Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (9): 1592-1596, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.1592.1596

Threshold Remote Attestation on Trusted Cloud Computing

[1]Yong Zhao, [1]Fei Xue and [2]Yanxue Zhang
[1]College of Computer Science, Beijing University of Technology, Beijing 100124, China
[2]College of Mathematics and Information Science, Hebei Normal University,
Shijiazhuang, 050000, China

Abstract: Remote attestation is the key technology of trusted cloud computing. The existed remote attestation schemes are not sufficient to consider the trusted measurement of the running virtual computing node. In this study, by the analysis and comparison of existing remote attestation schemes, we propose a trusted measurement of the running virtual computing node and a threshold remote attestation scheme based on the trusted measurement results. By RO security analysis and a simulation, we verify the security and efficiency of the scheme. The trusted measurement of the running platform is mainly based on the trusted measurement of the programs running on the platform and a total trust value of the platform by an algorithm. The Threshold remote attestation for trusted measurement of the running platform is based on K-CCA problem.

Key words: Trusted cloud computing, threshold remote attestation, dynamic measurement, K-CCA problem

INTRODUCTION

As the information technology develops, cloud computing becomes the most attractive word after personal computer and Internet (Dahbur *et al*., 2011). IaaS (Infrastructure as Service) lies in the base of the architecture of cloud computing which is the basics of higher lays such PaaS (platform as service) and SaaS (software as service). So the security of IaaS determines the security of the whole service of cloud computing (Brassil, 2010; Greveler *et al*., 2011.). In this study, we focus on the core technologies of remote attestation in the environment of IaaS. Remote attestation in the environment of IaaS is a application of trusted computing in computing. Here we give some introductions of remote attestation.

Remote attestation is one of the core technology of trusted computing and many achievements have been made in remote attestation. a typical research is the binary remote authentication proof which is supported by TCG and has become the basis of remote attestation (Wang *et al*., 2008; Schellekens *et al*., 2008). In the binary remote attestation the trust of the platform is determined by measuring the integrity of the platform. As long as the executable binary code has not been changed, the platform is trusted. However, this scheme exposes the platform configuration information and cannot guarantee the anonymity of the platform.

The authors in (Pirker *et al*., 2009; Chen *et al*., 2006; Li and He, 2009; Dong, 2012) proposed property-based remote attestation. The scheme don't need verify the platform configuration, but verify the property certificate of the platform. So that the integrity of the platform configuration is converted to the property certificate of the platform. However, to verify the platform security property level, the certificate generation center must have a unified industry standard which is difficult in implementation. Although this approach can avoid the exposure of the platform configuration, the certificate generation center is difficult to find a standard map between security property level and binary configuration. Automated Trust Negotiation (ATN) has been studied by (Holt *et al*., 2003; Bradshaw *et al*., 2004; Winsborough and Li, 2002). Automated Trust Negotiation technology, as a kind of property certificate, simulates the proof of study documents by property certificates, Each of which contains one or more properties of the certificate owner. However, the scheme has an important drawback that the transfer of the certificate cannot be prevented and the legitimate owner of the certificate can transfer the certificate to any others the providers are unknown about. The study (Hu *et al*., 2009) pointed out a new frame of remote attestation. In the framework, trust is built between the user terminal and the virtual machine applications. The service side can develop flexible, granular policies and help trusted virtual machines distributing and executing these strategies. However, the framework set strategy as a starting point and is lack of specific acts of quantitative indicators.

From the above-mentioned analysis, we can realized that there is a key shortcoming of the current remote attestation schemes that is, lack of study on the trusted

Corresponding Author: Yong Zhao, College of Computer Science, Beijing University of Technology, Beijing, 100124, China

group. Current research focuses on attestation of a certain virtual machine in cloud computing, it is neglected to consider the virtual machine as a group. The current schemes cannot forbid the remote attestation of malicious nodes.

In this study, Based on the existing schemes of the remote attestation on cloud computing, we design a dynamic measurement methods based on the state of the virtual computing node and complete the remote attestation by threshold strategy. This scheme can prevent the remote attestation of malicious nodes effectively.

DESIGN OF THE SCHEME

In our scheme of remote attestation, the basic framework of remote attestation in literature (Santos *et al*., 2009) is adopted. the procedures of remote attestation based state and threshold strategy. is described intuitively in Fig. 1.

