I.J. Wireless and Microwave Technologies, **2012, 2, 20-25**
Published Online April 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2012.02.04

Available online at http://www.mecs-press.net/ijwmt

A Multi-step Attack Recognition and Prediction Method Via Mining Attacks Conversion Frequencies

MAN Da-peng, LI Xue-zhen, YANG Wu, WANG Wei, XUAN Shi-chang

Information Security Research Center, Harbin Engineering University, Harbin, China, 150001

Abstract

Massive security alerts produced by safety equipments make it necessary to recognize and predict multi-step attacks. In this paper, a novel method of recognizing and predicting multi-step attacks is proposed. It calculates attack conversion frequencies, and then mines the multi-step attack sequences. On this basis, it matches the new alert sequences dynamically, recognizes the multi-step attacks and predicts the next attack step. The result of experiment shows that the proposed method is effective and accurate.

Index Terms: Network security*;* multi-step attack*;* alert correlation*;* attack conversion frequencies

1. Introduction

Nowadays the security equipments used in the network produce so massive security alerts that network administrators have large amount of workload, so many researchers are devoted to analyzing and correlate the security alerts to recognize multi-step attack scenarios.

Swiler [1] present an attack graph method to describe the attack activity and calculate the success probability of attacks. Templeton [2] uses precondition and results of attacks to correlate the alerts and mine multi-step attacks. Ning [3, 4] define a knowledge base including all attacks' possible precondition and results in his TLAA system and then match the alerts to generate attack correlation graph. This method can mine the causality relation of attacks, but its effect depends on the knowledge base, and needs huge amounts of resources while processing the massive attacks.

Wenke Lee and Qinxin Zhou [5, 6, 7] propose a method based on GCT and Bayesian model to correlate new attacks. In their method, they don't depend on the knowledge base of alerts. Wang Li [8] reference this method and propose a new sequential mining technique and attack scenarios construction method in their research. Our approach mainly draws lessons from the papers above.

The remainder of this paper is structured as follows. In section II, we analyze the historical security alerts, and calculates attacks conversion frequencies matrix. In section III, a multi-step attacks sequences mining algorithm

* Corresponding author.
E-mail address: mandapeng@hrbeu.edu.cn

is proposed according to the attacks conversion frequencies matrix above. In section IV, a multi-step attacks recognized and prediction algorithm is proposed. In section V, we use DARPA 2000 dataset to verify our approach. At last, we give the conclusion and discuss the future work in section VI.

2. Ease of Use Calculation of attacks conversion frequencies

Network attacks are always not single-step but complex and multi-step. A typical multi-step attacks sequence is shown in Figure1.

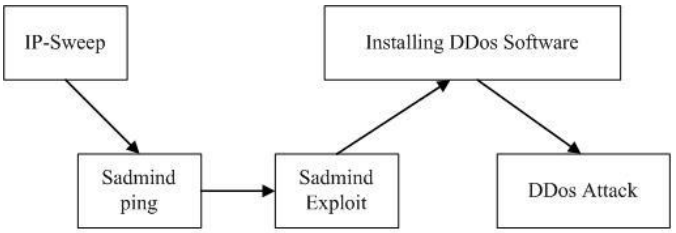

Figure 1. A DDOS attack aiming at Sadmind vulnerability

First, we define some terms.

Definition1. Attack Time Siding Window (ATSW). Attack time siding window T is a time value.

Definition2. Attack Conversion Frequency fa,b is the frequency that attack a is converted into attack b.

Definition3. Minimum Conversion Reliability MT is a value which is set according to expert experiences.

Now, we construct the attack sequence.

Range the alerts set Al produced by the security equipments by the time attribution to form the alert sequence S=s1,s2,⋯, sn, Set a attack type set A={a1,a2,⋯, an}, and define the translation function. f(si)=aj ↔ Alert si has the attack type aj, among which si ∈S, aj ∈A.

Then we will get attack sequence SA=sa1,sa2,⋯, san.

