A TPM-Based Protection Mechanism for Remote Attestation Evidence

Shi Guang-yuan, Gong Bei, and Zhu zhen-shan

Abstract Remote Attestation is very importance in trusted computing, and the attestation evidence is foundation of the Remote Attestation. However, the existing technologies are not pay close attention on the protection of attestation evidence. In this paper, through research the main technologies of Remote Attestation, and analyze the attestation evidence in each method, providing a TPM-based protection mechanism for remote attestation evidence. The mechanism for Remote Attestation to ensure the secure transmission of the attestation's information, and designing a common communication protocol to guarantee the confidentiality and integrity of remote attestation's information in the course of transmission.

Keywords Remote attestation • Protection • Communication protocol • Trusted computing

1 Introduction

With the rapid popularization of Internet applications, people are more closely associated with them in everyday life. At the same time, since the Internet is open and interconnected, there are many insecurity factors, such as virus, worms and Trojans attacked the terminals destructively by means of vulnerabilities, which threat computer security seriously.

S. Guang-yuan (✉) • G. Bei
College of Computer and Science, Beijing University of Technology, Beijing, China
e-mail: 118sgy@163.com; HyperionUl@gmail.com

Z. zhen-shan
College of Nuclear Science and Technology, Harbin Engineering University, Harbin, China
e-mail: Heu321@yahoo.com.cn

B. Xu (ed.), *2012 International Conference on Information Technology and Management Science (ICITMS 2012) Proceedings*, DOI 10.1007/978-3-642-34910-2_60,
© Springer-Verlag Berlin Heidelberg 2013

In this case, the program used to prove the terminal communicating in a network environment is safe and trustworthy becomes a research hotspot in the field of information security. In order to ensure the trustworthiness of the entire computer system, trusted computing conducts comprehensively research such as remote attestation, a very important part of it, which is the technology that attestator proves the trustworthiness of the local environment offering the trustworthy credentials to the remote challenger. At present, the major research work is as follows: TCG first introduced the concept of Remote Attestation (T.C. Group 2003). Sadeghi and Stuble (2004) proved the trustworthiness of the platform by computing the security properties of the platform. Vivek Haldar et al. (2004) proved it through the program semantics analysis by the virtual machine; R. Sailer et al. (2004) proposed the integrity measurement system based on the TCG specifications which proved it by measuring the integrity of entity; Xiao-yong Li et al. (2006) determine the trustworthiness of platform by analyzing the behaviors of the system. The programs above mainly concerned the framework and methodologies of remote attestation, but the research on protection mechanism for remote attestation evidence is not deep enough. First, if the attestation evidence is not protected and the attacker tempers the evidence, the result of attestation is not trustworthy. Second, there needs a common trusted network framework and communication protocol to ensure the transmission of information is safe and to protect the credentials from tampering as the remote attestation is carried out between multiple platforms.

In this paper, we analyzed the main methods of remote attestation and trusted computing technologies; we proposed a TPM-based protection mechanism for remote attestation evidence. The mechanism add a Attestation Evidence Transfer Agent, AETA, into Trusted Network Connection (Trusted Computing Group 2007; Trusted Computing Group. Federated TNC Version 1.0), and the AETA transfers the attestation evidence into a general information, and the general information will be encrypted by TPM, then the AETA will transmit the general information by the AGP (Attestation Generic Protocol) to ensure the confidentiality and integrity during the transmission of information. The second section of the paper analyzes the existing attestation mechanisms and gets the evidence content in every method. The third section introduced some trusted computing technologies. The fourth section proposed the protection mechanism and gave the Attestation Generic Protocol.

2 Mechanisms of Remote Attestation in Trusted Computing

Remote Attestation is the technology that attestator proves the trustworthiness of the local environment offering the trustworthy credentials to the remote challenger. Specifically, when the user on the platform A (Attestator) requests the services from platform B (Challenger), apart from the identify authentication and privilege verification, the challenger also verify that platform A is in the state of trustworthiness. A typical scenario of remote attestation is shown in Fig. 1.