Parameter setup: G_a, G_b are defined as multiplicative group whose order is p and P is the generator of G_a. Bilinear map is $c(G_a, G_a) \rightarrow G_b$ where c(P, P) = I. H: {0, 1}* $\rightarrow$ G is a cryptographic security function. So the public parameter is (G_a, G_b, P, c(P, P) = I, H). S = {S_1, S_2,... S_n} is defined as a set of n trusted entities where ID_i is defined as public information of signer S_i.

Private Key Generator (PKG) chooses $s \in Z^*_p$, $Sk \in G_a$ and issues Pk = sP, Sk as public parameters. PKG choose a random polynomial:

$$f(x) = s + a_1 x ..... + a_i x^{t-1} \bmod p \quad (1)$$

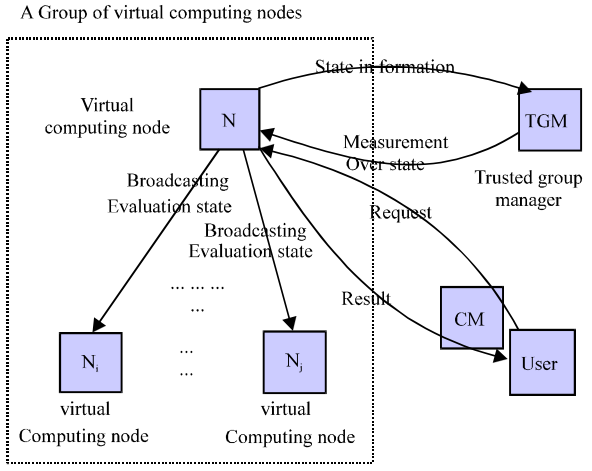

Fig. 1: The process for threshold remote attestation

where, s_i.....$a_t \in Z^*_p$. PKG broadcasts $g_i = a_i Sk$ $(0 \le i \le t-1)$ as public parameters.

PKG calculates and broadcasts the public key $pk_i = f(ID_i)P$ i = 1,....., t. Then, for the member S_i, i = 1,.....t, the following equation can be verified:

$$\sum_{i=1}^{t} L_i P = Pk \quad (2)$$

Where:

$$L_i = \prod_{j=1, j\neq i}^{t} \frac{ID_i}{ID_j - ID_i}, i = 1, ..., t \quad (3)$$

are Lagrange coefficients.

PKG calculates the secret key:

$$Sk_i = f(ID_i)Sk \quad i = 1, ..., t \quad (4)$$

Then, for S_i, i = 1,....., t, the following equation can be verified:

$$Sk_i = \sum_{j=0}^{t-1} ID_i^j g_j \quad (5)$$

PKG encrypts sk_i by the endorsement key of TPM s_i and send it to the number s_i.

Dynamic measurement: The dynamic measurement of the virtual computing node is achieved by a trusted third party Trusted Group Manager (TGM) which measures the snapshot of the virtual computing node. Trusted computer TGM evaluates the trust of the virtual computing node with five levels that is very trusted, trusted, critically trusted, untrusted and very untrusted. The trust of the virtual computing node is mapped to the corresponding evaluation level. Therefore, any time the virtual computing node evaluation includes a snapshot of the five possibilities. In this study, we complete the user's immediate state metric by Chang *et al.* (2005) and the specific method is listed as follows.

Define the evaluation function of the state of the virtual computing node as follows.

Let x be the platform and ET(x) be the evaluation function of the state of the user that ET: x$\rightarrow$[0, 1]. The PT has five possibilities:

- Very untrusted $0 \le ET(x) < E_0$
- Untrusted $E_0 \le ET(x) < E_1$
- Critically trusted $E_1 \le ET(x) < E_2$
- Trusted $E_2 \le ET(x) < E_3$
- Very trusted $ET(x) \ge E_2$

where, E_0, E_1, E_2, E_3 satisfy $0<E_0<E_1<E_2<E_3<1$.

We assume the current programs of the virtual computing node are $AP = \{ap_1, ap_2.....ap_l\}$. Let $E\pi = \{E_{k1}, E_{k2}, E_{kl}\}$ be the smallest trust value of the program $AP = \{ap_1, ap_2.....ap_l\}$. In this study, the key method is to define a suitable ET. A idea is that the measurement should be independent on the important programs. So let $\{ap_1, ap_2.....ap_k\}$ be important programs and $\{ap_{k+1}, ...ap_l\}$ be secondary programs, TGM calculates PT as follows. TGM chooses three positive constants σ_1, σ_2, λ and defines G(x, y) as follows:

$$G(x,y)=\begin{cases}\lambda > x, |x-y| \le \sigma_1\\ x, |x-y| > \sigma_2\end{cases} \quad (6)$$