Traverse the whole attack sequence from sa1 to san, and construct subsequences SA1,SA2,⋯,SAk in time siding window.

We traverse all the subsequences SA1,SA2,⋯, SAk. The frequency number of attack a converted into attack b in the ith subsequence is labeled as na,b(i). Then the frequency number of attack a converted into b is calculate as follow.

$$n_{a,b}=\begin{cases}\sum_{i=1}^{k} n_{a,b}(i), & \text{if } a \neq b \\ 0, & \text{if } a=\text{b}\end{cases} \tag{1}$$

In some situation, the conversion frequency numbers of some attacks are low, so we set a conversion frequency number threshold value G. Then, we define Formula 2.

$$n_{i,j}=\begin{cases}n_{i,j}, & \text{if } \left|n_{i,j}\right| \geq \text{G} \\ 0, & \text{if } \left|n_{i,j}\right| < G\end{cases} \tag{2}$$

Then we get attacks conversion frequencies matrix as Formula 3.

$$\text{ARR2}=\begin{bmatrix} 0 & n_{1,2} & \cdots & n_{1,m} \\ n_{2,1} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & n_{m,2} & \cdots & 0 \end{bmatrix}_{m\times m} \tag{3}$$

In a multi-step sequence, attack a is either an end of this sequence or converted into other attacks. We define fa,b in Formula 4.

$$f_{a,b}=\begin{cases}0, & \text{if } \sum_{b=1}^{m} n_{a,b}=0\\ \dfrac{n_{a,b}}{\sum_{b=1}^{m} n_{a,b}}, & \text{if } \sum_{b=1}^{m} n_{a,b}\neq 0\end{cases} \tag{4}$$

Then, we get Attack Conversion Frequencies Matrix F as follow.

$$\mathbf{F}=\begin{bmatrix}\mathbf{O} & f_{1,2} & \cdots & f_{1,m}\\ f_{2,1} & \mathbf{O} & \cdots & f_{2,m}\\ \vdots & \vdots & \vdots & \vdots\\ f_{m,1} & f_{m,2} & \cdots & \mathbf{O}\end{bmatrix}_{m\times m} \tag{5}$$

3. Prepare Pattern mining of multi-step attack sequences

Definition4. Subsumption Sequence. If the sequence S1[1…m] and S2[1…n](m≤n)have the following relation: if there is some number j(j＜n) which makes S1[i]=S2[j+i-1] tenable for every i (1≤i≤m), then sequence S1 can be called the subsumption of S2, labelled as S1 ⊂ S2.

Input: an attack sequence SA=sa_1,sa_2, … sa_n and attack conversion frequencies matrix.

Output: n-1 multi-step attack sequences Sequence[n-1].

```
For i=1 to n-1
  Push sa_i into Sequence[i];
  For j = i+1 to n
    if sa_j exists in Sequence[i]
      then continue;
    else
     a =  GetTail(Sequence[i]);   /*Looking for the Tail
                                    of Sequence[i] */
     b = sa_j;
       If (abs(b.time-a.time)<=T && f_a,b !=0)
         Push s sa_j into Sequence[i];
       End if;
    End if;
  End for
End for
```

Figure2. Multi-step attack sequences mining algorithm

In view of the attack sequence SA = sa1, sa2,⋯ san, we propose our mining algorithm shown in Figure2.

The Sequence[n-1] may have subsumption sequences. We traverse Sequence[n-1], and if there is Sequence[i] ⊂Sequence[j], then delete Sequence[i]. Finally, put the residual Sequences into NewSequence[t].

Till then, we get t multi-step NewSequence[t].

4. Multi-step Attack Recognition and Prediction Algorithm

A network attack has many kinds of attribution, the important ones of which are types, source IP, source port, destination port, destination IP and attack time. With the diversification of network attacks, attackers may use the different source port and IP to finish the different steps of a multi-step attack. But the destination IP can't be forged. So we just consider the types, destination IP and attack time.

The multi-step attack recognition and prediction steps are as follows.