TCG's remote attestation mechanism is that the attestator is asked to submit information in which encapsulated the information about platform state by the

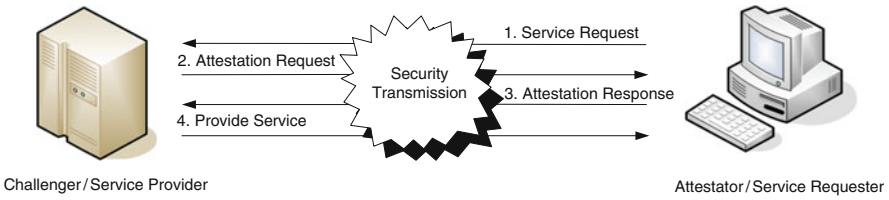

Fig. 1 A typical scenario of remote attestation

SHA-1(N.S. Laboratory 1995) algorithm including the event log and relevant PCR (Platform Configuration Register) values stored in the TPM to the challenger. PCR can be computed into one-to-one correspondence with certain state of specific events in the computing platform. The attestator signs the PCR first, and then sends the signature value, the event log, platform certificates and other relevant information to the challenger. Then the challenger authenticate the reports, determine the identity of the remote computing platform and judge whether the attestator is in the state of trustworthiness. The property-based attestation maps system configuration information to the system security properties first, and then the challenger determine whether the attestator is trustworthiness by verifying the security properties of it. In the bibliography Liqun Chen et al. (2006), it performs the functions including the anonymous attestation and revocation of binding between the configuration information and security properties. The mechanism of system behavior based attestation is that the challenger measures and verifies the system behaviors associated with the trustworthy state of the attestator's platform, and then determines whether the attestator is trustworthiness by the analysis of system behaviors based on security policies.

The methods above have their own advantages and shortcomings. TCG's method runs efficiently and develops simply. However, it only checks the PCR values and the platform certificates in which the amount of information contained is limited. It will be able to meet the requirements of users who have the lower security level. The other two methods need either to map system configuration information to the system security properties or to analyze system behaviors. However, they can provide more information and check the system security more comprehensive and accurate and are more appropriate to the users who have the higher security level. Thus, a common model compatible with a variety of attestation methods is required as different methods have their applicable targets.

3 The Trusted Computing

First, The TNC (Trusted Computing Group. Federated TNC Version 1.0) is an open solution architecture that enables network operators to enforce policies regarding the security state of endpoints in order to determine whether to grant access to

a requested network infrastructure. This security assessment of each endpoint is performed using a set of asserted integrity measurements covering aspects of the operational environment of the endpoint. The TNC is a new conceptual model proposed by TCG, while it is an open and common architecture, and the TNC does not depend on the specific technology or pattern.

The TNC architecture uses the Client/Server pattern. The three columns in this figure depict the three roles in the TNC architecture: the Access Requestor (AR), the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). The role of the AR is to seek access to a protected network in order to conduct activities on the network. The role of the PDP is to perform the decision-making regarding the AR's network access request, in light of the access policies. The PEP is the element which is connected to the AR; the role of the PEP is to enforce the decisions of the PDP regarding network access. Three horizontal layers of the architecture are indentified: the network access layer, the integrity evaluation layer and the integrity measurement layer. The TNC supports the platform integrity attestation: TCG-based attestation. It did not consider the subsequent remote attestations such as the property-based attestation and the system behavior based attestation. However, it can be the basic function module as it has a good scalability and the trusted connection can be established using the services provided by it.

The core specification of Trusted Computing Group (TCG) (Trusted Computing Group 2003) concerns the Trusted Platform Module (T.C. Group 2003), a component that provides certain cryptographic functions. The assumption is that this party is fully trusted. The current implementation of the TPM is a tamper-evident hardware chip. A TPM provides a secure random number generator, non-volatile tamper resistant storage, key generation algorithms, and cryptographic functions for encryption/decryption, digital signatures (RSA) and a cryptographic hash function (SHA-1). Moreover, the TPM includes a set of registers called Platform Configuration Registers (PCR), which can be used to store hash values.

$$PCR\_Extend(m) : PC\ \mathrm{R}_i^{new} \leftarrow SHA-1(PCR_i^{old}||m),$$

m is the message for measuring.