TGM calculates:

$$E_1 = \min_{1\le i\le k}\{E_i\}, E_2 = \min_{k+1\le i\le l}\{E_i\} \quad (7)$$

$$E = \frac{\min_{1\le i\le k}\{E_i\} + \lambda \min_{k<i\le l}\{E_i\}}{1+\lambda} \quad (8)$$

$$ET = G(E(x), \overline{E}) \quad (9)$$

where, $\lambda>0$ is a weighting factor. Then TGM decides whether the current state of the virtual computing node is trusted. The TPM of the virtual computing node carries out the remote attestation with ET.

Remote attestation for dynamic measurement: Let B be the virtual computing node. B sends the information:

$$PT = (AP, E\pi) = \{ap_1, ap_2.....ap_l, E_{k1}, E_{k2}.....E_{kl}\} \quad (10)$$

involved by TGM to carry out the dynamic measurement of B. Let the signature key of the TPM B be (x, xp). x is stored by TPM B and xP is sent to TGM:

- TPM B chooses $r_c \in Z^*_p$ and sends the request for dynamic measurement and $T = g_{fc}$ to TGM
- TGM sends $r \in Z^*_p$ to B
- TPM B calculates $r_0 = H(PT||r)x+r_c$. B sends r_0, PT to TGM
- TGM verifies $g^{r_0} = R \cdot Pk^{H(PT||r)}$. . If $g^{r_0} \neq R \cdot Pk^{H(PT||r)}$, the remote attestation fails. Otherwise TGM calculation ET by carrying out the dynamic measurement of B with PT

Threshold remote attestation: Let A be the user and be the virtual computing node. Let m be the information involved remote attestation. TGM set the smallest trust value σE. Let ET_i be the result of the dynamic measurement of s_i. If $ET_i>\sigma E$, TGM allow s_i to carry out the remote attestation. Otherwise, TGM forbids s_i to carry out the remote attestation:

- A sends $r \in Z^*_p$ to S_1. S_1 broadcasts m, r
- S_i, i = 1,..., t chooses $r_i \in Z^*_p$ and broadcasts $U_i = r_iP$
- TPM S_i, i = 1,..., tcalculates:

$$h_i = H(m \| r \| r_i \| Pk_i \| \sum_{i=1}^{t} U_i) \quad (11)$$

$$V_i = (r_i + h_i)^{-1} Sk_i \quad (12)$$

TGM send the signature information:

$$\delta = \left(m, r, \sum_{i=1}^{t} U_i, \sum_{i=1}^{t} V_i\right) \text{ to A}$$

CORRECTNESS

Correctness of remote attestation for dynamic measurement: Since:

$$e(T, R+PK) = e(\frac{1}{x+r_c}P, r_cP + xP) = e(P,P)^{\frac{x+r_c}{x+r_c}} = e(P,P) = I \quad (13)$$

So, the remote attestation for dynamic measurement is correct.

Correctness of threshold remote attestation: Since:

$$h_i = H\left(m \| r \| r_i \| Pk_i \| \sum_{i=1}^{t} U_i\right) \quad (14)$$

$$\prod_{i=1}^{t} e(L_iV_i, U_i + h_iP) = \prod_{i=1}^{t} e(L_iSk_i, P)^{\frac{r_i+h_i}{r_i+h_i}} = e(Sk, Pk) \quad (15)$$

So the threshold remote attestation is correct.

SECURITY ANALYSIS

Security of remote attestation for dynamic measurement: Construct an attacker A to interact with honest virtual computing node with TPM. The attacker impersonates honest virtual computing node to prove the algorithm secure. Construct a function C which is an attacker against CDH hard problem. In other words, this function knows the data $\{r_{01}, r_{02}.....r_{0k} \in Z^*_p, g, g^x, g^{r_{c1}}, g^{r_{c2}}.....g^{r_{ck}}\}$. Then function C takes attacker A as a sub-program owned by it and impersonates the public key generated by TPM of honest virtual computing node in order to response A.

Function C impersonates TPM of an honest virtual computing node. A sends r to C. If r$\in\{h_1, h_2,...h_k\}$, C sends $r_0 = H(PT||r)x+r_c$, $T = g^x$, PT to A. Otherwise, C sends $\perp$ to A. Since, A konws the piblic key of TPM, attacker A can verify $g^{r_0} = R \cdot Pk^{H(PT||r)}$. Since, H is a cryptographic security function, A cannot distinguish the real environment and the ideal environment.