1) Receive the alert al of security equipments and translate al into attack a. Note the destination ip address DesIp, attack type Type and attack time Time of a. Then one attack can be signed as a triple <DesIP, Type, Time>.

2) Traverse the t multi-step attack sequences NewSequence [t]. If attack a exists in NewSequence[i], then mark it and the element in it; if attack a exists in several attack sequences, then mark all the sequences.

3) Continue to receive the alert, and translate in into attack b. Traverse the singed attack sequence. If the last signed element a of the attack sequence NewSequence[i] meet the condition of $|$ a.time- b.time $|$ ⩽T and fa,b, then mark attack b in NewSequence[i]. Afterwards, attack b traverses other sequences, and repeat step 2).

4) Suppose the last signed element of i attack sequence is a. If there isn't new attack added into this sequence in a. Time+T, this sequence won't happen and remove the sign.

5) When the t continuous attack steps of NewSequence[i] are marked and the destination of the t attacks is the same, these t steps are a part of a multi-step. If n multi-step attack sequences have t continuous attack steps, there may be n possible attacks in next step. If the next attack conversion frequency of the jth attack sequence is ft,t+1(j), then the frontal t steps will be converted into jth multi-step attack sequence in a probability ft,t+1(j)/∑ft,t+1(i) Specially, if the t steps are only signed in one sequence, then it is converted the next step in probability 1.

5. Experiment

We simulate the attacks in a LAN and store the alerts into Mysql database. Several attack scenarios are simulated, and then we calculate attacks conversion frequencies and mine multi-step attack sequences.

By comparing the results of the test, we set the minimum conversion reliability MT as 0.2. Then we calculate the main attacks conversion frequencies. Some attack conversion frequencies are shown in Table1.

TABLE I. ATTACKS CONVERSION FREQUENCIES

Conversion Attacks	Conversion Frequencies
IP_Sweep->Port_Scan	0.853
Port_Scan ->OverFlow_ Attempt	0.42
Port_Scan->Remove_NTLM	0.25
OverFlow_Attmpt- >Remote_Login	0.562
Remove_NTLM -> Remote_Login	0.622
Remote_Login -> Kill_firewall	0.32
Remote_Login -> DDos	0.27

We use the multi-step attack mining algorithm in section 3 to mine attack scenarios according the time attribution of alerts. The data of Table Ⅰ is corresponding to two multi-step attacks scenarios.

1) IP_Sweep -> Port_Scan -> Remove_NTLM -> Remote_Login -> Kill_Firewall
2) IP_Sweep -> Port_Scan -> OverFlow_Attempt -> Remote_Login -> DDOS

Multi-step attack sequence1) sweeps hosts, uses NT-Server weak password to start the Telnet service of remote hosts, removes NTLM checking, and logins remote hosts and kill Firewall process. Multi-step attack sequence2) sweeps hosts, uses the buffer overflow vulnerability to attack hosts, and then logins remote hosts to launch a DDOS attack.

Our experiments are based on the intrusion detection dataset DARPA2000 LLDOS1.0 [MIT Lincoln Lab 2000]. We use it to mine multi-step attacks and verify our mining and predicting algorithm.

1) At the time of 10:30:00am July 25, 2009, we receive an alert with the type ICMP_PING_SWEEP and destination IP 172.16.112.10, which is a IP_Sweep attack. According to the conversion frequencies in table 1 and the multi-step attacks sequences mined above, the occurrence probability of attack Port_Scan is 0.853.

