarrow Q$. For example: $\delta(S_1,0)=S_1$ means M is read into character 0, the state would transfer for S_1; $\delta(S_1,1)=S_2$ means M is read into character 1, he state would transfer for S_2.

Ω means, during the attack process, the importance of a single-step attack and the extent of the damage on the target system. Ω is the integer between 0-10. Such as scanning attack can be set to 1, denial of service attack can be set to 6 or higher. It needs correct and reasonable assessment method to build correct weights. For simplicity, the specific values could be given directly by the experts through scoring.

S_0 is the node before the attack.

S_7 is the node after the attack.

Definition6 Attacks entities with the four-tuple expressing: $Attack=(A,B,\Phi,\mathrm{T})$. There into: $A=(a_1,a_2,\cdots,a_6)$ as a single-step attack, $B=(b_1,b_2,\cdots,b_6)$ as the attack cost of the corresponding single-step attack, $\Phi=(\varphi_1,\varphi_2,\cdots,\varphi_6)$ as the success rate for single-step attack, $\mathrm{T}=(\tau_0,\tau_1,\tau_2,\cdots,\tau_7)$ as action hidden entities' support for the attack process.

For the single-step attack, there are the successful attack and unsuccessful attack, the attack at a moment can be marked as $(a_i,0)$ or $(a_i,1)$. Therefore, the character set of the finite automaton Σ would be extended to Σ^* , $\Sigma^*=A\times\Sigma$, the corresponding, $\delta^*:Q\times\Sigma^*\rightarrow Q$, $M^*=(Q,\Sigma^*,\delta^*,\Omega,S_0,S_7)$. Definition6, which can extend the transfer function to meet the attack demand, increase the success rate of attack, the attack cost and the description of hidden support so that the attack behavior can get quantitative evaluation.

Definition7 An acceptable set of solving finite automaton $L(M^*)$, such as $\{(a_1,0),(a_1,1),\cdots,(a_6,1)\}$, a collection consisted of the attack sequences on the target system is called the attack sequence set of the system states.

C. Algorithm Description of Attack Model

Attack entities with the attack process are interrelated and need to make the following expansion: each single-step attack added a timestamp Domain Time, in order to facilitate algorithm description; if this step attack jump, Time is 0, or else Time is 1, each time the single-step attack makes iteration, Time value would be added 1. For meeting the attack conditions with attack entity a_i , and allow to launch $\delta(S_{i-1},(a_i,1))$, and otherwise, $\delta(S_{i-1},(a_i,0))$, with this manner to determine the direction of the status transfer. The specific algorithm is as follows:

Step1 Initialize system status S= S_0, i=1.

Step2 Attack= a_i , if Attack jump, *Time*[*i*]=0, it would be converted to Step4, otherwise, *Time*[*i*]=1, means there is attack behavior, and it would be converted to Step3.

Step3 Determine whether Attack meets the attack conditions, if it meets the attack conditions, and perform $S=\delta(S,(a_i,1))$, converted to Step6, otherwise, it would be converted to Step5.

Step4 $i=i+1$, converted to Step2.

Step5 *Time*[*i*]= *Time*[*i*]+1, converted to Step3.

Step6 If $S\in S_7$, it states to get the purpose of the attack, and stop attack, otherwise, converted to Step4.

The finite automaton is the regular languages recognizer. If there is the regular languages L, it can be a regular expression G such that $L=L(G)$. Because G is Right-Linear, so the rights of every production-rule only have one symbol. While the finite automaton approach to describing the set of the system states is same with the regular languages carry up the production-rule. For example, there is an attack event with three attack entities (a_1, a_5, a_6), a_5 gets the attack target in the second one while others get the target only once. The expression is $\{(a_1,1),(a_5,0),(a_5 1),(a_6,1)\}$, and the derivation process as follow:

$S_0 \Rightarrow (a_1,1)S_1$ cause $S_0 \rightarrow (a_1,1)S_1$

错 误 ！ 未 找 到 引 用 源 。 $(a_1,1)$ $(a_5,0)S_1$

cause $S_1 \rightarrow (a_5,0)S_1$

$\Rightarrow (a_1,1)\ (a_5,0)\ (a_5,1)S_5$ cause $S_1 \rightarrow (a_5,1)S_5$

D. Evaluation Method of Attack Model

The attack process is random, a probability event, vulnerable to the impact of various factors, difficult to accurately measure, can only approximate expression. The paper makes a quantitative evaluation on attack model from the attack cost, the success rate, exposure rate and the degree of attack hazards.