Trusted Software Stack (TSS) (Trusted Computing Group. TCG Software Stack) performs various functions like communicating with the rest of the platform or with other platforms.

4 Protection Mechanism for Evidence

The mechanism is separated into two parties: first is the evidence in the endpoints which is in attestation process need to be protected; second is the evidence should be protected in the transmission. Here are some stages:

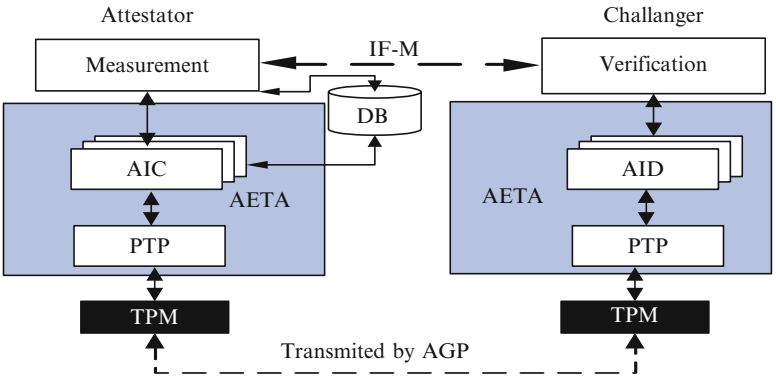

Fig. 2 Architecture of AETA

1. Collect and transfer the evidence. The evidence collected from result of measuring should be transferring into a form of general information.
2. Encrypt the general information by TPM and make sure the general information is not tampered.
3. Transmit general information by AGP.
4. Decrypt the general information, and resolve the general information.

4.1 Attestation Evidence Transfer Agent

Because of protecting the transmission of the evidence and extend the useless of the mechanism, we added a Attestation Evidence Transfer Agent, AETA, into TNC, show in Fig. 2. In the attestator, AETA is composed of AIC (Attestation Information Collector) and PTP (Protocol Transfer Proxy). AIC is responsible for collecting the evidence, which is the result of measurement. PTP is responsible for normalization of evidence and transmitting it. In the challenger, AETA is composed of AID (Attestation information Deliver) and PTP. PTP is responsible for transferring the general information into evidence, and AID is responsible for classifying the evidence and delivering the evidence to challenger. The design of the measurement module and verification module can reference the Sadeghi and Stuble (2004), Haldar et al. (2004), Sailer Reiner et al. (2004), Xiao-Yong Li et al. (2006).

PTP module is mainly responsible for normalizing the evidence files that provided by several Attestation methods, and the standard files will be used by Attestation Generic Protocol. PTP has two key functions: (1) trans- ferring the different evidence files into generic attestation information in the attestator. (2) transferring the generic attestation information into specific evidence files in the challenger.

