Modeling Attack Process of Advanced Persistent Threat

Weina Niu[1], Xiaosong Zhan[1](✉), Kenli Li[2], Guowu Yang[1], and Ruidong Chen[1]

[1] Center for Cyber Security, University of Electronic Science
and Technology of China, Chengdu 611731, China
niuweina1@126.com, {johnsonzxs,guowu}@uestc.edu.cn, crdchen@163.com
[2] Institute of Supercomputing and Cloud Computing,
Hunan University, Changsha 410082, China
lkl@hnu.edu.cn

Abstract. Advanced Persistent Threat (APT) with deep concealment has become one of the most serious network attacks. Modeling APT attack process can facilitate APT analysis and detection. However, existed modeling approaches neither reflects APT attack dynamically nor takes human factor into consideration. In order to achieve this, we propose a Targeted Complex Attack Network (TCAN) model for APT attack process. Compared with current models, our model addresses human factor by conducting two-layer network structure. Besides, our model introduces time domain to expand the traditional attack graph into dynamic attack network. Whats more, we propose dynamic evolution rules based on complex network theory and characteristics of the actual attack scenarios. Our simulation results show that the model can express the process of attack effectively.

Keywords: Attack process modeling · APT · TCAN · Human factor · Complex network theory

1 Introduction

Since Advanced Persistent Threat (APT) [1–3] coning as a new concept by the US Air Force in 2006 [4], it has flourished as a security marketing buzzword in network security. Nowadays, notion announced by the US National Institute of Standards and Technology [5] is widely acknowledged: an APT attack is launched by high-skilled and well-funded attackers. Such attack comprises multiple attack vectors used to exfiltrate information or sabotage the infrastructures. Explaining, detecting and predicting APT attacks are indispensable to model the procedure of APT attacks. Research of network attack modeling lasted for several years. Many models have been proposed so far, such as attack tree [6], attack graph [7] and attack net [8]. However, these traditional modeling methods present neither dynamic change of the actual APT attack nor consider the human factor.

The main goal of this paper is to identify the hosts that definitely involved in the attack process. To break current limitations, we propose a network-evolution-based approach to model the attack process of APT attacks. In our model, nodes

© Springer International Publishing AG 2016
G. Wang et al. (Eds.): SpaCCS 2016, LNCS 10066, pp. 383–391, 2016.
DOI: 10.1007/978-3-319-49148-6_32

and edges of traditional attack graph are redefined. Communication-contact network [9] is introduced to indicate the influence of social engineering since social engineering can be exploited in each APT case. In the simulated experiment, the free-scale network is used to express network structure. By analyzing the network formation, our approach can represent popular APT cases.

The remainder of this paper is organized as follows: Sect. 2 gives an overview of the related work; Sect. 3 represents how the TCAN is generated; Sect. 4 shows the preliminary experimental results; future work and conclusions are summarized in Sect. 5.

2 Related Work

In recent years, researches on modeling network attack have been proposed continually which bring about a number of models. However, few papers discussed APT attack modeling [10–14]. The attack pyramid model on attack tree proposed by Paul [10], which provide guidelines for detecting APT by the association of attributes and time. The attack kill chain model [12,13] can describe the phases of an APT attack based on the concept of intrusion kill chain [15], such as Chen et al. [12] divided APT attack into six stages. The impact on the target network caused by the next attack action can be measured using a probability. Thus, a novel Markov Multi-Phase Transferable Belief Model (MM-TBM) [13] was used to guide the network administrator to detect APT attack early. However, these three kinds of models lack the description of the state change.

Zhao et al. [11] proposed EPANM model combines attack scene, attack process, and state space by extending the structure of classical Petri net. However, EPANM model has poor adaptability because it limits attacks process to eight states. Thus, this model cannot reveal attack process dynamically. Fang et al. [14] use a game model to predict the optimal attack path of an attacker and the best-response strategies for a defender by quantifying rewards. However, this model did not consider the human factor.

3 Targeted Complex Attack Network

In this section, we give a detailed description of our network-evolution-based modeling approach [16]. At first, some definitions are shown; then the derivation of our model is described; the last part of this section expatiates the change of node state.