2) At 10:46:25am, we receive a port scanning alert with the type SADMIND_PORT_SCAN and the same destination IP 172.16.112.10, which is a Port_Scan attack. Then we calculate the occurrence probability of attack Overflow_Attempt and Remove_NTLM.

$$f(\text{Overflow\_Attempt}) = \frac{f(\text{Port\_Scan},\text{Overflow\_Attempt})}{\sum_{\substack{a \text{ is the next attack} \\ \text{after Port\_Scan}}} f(\text{Port\_Scan},a)}$$

$$= \frac{0.42}{0.42+0.25} = 0.609$$

$$f(\text{Remove\_NTLM}) = \frac{f(\text{Port\_Scan},\text{Remove\_NTLM})}{\sum_{\substack{a \text{ is the next attack} \\ \text{after Port\_Scan}}} f(\text{Port\_Scan},a)}$$

$$= \frac{0.25}{0.42+0.25} = 0.391$$

3) At 11:11:22am, we receive an alert with the type of SADMIND_OVERFLOW_ATTEMPT and the same DesIP, which is a Overflow_Attempt attack. In the situation of the first three attack step fixed, we calculate that the occurrence probability of multi-step attack IP_Sweep -> Port_Scan -> OverFlow_Attempt -> Remote_Login -> DDOS is 1. So we can predict the next attacks are Remote_Login and DDOS, and the administrator should examine the network.

4) At 11:11:22am and 12:07:24am, we receive the alert RSH_LOGIN with the destination IP 172.168.112.10 and the alert DDOS with the destination IP 131.84.1.31, which are attack Remote_Login and attack DDOS. The results prove our prediction of step 3).

According the description of MIT Lincoln laboratory, the attacker logins the inside hosts 172.16.112.10、172.16.112.50 and 172.16.115.20 launch DDOS attack in LLDOS 1.0 scenarios. The attack steps are sweeping surviving hosts, scanning the ports, finding the Sadmind vulnerability in Solaris OS, carrying out buffer overflow attack, remote login the host, installing Trojan DDOS software and launching DDOS attack. This is consistent with our experimental results, which prove our approach is effective.

6. Conclusion and Future work

In our paper, we analyse the historical security alerts, calculate attack conversion frequencies, and then mine the multi-step attack sequences. On this basis, we match the new alert sequences to recognize the multi-step

attacks and predict the next attack step. The result of experiment shows the proposed method in this paper is effective and accurate.

We verify our approach in DARPA 2000 Dataset LLDOS 1.0, which is not a real situation. We will do more experiments in a real environment in the future.

Acknowledgment

The project supported by New Century Excellent Talents in University of China (NCET-08-0633) and the Basic Research Foundation of Harbin Engineering University of China（HEUFT09011）.

References

[1] Swiler, L.P.; Phillips, C.; Ellis, D.; Chakerian, S., "Computer-attack graph generation tool," DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings , vol.2, no., pp.307-321 vol.2, 2001

[2] Templeton S，Levitt K. "A requires/provides model for computer attacks.," In Proceedings of the New Security Paradigm Workshop, September 18, 2000 - September 22, 2000, Anonymous Association for Computing Machinery, Ballycotton, Ireland, pp:31-38,2000

[3] P Ning, D Reeves，and Yun Cui. Correlating alerts using prerequisites of intrusions. Technical Report TR-2001-13，North Carolina State University，Department of Computer Science，USA ,:pp:23-39, 2001

[4] P.Ning，Yun Cui. An intrusion alert correlator based on prerequisites of intrusions.Technical Report TR-2002-01，North Carolina State University，Department of Computer Science，USA ,pp:31-43, 2002

[5] W.Lee and X.Qin.Statistical Causality Analysis of INFOSEC Alert Data.G.Vigna,E.Jonsson andC.Kruegel, Editors.RAID. Springer. Berlin, Heidelberg,:pp:73-93, 2003

[6] Q.Xinzhou and L.Wenke. Discovering novel attack strategies from INFOSEC alerts.Sophia Antipolis, France,ESORICS,pp:439-456,2004

[7] QIN,X and LEE,W.Causal discovery-based alert correlation.In:the 21th Annual Computer Security Applications Conference(ACSAC 2005).Tucson,AZ.,December,pp:33-40, 2005

[8] W., LI ZHI-TANG, JIE, L. AND YAO, L. “A novel algorithm SF for mining attack scenarios model.” In IEEE International Conference on e-Business Engineering, 24-26 Oct. 2006, Anonymous IEEE Computer Society, Los Alamitos, CA, USA.