1) Attack cost

From the definition6, we can see bi is attack cost of attack entity a_i , and attack entity a_i launched the attacks with $Time[i]$, clearly the attack cost of each step is added, which is called the overall cost of the attack.

$$B(N)=\Sigma b_i \times Time[i]$$

2) Success rate

By the algorithm analysis of the model, when $Time[i]\neq 0$, the attack entities take place attack behaviors, the success rates of all attack entities are multiplied, which is called the success rate of the process.

$$\Phi(N)=\Pi\varphi_i \qquad (Time[i]\neq 0, i=1,2,\cdots,6)$$

3) Exposure rate

The support of the obfuscate entities on the attack is non-exposed probability. If attack entities do not exist, then $\tau=1$, and during the entire attack procedure non-exposure rate:

$$T=\Pi\tau_i$$

Exposure rate：

$$\overline{T}=1-T=1-\Pi\tau_i$$

4) The degree of attack hazard

Definition6 shows that Ω as the output alphabet set of the finite automaton. It means that the importance of attack and the extent of the damage on the target system. From the view of the defense, the most seriously harmful place is the place which is the most need to defense, namely:

$$\Omega=MAX(\omega_1,\omega_2,\cdots,\omega_6)$$

IV. Application Examples and Analysis

Attack target host as the Windows operating system, and get access permissions of its file. Take the above for example, an attack process can be divided into: target reconnaissance (a_1) → scanning target host port (a_2) → getting host login account and password (a_3) → backdoor (a_6). Constructing a state transition diagram shown in Figure 3, where S_0 is the initial state, the attacker conducts reconnaissance on the target host, to collect basic information, such as network topology, and to make it transfer into S_1; the target host port scanning into state S_2; getting host login information into the S_3; backdoor into S_6. If $S_6 \in S_7$, the attack process will end, there will be into an acceptable state. This can get attack sequences (a_1, a_2, a_3, a_6) and a description of the set of states (S_0, S_1, S_2, S_3, S_6, S_7), combined with system states attack sequence sets, it will constitutes one finite automaton which have file access permissions to the Windows.

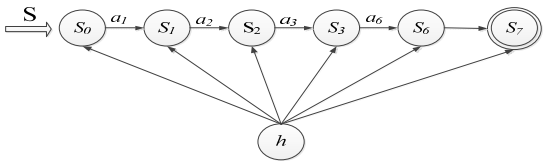

Figure 3. States transition diagram with access authority

If a_2 launched twice attacks, the result will be:

$$S_0 \Rightarrow (a_1,1)(a_2,0)(a_2,1)(a_3,1)(a_6,1)$$

The judgment of harm degree as the TABLE Ⅱ shows:

TABLE II. HARM DEGREE OF THE ATTACKS

attack entities	*harm degree*
a_1	1
a_2	1
a_3	4
a_6	3

Seen from the table, attack entity a_3 bring the most serious harm to the system, which should be a focus on defense. In practical application, according to the network environment and security needs to strengthen the defense of the attack entity a_3, so that network security will be greatly enhanced.

V. Conclusions

On the base of research on cyberspace environment, finite automaton theory and the attack model, this paper proposes the attack model based on finite automaton. The analysis of the model can meet the needs of cyberspace attack modeling and be effective on cyberspace attack detection and safety warning. Moreover, make an extension on this model to study offensive and defensive game model of the attack gains and defense costs.

References

[1] CHEN Chun-Xia and HUANG Hao. Analysis and Research of Attack Model. Application Research of Computers. 2005, 7:115-118.

[2] Koral Ilgun, Richard A. Kemmerer and Phillip A. Porras. State Transition Analysis: A Rule-Based Intrusion Detection Approach.IEEE Transactions on software engineering 1995, 21(3):181-199.

[3] LAI Hai-guang, HUANG Hao and XIE Jun-yuan. Attack model and its appication based on system states aggregation. Computer Applications. 2005, 25(7):1535-1539.

[4] SU Yi-Dan and LI Gui. The Research on Model Method of Large-scale Intrusion Based on DFA. Computer Engineering and Applications. 2003, 197-199.

[5] CHEN Xiao-su, LI Yong-Hui and XIAO Dao-Ju. Analysis of the state under IP spoofing. Journal of HUAZHONG University of Science and Technology(Nature Science Edition). 2003,31(5):3-5.

[6] Jason Andress and Steve Winterfeld. Cyber Warfare. USA: Syngress, 2011.

[7] JIANG Zong-Li and JIANG Shou-Xu. Formal Languages and Automata Theory. BEIJING: Tsinghua University Press, 2007.