ETA: A method of Dynamic Network Device Security Assessment

CHEN Mu1,*, DAI Zaojian1, SHAO Zhipeng1 and WANG Liming2

1 State Grid Key Laboratory of Information & Network Security, Global Energy Interconnection Research Institute, Nanjing China
2 Institute of Information Engineering, CAS, Beijing, China

*Corresponding author email: chenmu@geiri.sgcc.com.cn

Abstract. The normal operation of network devices is an important cornerstone of network security. The security evaluation of network device is very important to prevent network security problem. In order to dynamically evaluate the security level of network device and quantify the state, a method of dynamic network device security assessment is proposed. Firstly, this method makes full use of the alert log which includes state information of network device and combines with the idea of TF-IDF algorithm to analyze the frequency and the distribution of alert. Then, it puts forward a new algorithm ETA to calculate the value of event threat. Finally, these values are used for calculating the security index of network device. The experiment shows that the proposed method in this paper can find the network device in low-level security and provide effective decision support for network security administrator.

1. Introduction

With the rapid development of information technology, more and more activities of people rely on the Internet. At the same time, the number of cyber attacks is rising, such as Data leakage, privacy theft, security vulnerability, malicious code, mail bomb, virus infection. It is reported that 86% of companies in the world have experienced at least one cyber attack in 2017[1].

In network environment, network security evaluation is an important means to prevent cyber attacks. As the infrastructure of network, the evaluation results of network device have important reference value for network security evaluation. The significance of security assessment is mainly reflected in the following aspects: 1) understand current security risks faced by network device. It actively analyzes and evaluates the security risks existing in the device itself; 2) predict the possibility that network device may be attacked; 3) analyze security assessment results of network device and timely take measures for low-security device to prevent the spread of attacks. Traditional network device security assessment is mainly based on vulnerability and asset information, ignoring the dynamic information of device, which is unable to accurately evaluate the security state of device in the actual runtime process.

In this paper, a dynamic network device security evaluation method is proposed, which combines the TF-IDF algorithm and alert log to effectively quantify the security state of network device in runtime. By focusing on the security state of low-security device, Network security administrator can timely find out the hidden danger of network device and carry out targeted measures to ensure the smooth operation of network.
2. Previous work
In recent years, domestic and foreign scholars have done a lot of research work to deal with the increasingly network device security problems. Wei et al. [2] propose network security situational awareness model based on information fusion, which integrates external attack information, vulnerability information of host nodes and threat information of attack itself to evaluate the security state of host nodes. However, there is no unified evaluation standard for the construction of evaluation function and the selection of parameters, which needs to be evaluated with the knowledge and experience of experts in this field. Xing et al. [3] propose research on security detection and assessment technology of power information network nodes. Based on traditional node security assessment technology, this scheme abstracts assets, vulnerabilities, threats and overall risks of power information network to build a security assessment model of power information network nodes, but it does not take into account the security state of network nodes when they are running and the model is not general. Chao et al. [4,5] propose the network equipment information security evaluation method based on D-S evidence theory and principal component analysis. However, this method only analyzes the security of network device from the perspective of data storage and forwarding and lacks a comprehensive consideration of the security threat of network device. Zhang et al. [6] propose a risk assessment method for network equipment based on fuzzy 3D risk matrix. But the method is qualitative assessment with high, low and moderate levels. In addition, knowledge-based reasoning is still one of the hotspots of current research, but this evaluation method is limited by the formulation of reasoning rules and the acquisition of prior probabilities. Some scholars [7,8,9,10,11] have propose a method to evaluate the security of the whole network, but they ignore the safety of the equipment. Some scholars [12,13,14,15,16] propose to carry out network device safety assessment based on machine learning technology. Representative work includes: neural network, support vector machine, hidden markov model and gray relational degree. Although those methods based on machine learning have the characteristics of objectivity in the security evaluation, they need to collect more training data to learn parameters.

Dynamic security assessment method breaks through the limitation that traditional static security assessment method can't continuously assess the security of network device. Contributions are mainly reflected in: 1) The alert data is used to dynamically evaluate the security level of network nodes and quantify the security state of devices in runtime.2) The calculation of network device security index takes into account the historical state and current state of network device comprehensively.

