Implementing Trustworthy Dissemination of Digital Contents by Using a Third Party Attestation Proxy-Enabling Remote Attestation Model

Zhiyong Zhang, Qingqi Pei, Jianfeng Ma
Ministry of Education Key Laboratory of Computer Network & Information Security
Xidian University
Xi'an, P. R. of China
{zhangzy, qqpei, jfma}mail.xidian.edu.cn

Lin Yang
The Research Institute
China Electronic Equipment & Systems Engineering Corporation
Beijing, P. R. of China
yanglin61s@yahoo.com.cn

***Abstract*—A secure and trusted distribution of digital contents is a fundamental requirement for Digital Rights Management (DRM) system, so that the integrity of user terminal platform should be verified prior to contents' distribution in order to assure that the platform is free from a malicious modification and attack. Recent years the emerging trusted computing has better enhanced the necessary functionality, though existing remote attestation models and relevant protocols could not solve a critical problem of the privacy protection of the attested platform states, which include basic configurations and security attributes. We proposed an implementation of trustworthy dissemination of digital contents by using a third party attestation proxy-enabling remote attestation model with the privacy protection of the front-end user device environment. Also, a Xen virtualization-based terminal platform architecture, which primarily enforces the domain isolation among the processes or key components, was presented. Finally, an application case manifested the proposed model and platform architecture not only realized the remote integrity verification of user end devices that was carried out on the back-end contents server side, but effectively protected the platform states privacy, further improving the usability of DRM system.**

Keywords-Digital Rights Management; Trusted Computing; Remote Attestation; Virtualization Technology; Trustworthy Dissemination

I. INTRODUCTION

With the rapid developments of communication network technologies, users could access to digital resources and services by using multiple network admission methods, in anytime, at anywhere, which is much easier than before. In such a situation, free distribution, unauthorized usage of copyrights-protecting digital contents will be a common phenomenon, as the contents like electric book, image, music, movie and application software are easily duplicated without deterioration in quality. Thus, digital contents industry could be heavily damaged, and value chain could also be interrupted. An issue of contents protection and legitimate usage is, therefore, crucial. In order to solve the problems mentioned above, Digital Rights Management (abbr. DRM) has emerged at the beginning of the 1990s.

Recent years have witnessed the application researches on trusted computing technology in the field of DRM, which are involved with the trustworthily dissemination of digital contents and the corresponding license presenting usage policy, the secure storage of contents and relevant cryptographic key, as well as the trusted execution of DRM Controller, which is also referred to as DRM Agent, on the basis of several key techniques, such as Remote Attestation (RA) and the integrated virtualization-enabling trusted platform. A trusted terminal platform provided by the device manufacturer is crucial for a general DRM system or Mobile DRM, meanwhile is also helpful for enhancing the trust relationships between contents provider and consumer in the contents value chain.

The main contributions of the paper are to make a detailed analysis of RA approaches available and to implement a trusted distribution of digital streaming media contents based on a third party attestation proxy-enabling remote attestation model and the proposed Xen-virtualization-based user terminal platform.

II. EXISTING REMOTE ATTESTATION APPROACHS

Current researches on RA mainly aim at basic framework and protocol of TCG-RA, improving some disadvantages of existence including static and weak capability of binary-based measurement, platform privacy protection of remote terminal, which are not suitable for distribution application and commercial open system. Hence, some novel modes of trusted measurement and attestation are addressed from different viewpoints.

A. Binary-Based Remote Attestation (BBRA)

BBRA has been already adopted by TCG to measure and attest terminal in a series of Specs available [1]. The approach executes Hash function on binary codes of file, especially for EXE and DLL files, and signs these Hash merits by private key of AIK stored securely in TPM chip, and then sends to a challenger as the report of the platform integrity. Subsequently the challenger attests consistency between these merits and predefined references that are standard merits of Hash on a file. The model is suitable for local attestation of secure bootstrap, and could further validate whether key components of platform, OS and application are attacked or tampered with. Besides, in term of TCG-IMM (Integrity Management Model), a database of integrity references should be employed due to a mass of references needed by attestation.

