Simulation Modelling Practice and Theory 74 (2017) 28–45

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

A trusted access method in software-defined network

Jing Liu[a], Yingxu Lai[a,*], Zipeng Diao[a], Yinong Chen[b]

[a] Beijing University of Technology, Beijing, China 100124
[b] School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, AZ 85287, USA

ARTICLE INFO

Article history:
Received 25 November 2016
Revised 26 January 2017
Accepted 5 February 2017

Keywords:
Software-defined network
Network access
Trusted computing

ABSTRACT

In software-defined networks (SDN), most controllers do not have an established control function for endpoint users and access terminals to access network, which may lead to many attacks. In order to address the problem of security check on access terminals, a secure trusted access method in SDN is designed and implemented in this paper. The method includes an access architecture design and a security access authentication protocol. The access architecture combines the characteristics of the trusted access technology and SDN architecture, and enhances the access security of SDN. The security access authentication protocol specifies the specific structure and implementation of data exchange in the access process. The architecture and protocol implemented in this paper can complete the credibility judgment of the access device and user's identification. Furthermore, it provides different trusted users with different network access permissions. Experiments show that the proposed access method is more secure than the access method that is based on IP address, MAC address and user identity authentication only, thus can effectively guarantee the access security of SDN.

1. Introduction

Software-Defined Networks (SDN) is originated from Stanford University's Ethane project, which was named OpenFlow in 2006 by Professor Nick Mckeown. With the continuous development to mature, OpenFlow is officially named as SDN in Global Environment for Network Innovations (GENI) project. SDN architecture decouples the control plane and data plane [1] in order to implement the centralized control and management of the entire network. These basic features of SDN architecture increase the flexibility of network deployment and enhance the programmability of the network. Therefore, SDN architecture can meet the needs of a fast and efficient network.

The development of computing and communication industry increasingly requires network flexibility and programmability provided by SDN. However, security is becoming a key factor restricting the development of SDN. For example, most current SDN controllers do not have established user access control functions. This means there can be a problem of identity authentication when a user and a device access the network. The defect can lead to forgery attacks of identity for the purpose of illegally obtaining information, gaining control over the entire network to cause network congestion and even paralysis. In order to solve the problem of security checkup for access terminals, we proposed a method for trusted access in this paper for access authentication. We designed and implemented a trusted access method of the software-defined network, which may acted as the first shield of network access.

* Corresponding author.
E-mail addresses: jingliu@bjut.edu.cn (J. Liu), laiyingxu@bjut.edu.cn (Y. Lai), diaozipeng@emails.bjut.edu.cn (Z. Diao).

http://dx.doi.org/10.1016/j.simpat.2017.02.001
1569-190X/

The rest of the paper is organized as follows: Section 2 reviews security access technologies and Trusted Network Connect related studies in the traditional network, as well as the access security related studies in SDN. The architecture of SDN trusted access is presented in Section 3. The detailed description and Security analysis of the authentication protocol are elaborated in Section 4. Section 5 describes the implementation of trusted access method of SDN. Section 6 presents the experiments that show the credibility and effectiveness of the proposed architecture. Finally, conclusion and outlook of this paper are drawn in Section 7.

2. Related work

Security access of terminals mainly focuses on network users' authentication, which accurately identifies users and the characteristic parameters of the network they used, and verifies the legitimacy of the device and user identity. It restricts or grants the access permission of network by the network host and user's identity, which achieves the goal of access security.

