Anomaly Analysis Technology Based on Deterministic Characteristics of Intranet

Zhiwen Chen[1], Guihua Wang[1], Weiyan Zhang[1,a], Dali Zhou[1]

[1]Institute of Computer Application, China Academy of Engineering Physics, Mianyang, China.

Abstract. An enterprise intranet has the characteristics of service determination, limited network components, descriptive and observable characteristics, and the state of network components and network interaction behaviors need to strictly comply with security policies. Therefore, a variety of descriptive certainty can be used to describe the subject, object, and action of the network access. According to this important feature, the anomaly analysis method is simplified, and the abnormal discovery of the intranet is transformed into the problem of network dynamic feature collection and deterministic feature characterization. Based on the network state and behavior collection and analysis network dynamic characteristics, combined with the deterministic feature priori knowledge of the network, an anomaly analysis model which is especially suitable for deterministic intranet is proposed. Based on the model design, a traffic-based anomaly analysis system is implemented. The system can effectively find a variety of high-risk anomalies in the intranet.

1 Introduction

There are a lot of strict enterprise intranets, the boundary protection and architecture of these networks are clear, the network and security infrastructure are clear, and the behaviors allowed by the equipment and users are also determined. We call this kind of network with multi deterministic characteristics as a deterministic network.

In an ideal case, when all components and users of the deterministic network strictly comply with the security policy, the interaction between the network components will also show a variety of deterministic features, because the interactions allowed between the network components are determined. Although the permissible interaction between deterministic network components are deterministic, the existing technology cannot completely limit the impermissible behavior. Therefore, it is an important requirement for the intranet information security management to effectively discover these non permissible behaviors. The reason why the impermissible behavior can occur is either that there is no corresponding safety control measure, or that the corresponding safety control measures are invalid or there are vulnerabilities, so the anomaly analysis technique [1] is always as important as the safety control technology.

The conventional anomaly analysis technology is generally oriented to the universal Internet [2-3]. When many research results are applied to enterprise intranets, if we can make full use of the priori knowledge of a variety of deterministic characteristics of the intranet, it can be more effective to solve the common problems such as false positives and false negatives. Based on the characteristics of deterministic networks, this paper simplifies the related anomaly analysis methods, an abnormity analysis model for enterprise intranets is proposed.

2 The anomaly analysis model

2.1 Anomaly analysis model based on network deterministic characteristics

Due to the deterministic characteristics of the intranet, normal behavior of the normal network components should satisfy the corresponding deterministic characteristics. Conversely, abnormal components or abnormal behavior will destroy the deterministic characteristics of the system. Therefore, the abnormal analysis of deterministic networks can be transformed into the monitoring of deterministic characteristics, which is anomaly once the state or behavior does not satisfy the deterministic features that should be present. This is the main idea of the anomaly analysis model based on the deterministic characteristics of the network.

The proposed anomaly analysis model is shown in Figure 1. The first step of anomaly analysis is to analyze the relationship between components and components of the network, extract the deterministic features that satisfy the security policy, and then convert these features into constraints. By collecting the network state and user behavior, the anomaly can be found based on the constraint condition judgment.

The model divides the network components into three categories: terminal(PC), network and application. By analyzing the extracted deterministic features, the

[a] Corresponding author: 5749369@qq.com

knowledge of constraints of state and behavior can be established. This knowledge portrays the constraints that the normal state and behavior of terminal, network, and application should satisfy. The analysis of deterministic features can be carried out from a business perspective and a security policy perspective.

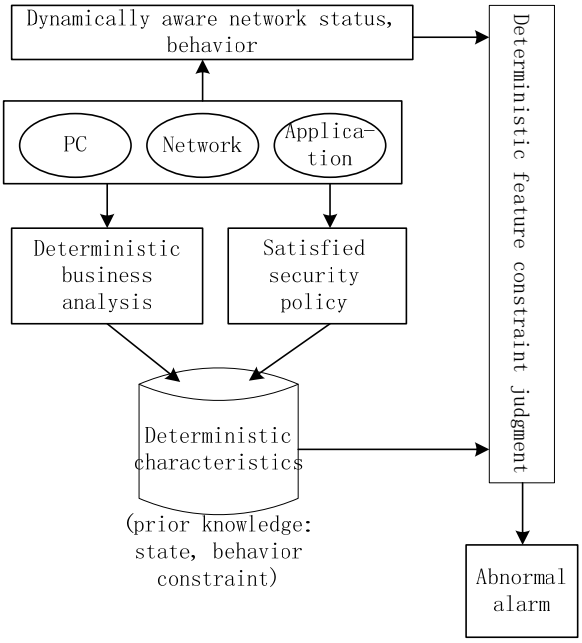

Figure 1. Anomaly analysis model.

