Detection of Back Attack based on Interval Temporal Logic

Juan Zhang¹, Fenfei Gu*¹
¹Institute of information engineering, Anhui Xinhua University, Hefei, Anhui, 230088, China
*Corresponding author’s e-mail: 295548153@qq.com

Abstract. Contrasted with other detection methods, based on temporal logic the intrusion detection method can deal with complex network attacks actively. However, due to the lack of network attacks temporal logic formula, common back attack cannot use the above methods of detection. Therefore, the Propositional Interval Temporal Logic (ITL) is used to establish temporal logic formulas for back attack. Firstly, the attack principle of back attack was analyzed. Secondly, the critical steps of the attack were break up into atomic actions and the atomic proposition was defined. Finally, the temporal logic formula for the attack was established based on the logical relationship between the atomic propositions. According to the principle of model checking, the obtained temporal logic formula can be used as the input for the model checker (intrusion detector). The automaton was utilized to model the log library as another input to the model checker. And the intrusion detection method for these three attacks was given. and it proved the validity of the novel method by some Simulation experiments

1. Introduction

As one of the important network security technologies, Intrusion Detection (ID) used to be classified into misuse detection and anomaly detection. caused the anomaly detection has the high false alarm rate, the misuse detection genarally is adopted internationally in deploying intrusion detection systems (IDS).

However, based on pattern matching the misuse detection has its own faults. due to the rapid increase of complex attack patterns in the network, the technologies of based on pattern matching lack of detection ability seriously. on the background, the model-based detection methods have been proposed [1-3].

Compared with the pattern matching method, the model-based detection method can effectively describe the variation of attack patterns [1-2, 4-5]. Pattern matching is usually used to detect inconsistencies between data, while the model detection of automata, temporal logic formulas and model detection techniques are used to detect inconsistencies in behavior. As a result, model-based methods have stronger detection capabilities than pattern-based methods because of the complex behavior in intrusion attacks [5]. The basic principle of model detection [6] can be summarized as follows: (1) describe the attack pattern and noted the attack process in audit log library automatically by using the temporal logic formula, (2) detect whether meet the formula automatically and whether the note in the library matches the attack pattern by using the model detection algorithm. The logical operators in timing formulas provide the flexibility to describe the various logical relationships between attack actions.

However, there are still some problems that need to be solved based on model detection of the present intrusion detection method. First of all, it cannot be fully tested for 39 attacks of the common

---

[1] IWAACE 2020
[2] Journal of Physics: Conference Series
[3] 1550 (2020) 032164
doi:10.1088/1742-6596/1550/3/032164
IWAACE 2020
Journal of Physics: Conference Series 1550 (2020) 032164
IOP Publishing
doi:10.1088/1742-6596/1550/3/032164

2. Interval temporal logics
Definition 1, (Syntax of propositional ITL [8-11], ITL for short)
• For all \( p \in AP \), \( p \) is a ITL formula.
• If \( \varphi, \psi \) are ITL formulas, the constructs are \( \neg \varphi, \varphi \lor \psi, \varnothing \varphi, \varphi ; \psi, \varphi^* \).
Definition 2, A interval of states is defined and also denoted as \( \sigma =< s_0, s_1, \ldots, s_j, \ldots > \), where \( s_i \) is a state.
Definition 3, An interpretation is a quadruple \( I = (\sigma, i, k, j) \), where \( \sigma \) is a sequence of states over \( \langle s_j, \ldots, s_k, \ldots, s_i \rangle \), \( i, k \in N \), \( s_k \) is the current state. We use the notation \( \text{len}(\sigma) = |\sigma| = j - i \) 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 \( s_p(k) = \text{true} \),
2) \( I \models \neg \varphi \) iff \( \neg(I \models \varphi) \),
3) \( I \models \varphi_1 \lor \varphi_2 \) iff \( I \models \varphi_1 \) or \( I \models \varphi_2 \),
4) \( I \models \text{skip} \) iff \( \text{len}(\sigma) = 1 \),
5) \( I \models \Box \varphi \) iff \( (\sigma, i, k + 1, j) \models \varphi \),
6) \( I \models \varphi_1 \land \varphi_2 \) iff \( \exists r, k \leq r \leq j \), 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 \( r_0, \ldots, r_n \in N \), such that \( k = r_0 \leq r_1 \leq \ldots \leq r_{n-1} \leq r_n = j \), \( (\sigma, i, k, r_i) \models \varphi \), and for every \( 1 \leq l \leq n \), \( (\sigma, i, k, r_{l-1}, r_l) \models \varphi \) . or \( k = j \).
Definition 5, (Derived ITL formulas).
\( \varnothing \varphi = \text{true}; \Box \varphi, \varnothing \varphi = \neg \Box \neg \varphi, \varphi \land \psi = \neg (\neg \varphi \lor \neg \psi) \), \( \varphi_1 \parallel \varphi_2 = \varphi_1 \land (\varphi_2; \text{true}) \lor \varphi_2 \land (\varphi_1; \text{true}) \)

3. The temporal logic model of back attack
3.1. Principles
apache web server is launched by the back attack, it contained a large number of requests of front slash characters (/) in URL descriptions. it can not deal with noraml request when server is attack by these request and it will reject the request service to its customers [12].