3.1 Definitions

Definition 1. A node is expressed by a three-tuple N = (description, host, status), which is used to indicate a device in the network.

The description is used to describe factors that affected nodes into connect-successful; represents node id, that is specified as an IP address; represents the node status, which is in one of the five states: susceptible, provide-information, attack-successful, active-propagation and removed.

Definition 2. An attack edge is expressed by a three-tuple $e = (n_i, n_j, R)$.

R represents relationships exploited by this attack behavior, which is subjected to $R = R^{Topology} \bigcup R^{Trust}$, indicated as T1, T2, where $R^{Topology}$ represents the topology relationship. If the value of R is R^{Trust}, this attack is going by social engineering. Thus, we take the human factor into consideration by using trust relationship to conduct an attack in the actual attack process.

Definition 3. The current attack situation is described by a complex attack network $CAN = (N, E)$ from the formalization perspective.

3.2 Model Derivation

According to the definition of a dynamic network [17], the dynamic attack network can be regarded as the attack sub-graph sequences over the series of consecutive time steps.

According to Definition 3, we define attack network at time t as $CAN_t = (N_t, E_t)$.

$N_t = \{n_i | i = 1, 2, ..., m_t\}$ represents the set of all nodes involved in the attack until time t, where n_i represents a node, indicated as "◯". $E_t = \{e_j | j = 1, 2, ..., s_t\}$, where e_j represents an attacking edge, indicated as "$\longrightarrow$".

Although the procedure of APT attack has a certain stability of time and space, with APT attack continues, there are new attack behaviors occurring. Thus, new nodes and edges need to join the attack network. If previous attacks failed, nodes and edges existed in the attack network need to be removed. However, most of the time attackers collect information about the target. This phenomenon is consistent with individual human mobility patterns, in other words, although most attack behaviors are placed soon after a previous attack behavior, occasionally there are long periods without any attack activity.

According to network evolution theory [16], APT attack process subjects the following steps:

1. Adding: Node and edges have characteristics of dynamic growth with the attack progress;
2. Removing: A node may become a failure node, once the previous attack behavior fails. For example, service as the prime attack target is shut down etc. before the attack succeeds.

Thus, the CAN at time t+1 can be expressed as $CAN_{t+1} = (N_{t+1}, E_{t+1})$, which meets the following conditions:

$$(1) N_{t+1} = (N_t \cup \{n_a^{t+1}\} - \{n_d^{t+1}\}),$$
$$(2) E_{t+1} = (E_t \cup \{e_a^{t+1}\} - \{e_d^{t+1}\}.$$

$\{n_a^{t+1}\}$ represents the new adding nodes. $\{n_d^{t+1}\}$ represents nodes set which needs to be removed from the attack network. $\{e_a^{t+1}\}$ represents the attack edges joining into the attack process. $\{e_d^{t+1}\}$ represents the attack edges removed from attack process once the target node is removed.

3.3 Change of Node State

In the target network, each node is in one of the five states: susceptible, provide-information, attack-successful, active-propagation and removed. In the beginning, we assume that all the devices in the network environment are susceptible and each device has a user. There are two layers in our multiplex network: communication network labelled A, contact network labelled B. A network and B network express trust relationship and topology relationship, respectively. There is no self-loops or repeated links in these two networks. Meanwhile, there is no correlation between the generated double-layer network. Each node in layer A is matched with that of layer B one-to-one.

The state of a device changes from susceptible to transitional in the following two situations: (1) this device has a connection to the active-propagation device, (2) the user of this device trusts the user of active-propagation device, that is to say, there is a trust relationship among the users of device changed status and device in active-propagation. A device changes stages from transitional to connect-successful, when this device in the selection region. After connecting with attackers successfully, this node will join into two statuses: provide-information and attack-successful. When a compromised node has been chosen as the stepping stone, the node is added to state active-propagation. Only this device is used as a stepping stone in the next attack step, it will infect other nodes. Moreover, the state transition from active-propagation to removed, attack-successful to removed in our model represent that the compromised computer is detected and fixed. Removed nodes will disconnect with the current active-propagation node in the target network. Nodes in provide-information state or nodes in the removed state are transformed into susceptible when these nodes connect to the current active-propagation node.