B. Property-Based Remote Attestation (PBRA)

In order to protect privacy of attested platform in RA, PBRA [2, 3] modes adopted security properties provided by platform and the trusted third party that issues property certificate as an attestation report. The report is sent to the

978-0-7695-3556-2/08 $25.00 © 2008 IEEE
DOI 10.1109/MMIT.2008.133

challenger for checking current attributes whether to be compliable to predefined policies or not. PBRA is not dependent on the attestation on the given hardware configures or software components, but the secure attributes of the challenged platform. Note that although PBRA is based on three parties and basic configure is not exposed by Trusted Third Party, but some attribute, for instance Multi-Level Security or domain-isolation, would be acquired by the challenger, as also directly results in the intended assault by some proper attack approaches in term of the exposed security features.

C. Semantic-Based Remote Attestation (SBRA)

Binary-based measurement could not attest behavior characteristics of application software and satisfy the requirements of trusted measurement at the running time, with the absence of the important rich semantic expression capability. For solving them, SBRA [4] adopted two-party-based attestation mode, with a goal to the remote attestation of the upper application by language-based virtual machine. It includes basic and dynamic attributes attestation of class objects or system, which is different from the above mentioned attestation models, as it has characteristics of complex, dynamical, platform-independent and advanced program. But SBRA model has still solved the issue of privacy protection.

D. SoftWare-based ATTestation (SWATT)

SWATT [5], proposed by CMU, was used to verify the main memory of an embedded device and to check the modification of main memory contents. It could provide the attestation of memory contents like TCG or NGSCB without physical access to memory. Owe to finding the modification of contents with high probability, SWATT could check virus, Trojan-horse and basic configures of a challenged device.

E. BEhavior-Based Remote Attestation (BEBRA)

As the above RA models and approaches available lack of dynamic measurement mechanism of software behavior and the significant consideration for the context of the running platform, behavior tree of processes in Unix was established, and the remote attestation of platform together with application was implemented by Behavior Monitoring Agent and Trust Attestation Module [6]. Also, Li et.al. [7] proposed a system behavior based trustworthiness attestation model, which was a trustworthiness attestation model based on system behavior of attesting computing platform in trusted computing environment.

III. TRUSTED DISTRIBUTION OF DIGITAL CONTENTS

A. Third Party-Enabling Remote Attestation Model

Although several RA approaches, such as PBRA and SBRA, are improvements of TCG-RA, the property certificate and semantic-based attestation provided a challenger with current security properties, the statuses of the challenged platform, dynamic attributes of object classes as well as software behavior features in some extent, therefore, the above mentioned models have yet solving the issue of privacy protection. For this purpose, we proposed a novel model, called AP^{2}RA (Attestation Proxy Party-supported Remote Attestation), based on the trusted third party named as Attestation Proxy Party (APP) [8]. AP^{2}RA introduces APP to improve traditional RA models, and adopts a new mode of the local trusted measurement, APP attestation and remote decision, thus better implementing the privacy protection of the attested system. If the attested party was attacked, APP still could actualize basic function of the attestation and assure of mid-results. AP^{2}RA model was illustrated as Figure 1. Here Measurement & Evaluation Unit (MEU) was an essential component for the verification of integrity and security characteristics of attested objects.