3.2. Details of back attack
The attacker sends much requests to the server with a pre-character (/) in the URL’s address description. The server attempts to process the large number of requests so that legitimate services cannot be served.

3.3. Atomic action of back attack
The critical steps can be formulated as follows: (1) The Apache Web server received an invalid web request from the attacker; (2) and the network host sends a legitimate http request to the Apache Web server. (3) The Apache web server receives a valid http request; (4) but the network host can not receive a packet that requests a reply.

3.4. Atomic sequence of back attack
In line with the key steps and the rules, inclue the atomic requests for atomic actions in back attack, as shown in Table 1.

| Atomic propositions            | Their means                                                                 |
|-------------------------------|-----------------------------------------------------------------------------|
| ApacheWebserver.receive.http.p| The Apache Web server received an http request with the field p.             |
| i.send.ApacheWebserver.http   | The network host i sends an http request to the Apache Web server.           |
| ApacheWebserver.receive.http_i| The Apache Web server receives a http request from network host i.          |
| i.receive.ApacheWebserver     | The network host receives the packet from the Apache Web server.             |

3.5. The formula for back attack
In line with key steps, the reules and the temporal relationships between the atomic requests, include the following ITL formula for Back attack:

\[(\text{ApacheWebserver.receive.http.p} \land \text{true})^* \rightarrow XF(\forall i(i.\text{send.ApacheWebserver.http} \land F(\text{ApacheWebserver.receive.http_i} \land G(\neg i.\text{receive.ApacheWebserver}))))\]  

(1)

4. Back attack detection method based on ITL
Accroding to the formula (1), The intrusion detection method based on ITL model checking for back attack as shown in Figure 1.
Figure 1. The ITL-based model checking for back attacks.

5. Conclusion

Temporal logic formula model for back attack is proposed in this paper. Generally, MC intrusion detection method can be used to detect such attacks. Do many simulation experiments by using MATLAB, And the experiment results are shown in table 2. contrasted with Linear temporal logic (LTL), Computation Tree Logic (CTL) and Time interval temporal logic (TITL), Just ITL method can detected this kind of attacks, which has the comparative advantages from new method. Caused intrusion detection method based on MC was stronger than (Pattern Matching) PM, the new method can effectively detect back attack with variable patterns. That is the main contribution of this paper.

Table 2. Comparison of different logic-based methods for the ability of detecting back attack.

| Methods based on different logical | Whether it can detect back attack |
|-----------------------------------|----------------------------------|
| LTL-based model checking          | No                               |
| CTL-based model checking          | No                               |
| TITL-based model checking         | No                               |
| ITL-based model checking          | Yes                              |

Acknowledgments

This work was supported by Natural Science Research Project of Colleges and Universities of Anhui Province (KJ2019A0869) and Excellent Talent Training and Innovation Project of Anhui Province (2019zyrc111).
References

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

[2] Olivain, J., Goubault-Larrecq, J. (2005) The Orchids Intrusion Detection Tool. In: Proceedings of the 17th International Conference on Computer Aided Verification, Lecture Notes in Computer Science. Edinburgh. pp. 286-290.

[3] Goubault-Larrecq, J., Olivain, J. (2008) A Smell of Orchids. Lecture Notes in Computer Science, 5289: 1-20.

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

[5] Zhu, W.J., Zhou, Q.L., Yang, W.D., et al (2013) A Novel Algorithm for Intrusion Detection Based on RASL Model Checking. Mathematical Problems in Engineering, 2013 (621203).

[6] Clarke, E., Grunberg, O., Peled, D. (1999) Model Checking. The MIT Press, London.

[7] KDD Cup 1999 Data [EB/OL] (1999). http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[8] Moszkowski, B. (1983) Reasoning about Digital Circuits. PhD thesis, Department of Computer Science, Stanford University.

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

[10] Tian, C., Duan, Z.H. (2009) Complexity of propositional projection temporal logic with star. Mathematical Structures in Computer Science, 19(1): 73-100.

[11] Duan, Z.H. (2005) Temporal Logic and Temporal Logic Programming. Science Press, Beijing.

[12] Zargar, S., Joshi, J. and Tipper, D. (2013) A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks. Communications Surveys & Tutorials, IEEE, 99: 1-24.

[13] Zhou, Q., Hu, W., & Zhu, W. (2015). Detection of Mailbomb Attacks Base on Time Interval Temporal Logic. 2015 International Conference on Computational Intelligence and Communication Networks (CICN). IEEE.