3. A Dynamic Network Device Security Evaluation Method

3.1 Dynamic security assessment framework of network device
In order to ensure the normal operation of the network, enterprises have deployed a large number of security device in the network. When the attack occurs, the security device will record the alert information related to the network device. That is to say, These alert data reflect the running state information of network device. The dynamic network device security evaluation method proposed in this paper mainly includes three parts: 1) preprocessing module. Different types of alert data are collected for uniform format, invalid alert deletion and false alert deletion to improve data quality.2) threat assessment of alert event. This module evaluates the threat value of alert event in network device.3) calculation module of security index. The dynamic security assessment framework of network device is shown in figure 1.
3.2 Preprocessing
A large number of heterogeneous alert logs are often generated in the daily network environment, but these alert data cannot be directly used for the calculation of network device security index. Firstly, different security devices define different alert log formats, which makes data processing difficult. Secondly, due to the inherent defects of existing security products or network transmission delay, there are redundant and non-standard data in the alert log. Therefore, it is necessary to preprocess the collected alert log to improve data quality.

3.2.1 Format standardization. Alert data refers to log information detected by intrusion detection system, vulnerability scanning system and other security devices. Data is expressed as six-tuple \(<\text{time}, \text{type}, \text{device}_\text{id}, \text{alert}_\text{id}, \text{priority}, \text{content}>\). \text{time} represents the time when the alert is generated; \text{type} represents the alert log type; \text{device}_\text{id} represents a unique identifier for the network device. \text{priority} represents the priority of warning information; \text{content} represents the alert content.

3.2.2 Invalid alert deletion. There are two types of invalid alerts. One is redundant data. Multiple records with the same properties are generated by the same network device within a specific time range. The other is non-standard data, such as incomplete fields, parameter errors. This article deletes invalid alert by setting filtering rules.

Definition 1: repeated alert. For two alerts \(\text{alert}_1\) and \(\text{alert}_2\) generated by the same network device at time \(t_1\) and \(t_2\), if \(|t_2-t_1|<\Delta t\) and \(\text{alert}_1=\text{alert}_2\), it represents those alert are repeated alert. \(\Delta t\) is the time threshold which represented by the mean value of the known duration of attack. Referring to snort data set adopted in experiment, reference [17] gives the time threshold \(\Delta t=50s\).

3.2.3 False alert deletion. Normal network activities will also cause a large number of trivial alerts and easily drown out the alerts generated by real attacks, which will interfere with the security assessment of network device. In the actual network, it is found that: 1) frequent alerts have periodic characteristics; 2) most devices have the same alert subsequence. Based on the above two points, false alert deletion includes periodic alert deletion and frequent alert sequence deletion.
(1) periodic alert deletion
According to the preprocessing data flow obtained, the proportion \(V\) of each alert type and \(U\) of each network device is determined. Set threshold \(\alpha\) and \(\beta\). If \(V>\alpha\) and \(U>\beta\), we record alert type and corresponding device, which is expressed as two-tuple \(<\text{alert}_\text{id}, \text{device}_\text{id}>\). For each tuple, the number of alerts generated per hour by network device \(i\) is used to construct the time series \(\{x(t), t \in \mathcal{N}\}\), \(x(t)\) represents the number of alerts generated per hour. In order to achieve the purpose of deleting periodic alert, reference [18] proposed to use correlation

![Figure 1. Dynamic security assessment framework of network device](image)
analysis, Fourier transform and F distribution model to calculate period. Firstly, Time series \( \{x(t), t \in N\} \) is processed into autocorrelation sequences \( \{R(\Delta t), 0 \leq \Delta t < N\} \) through correlation analysis. \( R(\Delta t) \) represents the relationship measure of interval \( R(\Delta t) \) hours. Secondly, The autocorrelation sequence \( \{R(\Delta t), 0 \leq \Delta t < N\} \) computes the period \( T_0 \) by discrete Fourier transform. Finally, If there is a period \( T_0 \), F distribution model is constructed for the time series \( \{x(t), t \in N\} \) to verify the reasonableness of the period \( T_0 \).