4 Experiments

4.1 Experiment Set-Up

To validate our models applicability to different attack scenarios, we choose the scale-free network and small-world network as the topology and trust relationship, respectively [17]. Experimental results reported below are the average of 100 repeated experiments. The measures of interest include the number of nodes in the attack-successful state, provide-information state, and remove state at the end of the attack, attack steps acquired by this attack. To jumpstart the APT attack progress, the initial number of active-propagation nodes is set to one. In other words, the statue of the attacker is active-propagation.

4.2 The Baseline Experiment

The first simulation is the baseline experiment. The number of topology size is set to 10. The topology and trust relationship of the target network is shown in Fig. 1. Node 5 is in active-propagation state. Node 9 is the target node. The parameter of probability provide-information is set to 0.8. The parameters of removal rate and failure rate are set to 0.1.

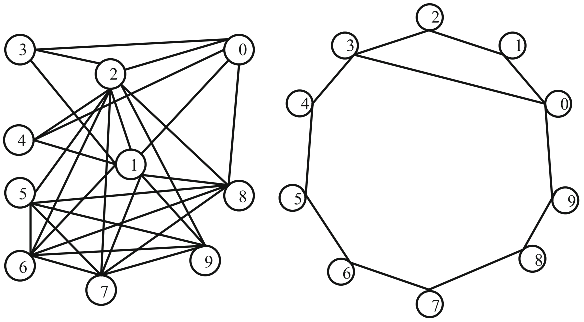

Fig. 1. Detection effect of flow-based and conversation-based features

Status of nodes in the target network at every attack step is shown in Fig. 2. Figure 3 presents the detailed attack path, where T1 is the topology relationship, and T2 is the trust relationship. PI, CI, A, P, R represent provide-information, collect-information, attack-successful, active-propagation, removed state, respectively. Meanwhile, they are descripted using cycle with different colors, like black cycle denotes attacker, yellow cycle node in provide-information state, blue cycle node in attack-successful, green cycle node in active-propagation state, the red cycle is target node.

4.3 The Baseline Experiment Analysis

In this simulated experiment, attacker collects information about target network from a public source, indicated as node 1, 2, 4, 6, 7, 9. Then attacker breaks into the node 8 through network infiltration method. Finally, the attacker controls the target node using social technologies. This attack pattern is similar to Operation Aurora [18]. Operation Aurora was a serious cyber attack caused by APT in 2009. In this attack, the user names and passwords of sensitive users accessed to google server were stolen. Its consequences led to the theft of important email information about these sensitive users.

The following analysis is implemented using the proposed TCAN on the background of Google Auraro.

