

An Effective Approach for Remote Attestation in Trusted Computing

Xin Huang^{1,2}, Yuxing Peng³

¹ National Engineering Research Center for Multimedia Software, Wuhan University, Wuhan, China

² Human & Social Science College, Wuhan University of Science and Engineering, Wuhan, China

Email: first.bossmehx@126.com

³ School of Computer Science, National University of Defense Technology, Changsha, China

Abstract—The e-commerce demands end-user systems that adhere to well-defined security policies. In this context Trusted Computing is a new security solution proposed by the Trusted Computing Group Trusted Computing (TC). It aims at providing a framework and effective mechanisms that allow computing platforms and a distributed system to gain assurance about each other's integrity and trustworthiness. In TCG architectures Remote attestation is one of the core functionalities provided by trusted computing platforms. It was introduced in TCG specifications to determine whether a remote system is trusted to behave in a particular manner for a specific purpose. However, most of the existing approaches is static, inexpressive and attest only the integrity state of a remote system. This paper proposes an effective approach for remote attestation in trusted computing from the automated negotiations that an application authenticates itself to a remote party automatically. We suggest a model automated negotiation for remote attestation that is completed by both sides through the automated negotiations, and discuss the process of automated negotiations.

Index Terms—Remote Attestation; Trusted Computing; TPM; Automated Negotiations

I. INTRODUCTION

With the rapid development of computer technologies and internet, more and more people cannot live without network. For example, the application of computer and internet has been permeated into all kind of fields such as politics, economy, society, education and military affairs. Whether applications are private or commercial, both of them require IT systems that guarantee confidentiality, authenticity, integrity, privacy, as well as availability become all kinds of attacks such as virus, Trojan Programs and hacker's attacks have made current compute network systems very vulnerable.

In this context some fundamental and challenging issues are how to define and to determine, verify the integrity and trustworthiness of a computing platform or in general of an IT system, and how common computing platforms could support such functionalities. Note that even a perfectly secure operating system cannot verify its own integrity [6]. Trusted Computing is a new security solution proposed by the Trusted Computing Group (TCG) [1] based on Trusted Platform Module (TPM) [7] that is a microprocessor chip attached to the main board with capability of creating and storing keys, providing cryptographic algorithms, identity authentication and integrity measurements. TPM serves as the trusted root of

integrality report denies download and implementation of all the unregistered malicious code such as computer virus, and guarantee the trusty of computing unity [8].

In TCG architectures, Remote attestation [9] is one of the important functionalities provided in the trusted computing platforms. A terminal platform [10], host of the TPM, can attest to its description of characteristics to a remote party. To guarantee the trustworthiness and freshness, the description of characteristics needs to be signed by the TPM. Usually this signature is generated by using the Endorsement Key (EK) of TPM, and the Endorsement Key of TPM is the Root of Trust for Reporting (RTR) which is the cryptographically unique and bound to the TPM. For vouching the accuracy of the information and protecting the privacy of the host of the TPM, TCG develops a solution using a trusted third party (Privacy CA). By negotiating securely with the Privacy CA, TPM gets an Attestation Identity Key (AIK) certificate from Privacy CA and signs the message by using the AIK instead of EK. However current methods of remote attestation suffer from many critical drawbacks. For example, the Privacy CA needs to be involved in all the transactions of the attestation. Remote attestation in TCG architectures is static, inexpressive and fundamentally incompatible with today's heterogeneous distributed computing environments.

In this paper, an effective approach for remote attestation in trusted computing is presented, which is automated negotiations of remote attestation that an application authenticates itself to a remote party automatically. Remote attestation is completed by both sides through the automated negotiations.

The remainder of this paper is structured as follows: Section 2 refers to related work. Section 3 is an overview of trusted computing. In section 4, we suggest a model automated negotiation for remote attestation and discuss the process of automated negotiations. We give our conclusion and suggest further work in section 5.

II. RELATIVE WORK

One of the purposes of remote attestation is to attest the remote platform is trusty but not revealing the actual identity of the platform, and is the process by which software authenticates itself to remote parties. The TCG solution for platform authentication is sometimes called remote binary attestation, remote binary binding, and binary sealing. Loosely speaking, they are based on a measurement of the chain of executed code using a

cryptographic digest and some trust assumption. Binary attestation, however, has several shortcomings, in particular for application attestation, regarding flexibility and security/privacy as pointed out in [11]. Researcher [15] on the meaning and method of remote attestation, divide the abstract models into four types and analyze the shortcoming of the existing models and the improved method.

A more general extension to the binary attestation is property-based attestation [12], which should determine whether the target machine to be attested fulfills certain requirements.

