2014 3rd International Conference on Informatics, Environment, Energy and Applications
IPCBEE vol.66 (2014) © (2014) IACSIT Press, Singapore
DOI: 10.7763/IPCBEE. 2014. V66. 14

The Common Network Attack Model Based on Interval Temporal Logic

Qinglei ZHOU, Xiyue CHEN and Weijun ZHU[+]

School of Information Engineering, Zhengzhou University, Zhengzhou, 450001, China

Abstract. Compared with the intrusion detection methods based on model checking linear temporal logic (LTL) , the intrusion detection methods based on the interval temporal logic (ITL) model checking improves the ability to detect intrusion detection system. However, the latter technique is still not able to establish universal model on the process for common network attack .To this end, we use eight ITL sub-formulas to build formula model for 8 stages of the procedure of common attacks respectively, and use the interval operator to connect these eight sub-formulas , so that we get the common network attack model. On this basis, we can use the existing ITL based model checking algorithm for automatic monitoring of the general procedure of attacks. Compared with the existing methods, the new method is not specific to a particular attack model, but detecting all types of attacks based on universal principles. This is the comparative advantage of the new method.

Keywords: Intrusion Detection, Model Checking, Interval Temporal Logic.

1. Introduction

Intrusion Detection (ID) is an important network security technology. According to different detection principles, it can be classified into misuse detection and anomaly detection. Due to the high false alarm rate of anomaly detection, the deployed intrusion detection systems(IDS) mostly adopt misuse detection internationally .

However, the misuse detection based on pattern matching has its own defects. Facing lots of increasingly complex attack patterns in the network, technologies based upon pattern matching fall short of detection ability seriously. For this reason, the model-based detection methods have been proposed [1] [2] [3].

The basic principle of MC-based IDS technology is as follows: First, use an LTL formula to describe a type of attack; secondly use automata to build models for the log database, so that intrusion detection problem was reduced to the MC problem: If the model checking algorithm determines that the automaton satisfies a formula, it means that log records match attack mode and intrusion detector will alarm attack.

However, for the current intrusion detection method based on model checking, the established intrusion detection models are specific to a particular type of attack or several types of attacks. The model created for common process of network attack is still in deficiency. This is what will be studied in this paper.

2. Interval Temporal Logic

Definition 1, (Syntax of propositional ITL [6][7][8], ITL for short)

For all $p \in AP$, p is a ITL formula.

If φ,φ are ITL formulas, so are the constructs $\neg\varphi$, $\varphi \vee \psi$, $\bigcirc\varphi$, $\varphi;\psi$, $\varphi*$

Definition 2, A interval of states is defined and also denoted as $\sigma = < s_0, s_1, ..., s_i, ... >$, where s_i is a state.

[+] Corresponding author..
E-mail address: zhuweijun76@163.com.

Definition 3, An interpretation is a quadruple $I=(\sigma,i,k,j)$, where σ is a sequence of states over $<s_i,...,s_k,...,s_j>$, $i,k,j\in N$, s_k is the current state. We use the notation $len(\sigma)=|\sigma|=j-i$ for the number of states in interval.

Definition 4, (Semantic of ITL). Let $c\in N$ and $s_p(k)$ be the true value of $p\in AP$ in state S_k. The satisfaction relation is inductively defined as follows:

1) $I\models p$ iff $s_p(k)$=true,

2) $I\models\neg\varphi$ iff $\neg(I\models\varphi)$,

3) $I\models\varphi_1\vee\varphi_2$ iff $I\models\varphi_1$ or $I\models\varphi_2$,

4) $I\models skip$ iff $len(\sigma)=1$,

5) $I\models\bigcirc\varphi$ iff $(\sigma,i,k+1,j)\models\varphi$,

6) $I\models\varphi_1;\varphi_2$ iff $\exists r,k\le r\le j,$ such that $(\sigma,i,k,r)\models\varphi_1$ and $(\sigma,i,k,r)\models\varphi_2$

7) $I\models\varphi^*$ iff: i) there exist finite many $r_0,...,r_n\in N_\omega$, such that $k=r_0\le r_1\le...\le r_{n-1}\le r_n=j$, $(\sigma,i,k,r_0)\models\varphi$, and for every $1\le l\le n$, $(\sigma,r_{l-1},r_{l-1},r_l)\models\varphi$。 ii) or $k=j$.

Definition 5, (Derived ITL formulas).