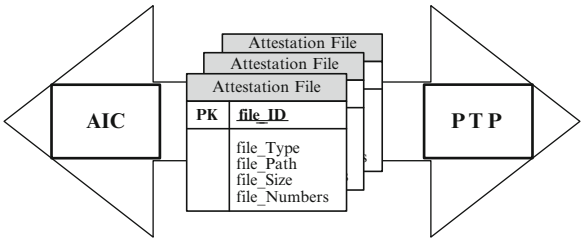

Fig. 3 Attestation information

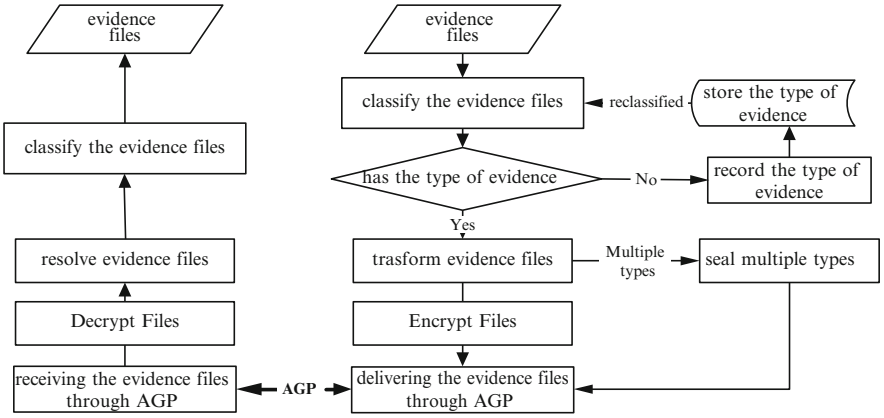

Fig. 4 Flow diagram of PTP

First, AIC collects the attestation information. The attestation information (see Fig. 3) involves the evidences files, the type of evidence, the quantity of evidence, the size of evidence and so on.

When the PTP module receives the evidence files, it uses the dual method to map the evidence files into generic information used by AGP. The flow diagram of PTP is shown in Fig. 4.

Definition 1 Set T is the set of attestation information, $T = \{A = \{a1, a2, a3 \ldots\}, B = \{b1, b2, b3 \ldots\}\}$, Set A is the subset of T and is the set of attestation type, each element of A represents a type of evidence files. For example, a1 represents TCG type, a2 represents property-based type and so on. The subset B is evidence files, each element represents the evidence files, for example, property certificate, kinds of measurement results and security logs.

Definition 2 Assuming ξ represents the generic information, and it is comprised of attestation type (AT), Attestation Information (AI), and some other information.

The formal description of PTP transformation mechanism: PTP uses dual method for transferring the different evidence files into attestation generic information.

Assuming the set of evidence files is Σpoof, the set of generic information is Σm, giving a information dual set K,

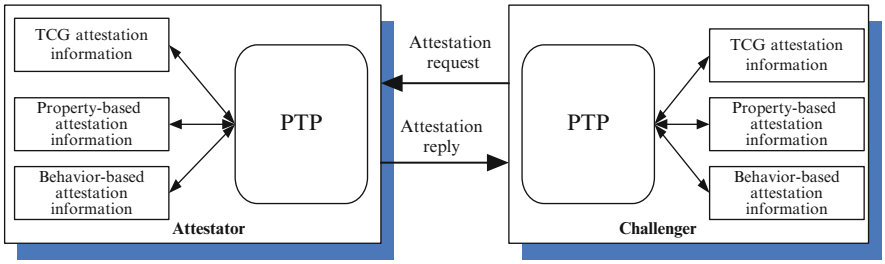

Fig. 5 Protocol transfer proxy module

$$K = \left\{ < a,\ m > | ai \in \sum poof,\quad mi \in \sum m,\quad i = 1,\ 2, \ldots \right\},$$

$$P = \{a1, a2, \ldots, ak\} \subseteq \sum poof,\quad M = \{m1,\ m2, \ldots, mk\} \subseteq \sum m$$

K defines a mapping function φ, which maps the set P to set M, φ(ai) = mi.

$$\varphi(a_i) = \begin{cases} m_i = AT, & a_i \in A \\ m_i = AI, & a_i \in B \\ \ldots \end{cases}$$

each element of the dual set represents one pair of primitive information and generic information. If ai belongs to set of attestation type A, it will be mapped into AT, AT ∈ ξ, also, if ai belongs to set of attestation file B, it will be mapped into AI, AI ∈ ξ (Fig. 5).

When the attestation platform will send the attestation information to the challenger, first, PTP should transfer attestation information t ∈ T into generic information ξ. During the transformation, it will add some information like attestation type a_i, $a_i \in A$, attestation type is used for deciding which type the attestation information is. Then evidence files b_i, $b_i \in B$ will be mapped, for example, TCG attestation method will sign the measurement value of components PCR, Sign(PCR), and then evidence files involve the Sign(PCR), event log file EventLog, and platform certificate Cert, b_i = {Sign(PCR), EventLog, Cert}. Than a_i will be mapped into AT in ξ, b_i will be mapped into AI. Finally, ξ will be encapsulated in the AGP, and sent to challenger.