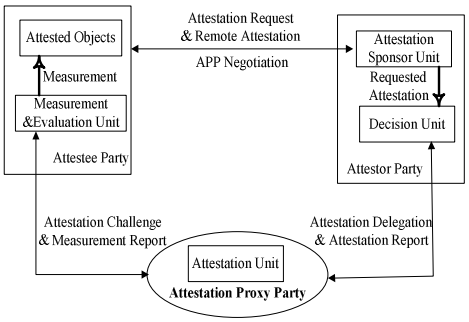

Figure 1. Attestation Proxy Party-supported Remote Attestation Model

AP^{2}RA model is mainly composed of three basic entities, which are Attestee Party, Attestor Party and APP, and key components inside entity, such as Measurement & Evaluation Unit, Attestation Unit, Decision Unit, etc. The conceptual definitions of three fundamental entities are as follows in detail, and their formal definitions is in [8]:

- **Attestee Party (abbr. AteeP)** is an effector of remote attestation. In trusted computing environment, it is usually terminal (e.g. PC, Laptop, PDA, etc.) platform itself and inner components of software or hardware, but not denoting user entity. The discussion of user identification is beyond the paper's scope. AteeP consists of Attested Objects that are locally measured, then reporting trusted measurement merits outwards.
- **Attestor Party (abbr. AtorP)** is a sponsor of RA. It denotes a remote platform or a user entity. AtorP sends the request of attestation according to application's needs, as well as making access decision in cooperative work and resource sharing, or controlling trusted network connection in virtue of attestation results and security policies.
- **APP** is an actor of RA, and a trustworthy third party. After receiving the measurement merits that are sent by AteeP, APP evaluate current state of platform by integrity references and security policies, and providing trusted evaluation report to AtorP.

The main components relative to the above mentioned entities belongs to logic unit, which is implemented by software or hardware, and could be not only a physical unit, but also a section of codes in program. It is noted that they must have the following logic functions.

- **Attested Object** is an attested firmware, components and program in RA. They constitute the software and hardware environments of platform, that is, BIOS, OS loader, OS kernel and application, as well as some attested processes.

- **Measurement & Evaluation Unit** is a software-component or a hardware chip accomplishing trusted measurement and evaluation mechanism. It locates AteeP and trustworthily reports measurement merits and evaluation properties for APP. In the procedure of OS kernel being loaded, namely a trust chain establishment from BIOS to OS kernel in bootstrap, the principal function of MEU is integrity measurement that is implemented by CRTM in BIOS and Trusted Chip Module practically. After OS kernel having been loaded, MEU mainly measures and evaluates OS service programs and upper applications.
- **Attestation Unit** is a hardware component or program accomplishing trusted attestation mechanism. Being a logic function component in APP, Attestation Unit compares the current merits of AO with trusted measurement reference including integrity measurement's and security evaluation's, and then determining basic configure and security state of system.
- **Attestation Sponsor Unit** denotes an initial activation of RA request. It pertains to AtorP side and is generally a section of program codes that actives RA procedure in terms of the requirements of an application, then continues to execute other steps of the application after receiving RA results sent by other units.
- **Decision Unit** provides the function of trusted attestation decision. It is also components or program having logic function features. Not only accepting attestation report of platform capabilities from APP, DU also determines whether or not AteeP passes trusted remote attestation based on application-level security policies, and further acquiring sharing resource or accessing to network.

B. Xen-based Platform Architecture Combined with Trusted Computing

To accomplish the trusted measurement of Attested Object (AO) and the security of MEU, we employed Xen virtualization technology in the trusted computing-enabled terminal platform. The establishment of virtualization environment based on the trusted OS kernel could implement the domain-isolation execution and protect the processes in a lesser trusted boundary, so better satisfying trustworthiness of AO in combination with the trusted measurement, storage and report mechanisms provided by the nature of trusted computing. A Xen virtualization-based Platform Architecture (XPA) was shown in Figure 2, where several fundamental data streams among the key components were involved in that the access to platform hardware and system functions, integrity measurement and security evaluation, as well as trusted measurement merits storage, etc.