Attacker A impersonates honest TPM. During this phase, function C impersonates honest verifier. Function C sends $r \notin \{r_1, r_2,....r_n\}$ acording to (PK, r_0, T_i). If attacker A outputs $r_0 = H(PT||r)x+r_c$, $T = g^x$ successfully which makes $g^{r_0} = R \cdot Pk^{H(PT||r)}$ hold. Since, H is a cryptographic security function, the probility that H(PT||r) is visited conbe omited. In other words, attacker A find a solution of CDH problem that is, A obtains:

$$x = \frac{r_0 - r_c}{H(PT \| r)} \tag{16}$$

from $r_0 = H(PT||r)x+r_0$. Obviously, it is impossible within computational ability of polynomial. So this scheme is security.

Security of threshold remote attestation: The process is similar with the 4.1. We assume that attacker A impersonates TPM S_1. Attacker A knows:

$$\sigma E, r, \bigcup_{i=1}^{t} U_i, \bigcup_{i=2}^{t} V_i$$

the aim of attacker A is to solve V_1. From:

$$\prod_{i=1}^{t} e(L_i V_i, U_i + h_i P) \prod_{i=t+1}^{m} e(L_i Sk_i, P) = e(Sk, Pk) \tag{17}$$

We have:

$$e(L_1 V_1, U_1 + h_1 P) = \prod_{i=2}^{t} e(-L_i V_i, U_i + h_i P) e(Sk, Pk) \cdot \prod_{i=t+1}^{m} e(-L_i Sk_i, P) \tag{18}$$

Then, from $V_i = (r_i+h_i)^{-1}$ Ski , to obtain suitable V_1 satisfying the above equation is equivalent to solve Sk_i. Since:

$$Pk_i = f(ID_i)Pk, Sk_i = f(ID_i)Sk \tag{19}$$

That is equivalent to solve CDH problem.

SIMULATION

We use NetLogo to simulate the remote attestation in cloud computing for the scenario under study. In the simulation scenario, we adopt conditions as follows: Intel(R) Pentuim(R) 2.90G, 4G memory and Win7 operating system. The parameters in simulation are shown in the following Table 1.

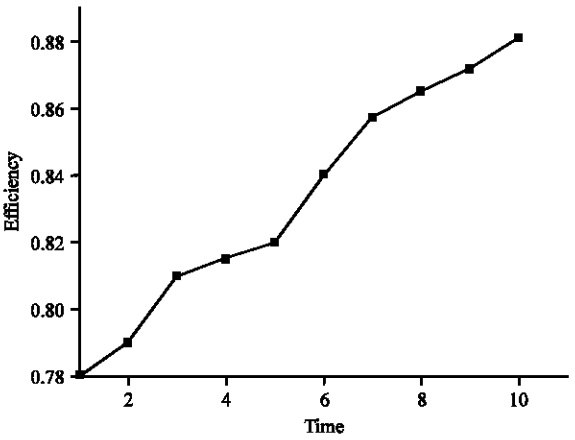

Fig. 2: The efficiency with 30% unrusted nodes

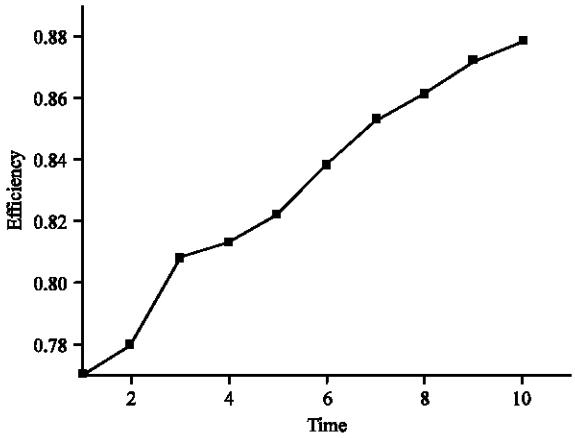

Fig. 3: The efficiency with 70% unrusted nodes

Suppose the platform conduct x times of remote attestation during the evaluation period of system running. Out of x times, trusted nodes conduct y times. So the effective rate of remote attestation under study is defined as:

$$\mu = \frac{y}{x} \tag{20}$$

We simulate and study the effective rates when the rate of unrusted nodes is, 30 and 70%, respectively. The experimental data are shown in the following Fig. 1 and 2, respectively.