4.2 Attestation Generic Protocol

PTP module is response for transferring different evidence files into standard attestation information, therefore, a novel communication protocol for remote attestation needs to be designed. When attestation is required, the attestator firstly

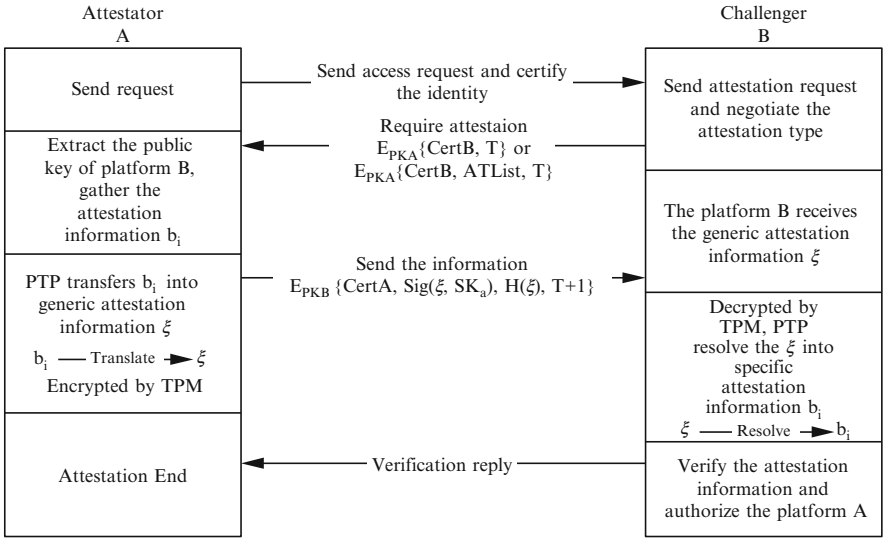

Fig. 6 Communication protocol flow

collects the attestation information, because of diversity of attestation methods, there are several kinds of attestation information. Then the attestator certifies its identity to a challenger, and attestator will send the attestation information after the certification is successful, the challenger will verify the information and authorize attestator depend on the verification results. Communication protocol flow is shown in Fig. 6.

We will give a detailed explanation of the commutation protocol flow. The platform A is attestator and platform B is challenger. The platform A firstly needs to certify its identity when A sends the serve request. Selecting a prime group G which rank is p, and an integer ring Z_p, G is a multiplication cyclic group, and g is a multiplication cyclic group, define two hash functions:

$H_{id} : \{0,1\}^{lid} \rightarrow G$, $H_m : \{0,1\}^{lm} \rightarrow Z_p$ (H_{id} and H_m have no collision probability, they are both strong one-way functions), selecting $g_1 = g^x$, $x \in Z_p$, $g_2 \in G$, define $e : G \times G \rightarrow G_T$ is the bilinear mapping from G to G_T, $e(g, g) = I$, the parameters of the whole system are $(G, G_T, e, p, g, g_1, g_2, H_{id}, H_m, I)$.

4.2.1 Certify the Identity of TPM

Considering the importance of TPM, TPM can be used to complete platform authentication. Because of the limitation of the TPM computing power, so the way of authentication is following:

TPM selects $x \in {}_R Z_P^*$, and computes $PK = g^x$, and PK is the public key of platform, then apply for Certificate Cert from CA, Cert contains identity of platform

and PK. First, attestator sends the PK of TPM to CA, then CA selects $x \in {}_R Z_P^*$, and sends it to attestator, then attestator computes $R = g^{\frac{1}{r+x}}$ and sends the result to CA, CA is certifies validity of $e(R, g^r PK) = I$, and determines whether the identity of TPM is legal, CA encrypts $v' \in Z_p$ by the attestator's PK and sends it to attestator.