$\Diamond\varphi=true;\varphi$,

$\Box\varphi=\neg\Diamond\neg\varphi$,

$\varphi\wedge\psi=\neg(\neg\varphi\vee\neg\psi)$, $\varphi_1\|\varphi_2=\varphi_1\wedge(\varphi_2;true)\vee\varphi_2\wedge(\varphi_1;true)$

3. Intrusion Detection Algorithm based on Interval Temporal Logic Model Checking

Theorem 1 [4], let an ITL formula be a model of attack behavior, and automaton A be the model of log records , then the ITL model detection algorithm M could detect whether records in A satisfy φ or not).

4. The basic process of network attacks

Network attacks are ever-changing with various means and different effects. However, all successful attacks have substantially similar procedure [9]. [9] provides a universal process for the definition of network attacks. This process divides network attack into 8 stages. For each stage, the methods/techniques/steps attackers used are shown in Table 1---Table 8.

.

Method Number	Method Description
A1	Use the infected host as a springboard
A2	Apply telephone switching technology to hid attacker identity/hid the identity of attacker
A3	Steal other's Internet account/Theft of account for online
A4	Carry out attacks through a free proxy gateway
A5	Forge IP address
A6	Personate user’s accounts

Table 1: attack identity and location hidden

Method Number	Method Description
B1	Use the scanner tool : NMAP, SHADOWSCAN, CIS, SUPERSCAN, HOLESCAN
B2	Use vulnerability checking tools :Nessus
B3	Use large range scanning tool X-SCA
B4	Use graphical tracking tool NEOTRC

Table 2: target system information collection

Method Number	Method Description
C1	Use SNIFFER tools: TCPDUMP, WINDUMP, SNIFFIT, NETXRAY
C2	Use password hacking tool: DSNIFF
C3	Use password cracking tools: PWDDUMP, L0PHTCRACK
C4	Use disassemble tool, debugging tool

Table 3: vulnerability information mining and analysis

Method Number	Method Description
D1	Crack Root password
D2	Acquire authority by exploiting system management flaw
D3	Run the Troy Trojans to intercept login password
D4	Hacking the administrator password

Table 4: target acquisition access to hidden attack

Method Number	Method Description
E1	Pretend to be other users, modify LOGNAME environment variable, modify login log files, use IP spoofing

	technology
E2	Use PS redirection technology to reduce information given by process-look-program , replace PS with Trojan horse.
E3	Use similar string to paralysis system administrator, or modify the file attributes so that ordinary display method cannot get access to files
E4	Use the operating system to loadable the characteristics of module, hiding attack information.

Table 5: concealed attack behavior

Method Number	Method Description
F1	Through the access to information, use, destroy or tamper with the information; Through the use of proprietary information, credit card information, personal information and confidential information to gain interests
F2	By using high speed computer system or a high-speed network system to attack other trusted host or network
F3	Modify or delete important data, delete user accounts, stop network services.

Table 6: launch attack

Method Number	Method Description
G1	broaden the file permissions
G2	reopen insecurity services such as REXD ,TFTP, etc
G3	Modify the system configuration such as system startup files, web services configuration file
G4	Replace the shared file system

G5	Modify the original program, install all kinds of Trojan horse
G6	Install the sniffer
G7	Establish concealed channel

Table 7: open the back door

Method Number	Method Description
H1	Tampering with the audit information in the log file
H2	Change system time, resulting in the log file data disordered
H3	Remove or stop the audit service process
H4	Interfere with the normal operation of the intrusion detection system
H5	Modify the integrity test label

Table 8: the elimination of attack traces

5. Use Interval Temporal Logic formula to establish the general network attack model

Define 6. Suppose the serial number of methods listed in table 1--8 methods as ITL atomic proposition formula respectively, the general model of the network attack is defined as follows:

φ= (A1∨A2∨A3∨A4∨A5∨A6)*;(B1∨B2∨B3∨B4)*;
(C1∨C2∨C3∨C4)*;(D1∨D2∨D3∨D4)*;
(E1∨E2∨E3∨E4)*;(F1∨F2∨F3)*;
(G1∨G2∨G3∨G4∨G5∨G6∨G7)*;
(H1∨H2∨H3∨H4∨H5)*

For the eight stages of general procedure, they have ordinal relation. Therefore, we use the interval operator ";" to describe the relationship of different stages of the sub-formula. Each stage of the implementation is possible to cycle, so we add operator "*" to express each stage of the sub-formulas. At each implementation process stage, the attacker may employ different methods/techniques/procedures, so we use operator“∨”to describe different atomic propositions of methods/techniques/procedures to connect.