(2) frequent alert sequence deletion
Firstly, the number of alerts generated by network devices within one hour is sorted in ascending order and the shortest alerts sequence \( \{s_i, 1 < k < C\} \) generated by the first \( C \) normally running network devices is selected as the alternative sequence. Secondly, Find the union set \( \{s_{1,j}, 1 \leq z \leq n_o\} \) of all subsequences of alert sequence \( \{s_i, 1 < k < C\} \). \( n_o \) represents the number of subsequences. Finally, the \( p_z \) calculated by formula (1) determine whether the subsequence \( s_{1,z} \) is added to the rule library.

\[
p_z = \frac{\sum_{j=1}^{n-1} f_{device_id}(s_{z_j})}{N} \quad 1 \leq z \leq n_o
\]

\( f_{device_id}(s_{z_j}) \) indicates whether the sequence \( s_{z_j} \) is a subsequence of the alert sequence generated by the network device \( i \). If so, \( p_z = 1 \); otherwise, \( p_z = 0 \). \( N \) represents the number of network devices in a network. \( p_z \) represents the ratio of the number of network devices with subsequence \( s_{z_j} \) to the total number of network devices. When \( p_z \) is greater than the threshold, the subsequence \( s_{z_j} \) is added to the rule library. Figure 2 shows the flow chart of false alert deletion.

3.3 Threat assessment of alert event
Different types of alert events cause different degrees of damage to network device. This paper put forward ETA (Event Threat Assessment) algorithm which draws on the idea of TF-IDF algorithm [19], considering alert frequency and distribution to evaluate the dangers of different alert events on the network device.

First, calculate the frequency of alert events. The alert data in \( T \) time are clustered according to the network device. The frequency of different alert types in network device \( i \) is expressed by \( <device_id, alert_id, alert_count> \) \( (1 \leq i \leq n, 1 \leq j \leq m) \). \( device_id \) represents the network device \( i \), \( alert_id \) represents class \( j \) alert. \( alert_count \) represents the number of class \( j \) alert in the network device \( i \). \( n \) represents the number of devices, \( m \) represents the number of alert
Second, calculate the distribution of alert events. The alert data are clustered according to the alert types in the period of \( T \). The distribution of class \( j \) alert is represented by \( alert_id \), \( total \), \( device_count \), \((1 \leq j \leq m) \). \( total \) represents the number of class \( j \) alerts in the network, \( device_count \) represents the number of devices generating the class \( j \) alert.

\[
\text{alert_count}_j = \sum_{\text{device_id}} \text{sum(alert_id)}_j
\]  

In the period of \( T \), the formula for calculating the threat value of class \( j \) alert in network device \( i \):

\[
ET_i^T(j) = (\frac{\text{alert_count}_j}{\text{total}_j+1}) \times \lg(\frac{N}{\text{device_count}_i}+1) 
\]  

3.4 Security index of network device

The security index of network device can be obtained based on the threat index of different alert events. The security index \( DT_i^T \) of network device \( i \) at time \( t \) is composed of two parts. One is the security index of network device \( i \) in the period of \( T \), the other is that the security index of network device \( i \) at time \( t-T \). If network device \( i \) was attacked before \( t-T \) and network security administrator did not take effective measures to deal with it, those attacks will continue to affect the computation of security index in next cycle.

The influence value of the security index at time \( t-T \):

\[
E_i^{t-T} = g_i^{t-T}(x) = \begin{cases} DT_i^{t-T} & \text{if } x = 0 \\
100 & \text{if } x = 1 \end{cases}
\]  

\( x \) represents whether the threats in network devices have been effectively dealt with within the period of \( T \). \( x=0 \) means that no measures have been taken to deal with the threat. \( x=1 \) means that the threat has been lifted.

The security index of network device \( i \) in the period of \( T \):

\[
F_i^T = \exp\left(-\sum_{j=1}^{m} p(j) \times ET_i^T(j)\right) \times 100 
\]  

The security index of network device \( i \) at time \( t \):

\[
DT_i^T = \left(1 - \frac{E_i^{t-T}}{100}\right)E_i^{t-T} + \frac{E_i^{t-T}}{100} \times F_i^T 
\]  

\( p(j) \) that Can be set according to the priority of alert represents the weight of class \( j \) alert.

4 Experiment and analysis

4.1 Experimental environment and data

The algorithm program in this experiment is written in Java language and uses Eclipse development platform. The experimental environment was a desktop computer with Windows 7 x64 operating system, Inter (R) Core i7 processor and 8G memory.