2.2 Deterministic analysis of business

Information such as what kind of service is carried by the deterministic network, the business rules that the service meets, the objects of the service, the services mode of the service, and the specific location of the business deployment are all determined by deterministic networks. The constraints of terminal, network and application can be extracted by professional analysis. For example, the constraint formed by the relevant deterministic feature of the service A can be represented by a set of rules, each rule being represented by multiple attribute constraints, and a rule R can be expressed as:

R(service A)={ user(A1), terminal(A2), software(A3), protocol(A4), net path(A5), business rule(A6)}

A rule describes that the attributes of the different dimensions of the service A should satisfy the constraints:

(a) The service A can be accessed by the user or user role A1 only.

(b) User access the service A should use the A2 terminal.

(c) Access to service A should use software with A3 features.

(d) Access to service A should use the A4 protocol through the A5 network path.

(e) Business access should adopt the A6 business rules.

Based on the established constraints, the abnormality detection can be detected from multiple dimensions. The constraints those do not satisfy any one of the dimensions can be regarded as abnormal. Therefore, when anomaly detection based on the business deterministic features is implemented, different anomaly detection points can be selected according to the difficulty of collecting the deterministic feature detection information.

2.3 Deterministic analysis of security policy

The typical feature of an enterprise intranet is that it has strict and explicit security policies. By analyzing the security policies related to the system configuration and user behaviour, the deterministic features that the policy should have can be obtained. Because different types of security policies involve different objects or behaviours, the dimensions of deterministic features are different, but they can still be represented as a set of attribute constraint rules for terminals, networks, and applications, and a rule R can be expressed as:

R (policy P) = {terminal(P1), network(P2), application(P3)}

Rule R (policy P) indicates the constraints that the terminal, network, and application that satisfy the policy P should satisfy. The deterministic feature analysis from the perspective of security policy can be analyzed according to the specific policy, and any dimension of constraint condition is not satisfied can be regarded as an exception.

For example, a security policy of an intranet requires that the network terminal should be installed with the X host monitoring and auditing system. From the perspective of terminal, network, and application, the deterministic feature {terminal(P1), network(P2), application(P3)} that satisfies the policy can be extracted:

(a) The terminal should be installed the X host monitoring and auditing system client software.

(b) In the fixed time, the active terminal should generate communication traffic with the server of the X system.

(c) The communication ports and protocols used by the X system installed by the server are determined.

(d) Communication between client and server meets some basic features, such as heartbeat communication every ten minutes.

These are the deterministic features that satisfy the security policy P in this example. Once the terminal violates the policy, the anomaly can be detected by monitoring these features. For example, when the network traffic is monitoring directly, once the activity time period exceeds the threshold, but the communication between the terminal and the X system server does not meet the characteristics, such as the characteristic of (c) or (d). In the case of determining that the X system is normal, the terminal may be abnormal, or the X system client is not installed, or the X system client does not work normally, and any situation in these cases is abnormal.

3 The application of the anomaly analysis model

Applying the anomaly analysis model based on network deterministic features, ideally, a deterministic network model should be constructed for deterministic network components, deterministic services, deterministic security strategies and other deterministic information for the target network, and a complete description of all deterministic characteristics that the network should be satisfied is fully described. In this way, a knowledge base of constraint knowledge for all permissible behaviors of the target network is established. Then comprehensively collect the corresponding state and behavior of the terminal, network, and application, and detect based on the established constraint knowledge base, can discover various abnormal behaviors that violate the constraint conditions. However, with the existing technology, the realization of this ideal anomaly detection scheme will face many difficulties and the cost is too high. Therefore, in practical applications, partial constraints can be selected for anomaly detection according to the security goals pursued by the user.

In order to monitor the legitimacy of an enterprise intranet terminal and the effectiveness of firewall ACL, we propose an anomaly analysis method based on network flow, and implement the corresponding prototype system by using the idea of the anomaly analysis model based on network deterministic characteristics.

3.1 The anomaly analysis method based on network flow

We analyze a company's intranet from the perspective of business and security policies, and extract the deterministic features that legitimate terminals should have on network traffic:

(1) All IP of the network communication is determined.

(2) The IP pair formed by both sides of the communication is determined, that is, t which servers the terminal can communicate with are determined.

(3) The firewall ACL settings are known and determined, and the traffic must satisfy the ACL.

(4) The terminal adopts domain control management, and maintains TCP communication with the domain control server and generate traffic.