4.2.2 Certify the Identity of Platform

(a) After verifying the identity of TPM, the attestator selects $r \in Z_p$, and computes $v = v' + r$ after it receiving v'.
(b) sign the message M, compute $m = Hm(M)$, attestator computes its private key $di = (g_2^x \ \gamma_i^y, g^v)$.
(c) select $r_1, r_2 \ldots r_n \in Z_p$, compute

$$\sigma = \left(\left(g_2^x \gamma_i^{v+m} \prod_{i=1}^{n} \gamma_i^n \right), g^{r1}, g^{r2} \ldots g^{v+m} g^{ri}, \ldots g^{rn} \right)$$

$\sigma = (S, f_1, f_2 \ldots f_n)$ as signature of platform i.
(d) verifier computes $m = H_m(M)$ according to $\sigma = (S, f_1, f_2 \ldots f_n)$, then verifier verifies the equation:

$$e(S, g) = e(g_1, g_2) \prod_{i=1}^{n} e(\gamma_i, f_i)$$

if the verification is successful, the attestator is permitted, otherwise, the attestator is rejected.

4.2.3 Attestation Information Transmission

After finishing certification, and receiving the attestation request of platform B, the CertA and CertB contains the EK of TPM respectively, the platform A firstly decrypts the request packets with private key of platform A SKA, and extracts the public key PKb from public key certificate of Platform B CertB, AIC will gather the attestation information b_i, $b_i \in B$, and deliver to PTP. PTP transfers attestation information into generic attestation information ξ, then and computes the hash value of ξ H(ξ) by using one-way hash function. Platform A send ξ, public key certificate of platform A to platform B. logical expression is:

$$PA \rightarrow PB : E_{PkB}\{CertA, Sig(\xi, SK_a), \mathrm{H}(\xi), T + 1\}$$

and $Sig(\xi, SK_a)$ is attestation information signed by private key SK_a. Platform B unpacks the packets with its private key SKb after receiving the attestation reply,

and extracts the public key certificate CertA and signing message. Then B extracts the attestation information using public key of platform A, and verifies then integrity of the attestation information by H(ξ). Then B delivers the generic attestation information ξ to PTP, PTP resolves the ξ into specific attestation information b_i, $b_i \in B$, and platform B will verify b_i.

4.3 Security Analysis of the Communication Protocol

4.3.1 Correctness

According to the quality of Bilinear group, we can deduce following equations:

$$e(S,g) = e\left(g_2^x \gamma_i^{v+m} \prod_{i=1}^{n} \gamma_i^{ri}, g\right) = e(g_2^x, g) \cdot e(\gamma_1, g)^{r1} \cdot \ldots$$

$$.e(\gamma_i, g)^{v+m+ri} \ldots e(\gamma_n, g)^{rn},$$

$$e(R, g^r PK) = e(g^{\frac{1}{r+x}}, g^r g^x),$$

and based on the mapping quality of Bilinear group, we can obtain:

$$e(g^{\frac{1}{r+x}}, g^r g^x) = e(g,g)^{\frac{r+x}{r+x}} = e(g,g) = I,$$

$$e(g_2^x, g) \cdot e(\gamma_1, g)^{r1} \cdot \ldots e(\gamma i, g)^{v+m+ri} \ldots e(\gamma_n, g)^{rn}$$

$$= e(g_1, g_2) \prod_{i=1}^{n} e(\gamma_i, f_i),$$

so we can arrive at the conclusion is that the signature and verification scheme is correct.

4.3.2 Security Analysis of Verification of Identity

Function simulate the honest attestator $P_i = \{P_1, P_2 \ldots P_n\}$, attacker A interact with P_i simultaneously, all of Pi have the same public key $PK = g^x$, attacker A pretends as verifier V, and transmits $r_i \in {}_R Z_p^*$, $i \in 1, 2 \ldots n$ to P_i, P_i answers the R_i or $\perp$ for $r_i \in {}_R Z_p^*$, if $r_i \in \{h_1, h_2 \ldots h_k\}$, then P_i sends $g^{\frac{1}{hi+x}}$ to attacker A, if not, gives $\perp$ to A. Because A knows the PK of attestator P_i, so $e(R_i, g^{ri} PK) = I$, A can't distinguish the true situation and idea situation.

