Integrity Measurement based on Trusted Computing

Yiming Li[1, a], Haihe Ba [2, b] and Jiangchun Ren[3, c]

[1] College of Computer, National University of Defense Technology, Changsha, Hunan 410073, China

[2] College of Computer, National University of Defense Technology, Changsha, Hunan 410073, China

[3] College of Computer, National University of Defense Technology, Changsha, Hunan 410073, China

[a]email: jason.24@qq.com, [b]email: bahaihe@hotmail.com, [c]email: wwwrjc@163.com

Keywords: Trusted Computing; Integrity Measurement; Remote Attestation

Abstract. With the rapid development of modern information technology, more and more people believe that the protection of hardware equipment must be enhanced in order to improve the security capabilities of computer information systems better. Trusted computing improve the trustworthiness of system through the secure chip from hardware level, using the trusted root, chain of trust, trusted model to ensure the integrity of the system, and expands the trusted chain to application layer, ensures the credibility of software through measurement and verification technology. In this paper, we will introduce related hot research about integrity measurement.

Introduction

The idea of trusted computing derived from successful management experience in human society, that is, each country has a stable root of trust, and build trust chain security mechanism based on it, which is responsible for the management and implementation of the national levels of assessment. However, at present, has not yet formed a unified definition on trust. Trusted Computing Group (TCG) defined a trusted entity's behavior is always in the expected way, to achieve the desired goal, then call this entity is trusted [1,2]. A system is trusted if the operation or procedure of components involved in the computing is predicable in any conditions, and can protect against viruses and physical disturbance, defined by International Organization for Standardization/International Electro Technical Commission (ISO/IEC).

Measure the trustworthiness of computing systems, and store measurement securely; provide attestation report when remote object asked for system's trustworthiness, this mechanism referred to "Measure-Storage-Report" mechanism. This mechanism does not only ensure the trustworthiness of the trusted computing system, but also have the ability to provide trusted proof outward. Root of trust is the basis point of trusted computer system, there are 3 trusted roots of trusted computing platform, which is Root of Trust for Measurement (RTM), Root of Trust for Storage (RTS) and Root of Trust for Report (RTR). They are the trusted base points of computer system, measurement of platform and storage of platform separately. As shown in Fig 1, chain of trust reflects "Measure-Storage-Report" mechanism well, that is, measure the trustworthiness of computing platform, store measurement value and provide attestation report. Chain of trust is the technical implementation of trust measurement model, to extend trust relationship from root of trust to entire computing platform. Using an iterative calculation of hash value, which is connecting present value with new value, and then calculate hash value as a new measurement. After measurement and storage, providing attestation report when the remote entity asked. This mechanism is called Remote Attestation.

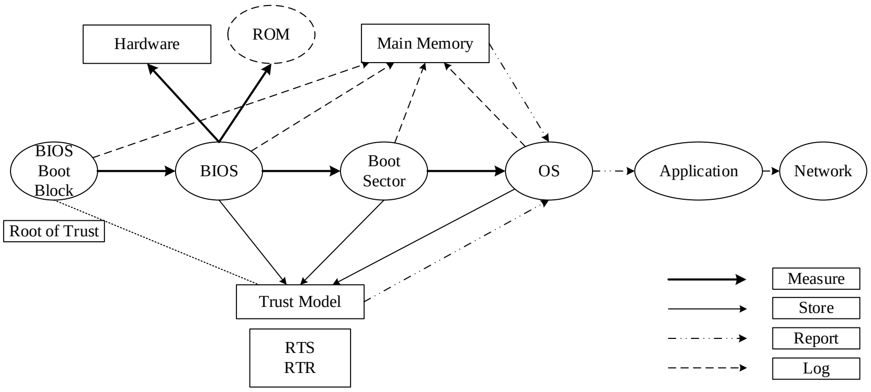

Fig.1. Chain of trust model

Integrity Measurement based on Static Root of Trust Measurement

Application integrity measurement and verification need to prove whether the trustworthiness of local computing system is in line with the prediction of both local and remote authenticator.

a. Binary-based

Early integrity measurement and verification is mainly about integrity measurement of binary code image, software configuration. That using TPM signature and log of integrity measurement to prove the integrity status of software. This method requires platform more stringent, is not flexible enough, there are two disadvantages:

(1) Privacy. Integrity measurement based on binary needs TPM signature, and contains chain of trust, exposing the configuration information of platform, provide a breakthrough to hostile to some extent, so that local computing system is more vulnerable to various attacks.

(2) Difficult to update. Chain of trust involving multiple system components, the information and version different from each other. System update likely to cause the integrity information is difficult to verify.

IBM has designed and implemented IMA (Integrity Measure Architecture)3 based on TCG specifications, measure an integrity in the order from root of trust, BIOS, boot sector, OS to applications, progressive measure and trust level by level. This method is able to detect current operating status of system, which could find possible tampering. IMA measurement module has been used as a part of Linux security mechanisms, and are widely used in a variety of practical applications.

b. Property-based

To overcome the shortcomings of binary authentication, Haldar proposed semantic remote authentication scheme [4], using a trusted virtual machine to verify certain semantic properties of program, achieving a complex and dynamic integrity measurement of advanced application program in a platform-independent way; Chen from HP Labs proposed the property-based remote attestation, converted binary attestation to property-based attestation by using the main functions of TCG, solved issues like sensitive information leakage and update difficulty caused by binary measurement, and selected a trusted third party as the issuer of property-configuration certificate. The authentication method based on property proposed by Sadeghi et al.[5] is able to establish mapping between properties and platform configurations by reporting platform’s properties, and establishing properties by trusted certificate authority.

