ISBN 978-981-11-0008-6
Proceedings of 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016)
Tokyo, Japan, 17-19 June, 2016, pp. 792-795
doi: 10.18178/wcse.2016.06.142

Application Research on Trust Verification of Cloud Service Resources based on Trust Negotiation Mechanism

Mu-Dan Gu[1] and Hui-Kui Zhou[1]
Nanchang Institute of Science & Technology, Nanchang City, Jiangxi Province, China

Abstract: In the cloud environment, the service resources are widely distributed and migrate frequently, and the trust relationship between resources is not easy to establish and maintain. Through the research of cloud service resource trust verification method, a remote authentication method based on attribute negotiation is proposed, which solves the problems of traditional trusted computing remote verification method, such as performance bottleneck and calculation complexity. The risk of sensitive information leakage and the efficiency of computation are reduced by using the ring signature algorithm and the attribute based sensitive information protection mechanism.

Keywords: Data security, trusted computing, remote attestation, automated trust negotiation

1. Introduction

With the rapid development of Internet technology, the distributed application based on network has been in many fields, such as business affairs, government affairs, scientific activities and so on. But in the cloud computing environment, service resources have the characteristics of flexible combination and frequent migration. How to establish a trust relationship between service providers and suppliers in an open and independent network environment three, and to effectively support the information resources sharing and collaborative computing with domain security. In order to effectively manage these resources, security domain is usually used to control the access and security level of resources. Due to the wide distribution of cloud services resources, centralized security management is more difficult. The relationship between the security of non-trusted resources and the trust relationship in the domain of foreign countries is not easy to establish and maintain. Remote attestation in protecting the privacy of the problem by the many concerns, how to effectively implement the remote attestation at the same time, protecting compute platform for privacy information not only in theory also in the practical application has very important significance[1,2].

2. Trusted computing method

Computing Trusted is a set of information security standard, the standard system proposed by Trusted Computing Group (TCG)[3]. The initial state of the traditional security architecture is secure, which is secure against the trusted computing, and the rule of conversion is also secure. A trusted computing platform is required to have unique identity on the network, rather than changing or dynamically allocating the IP

Corresponding author. Tel. 15270809589
E-mail address: *583517476@qq.com*

address as a label as a traditional computer. Trusted computing, including 5 key technology concepts, they are necessary for the integrity of the system, the system will comply with TCG specification.

Remote authentication allows users to change the perception of the authorized party on the computer. The purpose is to prove that the identity of the remote platform or configuration information is credible. [6]There are some differences in the signature methods of the two remote attestation methods provided by TCG. CA Privacy method requires the authentication center to participate in the authentication process each time and the authentication side, such a mechanism is very easy to cause the performance bottleneck of the authentication process. In order to solve the problem of CA Privacy authentication method, the DAA method is based on zero knowledge proof and C-L signature, and no need for third party to participate in the platform to complete the trust verification. [8]

3. Trusted cloud platform trust verification method

Trusted cloud platform is the extension of trusted computing in open environment, and it is suitable to describe the cloud computing based on hierarchical service. The trust verification is a relatively independent process in the cloud environment. It is difficult to verify the legitimacy of the identity of each other through the centralized Trust Center. In order to adapt the characteristics of cloud service resource remote verification, and improve the efficiency of trust building, we introduce the method of ring signature to sign the interactive message. Platform B send information to the platform A, ensure that the information sent does not contain harmful code, the way to prove their identity to the other side of the way called push proof.

The establishment of the ring signature only needs to input the information of the ring member public key, the signature message and the security parameters for generating the key. In the trusted cloud computing platform, the remote attestation method based on ring signature consists of 3 stages, which are initialization security parameter, signature generation and signature verification. [7]

Parameter initialization stage: set up the platform B, A is to carry out the remote automatic negotiation proof of the two sides. External attribute certificate attribute corresponds to a variety of configuration platform $C_1, C_2, \cdots, C_t$, TPM based on RSA algorithm $p_A, q_A, n_A = p_A q_A$, e_A and $(p_A - 1)(q_A - 1)$ distinct large prime numbers, e_A and $(p_A - 1)(q_A - 1)$, $e_A d_A = 1 \bmod (p_A - 1)(q_A - 1)$, (e_A, n_A) and (d_A, n_A), $H(), H_1()$ for the two collision resistant hash functions.

Signature: TPMA randomly selected a private information to extract stored in the corresponding PCR configuration information for the abstract value of Cr (1 < R < T), combined with TPM host computing attribute value hidden $y_A = (g_A{}^{x_A} - H(P, C_1, C_2, ..., C_t))^{d_A} \bmod n_A$, TPMA to sign the information for the $m = (n_A, g_A, e_A, y_A)$.

A signed ring is composed of a TPM, and the corresponding public key $P_1, P_2, \cdots, P_t$, TPMA host computing hash value $k = H(m, P_1, P_2, \cdots, P_t)$, Random selection of initial value and random number sequence $x_1, \cdots x_{s-1}, x_{s+1}, \cdots, x_t$, Calculated $y_i = f(x_i), i \neq s$.

