Operating System based Compliance Validation of Trusted Computing

Madan Singh[1], Surekha Chauhan[2]

1 Associate Professor, Shoolini University of biotechnology & Management, Bajhol ,Solan, (H.P.),sINDIA

2 Sr. Lecturer, Mody university, Sikar, Rajasthan, INDIA

Abstract

The concept of trusted computing given was by Anderson [2]. Trust is an expectation that a device behaves in a particular manner. A trusted component, operation or process is one whose behavior is predictable under almost any operating condition which is highly resistant to viruses or any physical interference. Trusted computing is one of the key technologies in the field of information security. It is the security solution proposed by TCG [1]. Its core concept is "chain of transitive trust", which means measurements and authentications are performed level by level based on Roots of Trust to assure the booting process, operating system and applications of a computing platform have executed correctly within users' expectations. The main idea of trusted computing is to equip computer systems with a device that can be trusted by all. The Trusted Computing Group (TCG) has addressed a new generation of computing platforms employing both supplemental hardware and software with the primary goal to improve the security and the trustworthiness of present and future IT systems. The Trusted computing platform proposes to address the problem of remote trust. The Trusted Computing Platform (TCP) implies some party trusts the platform which is under consideration. The core component of the TCG proposal is the Trusted Platform Module (TPM) [1] providing certain cryptographic functions. Many vendors have already started to equip their platforms with a TPM claiming to be TCG compliant. However, there is no feasible way for application developers and users of TPM-enabled systems to verify the compliance. Compliance test is performed to assess whether a system considered, functions perfectly according to the given specifications. Testing can be very expensive if performed by brute force. Hence, one of the basic approaches for compliance testing is performed by constructing a Finite State Automata which can perform test in an inexpensive manner.

1. Introduction

1.1 Trusted Platform

A *Trusted (Computing) Platform* (TP) is a platform that is trusted by local users and remote entities including users, software and web sites.

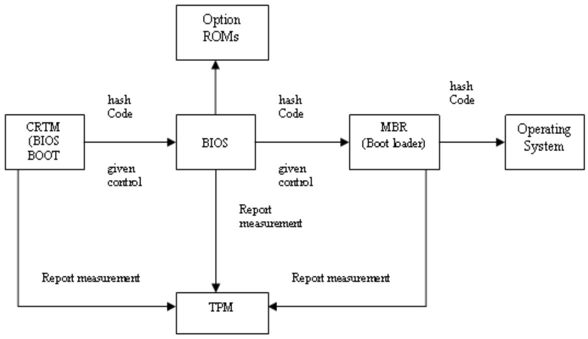

Fig.1 Architecture Diagram of the TCG Authenticated Boot Process [7].

To enable a user to trust such a platform, a relationship of trust must be established between the user and the computing platform so that the user believes that an expected boot process, a selected operating system, and a set of selected security functions in the computing platform have been properly installed and operates correctly.

1.2 Roots of Trust

Root of trust provides at least functionality for measurement, storing, and reporting of characteristics that affect the trustworthiness of the platform. Commonly there is one root of trust for each capability: a Root of Trust for Measurement (RTM), a Root of Trust for Storage (RTS), and a Root of Trust for Reporting (RTR) [8].In the trusted platform specified by the Trusted Computing Group

(TCG), the Trusted Platform Module (TPM) acts as the RTS as well as the RTR whereas the Core Root of Trust for Measurement (CRTM) is most often part of the BIOS.

The Trusted Computing Group, has defined an open specification for a TPM, which has been implemented by multiple chip vendors; and incorporated into desktop and mobile systems from major PC manufacturers. The TPM is a small, low cost, hardware security device, intended to perform critical security services for a client machine.

1.3 Trusted Computing Module (TPM)

TPM basically consists of following modules

1. Cryptographic functions: (P) RNG, SHA-1, HMAC, RSA.
2. Secure storage and reporting of hash values representing a specific platform configuration.
3. Protected key and data storage.
4. Initialization and management functions.

Trusted computed module generates three keys

a) **Endorsement Key**: The Endorsement Key is a 2048 bit RSA public and private key pair which is created randomly on the chip at manufacture time, and cannot be changed.

b) **The Storage Root Key (SRK)**: The Storage root key is a 2048 bit RSA key pair. It is initially empty, and is created as part of taking ownership. This key never leaves the chip. It is used to encrypt (wrap) private keys for storage outside the TPM, and to decrypt them when they are loaded back into the TPM.

c) **The Owner Authorization Key (OAK)**: The owner authorization key is a 160 bit secret shared with the owner of the TPM. The owner loads it into the TPM as part of taking ownership of the chip. This secret key is used to authorize sensitive owner command requests.