Binary-based measurement mechanism provides basic protection for the integrity of systems and applications, but there is a huge application limitations, especially in the system with multiple versions of modules; property-based integrity measurement can overcome the limitation of binary-based integrity measurement, play an effective role in the binary image with same property but different hashes, the specific differences is shown in Table 1.

Table 1. Comparison between different types of integrity measurement

	Binary-based	Property-based
Objects	Executable binary code	Property of platform
Typical Systems	IMA [3], PRIMA [6]	PBA [7], CPBA [8]
Privacy	May leak privacy	Protect privacy
Effects	Low efficiency	Practical and scalable

Integrity Measurement based on Dynamic Root of Trust Measurement

The measurement above is IMA integrity measurement architecture based on Static Root of Trust Measurement, measure integrity only when system startup, cannot guarantee the integrity of the process. To make up for these shortcomings, TCG 1.2 specification [9] defines a new mechanism: verify the startup process by Dynamic Root of Trust Measurement (DRTM). Intel’s TXT (Trust Execution Technology) [10] and AMD’s SVM (Secure Virtual Machine Extension)[11] are both using DRTM as underlying trust mechanism.

The dynamic establishing process of trusted environment based on DRTM is known as Late Launch in TCG 1.2 specification, to guarantee a trusted startup of a virtual machine manager. BIND [12] proposed by Carnegie Mellon University is fine-grained security certification service for distributed systems, by using TPM-based measurement and signature mechanism, insert a measure point in each process and protect running process by using secure kernel based on AMD secure coprocessor, to achieve dynamic measurements of trusted processes. Bernhard Kauer [13] analyzed trusted computing system based on Static Root of Trust Measurement (SRTM) in detail, pointed out the security vulnerabilities of this RTM, and proposed a safe opening loader OSLO, transferred root of trust from SRTM to DRTM by using AMD’s skinit instruction, narrowed the trusted computing base of application and weakened the attacks against TPM and BIOS. Carnegie Mellon University Cylab laboratory designed TrustVisor [14] based on virtual machine monitor, which provides memory isolation, DMA protection and several virtual TPM interfaces (such as Seal/UnSeal, Extend, Quote, etc.), as a result, not only protects user’s secure sensitive code but also reduces the impact of DRTM for running efficiency.

Unlike SRTM, DRTM is able to start at any time and be repeated any number of times. There are a great difference between chain of trust based on SRTM and DRTM, the specific comparison as shown in Table 2.

Table 2. Comparison between different chains of trust

	DRTM-based	SRTM-based
Configuration	TPM/TCM chip	TPM/TCM chip, CPU supported special instruction
Protection	No special hardware protection	Disable DMA and interrupt
Construction time	Only when system power up	Any time when system is running
Trusted computing base	RTM, BIOS, boot sector, OS and upper layer application	Special instructions in Intel and AMD

Conclusion

Security and trustworthiness of current services focused on protection of message layer, trusted computing and security services has not formed an effective interaction, it also makes the current information system face enormous challenges. This paper describes the services and security technologies, trusted computing base, static measurement techniques of program, behavior and some principles and techniques of traditional trusted computing, introduces the latest development of trusted computing technology, comparing the advantages and disadvantages of various techniques.

References

[1] Trusted Computing Group (TCG). http://www.trustedcomput- inggroup.org.

[2] Module T P. Main Specification, Level 2, Version 1.2, Revision 116 (2011) [J].

[3] R. Sailer, X. Zhang, et al. Design and implementation of a TCG-based integrity measurement architecture. Proceedings of the 13th Usenix Security Symposium, August 2004, pp.223-238.

[4] V. Haldar, D. Chandra, et al., Semantic Remote Attestation-Virtual Machine Directed Approach to Trusted Computing. Proc. of the 3rd Virtual Machine Research and Technology Symposium, 2004, pp.29-41.

[5] R. Sadeghi, et al., Property-based attestation for computing platforms: caring about properties, not mechanisms. Proc of the New Security Paradigms Workshop, 2004, pp.67-77.

[6] T. Jaeger, R. Sailer, et al., PRIMA: Policy-Reduced Integrity Measurement Architecture. Proc. of ACM Symposium on Access Control Models and Technologies, 2006, pp.19-28.

[7] Chen L, Landfermann R, Löhr H, et al. A protocol for property-based attestation[C]//Proceedings of the first ACM workshop on Scalable trusted computing. ACM, 2006: 7-16.

[8] Yu Qin, Dengguo Feng. Remote attestation based on component property [J]. Journal of Software, 2009, 20(6): 1625-1641.

[9] TCG. PC client specific tpm interface specification. Version 1.2, revision 1.00. http://www.trustedcomputinggroup.org, July 2005.

[10] Intel trusted execution technology mle developers guide. http://www. intel.com/technology.

[11] AMD64 virtualization: Secure virtual machine architecture reference manual. AMD Publication No. 33047 rev. 3.01, May 2005.

[12] Elaine Shi, Adrian Perrig, Leendert Van Doorn. BIND: A Fine-grained Attestation Service for Secure Distributed System. Proc. of the IEEE Symposium on S&P, 2005,pp.154-168.

[13] Kauer B. OSLO: Improving the security of Trusted Computing[C] // Proceedings of the USENIX Security Symposium. 2007, 24(25): 173.

[14] McCune J M, Li Y, Qu N, et al. TrustVisor: Efficient TCB reduction and attestation[C]//Security and Privacy (SP), 2010 IEEE Symposium on. IEEE, 2010: 143-158.