In order to verify the effectiveness of the scheme, open source snort data set of maccdc2012 [20] is used. This data set contains 2125,795 records generated by 2,092 network devices from 8:00 to 16:00 on March 16, 2012, involving 23 alert types. Snort log contain alert time, alert type, priority, protocol, source IP address and port, destination IP address and port. According to priority, alert types are divided into three categories. Class I, the highest threat level, Attack types include web application attack, administrator access alert, user access alert, Trojan detection alert, information disclosure alert, executable code detection and enterprise privacy disclosure. Class II, medium threat level. Attack types include default user name and
password login, denial of service attack, suspicious file detection, access to vulnerable WEB applications, RPC query decoding etc. Class III, low threat level. Attack types include unknown activities, network scanning alert, detection of suspicious strings, general protocol command decoding, trying to obtain user permissions etc.

For the remaining 356,596 records after preprocessing, select \( T = 1h \), the security index of each device in different periods was calculated. On this basis, we analyzed the security index distribution of all devices, The relationship between security index and frequency, the change trend of security state of network device.

4.2 Analysis of experimental results

(1) network device security index distribution

Figure 3 shows the security index distribution of 2092 devices at 16:00. The horizontal axis represents the interval where the network device security index is located. The vertical axis represents the number of devices.

As shown in figure 3, 98% of network devices are in the range of security index [80,100] and state is in high-level security.1.8% of network devices are in the range of security index[20,80] and state is in medium-level security.0.3% of network devices are in the range of security index [0,20] and state is in low-level security. After analysis, two of the five devices in low security belong to the web application server, and three devices belong to the personal host. This result shows that most devices in the network are in a safe state, while the core server or a few devices with weak security protection are in a low security state, which is consistent with the situation in most actual networks.

![Figure 3. Network device security index distribution](image)

![Figure 4. The relationship between security index and alert frequency](image)

Table 1. Part of the device alert statistics

| IP           | security index | number of alert types | alert frequency | content of specific alert                              |
|--------------|----------------|-----------------------|-----------------|--------------------------------------------------------|
| 192.168.27.253 | 0.22           | 15                    | 6022 I(3133)II(345)III(22) | Trojan detection(118) User permissions were obtained successfully(29) Information disclosure(12) |
| 192.168.202.68 | 0.59           | 4                     | 26 I(8)III(18)  | User permissions were obtained successfully(6) Disclosure of trial information(2) Web application attack(2) |
| 192.168.28.152 | 28.53          | 13                    | 87 I(31)II(34)III(22) | Web application attack(12) Attempt to obtain administrator privileges(12) Accessing fragile WEB applications(7) Disclosure of trial information(4) Attempt to obtain user permissions(2) Suspicious string detected(2) Executable code detection(2) Trojan detection(2) |
| 192.168.206.44 | 55.53          | 4                     | 981 I(967)III(14)  | Disclosure of trial information(747) Possible traffic attacks(220) Unknown activities(12) Network scan(2) |

(2) the relationship between security index and alert frequency

Figure 4 shows the relationship between the number of alerts generated by network devices within 8
hours and the security index at 16:00. The horizontal axis represents the number of alerts generated by each device within 8 hours, and the vertical axis represents the security index of network device.

As shown in figure 4, the alert frequency of the 5 devices with the lowest security index varies greatly, the device with the highest number of alert does not have the lowest security index. That is to say, high-risk devices may generate a small number of alerts. Table 1 lists the alert statistics of four devices in low-level and medium-level security, including IP, security index, number of alert types, alert frequency (number of I, II and III) and content of specific alert. the number in brackets in the fifth column indicates the specific alert frequency. We come to the following three conclusions: 1) 192.168.27.253 and 192.168.202.68 has been successfully obtained user permissions by intruders, so those devices have the lowest security index. 2) 192.168.28.152 involves 13 alert types, which indicates attackers attempt multiple types of attacks against the network device. For the purpose of controlling the device, the attacker attempts to send executable malicious code or Trojan virus to the device. 3) 192.168.206.44 has a large number of attempted attack alerts, but there is no trace of successful intrusion by the attacker. therefore, security index of 192.168.206.44 is significantly higher than other.