Verification: A pretends as attestator, function F is honest verifier, F sends $r \notin \{r_1, r_2.....r_n\}$ by reference (PK, r_i, R_i), if A gets the result r and makes $e(R_i, g^{ri} PK) = I$ is true, then A finds answer of K-CCA, this is impossible in the computing ability of polynomial, so the protocol is security.

4.3.3 No Forgery of Signature

Because of only the certified member of ring can pass the verification and get v'. Computing $v = v' + x_1 + x_2$, and then generate the signature key $di = (g_2^x \gamma_i^y, g^v)$, because the signature scheme is based on DDH assumption, so it can't get any information of signature key from $\sigma = (S, f_1, f_2 \ldots f_n)$ in the Polynomial-time, so from an engineering perspective, the signature can't be forgery in the duration of validity.

5 Conclusion

Trusted remote attestation is an important research field in the trusted computing area, there has been many attestation methods to propose, in order to assure the security transmission of the attestation information between many computing platforms, this paper provides a TPM-based protection mechanism, and designs a generic communication protocol. We added A Attestation Evidence Transfer Agent in endpoint, and made use of Protocol Transfer Proxy module to transfer different attestation information into generic information. We also designed a generic communication protocol; this protocol can guarantee the integrity and confidentiality of attestation information by using the technologies of authentication, digital Signature and integrity verification. This paper is supported by the National High-Tech Research and Development Plan of China under Grant No 2006AA01Z440, 2009AA012437 and National Basic Research Program of China (973 Program 2007CB311100), and the open project of key state laboratory of Harbin Engineering University "the research on critical security technologies of the third generation nuclear power information system", No.HEUFN0801.

References

Haldar V, Chandra D, Franz M (2004) Semantic remote attestation-a virtual machine directed approach to trusted computing. In: Proceedings of the third virtual machine research and technology symposium USENIX 2004

Liqun Chen, Rainer Landfermann, Hans Lohr, Markus Rohe, Ahmad-Reza Sadeghi, Christian Stüble (2006) A protocol for property-based attestation. In: STC'06: proceedings of the first ACM workshop on scalable trusted computing, ACM Press, New York, NY, USA, pp 7–16

N.S. Laboratory (1995) Secure hash standard. Federal Information Processing Standards Publication 180–1, April 1995

Sailer Reiner, Zhang Xiao-Lan, Jaeger Trent, van Doorn Leendert (2004) Design and implementation of a TCG-based integrity measurement architecture. In: SSYM'04: proceedings of the 13th conference on USENIX security symposium, USENIX Association, Berkeley, CA, USA, pp 16–16

Sadeghi A-R, Stuble C (2004) Property-based attestation for computing platforms: caring about properties, not mechanisms In: NSPW'04: proceedings of the 2004 workshop on new security paradigms, ACM Press, New York, pp 67–77

T.C. Group (2003) TPM main specification, November 2003, Version 1.2

Trusted Computing Group (2003) http://www.trustedcomputinggroup.org

Trusted Computing Group (2007) TCG specification architecture overview specification revision 1.4[Z]. TCG Published, August 2007

Trusted Computing Group. TCG Software Stack (TSS) specification, Version1.2. http://www.trustedcomputinggroup.org/resources/tcg_software_stack_tss_specification

Trusted Computing Group. Federated TNC Version 1.0, Revision 26.http://www.trustedcomputinggroup.org/resources/federated_tnc_version_10_revision_26

Xiao-Yong Li, Chang xiang Shen, Xiao-Dong Zuo (2006) An efficient attestation for trustworthiness of computing platform. In: IIH-MSP, Pasadena, California, USA, pp 625–630