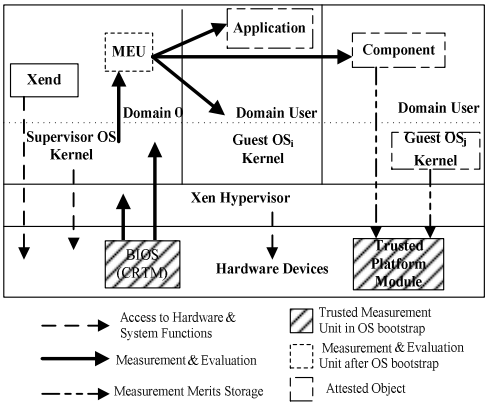

Figure 2. Xen-based Platform Architecture for AP^{2}RA Model and Fundamental Data Streams Inclued the Platform

XPA integrated the bottom hardware platform, whose motherboard is welded with a trusted chip module, and Xen-Hypervisor located in the upper layer of the architecture. According to Ring Architecture of X86, Hyperivsor runs in Ring 0, whereas Supervisor OS Kernel running in Ring 1. Other upper Guest OS Kernels access to virtual devices by using the virtualization of hardware devices, which is provided by Hypervisor and Doamin 0. In domain 0 the controller of Xen, named as Xend, is responsible for establishing, destroying, migrating of a given domain. Domain U, where multiple applications could concurrently run, implements isolation execution of different components for enhancing security. For instance, MEU runs in Domain 0, as it is based on modified secure Linux kernel; in general AO is Guest OS kernel or it upper application, which is authoritatively measured by MEU. Not that CRTM in BIOS is in charge of integrity measurement from the startup of Hypervisor to the load of Super OS Kernel and MEU. Thus, MEU and AO could be protected by the isolation approach. If AO was captured, the integrity and trustworthiness of MEU would be still satisfied.

C. An Application Case of Trusted Distribution of Streamingmedia Digital Contents

With regard to the protection of the digital media contents and the corresponding copyrights, an integrated DRM system is involved with the comprehensive procedure including contents building and packaging, distribution, transmission, promulgating and using of digital contents, and the security, integrity and availability of media contents are to date faced with fearful challenge, even influencing on survivability of digital contents industry [9]. The original goal of trusted computing roots in copyrights protection from contents providers' perspective, so it would better protect secure and trusted distribution, as well as legitimate usage of media contents. But, note that RA application in DRM system would have direct influence on Fair Use of digital contents [10].

A framework of trusted distribution of DRM-enabling contents was shown by Figure 3. The architecture consists of front-end XPA-enabling terminal platform, back-end digital streamingmedia contents server, APP Server and Integrity Reference & Security Policies Database conformable to the TCG-IMM model.

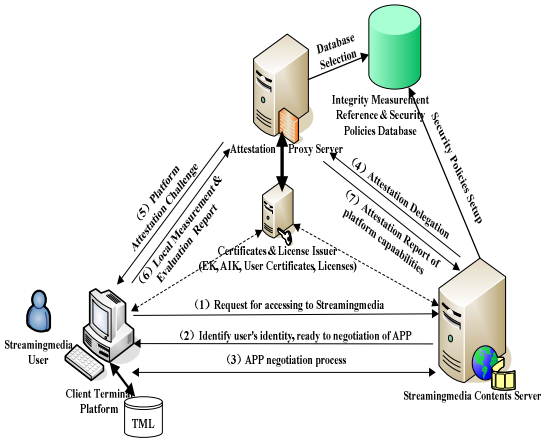

Figure 3. A framework of Trusted Distribution of Streaming Media Contents Based on Trusted Computing

The frame laid emphasis on integrity verification of user end platform involved with basic configures of hardware and software environment in a whole system bootstrap procedure and dynamic run-time shotsnaps Beside, the authentication of user identity is also a primary functional step that ensures the legitimacy of user requesting access to media contents prior to the distribution, but its discussion is beyond scope of the paper. The procedure of trustworthy dissemination of contents is as follows:

