Simulation Modelling Practice and Theory 51 (2015) 157–169

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

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

Design and analysis on trusted network equipment access authentication protocol

Yingxu Lai [a,*], Yinong Chen [b], Qichen Zou [a], Zenghui Liu [c], Zhen Yang [a]

[a] College of Computer Science, Beijing University of Technology, Beijing 100124, China
[b] School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe 85287, USA
[c] Automation Engineering Institute, Beijing Polytechnic, Beijing 100176, China

ARTICLE INFO

Article history:
Received 19 August 2014
Received in revised form 9 October 2014
Accepted 26 October 2014
Available online 7 January 2015

Keywords:
Trusted network equipment
Authentication
Security protocol
BAN logic
Attack detection model

ABSTRACT

Cloud security is a system engineering problem. A common approach to address the problem is to adapt existing Trusted Network Connection (TNC) framework in the cloud environment, which can be used to assess and verify end clients' system state. However, TNC cannot be applied to network equipment attached to the cloud computing environment directly. To allow the network devices to access the trusted network devices safely and reliably, we first developed a Trusted Network Equipment Access Authentication Protocol (TNEAAP). We use the BAN logic system to prove that TNEAAP is secure and credible. We then configure the protocol in an attack detection mode to experimentally show that the protocol can withstand attacks in the real network. Experiment results show that all the nine goals that decide the protocol's security have been achieved.

1. Introduction

Cloud computing environment is emerging as a key platform supporting data-intensive processing and big data analysis in information technology. The advantages of convenience, economy, and high extensibility draw the attention of more and more researchers and practitioners. However, cloud computing is just like a double-edged sword, it brings us great convenience, and at the same time, it also carries additional problems, such as performance, reliability, trustworthiness, and security [1,2]. With the popularity of cloud computing, the significance of security issues is gradually increasing, and it has become an important factor to restrict cloud applications. The solution of cloud security is complex. A common approach is to adapt existing Trusted Network Connection (TNC) [3] solutions to the cloud computing paradigm. The basic objective of TNC from the perspective of endpoint integrity is to deny those network accesses to endpoints that do not meet certain minimum security criteria [4–6]. In the network access control research, many related studies have been conducted in the field of improving network connection protocol and improving TNC architecture.

1.1. Trusted network connection protocol

Luo et al. [7] followed the TNC framework to design an improved network access control system, T-NAC, which emphasized the platform authentication and communication security. A network access control system based on the network

* Corresponding author. Tel.: +86 13439195095; fax: +86 01067391742.
E-mail address: laiyingxu@bjut.edu.cn (Y. Lai).

http://dx.doi.org/10.1016/j.simpat.2014.10.011
1569-190X/

processor platform IXP2400 was designed. Latze et al. [8] proposed a strong bidirectional authentication protocol, which was based on TPM (Trusted Platform Module) and EAP-TLS authentication method. Latze et al. [9] later proposed a new authentication protocol: EAP-TPM. The first EAP-TPM system was built in Switzerland. Then Latze et al. [10] improved EAP-TPM protocol based on zero-authentication. However, these protocols did not address the problem of Man-in-the-middle attacks. Wang et al. [11] analyzed the D–H (Diffie–Hellman) keys exchange protocol, and proposed a digital signature and signature verification end-to-end protocol to solve the problem of Man-in-the-middle attacks. Yu et al. [12] studied the platform anonymous identity management defects of TNC and proposed a new method to improve these impairments. The new trusted certification generation method was based on ID (Identity) encryption mechanism and improved DAA (Direct Anonymous Attestation) protocol. The protocol was more flexible and security to manage identity on terminal platforms.