The authors [13] propose model-driven remote attestation that is attesting remote system from behavioral aspect. The model-driven remote attestation verifies two compliance requirements to prove the trustworthiness of a remote system: expected behavior compliance and enforced behavior compliance.

The authors [14] propose semantic remote attestation that is a virtual machine directed approach to trusted computing. Using language based virtual machines enables the remote attestation of complex, dynamic and high-level program properties in a platform. Though remote attestation for trustworthiness of computing platform is a focus research work in Trusted Computing, many challenges remain to be solved and are subject of ongoing research.

III. OVERVIEW OF TRUSTED COMPUTING

For the sake of information system security, Trusted Computing (TC) is promoted by the TCG, which is a not-for-profit industry-standards organization with the aim of enhancing the security of the computing environment in disparate computer platforms. The TC systems would cryptographically seal off parts of the computer that deal with data and applications and give decryption keys only to programs and entities that were judged to be trusted [2]. “Trust” is a complicated notion that has been studied and debated in different areas (social science and humanities as well as computer science). A possible definition of the notion “trustworthy” is the degree to which the (security) behavior of the component is demonstrably compliant with its stated functionality [4]. TCG defined as “an entity can be trusted if it always behaves in the expected manner for the intended purpose”.

A. Reference Architecture of Trusted Platform

The TCG has published several specifications on various concepts of trusted infrastructures [3]. The core component of the TCG specifies is the Trusted Platform Module (TPM). The current widespread implementation of the TPM is a small tamper-evident cryptographic chip attached to the main board with capability of creating and storing keys, providing cryptographic algorithms like RSA, SHA-1, HMAC and functions as digital signing, identity authentication and integrity measurements.

Many vendors already ship their platforms with TPM. A TPM can be used to ensure that each computer will report its configuration parameters in a trustworthy manner. Platform boot processes are augmented to allow

the TPM to measure each of the components in the system (both hardware and software) and securely store the results of the measurements in Platform Configuration Registers (PCR) within the TPM. Emergency response personnel can use these measurements to determine which computers are vulnerable to virus attacks. IT managers may install system processes that use the PCR values in a TPM to identify unsafe configurations at system boot thereby preventing inadvertent network connection while in an unsafe mode.

B. Transitive Trust in TPM

One trusted computer system is composed of root of trust, trusted hardware platform, trusted operating system and trusted applications, which is shown in Fig.1. A trust chain, starts from root of trust to hardware platform, operating system, and applications. The previous portion of code that is executed checks the integrity of the next component to be executed and passes trust, then trust can be extend into the whole computer system. Whether the root is trusted is guaranteed by taking managerial approaches and physical protection mechanisms.

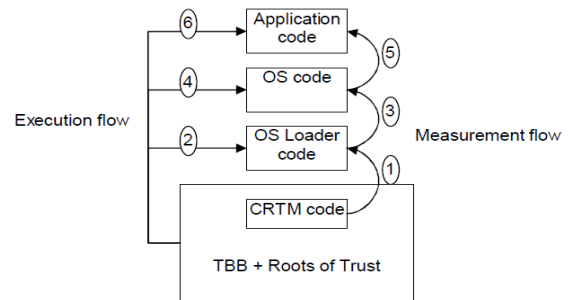


Fig.1 A trust chain in the process of TPM transitive

Transitive trust is applied to system booting from a static root of trust. Root of trust is the only trusted model when the computer power on. Trust boundary is extended to include the code that didn’t natively reside within roots of trust through transitive trust. The process of can be reasoned about with our predicate calculus.

C. Remote Attestation

Attestation is the process of vouching for the accuracy of information. External entities can attest to shielded locations, protected capabilities, and Roots of Trust. A platform can attest to its description of platform characteristics that affect the integrity (trustworthiness) of a platform. All forms of attestation require reliable evidence of the attesting entity [2].

Remote attestation is one of the core functionalities provided by trusted computing platforms. It holds the promise of enabling a variety of novel applications. It is the process by which an application authenticates itself to a remote party. When asked to attest itself, Attester (the attesting party) reports to a remote party (the verifier) the configuration of a machine(s) to be attested through TPM. To guarantee integrity and freshness, PCR values and a fresh nonce provided by the remote party are digitally

signed with an asymmetric key called Attestation Identity Key (AIK), which is under the sole control of the TPM. A trusted third party called Privacy Certification Authority (Privacy-CA) is used to guarantee the pseudonymity of the AIKs. As shown in Fig.2, it is the attesting between the attester and the verifier.