TPM select ring equation as shown in formula

$$C_{k,v}(y_1, y_2, \cdots y_t) = E_k(y_t \oplus E_k(y_{t-1} \oplus E_k(..... \oplus E_k(y_1 \oplus v).....))) = v \qquad (1)$$

Among them, $E_k()$ for the symmetric encryption algorithm (can be used in the TPM specification of the recommended candidate symmetric encryption algorithm [5] AES), $k = H(m, P_1, P_2, \cdots, P_t)$ Key for symmetric encryption algorithm, $\oplus$ is Specific or arithmetic. Calculated according to the ring equation

$$y_s = E_k(y_{s-1} \oplus E_k(y_{s-2} \oplus E_k(\cdots \oplus \cdots E_k(y_1 \oplus v)\cdots)) \oplus D_k(y_{s+1} \oplus D_k(y_{s+2} \oplus D_k(\cdots \oplus D_k(y_t \oplus D_k(v))\cdots)))$$

$D_k()$ is the corresponding symmetric decryption algorithm, and then use the private key to calculate $x_s = g(y_s)$. At this point, TPMA combined with its host to complete the signature, $m = (n_A, g_A, e_A, y_A)$ send messages and $\text{TPMSign}(n_A, g_A, e_A, y_A)$ signatures to the platform B.

Cross validation stage: push proof, platform B after receiving the attribute certificate issued by the platform a sends the message and TPM, first verify that signature is legitimate, if appropriate rules to discard messages received, otherwise randomly selected private information, calculate $k_1 = H_1((y_A^{e_A} + H(P, C_1, C_2, ..., C_t))^{x_B})$ and send $g_A^{x_B}$ to A platform. TPM A and host cooperative computing and return $k_2 = H_1((g_A^{x_B})^{x_A})$ to each other, through the verification platform of B to determine whether the person has property P.

Remote attestation allows a user or other person to detect changes in the user's computer. This can avoid sending private messages or important commands to a computer that is not safe or compromised. Remote attestation by hardware to generate a certificate stating what software is running. The user can take this certificate to a remote party to show that his computer has not been tampered with.

4. Research on trusted platform module

The trusted attribute is used to describe the security requirements to meet the platform, the verification process is to verify the platform or configuration information is able to meet the need of security attributes of the. This verification can shield configuration information platform of software and hardware, for the dynamic information updating platform can flexibly change. For some trusted attribute sensitive and should be protected and hidden, to prevent the unnecessary attribute information leaked to the other. Trusted computing platform needs to provide at least the following basic functions: data security platform, identity, integrity measurement, storage and reporting. TCG defines the logical structure of the trusted platform module (TPM), it is a kind of SOC (system on chip) , complete storage to measure the trustworthiness, trusted measurement report, supervise and control the system, key generation, digital signature and encryption, data security storage function. By using the password mechanism, the integrity of the system platform component is measured, stored and reported to ensure the integrity of the platform.

5. Efficiency analysis

In the trust verification program, the main use of the calculation has Exponential computing, Hash computing and Encryption Symmetrical computing. We use E on behalf of the index operation, H on behalf of the hash operation, SC represents the symmetric encryption operation. The efficiency of the algorithm is analyzed (Table-1). The size of T is related to the size of the ring which is selected by TPMA. So it is high efficiency in the choice of the appropriate size of the ring.

Table-1 Efficiency Analysis

Stage Name		computing method	E	H	SC
Signature stage		A	T+2	2	T
Interactive verification	Push proof	B	4	2	
		A	2	1	
	Pull proof	B	3	2	1
		A	1	1	1

It can be seen that the calculation efficiency, cross validation and the protection of sensitive information are the key concerns in the process of remote attestation through the research on the current results of remote attestation in trusted computing. The remote verification method based on attribute negotiation solves the problem of traditional trusted computing remote verification method, such as performance bottleneck and calculation complexity. The ring signature algorithm and based on the sensitive information protection properties, reduce the risk of leaking sensitive information and improve the calculation efficiency.

6. Reference

[1] Hongwei Chen,Shuping Wang,Hui Xu,Zhiwei Ye,Chunzhi Wang. Automated Trust Negotiation Model based on Dynamic Game of Incomplete Information[J]. Journal of Software,2013,810.

[2] Ding Yong, Lv Haifeng, Yu Xiaolong, Gui Feng, Xin-guo remote attestation scheme based on intelligent terminals [J] password Sinica, 2015,02: 101-112.

[3] Feng Wei Ning, Zhang Zhiyong, Zhao Changwei. For multimedia digital copyright protection commission authorized remote attestation protocol [J]. Computer Science, 2015.

[4] Zhang Xiaowei, Wang Zheng, Chen Yongle prove a long-range program user properties [J]. Taiyuan University of Technology, 2015(02).

[5] Huang Xiuwen. Based on remote attestation of trusted computing [J]. Wuhan Textile University, 2015(06).

[6] Wooyoung Kim Martin Diko Keith Rawson .Network Motif Detection： Algorithms, Parallel and Cloud Computing,and Related Tools,Tsinghua Science and Technology.2013(5): 469-489.

[7] Hailun Tan,Wen Hu,Sanjay Jha. A remote attestation protocol with Trusted Platform Modules (TPMs) in wireless sensor networks. [J]. Security Comm. Networks,2015.

[8] Yulei Wang,Jie Yang,Weining Feng. A Delegation Authorization Security Protocol Based on Remote Attestation for Multimedia Usage Control[J]. Recent Advances in Electrical & Electronic Engineering,2015.

[9] Shelly Salim, Sangman Moh. On-demand routing protocols for cognitive radio ad hoc networks[J]. EURASIP Journal on Wireless Communications and Networking, 2013.