1. The attacker collects information about staff in target network from open source.

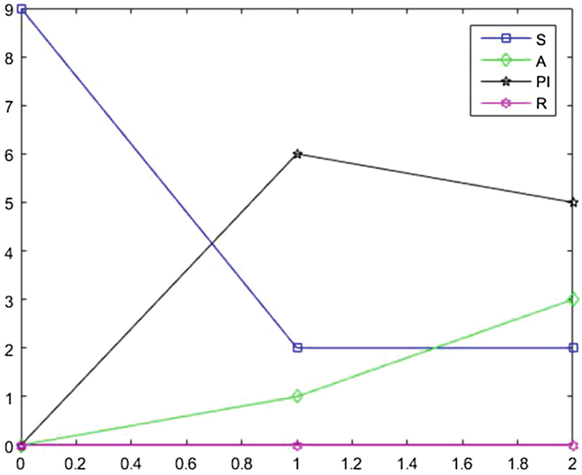

Fig. 2. The number of different states node

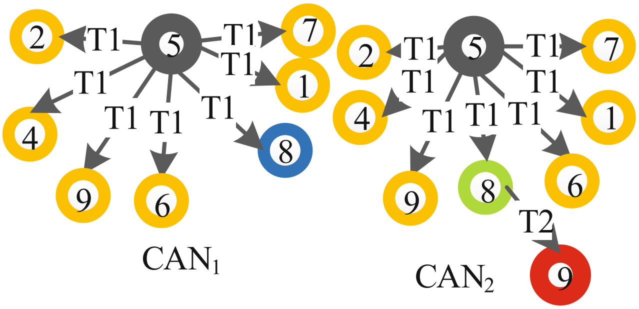

Fig. 3. A TCAN evolutionary process

2. A certain employee E is targeted. Then, the attacker collects information about this certain employee E from social network websites like Facebook, Twitter, and LinkedIn. Next, specific friend F who likes photograph is selected. Followed is that the attacker breaks into the host of friend F through network infiltration method.
3. The attacker pretends to be the friend E and sends an instant message to this employee in order to invite him to enjoy the latest photos. But the URL points to a web page loading shellcode and Javascript, which is managed by a Web server forged by an attacker. The employee E clicks the link to enter the malicious web site forged by the attacker, which can cause the overflow of IE browser with this specific employee in Google. The host of this specific employee executes FTP download program locally. The host of this specific employee downloads more programs to execute, such as Trojan. Then, the connection is established between target host and attacker host through SSL Tunnel.

Table 1. The attack steps to different probability of provide-information

The probability of provide-information	Attack steps
0.5	8
0.6	29
0.7	108
0.8	217
0.9	27

We found that there are many factors influencing attack choice. For example, the sometimes attacker chooses the sub-optimal attack path to escape detection. Thus, there are five kinds of nodes, including initial nodes, failure nodes, information nodes, immune nodes, and target nodes in our model. Failure nodes explain percolation phenomena in actual APT attacks. We cannot reconstruct the entire attack path when the failure nodes existing in this attack process. Immune nodes exist outside the attacking net in isolation, which reveals the herd immunity phenomena. There are no edges pointing to other nodes of information nodes, which illustrates cumulative advantage existing in the derivation of TCAN. At the same time, there is at least one node called target node, which does not have outing edges of the TCAN model. The TCAN model building completes after the target node added to the net.

4.4 Experiments of Different Probability Provide-Information

Table 1 shows the sensitivity of APT attack progress to different probability provide-information. It is obvious that the larger probability provide-information

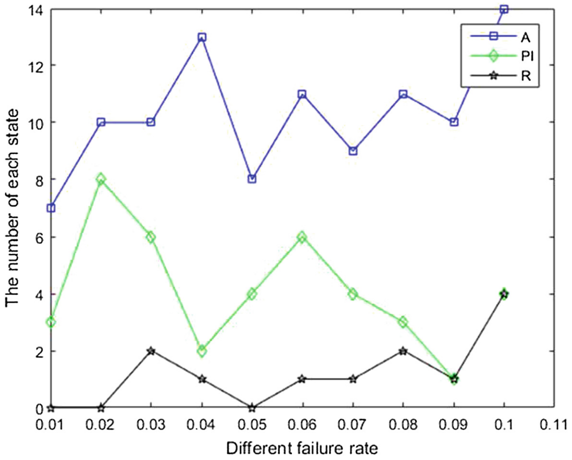

Fig. 4. The number of each state at the end of this attack to different failure rate

results in larger attack steps. The number of nodes involved in the attack progress increases with the probability provide-information as well. It can be seen that a serious fall in attack steps when the probability of provide-information increases to a certain size. Thus, we can make a conclusion that the more information about the target node collected by attackers, the faster, more cost-effective to reach their attack goal.

4.5 Experiments of Different Failure Rate

In the end of this section, we study the effect of failure rate on APT attack progress. It is obvious from Fig. 4 that different failure rates have their impacts on the attack progress. The anti-malware systems deployed in the target network defend network attacks at a fast-enough rate, then this APT attack can actually increase attack steps.

5 Conclusion

In this paper, a network-evolution-based attack network generating mechanism is introduced to express APT attack. A double-layer network is introduced to elucidate the effects of human interaction in layer A, topology link in layer B. Our proposed model focused on attack network that helps security analysts to understand APT attack mechanism. This work considers suspicious hosts involved in APT-related activities by social engineering and network penetration. Moreover, our model demonstrates the attack situation dynamically based on network evolution. In the simulated experiment, the free-scale network is used to express network structure.