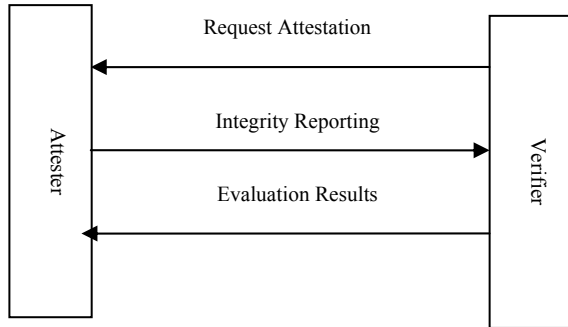


Fig.2 Process of Remote attestation

It can be described with formal specification below:

Step1 Verifier : Generate a Nonce (160bit random number)

Step2 Verifier→Attester: {Nonce}

Step3 Attester→Verifier: {Sig {PCR, Nonce} AIK (Attestation Identity Key) , SML (Storage Measurement Log) , Cert(AIKpub)}

Step4 Verifier : Firstly attest Cert (AIKpub) , Secondly attest Sig {PCR, Nonce} AIK , Finally authenticate Freshness of Nonce and coherence of SML through the PCR.

IV. AUTOMATED NEGOTIATIONS FOR REMOTE ATTESTATION

A. Automated Negotiation Model

Automated negotiations for remote attestation are an effective approach that an application authenticates itself to a remote party automatically. In the Trusted Computing Platform, computer will enter a safe operating environment under the guidance of the CRTM. Before the network entities process automated negotiations for remote attestation each other, attester with an embedded key called the Endorsement Key (EK) in TPM provide credentials to third party (verifier), who can provide service of authenticating them, and stored them in the PCRs. The two sides will exchange AIK to indicate the identity of each other and then enter into the phase of request attestation, when they begin to carry out attestation. If the phase can be finished successfully, that is to say, both sides can successfully carry out negotiations through the credentials requested for attestation, the key negotiations will be carried out. Then, both sides started the exchange of security credentials in the negotiation process for authenticating the session key of the communication. As shown in Fig.3, it is a model automated negotiation for remote attestation.

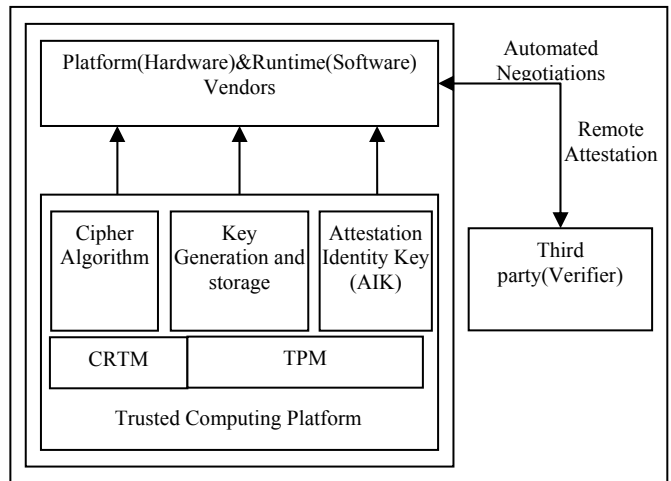


Fig.3 Model Automated Negotiation for Remote Attestation

B. Process of Automated Negotiations

In the automated negotiations for remote attestation, the process of automated negotiations is no longer dependent on the third party who provides cryptographic service, but is completed by both sides through the negotiations (as shown in Fig.4).

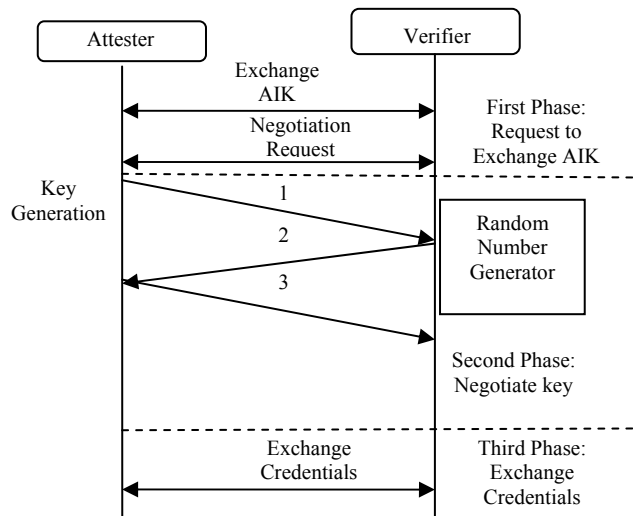


Fig.4 Process Automated Negotiations for Remote Attestation

1) With key generation function of TPM , attester generate a key K for symmetric encryption algorithm. The key K that has been borne the signature by the private key KAS of the local AIK is encrypted with the KAS from the verifier, and then sent to verifier.