Considering the methods/techniques/procedures may be composed of finer-grained technical steps, we can further refine the general formula model in definition 6. The method is: use ITL sub-formula to express the process of finer-grained technical steps , then replace the atomic propositions in definition 6 . Through the above successive refinement method , we can get accurate enough ITL formula φ' to establish finer-grained universal model of attack process , and put φ' as the input of the algorithm M in theorem 1 , and set the automaton as the other input , then we can operate the algorithm and attack detection results are obtained.

6. Conclusions

We use the formula of interval temporal logic to establish the universal model of general process for network attack, on the basis, the core method for detection is presented. The existing experimental study [4] [10] confirmed the validity of the intrusion detection technology based on interval temporal logic, consequently, the new method is feasible. The new universal model can cover the general process of network attacks, but similar existing methods can't do it yet. In order to explorer the modelling ability of the new

method, we have conducted some simulation experiments. The fig.1 gives a comparison between the method presented in this paper and the one in [1] by using MATLAB. The results indicate that the new method can model more attacks than the existing method due to the stronger model which embeds into the new method. For example, the new method can describe the same amount DOS attacks as the method presented in [1]. And for Probing, U2R and R2L attacks, the new method can do more than the one in [1]. This is the comparative advantage of this new method.

Carrying out intrusion detection based on the new model is helpful to the promotion of the generic technology based on model checking to all types of attack detection, thus to provide a universal technology framework for realizing high detection ability for common attack types. This is the contribution and significance of our work.

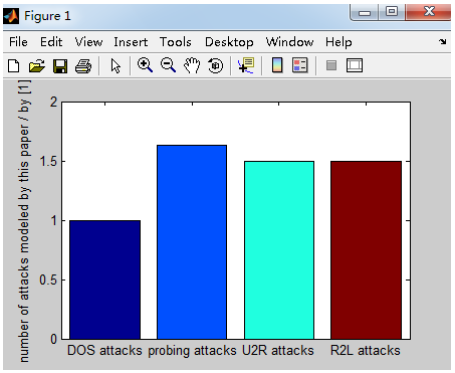

Fig.1: a comparison of modeling ability for four categories of attacks

7. Acknowledgements

This work has been supported by the National Natural Science Foundation of China under Grant No.U1204608 and No.61250007, as well as China Postdoctoral Science Foundation under Grant 2012M511588.

8. References

[1] M Roger, J Goubault-Larrecq. Log Auditing through Model-Checking, Proceedings of the 14th IEEE workshop on Computer Security Foundations. *IEEE Computer Society* .Washington, DC, USA, 220-234, 2001.

[2] J Olivain, J Goubault-Larrecq. The Orchids Intrusion Detection Tool, Proceedings of the 17th International Conference on Computer Aided Verification, Lecture Notes in Computer Science, 3576:286-290, Springer. *Edinburgh*. Scotland, UK, 2005.

[3] J Goubault-Larrecq , J Olivain, A Smell of Orchids, Runtime Verification: 8th International Workshop, RV 2008, pp1-20. *Budapest, Hungary*. March 30, 2008.

[4] W Zhu, Z Wang, H Zhang, A novel algorithm for Intrusion Detection based on Model Checking Interval Temporal Logic.*China Communications*. 8(3): 66-72, 2011.

[5] W Zhu, Q Zhou, W Yang, et al, A Novel Algorithm for Intrusion Detection Based on RASL Model Checking, mathematical problems in engineering, vol. 2013, Article ID 621203, 10 pages, 2013. DOI:10.1155/2013/621203.

[6] B Moszkowski, Reasoning about Digital Circuits, PhD thesis. *Department of Computer Science*. Stanford University, 1983.

[7] Z Duan, C Tian, L Zhang， A decision procedure for propositional projection temporal logic with infinite models. *Acta Informatica*. 45(1):43-78, 2008

[8] Z Duan, Temporal Logic and Temporal Logic Programming, Beijing: *Science Press*. 2005.

[9] H Liu，Principle and Implementation of Computer Network Security，BeiJng：*Machinery Industry Press*.2009, (in Chinese).

[10] W Zhu, Q Zhou, P Li, Intrusion detection based on model checking timed interval temporal logic，IEEE International Conference on Information Theory and Information Security. *Beijing, IEEE press*.503-505, 2010.