First of all, user terminal sponsored a request for accessing to streaming media contents, and subsequently server authenticated user's identity. If user was legal or authorized, and server begin to negotiate with APP in order to enforce remote verification on user platform. After the negotiation is passed and APP has been recognized by two parties, server could delegate an attestation on APP by using our proposed protocol [8] and accept final the integrity report. Afterwards, APP was responsible for the attestation procedure. It challenged a requesting user terminal platform for attestation, and the XPA-enabling platform correspondingly implemented local trusted measurement on basic components and applications (e.g. media player, the third party optional components, etc.) by using the trusted physical chip welded on the terminal motherboard, together with local evaluation of security property. The following step was that terminal sent the trusted measurement merits and TML (Trusted Measurement Log) to APP. Subsequently, APP queried Integrity Measurement References & Security Policies database, and verified current integrity merits with references by using MEU. At the same time, some security attributes of the platform, such as OS patch, Anti-Virus database, version of key component, and system security level, also were evaluated based on predefined security policies in the database. If the attested object was not attacked outside and compliable to security policies, APP would provide a capability report of the intact terminal platform to contents server side. Note that AO would be interfered from inside owing to the Xen-based domain isolation mechanism of existence. Finally, a final decision on access to contents was yielded as a permission or prohibition of contents distribution and usage.

IV. CONCLUSIONS

The paper proposed an implementation of trusted distribution of digital contents based on the third party proxy-enabling remote attestation model, which could protect the privacy of attested terminal platform and is different from existing RA models. Also, the trusted computing-enabled terminal platform architecture with domain-isolation execution feature was presented in detail. The DRM application realized the trusted attestation of user terminal platform on streaming media server side and protected distribution and usage of digital contents. The future work is to implement the trusted enforcement of digital license based on the proposed Xen-virtualization-enabled trusted platform.

ACKNOWLEDGMENT

The work is supported by National Natural Science Foundation of China Grant No. 60803150 and China National 111 Program of Introducing Talents of Discipline to Universities Grant No.B08038.

REFERENCES

[1] Trusted Computing Group, "TCG Specification Architecture Overview Specification Revision 1.4," https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf, Aug. 2007.

[2] A. R. Sadeghi, and C. Stüble, "Property-based Attestation for Computing Platforms: Caring about properties, not mechanisms," Proc. of the 2004 Workshop on New Security Paradigms, ACM Press, Sep. 2004, pp. 67-77.

[3] L. Chen, and R. Landfermann, H. Lohr, M. Rohe, A. R. Sadeghi, and C. Stüble "A Protocol for Property-Based Attestation," Proc. of the First ACM Workshop on Scalable Trusted Computing (STC 06), ACM Press, Nov. 2006, pp.7-16.

[4] V. Haldar, "Semantic Remote Attestation," Ph. D. Dissertation, University of California, Irvine, 2006.

[5] A. Seshadri, A. Perrig, L.V. Doorn, and P. Khosla, "SWATT: SoftWare-based ATTestation for Embedded Devices," Proc. 2004 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, May 2004, pp.272-282.

[6] H. Zhang, and F. Wang, "A Behavior-Based Remote Trust Attestation Model," Wuhan University Journal of Natural Sciences, vol. 11, Nov. 2006, pp.1819-1822.

[7] X. Li, X. Zuo, and C. Shen, System Behavior Based Trustworthiness Attestation for Computing Platform. Acta Electronica Sinica, vol. 35, Jul. 2007, pp. 1234-1239.

[8] Z. Zhang, Q. Pei, L. Yang, and J. Ma, "Attestation Proxy Party-supported Remote Attestation Model and its Secure Protocol", Journal of Xidian University, vol. 36, Jan. 2009, in press.

[9] S. K. Nair, B. C. Popescu, and C Gamage, B. Crispo, and A. S. Tanenbaum, "Enabling DRM-preserving Digital Content Redistribution," Proc. the Seventh IEEE International Conference on E-Commerce Technology, IEEE Computer Society Press, Jul. 2005, pp. 151-159.

[10] Y. Yu, and Z. Tang, "A Survey of the Research on Digital Rights Management," Chinese Journal of Computers, vol. 28, Dec. 2005, pp.1957- 1968.