In the traditional network, researchers are constantly introducing new technologies and methods to solve the problem of terminal security access. The concepts such as active defense and trusted access have been proposed accordingly. Currently, the common access authentication technologies include Point-to-Point Protocol over Ethernet (PPPoE), 802.1x, Mac Address Bypass, web authentication technology, etc. [2]. The typical application of PPPoE lies in Asymmetric Digital Subscriber Line (ADSL) access, which is widely used by Internet Service Provider (ISP) for network access of individual customers due to its maturity as a technology. However, this authentication method is not suitable for multi-access networks, such as LAN access authentication [3]. 802.1x protocol is based on the access control and authentication protocol of client/server mode that can restrict unauthorized users and devices to access network through the access port. The protocol implements the separation of authentication and services and ensures the efficiency of network transmission. However, 802.1x itself does not have the related setting for maintaining connection. Consequently, it is necessary to determine the user's status by periodically sending authentication requests. This approach increases the burden on authentication system. In the data center network (flexible SDN network), frequent network changing or moving accessed devices will increase the cost, lower the user's experience, and delay the service. Web authentication is usually combined with DHCP server, which allows user to be authenticated via web pages. So there are no constraints of across layers and multicast protocols. Since the authentication is based on the highest layer of network, Web authentication is convenient with high degree of freedom. However, it also makes it difficult to detect users' abnormal situations caused by the underlying network.

Trusted Network Connect (TNC) theories were proposed in 2003. The main idea is based on the fact that trusted computing technology [4] can complete the integrity measurement of user's platform when the user accesses network. By judging whether conforming to the security policies, it can verify the credibility of the platform. The achievement of these authentications requires binding of the Trusted Platform Module (TPM) [5]. To some extent, TNC is an extension of the network environment from TPM launched by Trusted Computing Group (TCG). Compared with traditional network access technology, TNC increases the credible verification of the platform, which is a proactive network security protection technology. TNC is an open and common architecture that can work with existing network technologies and devices, such as combining 802.1x and PPP to achieve the function of access control. In the past decade, many scholars have carried out thorough studies and discussions of various aspects about the application of TNC in the traditional network. Based on Extensible Authentication Protocol and 802.1x access control architecture, Lin [6] proposed an improved trusted network access solution with fine-grained trusted certification for each accessed terminal to achieve quantitative assessment of the state of credible and access control. Luo et al. [7] proposed a method of security quantitative analysis and security enhancement mechanism. The method was based on semi-Markov process, aiming to TNC protocol. Using Intel IXP2400 network processor, it built a TNC prototype system. Yan et al. [8] proposed a security authentication protocol based on TNC structure and the idea of terminal integrity measurement of TNC. There are studies that combined terminal integrity measurement technology and Public Key Infrastructure (PKI) to ensure the credibility of the terminal platform. Liu [9] with intention of implementation issues about trusted access for WiMAX presented wireless credible access protocol based on EAP-TTLS. Many companies have product supporting TNC architecture, such as Symantec, Juniper Network, Still Secure, Wave Systems, and Extreme Networks. In the traditional network, to ensure the terminal security access via TNC technology has achieved substantial research results, inflicting a significant impact on solutions to network security.

In recent years, as the most promising emerging technology, studies on security mechanisms of SDN have become one of the important research directions. Many researchers have begun to explore the access security issues of SDN. FortNOX [10] architecture, designed by Porras et al., is a security kernel aimed for open source controller NOX with the increase of role-based authentication module. It is used to sign each flow rules and specify the appropriate privileged category to candidate flow rules. The literature proposed the FortNOX prototype system, which is an effective extension for increasing the security performance of the NOX controller. However, NOX was implemented in C language, which brings many difficulties in the development. As a consequence, it has been replaced by a more mature architecture controller. Sasaki et al. [11] combined the user authentication registry and user roles and proposed the role-based access control (RBAC) in the OpenFlow network, which has some positive effects on globally monitoring the entire internal network. However, on the definition of the users, the article in coarse-grained manner is not able to define multi-dimensional access control function. Mattos and Duarte [12] proposed AuthFlow, an authentication and access control mechanism based on host certification. It offered AAA authentication services in conjunction with the controller. It intercepted RAP messages between the host and the RADIUS authentication server, and reported authentication status to OpenFlow controller. The controller could allow or deny the traf-