Analysis methods of the dynamic network are still at its beginning the work focuses on studying the properties of TCAN model from the angle of the network is a meaningful future work.

Acknowledgments. This work is supported by National Natural Science Foundation of China (Grant Nos. 61572115, 61502086 and 61402080), Chinese Postdoctoral Science Foundation (Grant Nos. 2014M562307).

References

1. Li, F., Lai, A., Ddl, D.: Evidence of advanced persistent threat: a case study of malware for political espionage. In: 2011 6th International Conference on Malicious and Unwanted Software (MALWARE), pp. 102–109. IEEE (2011)
2. Jeun, I., Lee, Y., Won, D.: A practical study on advanced persistent threats. In: Kim, T., Stoica, A., Fang, W., Vasilakos, T., Villalba, J.G., Arnett, K.P., Khan, M.H., Kang, B.-H. (eds.) Computer Applications for Security, Control and System Engineering. CCIS, vol. 339, pp. 144–152. Springer, Heidelberg (2012)
3. Ask, M., Bondarenko, P., Rekdal, J.E., Nordbø, A., Bloemerus, P., Piatkivskyi, D.: Advanced persistent threat (APT) beyond the hype, Project report in IMT4582 NetworN security at GjoviN University College. Springer (2013)

4. Cloppert, M.: Security intelligence: Introduction (pt 1), SANS Digital Forensics and Incident Response Blog (2009)
5. Furlani, C.: Managing information security risk: organization, mission, and information system view (2011)
6. Schneier, B.: Attack trees. Dr. Dobbs J. **24**(12), 21–29 (1999)
7. Jajodia, S., Noel, S., OBerry, B.: Topological analysis of network attack vulnerability. In: Kumar, V., Srivastava, J., Lazarevic, A. (eds.) Managing Cyber Threats, pp. 247–266. Springer, Heidelberg (2005)
8. McDermott, J.P.: Attack net penetration testing. In: Proceedings of the 2000 Workshop on New Security Paradigms, pp. 15–21. ACM (2001)
9. Liu, Q.H., Wang, W., Tang, M., Zhang, H.F.: Impacts of complex behavioral responses on asymmetric interacting spreading dynamics in multiplex networks. Sci. Rep. **6** (2016)
10. Giura, P., Wang, W.: A context-based detection framework for advanced persistent threats. In: 2012 International Conference on Cyber Security (CyberSecurity), pp. 69–74. IEEE (2012)
11. Zhao, W., Wang, P., Zhang, F.: Extended petri net-based advanced persistent threat analysis model. In: Wong, W.E., Zhu, T. (eds.) Computer Engineering and Networking, pp. 1297–1305. Springer, Heidelberg (2014)
12. Bhatt, P., Yano, E.T., Gustavsson, P.: Towards a framework to detect multi-stage advanced persistent threats attacks. In: 2014 IEEE 8th International Symposium on Service Oriented System Engineering (SOSE), pp. 390–395. IEEE (2014)
13. Ioannou, G., Louvieris, P., Clewley, N., Powell, G.: A Markov multi-phase transferable belief model: an application for predicting data exfiltration APTs. In: 2013 16th International Conference on Information Fusion (FUSION), pp. 842–849. IEEE (2013)
14. Fang, X., Zhai, L., Jia, Z., Bai, W.: A game model for predicting the attack path of APT. In: 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 491–495. IEEE (2014)
15. Hutchins, E.M., Cloppert, M.J., Amin, R.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead. Issues Inf. Warfare Secur. Res. **1**, 80 (2011)
16. Skyrms, B., Pemantle, R.: A dynamic model of social network formation. In: Gross, T., Sayama, H. (eds.) Adaptive Networks, pp. 231–251. Springer, Heidelberg (2009)
17. May, R.M., Lloyd, A.L.: Infection dynamics on scale-free networks. Phys. Rev. E **64**(6), 066112 (2001)
18. Kurtz, G.: Operation “aurora” hit google, others, vol. 80 (2010). http://siblog.mcafee.com/cto/operation-%E2