(3) the change trend of security state of network device

As shown in figure 5, the security index of 192.168.24.254 continued to exceed 80%. After analysis, 192.168.24.254 was not attacked at all. the security index of 192.168.202.68 at 12:00 dropped significantly and continued at 16:00. After analysis,192.168.202.68 was attacked at 12:00 by successfully obtaining user permissions and network security administrator did not take effective measures to deal with it.

5. Conclusion

Network device security assessment is the basis of discovering network threats. The dynamic network device security evaluation method proposed in this paper makes full use of the network device state information contained in alert data to effectively quantize the security level of network device in runtime and timely identify network device in low-level security. However, the scheme proposed in this paper is unable to evaluate the damage to network device caused by unknown threats without warning. The next step is to analyze the abnormal behaviors of network devices and evaluate their ability to cope with unknown threats.

Acknowledgments
This work was supported by the State Grid of China, the key technology research of power mobile terminal security threat analysis and monitoring (No. SGRIXTKJ[2017]265).
References

[1] Tencent 2017 annual Internet security report, http://tech.china.com/article/20180131/20180131104056.html

[2] Yong W, Yifeng L, Dengguo F. Network security situational awareness model based on information fusion [J]. Journal of Computer Research and Development, 2009, 46(3):353-362.

[3] Jingyu X. Research on security detection and assessment technology of power information network nodes [D]. Beijing University of Posts and Telecommunications, 2015

[4] Yuan C, Lu Y, Gan J. Evaluating network equipment information security based on D-S evidence theory and principal components analysis [C] // IEEE Second International Conference on Data Science in Cyberspace. IEEE, 2017:554-560.

[5] Zihao L, Bin Z, Ning Z. Hierarchical network threat situation assessment method for DDoS based on D-S evidence theory [C] // IEEE International Conference on Intelligence and Security Informatics. 2017:49-53

[6] Zhang D, Han J, Song J, et al. A risk assessment approach based on fuzzy 3D risk matrix for network device[C] // IEEE International Conference on Computer and Communications. IEEE, 2017:1106-1110.

[7] Zanyu T, Hong L. Study on evaluation method of network security situation under multi-stage large-scale network attack [J]. Science and Technology, 2018, 45(1):245-248.

[8] Wang W H. Research on network security situation assessment model[J]. Journal of Qingdao Ocean Shipping Mariners College, 2017.

[9] Chang C, Yan R, Management S O, et al. Research on safety risk evaluation and management measures of prefabricated construction [J]. Journal of Shenyang Jianzhu University, 2017.

[10] Shuwen Z, Xiaowu L, Xueyan S. Hierarchical awareness of network security situation based on multi-source fusion [J]. Computer Technology, 2016, 26(10):77-82.

[11] Yixian L, Dejun M. Research on network security assessment method based on weight of node [J]. Information Technology, 2018(2):19-21.

[12] Siqin W, Biao W. Computer network security evaluation simulation model based on neural network [J]. Model Electronics Technique, 2017, 40(3):89-91.

[13] Yang L, Bai Y, Tong F, et al. Safety evaluation of China's power equipment manufacturing industry based on fuzzy neural network model[J]. Power System & Clean Energy, 2015.

[14] Xia J B, Bai J. Network running quality evaluation method based on relevant vector machine[J]. Electronic Design Engineering, 2016.

[15] Xiao W, Qianmu L, Yong Q. Real time analysis method of network security risk based on markov model [J]. Computer Science, 2016, 43(s2):338-341.

[16] Jiang Y, Chenghai L. Computer network security assessment based on grey hierarchy model [J]. Measurement and Control Technology, 2017, 36(10):109-113.

[17] Qian H, Junyong L, Meijuan Y et al. Method of duplicate removal on alert logs based on attributes hashing [J]. Computer Science, 2016, 43(s1).

[18] Dong L, Zhitang L, Jie L. Research on the method of reducing false positives with periodicity [J]. Journal of Chinese Computer Systems, 2009, 30(7):1336-1340.

[19] Zhanghao S. Improvement and application of TF-IDF method in Chinese text classification [J]. Science and Technology, 2014(22).

[20] SecRepo.com - Samples of Security Related Data, http://www.secrepo