(5) The terminal requires the specified host monitoring and auditing software and anti-virus software to be installed. The analysis shows that the normal terminal maintains a TCP connection with the specific port of the host monitoring and auditing server and the anti-virus server, and the interval between the two communications does not exceed 10 minutes.

(6) Normal terminals will not produce traffic with other application servers before they communicate with the domain control server, the host monitoring and auditing server, and the antivirus server.

In this example, based on these deterministic characteristics of normal terminal network communication, a traffic-based anomaly terminal detection method is designed as shown in Figure 2.

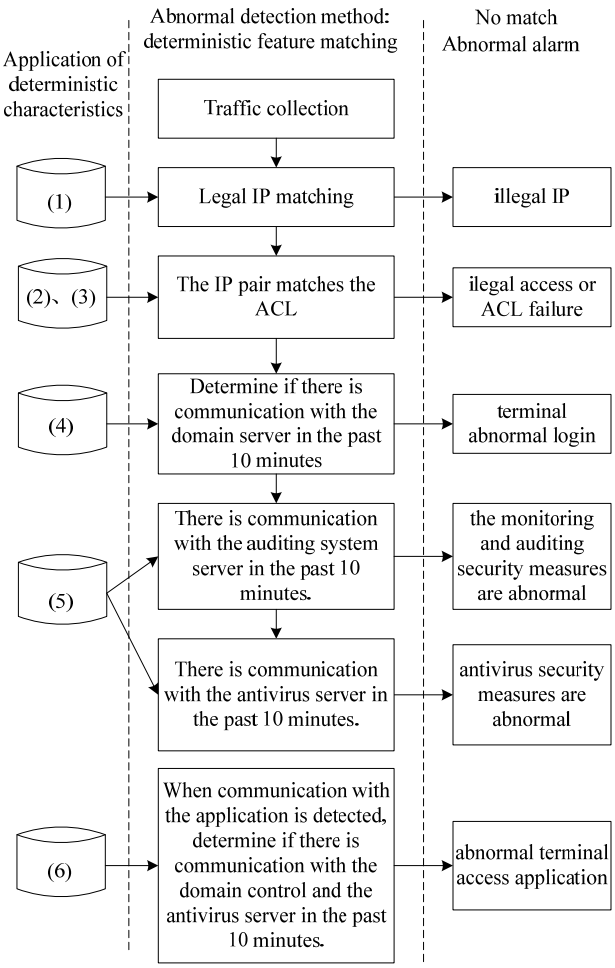

Figure 2. Traffic-based anomaly terminal detection

3.2 The prototype system

Based on the modification of the open source Suricata [4] network intrusion detection system, we have implemented the prototype system which implement the traffic-based anomaly terminal detection method. Through the simulation of the actual environment, the traffic based anomaly analysis method based on the network deterministic feature can effectively detect a variety of anomalies, especially forging fake IP/MAC illegal access network terminals, once they access network will violate (4) (5) (6) three deterministic characteristics and triggers alarm.

4 Conclusion

Different from the conventional anomaly analysis technology, we analyze the service and security strategy of the target network before the anomaly detection, and extract the deterministic characteristics that the network should have. Based on the deterministic features, the related anomaly analysis can be effectively simplified.

At present, our analysis and extraction of deterministic features mainly depends on the analysis of professionals. In the future, we will explore the feasibility of using machine learning combined with principal component analysis [5] to assist or automatically discover

deterministic features. In the application of the model, we will gradually build the deterministic features database of terminals, networks, and applications, and realize more types of anomaly detection by sensing the dynamic characteristics of terminals, networks, and applications.

Acknowledgments

This work is supported by Defense Industrial Technology Development Program JCKY2016212C005.

References

1. Pavel Nevlud, Miroslav Bures, Lukas Kapicak. Anomaly - based Network Intrusion Detection Methods. Information and communication technologies and services,11 (2013), pp.468-474.
2. Anderson HiroshiHamamoto, Luiz Fernando Carvalho, Lucas Dias HieraSampaio. Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic. Expert Systems with Applications, 92(2018), pp.390-402.
3. Bereziński P, Pawelec J, Małowidzki M, Piotrowski R. Entropy-Based Internet Traffic Anomaly Detection: A Case Study. Intelligent Systems and Computing, 286(2014). Springer, Cham.
4. Eugene Albin, Neil C. Rowe. A Realistic Experimental Comparison of the Suricata and Snort Intrusion-Detection Systems. 2012 26th International Conference on Advanced Information Networking and Applications Workshops,2012, pp.122-127.
5. Dingde Jiang, Cheng Yao, Zhengzheng Xu, Wenda Qin. Multi-scale anomaly detection for high-speed network traffic. Transactions on Emerging Telecommunications Technologies, 26(2015), pp. 308-317.