2) Verifier will verify its signature, after he receives the key K and decrypt it. If the signature is attested successfully, a random number R is generated by the random number generator function in TPM and encrypted with the key K from the attest. Then, the verifier link up the random number R with the ciphertext signatures of the private key KBs from the local AIK , and send them to the attester finally.

3) Attester receives them to attest their signature and separate a random number R from ciphertext. Then,

attester put to use K to decrypt the ciphertext and compare with R . It is successful in automated negotiations for remote attestation if the R and decrypted ciphertext is the same. Thereafter attester encrypt negotiation request with decrypted ciphertext and send them to verifier, which is not only confirmation of the process of automated negotiations for remote attestation, but also is the beginning of the next phase of automated negotiations. All the credentials are used to negotiate the keys for encryption in the phase of Exchange Credentials, which will ensure that credentials are in the information security.

V. CONCLUSION

In this paper, the automated negotiation for remote attestation is proposed to cope with the shortcoming of the existing approaches for remote attestation which is static, inexpressive and attest only the integrity state of a remote system. In the automated negotiations for remote attestation, the process that is from key generation to exchange credentials is no longer static and dependent on the third party who provides cryptographic service, but is completed by the automated negotiations between attester and verifier. For further extensive applications, some details in the automated negotiation are proceeding. Meanwhile, the model automated negotiation for remote attestation is in constant refinement and validation also.

REFERENCES

- [1] The Trusted Computing Group. <http://www.trustedcomputinggroup.org>
- [2] TCG, TCG Specification Architecture Overview, Specification Revision 1.4, 2nd August 2007, <http://www.trustedcomputinggroup.org>
- [3] Trusted Computing Group (TCG). About the TCG <http://www.trustedcomputinggroup.org/about/>
- [4] Benzel, T.V., Irvine, C.E., Levin, T.E., Bhaskara, G., Nguyen, T.D., Clark, P.C. Design principles for security. Technical Report NPS-CS-05-010, Naval Postgraduate School (September 2005)
- [5] YU Rong-wei, WANG Li-na, KUANG Bo. Method of designing security protocol for remote attestation, Journal on Communications, Vol.29 No.10, October 2008
- [6] Ahmad-Reza Sadeghi, Trusted Computing — Special Aspects and Challenges, SOFSEM 2008, High Tetras, Slovakia, January 19-25, 2008, pp. 98–117
- [7] TCG, TCG TPM Specification Version 1.2 Revision 103, <https://www.trustedcomputinggroup.org/specs/TPM/>
- [8] ZHOU Zheng, ZHANG Jun, LI Jian, LIU Yi. Protecting Terminals by Security Domain Mechanism Based on Trusted Computing. Wuhan University Journal of Natural Sciences Vol.11 No.6 2006
- [9] Joshua Guttman, Amy Herzog, Jon Millen, Leonard Monk, John Ramsdell, Justin Sheehy, Brian Snien, George Coker, NSA, Peter Loscocco, NSA. Attestation: Evidence and Trust, MITRE TECHNICAL REPORT, MTR080072
- [10] Jiqiang Liu Jia Zhao Zhen Han, A Remote Anonymous Attestation Protocol in Trusted Computing, The 4th International Workshop on Security in Systems and Networks (SSN2008), 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS 2008)
- [11] A.-R. Sadeghi and C. Stübke. Property-based attestation for computing platforms: Caring about properties, not mechanisms. In The 2004 New Security Paradigms Workshop, Virginia Beach, VA, USA, Sept. 2004. ACM SIGSAC, ACM Press.
- [12] Kühn, U., Selhorst, M., Stübke, C.: Property-Based Attestation and Sealing with Commonly Available Hardware and Software. In: ACM-STC (2007)
- [13] Liang Gu, Xuhua Ding, Robert H. Deng, Yanzhen Zou, Bing Xie, Weizhong Shao, Hong Mei, Model-Driven Remote Attestation: Attesting Remote System from Behavioral Aspect. The 9th International Conference for Young Computer Scientists, Zhang jiajie, China, November 18, 2008
- [14] Vivek Haldar, Deepak Chandra and Michael Franz, Semantic Remote Attestation — A Virtual Machine directed approach to Trusted Computing. USENIX Virtual Machine Research and Technology Symposium, 2004
- [15] ZHANG Qiang, ZHU Li-na, ZHAO Jia. Research on Method of Remote Attestation in Trusted Computing, Control & Management, Microcomputer Information, Vol.24, No.4, 2008