Figure 2 and 3 show that the efficiency of the scheme is gradually increased over time. The reason is that the

Table 1: The parameters of simulation

	Value	Sensitivity (mv T^{-1})
N	90	The number of signers
M	270	The times of snapshots for the signers
E_0	0.2	Threshold for very untrusted
E_1	0.4	Threshold for untrusted
E_2	0.5	Threshold for critically trusted
E_3	0.8	Threshold for trusted

dynamic measure of the virtual computing node is a long process, so as the increasing number of the dynamic measurement of the platform TC collected, the efficiency will gradually rise.

CONCLUSION

This study presents a trusted measurement model based on the running virtual computing node and proposes a threshold remote attestation scheme based on the measurement model and K-CCA hard problem. Using random oracle, we prove the correctness and security of the scheme and show that this scheme can be well done with the evaluation of the turst of the running virtual computing node by simulation.

ACKNOWLEDGMENT

This study was supported by National Science and Technology Major Project under Grant No. 2012ZX03002003.

REFERENCES

Bradshaw, R.W., J.E. Holt and K.E. Seamons, 2004. Concealing complex policies with hidden credentials. Proceedings of the 11th ACM Conference on Computer and Communications Security, October 25-29, 2004, Washington, DC, USA., pp: 146-157.

Brassil, J., 2010. Physical layer network isolation in multi-tenant clouds. Proceedings of the 30th International Conference on Distributed Computing Systems Workshops, June 21-25, 2010, Genoa, Italy, pp: 77-81.

Chang, E., P. Thomson, T. Dillon and F. Hussain, 2005. The Fuzzy and Dynamic Nature of Trust. In: Trust, Privacy and Security in Digital Business, Katsikas, S., J. Lopez and G. Pernul (Eds.). Springer-Verlag, Berlin, Germany, pp: 161-174.

Chen, L., R. Landfermann, H. Lohr, M. Rohe, A.R. Sadeghi and C. Stuble, 2006. A protocol for property-based attestation. Proceedings of the 1st ACM Workshop on Scalable Trusted Computing, November 3, 2006, Alexandria, VA, USA., pp: 7-16.

Dahbur, K., B. Mohammad and A.B. Tarakji, 2011. A survey of risks, threats and vulnerabilities in cloud computing. Proceedings of the 2nd International Conference on Intelligent Semantic Web-Services and Applications, April 18-20, 2011, Amman, Jordan.

Dong, J.L., 2012. Efficient certificateless anonymous attestation to trusted cloud computing platforms. Int. J. Adv. Comput. Technol., Vol. 4

Greveler, U., B. Justus and D. Loehr, 2011. A privacy preserving system for cloud computing. Proceedings of the 11th IEEE International Conference on Computer and Information Technology, August 31-September 2, 2011, Pafos, Cyprus, pp: 648-653.

Holt, J., R. Bradshaw, K. Seamons and H. Orman, 2003. Hidden credentials. Proceedings of the ACM Workshop on Privacy in the Electronic Society, October 27-30, 2003, Washington DC, USA., pp: 1-8.

Li, S.J. and Y.P. He, 2009. On privacy of property based remote attestation. J. Commun., 30: 146-152.

Pirker, M., R. Toegl, D. Hein and P. Danner, 2009. A PrivacyCA for Anonymity and Trust. In: Trusted Computing, Chen, L., C.J. Mitchell and A. Martin (Eds.). Springer-Verlag, Berlin, Germany, pp: 101-119.

Santos, N., K.P. Gummadi and R. Rodrigues, 2009. Towards trusted cloud computing. Proceedings of the Conference on Hot Topics in Cloud Computing, June 14-19, 2009, Berkeley, CA, USA.

Schellekens, D., B. Wyseur and B. Preneel, 2008. Remote attestation on legacy operating systems with trusted platform modules. Sci. Comput. Programm., 74: 13-22.

Wang, J., Y.Z. Shao and G. Li, 2008. Study of trusted chain technology of computing trusted. Comput. Eng. Des., 29: 2195-2198.

Winsborough, W.H. and N. Li, 2002. Protecting sensitive attributes in automated trust negotiation. Proceedings of the ACM Workshop on Privacy in the Electronic Society, November 21, 2002, Washington, DC, USA., pp: 41-51.

Hu, J.F., L.X. Li, Y.Z. Zhou *et al*. 2009. Dynamic remote attestation framework based on the strategy and virtual machine technology [J]. Wuhan University (Natural Science Edition) 1671-8836(2009)01-0045-04