The RSA key generation engine is used to create signing keys and storage keys. A TPM must support up to 2048-bit RSA keys, and certain keys must have at least a 2048-bit modulus. There is no requirement concerning how the RSA algorithm is to be implemented. TPM manufacturers may use *Chinese Remainder Theorem* (CRT) implementations or any other method.

1.3.1 Security services from TPM

The TPM chip can provide several essential hardware based security services:

a) Secure authentication
b) Secure storage
c) Integrity measurement
d) Integrity attestation

1.4 What is TPM compliance?

Being the start of chain of trust, root of trust must ensure the trustworthiness including the conformance to specifications. As for TPM although TCG has already decided a set of specifications as the standard for designing and implementation, there must be some checks available whether or not TPM is following those specifications. These checks are basically called as compliance validation. It is usually the assessment of a system to verify that is behaving as expected.

1.5 Why do we need Compliance validation?

A compliance deviation from the specification may bring crucial security impacts. For instance, a correct TPM command with valid parameters will lead to the return code TPM SUCCESS. If these parameters are modified to be wrong; TPM should return specific error codes to indicate the invalid parameter according to specifications. However, in some implementations of TPM, TPM SUCCESS or some error codes completely unrelated to the actual command are returned when the input buffer is manipulated which may be used as an entry point by attackers.

Furthermore, some security sensitive applications may react differently to different error codes. Such impacts can be enlarged when applying TPM in distributed environment using a remote TPM. In that case, if the TPM is not compliant with specifications, collaboration will either terminate immediately or process without protection from hackers. Despite the fact that TPM has already performed self test during its initiation, the result of self test is a manufacturer-specific block which does not contain any compliance information.

To prevent such exploits, it is necessary for TPM to remain compliant. Compliance is not only required for the TPM but also required for other components of the computing platform. TCG has already applied with some form of credentials. One such credential is Root of Trust for Conformance (RTC) , taking it start of compliance chain. Validating mechanism can act as a further protection in the application level. In this way, the security and trustworthiness of the platform is enhanced because every component is assured to have no exploits against specifications.

1.6 Conclusion

In our research work we will focus and work on mechanism to transfer and map the compliance validating mechanism to OS level. It is expected that it will help to definitions and improve framework. The tests performed during the booting process will be more effective, assuring compliance before OS is loaded. we will try to evolve a prototype test suite for TPM compliance tests according to the TCG specification. The results of test sample can be used to find non-compliance and bugs of several TPM implementations; and security problems that can arise as consequence of non-compliance can be pointed out. The present work is a broad framework for setting up research agenda and exploration of TCG compliance and may be able to address some of the core issues of this area of development including addressing some of the misgivings about the framework.

References

[1] A survey of trusted computing specification and related technologies by Richard Kelly, SANS Institute,2003.

[2] A Trusted Computing Model Based on Code Authorization by Guoheng Wei, Xueguang Zhou, Huanguo Zhang Int. Symposium on Info. Proc.,2008.

[3] An Information Flow Security Model To Trusted Computing System by Hu Jun, Shen Changxiang First Int. Symposium on Data, Privacy and E-Commerce,2007.

[4] Design and Implementation of Security Operating System Based on Trusted Computing by Xiao-weinie, Deng-guo Feng, Jian-jun Che, Xin-pu Wang Proc.ofthe fifth Int. Conf. on Mobile Learning and Cybernetics, Dalian,13-16, Aug.,2006.

[5] Protected Computing Vs Trusted Computing by Antinio Mana, Antonio Munoz IEEE 2006.

[6] An Approach for Compliance Validation of Trusted Computing Application by Qi Cui, Wenchang Shi, Workshop on Knowledge discovery and Data Mining,2008.

[7] Exploring the Integration of Memory Management and Trusted Computing, Dartmouth Computer Science Technical Report TR2007-594,A Thesis of Master of Science by Nihal A. D'Cunha DARTMOUTH COLLEGE Hanover, New Hampshire May 31st, 2007.

[8] Trusted Computing Group (TCG), Architecture Overview Specification, Revision 1.3,https://www.trustedcomputinggroup.org/groups/TCG_1_3_Architecture_Overview.pdf,March, 2007.