1.2. Trusted access model

To make the trusted network access mechanism more practicable, researchers proposed different solutions that focused on TNC architecture. Jungbauer and Pohlmann [13] proposed a method to determine the integrity of endpoints which served as a basis for trustworthy communication. The model did not require specific hardware such as TPM (Trusted Platform Module) or special operating system structure. It also supported exiting network infrastructures. Rehbock and Hunt [14] proposed a protocol stack that enabled the use of TNC in web-based environments and changed the TNC architecture to ensure additional security. The potential use of the TPM functionality within the TNC framework and experiences were given by Bente [15] and Heldenin [16], respectively. They further defined a conceptual model for client-side policies that was based upon TNC's IF-M (Interface-Measurement) protocol and showed that many policies can be enforced by extending the standard TNC framework [17]. Tang et al. [18] proposed a trusted network model based on the TPM, through which a trusted chain from terminals to network was established. Zhang [19] designed a TNC security model based on UCF (Universally Composable Framework) that can be extended to describe more security properties, such as anonymity. The model can be applied to analyze more protocols in the TNC architecture.

Cloud security is a system engineering problem. It requires additional security features not only for the endpoint security techniques, but also for the switches and routers, which are the core network equipment of Ethernet. In general, the existing TNC framework can be used to assess and verify end clients' system state, but cannot be applied to network equipment directly. There are certain differences between network equipment and the endpoints to join in a network. Network equipment undertakes forwarding packets within routing or switching function in the network. They are service providers, whereas, endpoints use network only, and they are service clients. If accessed network equipments failure, it will affect the part of the cloud network, whereas, a failure endpoint only affects itself. Thus, network equipment pays more attention on trusted boot up process and trusted network services than terminals do. Trusted boot up process ensures network equipments static trust, trusted network service ensures its dynamic trust.

On the other hand, existing authentication protocols of network equipment have various weaknesses and are difficult to be applied in the trusted network. For example, PAP (Password Authentication Protocol) is often used in router access authentication. However, PAP is not a strong and effective method of authentication. The password is transported in plain text. CHAP (Challenge Handshake Authentication Protocol) [20] is another router authentication protocol. The protocol is more secure than PAP. In CHAP, (1) the remote access server sends a challenge to the remote client that consists of a session ID and an arbitrary challenge string. (2) The remote client must return the user name and a Message Digest 4 (MD4) hash of the challenge string, the session ID, and the MD4-hashed password. (3) The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection SHOULD be terminated. (4) At random intervals, the authenticator sends a new challenge to the peer, and repeats steps 1–3. However, CHAP [21] also has its weaknesses: (1) In the authentication server, the user's password was stored in plain text, which provided opportunities for intruders to obtain a user's password. (2) The protocol supports one-way authentication only. (3) The user password in CHAP is shared between two communication parties, and thus keys distribution and updating can cause inconsistency problems. (4) If a user used a simple password, the protocol could not prevent the dictionary attack. (5) In order to prevent the insertion channel attacks, the authentication server must reprint certification periodically. If the cycle time interval is too long, it can give the intruder opportunities.

This paper presents a network device access authentication protocol. In our protocol, in addition to equipment's platform authentication, the administrator also should be authenticated. The identification authentication process is actually the binding administrator to the trusted platform, to ensure the administrator is legal on trusted platform. Our protocol is to avoid malicious behavior from illegal administrator login trusted platform or legitimate user login illegal platform. The authentication protocol achieves these targets: safety, credibility, and low overhead. The security of the protocol is analyzed by a formalization method based on BAN (Burrows–Abadi–Needham) logic, which can reveals vulnerabilities and redundancy [22]. The protocol processes are formalized with HLPSL (High-Level Protocol Specification Language) [23]. The formalization of the protocol processes is tested by plugging into an attacking model of the safety testing tool to check whether the protocol is secure or not.

In the rest of the paper, Section 2 shows the design of the authentication method for the trusted network devices to join in the network. Section 3 formalizes our protocol by BAN logic for safety analysis. Section 4 presents the experiment, which uses the attack model to attack the protocol and to demonstrate that protocol is secure. Section 5 gives the network equipment performance evaluation. We conclude the paper in Section 6.