

Secure DRM Scheme for Future Mobile Networks Based on Trusted Mobile Platform

Yu Zheng, Dake He, Hongxia Wang, Xiaohu Tang

Lab. of Information Security & National Computing Grid, Southwest Jiaotong University, Chengdu 610031, P. R. China
zhyu_swjtu@163.com or cdzhengyu@yahoo.com.cn

Abstract—With the emergence of wide bandwidth wireless networks, mobile Internet is set to provide a significant channel for multimedia content distribution. The need for mobile digital right management (DRM) solution is thus intensified in order to safeguard mobile media content. The Open Mobile Alliance (OMA) has been set to define open DRM technologic specifications to protect copyrighted content against piracy, unauthorized use and distribution over mobile networks. However, we argue that there still are some potential security flaws in its recent version 2 specifications. A secure DRM scheme based on Trusted Mobile Platform (TMP) is proposed in this paper to enhance the security of OMA DRM specification v2 and provide interoperability and compatibility between Trusted Computing (TC) and OMA DRM. According to our analysis thereafter the TMP in conjunction with OMA DRM v2 may offer a considerably more robust DRM system for future mobile networks.

I. INTRODUCTION

Mobile equipments (ME) with advanced multimedia and networking capabilities introduce new business opportunities by enabling provision of rich content such as games and multimedia for mobile users. However, content piracy is seen as a major obstacle when realizing these business prospects. The need for mobile digital right management (DRM) solution is thus intensified in order to provide a controlled consumption of digital content to protect the intellectual property rights of the authors and the content providers [1,2].

The Open Mobile Alliance (OMA) [3] formed in June 2002 has been working on mobile DRM to introduce and promote open standards and specifications for the application and services over mobile networks. In September 2002, OMA approved version 1.0 for the DRM specification [4], which specifies three different methods that vary in complexity requirements and offer different levels of security for the distributed content. The recent version 2 specifications [5] issued in December 2004 are expected to provide mechanisms for secure authentication of trusted DRM Agents, and for secure packaging and transfer of usage rights and DRM Content to trusted DRM Agents.

However, we argue that the OMA DRM system based on its v2 specifications has to face the following potential risks. At first, current mobile platforms including its software and hardware are untrusted. E.g. since current mobile operating

systems, such as Palm OS and Symbian, still have a large number of open security gaps [6] and can not enforce mandatory access control policies [7], users who receive the legal content can become potential attackers by employing software that allows illegal forwarding of the copyrighted content after the received digital content is decrypted by DRM Agent. Meanwhile, since there is no process separation mechanism in current hardware and software of mobile platform, attacker and/or virus can access DRM Agent's process easily to compromise some sensitive information such as Content Encryption Key (CEK) of the Digital Content Format (DCF) and DRM Agent's private key etc, which may cause fragmentation of the OMA DRM system. Secondly, OMA DRM systems do not provide a way to protect a digital content from the Right Issuer (RI). If the owners of the Content Issuer (CI) and that of RI are not the same, the RI may become another potential attacker to distribution digital content with its received CEK from CI. Finally, current OMA DRM v2 specifications have provided mutual authentication mechanism between RI and DRM Agent. Nevertheless, the CI does not identify the consumer before they download the DCF. Since the content download will consume a large number of channel and bandwidth particularly for wireless networks, the uncontrolled download may result in possible Deny-of-Service (DoS) attack on CI and wireless network operator.

The schemes that utilizes watermarking as complementary solution for DRM on ME is presented in [8, 9] to enhance the security of copyrighted media distribution. However, they just distinguish the un-copyright content from the genuine ones but can not prevent abusing of the content and can not solve the above presented security flaws in current OMA DRM systems either. The concept of DRM scenario based on Trusted Computing (TC) [10] for personal computer (PC) and wired networks is discussed in [11]. Meanwhile, enforcement of a mandatory access control policy, observance of the principle of least privilege and provision of trusted paths were identified in [11] as key requirements of DRM system, which are absent in mainstream PC operating system. However, it does not provide any detail scheme for establishing DRM system, particularly mobile DRM system, over TC architecture. Moreover, we still confuse about how to support interoperability and compatibility between TC and DRM.

In this paper we aim to present a TC-based DRM system for mobile networks to overcome the above proposed security flaws in current OMA DRM v2 system. The interoperability and compatibility between TC architecture for ME and OMA DRM system is also discussed. According to our analysis thereafter the TC specifications for ME in conjunction with OMA DRM v2 may offer a considerably more robust platform for mobile DRM.

II. COMBINATION OF TMP AND OMA DRM

2.1 Trusted Mobile Platform (TMP)

In October 2004, Trusted Computing Group (TCG) [10] develops Trusted Mobile Platform (TMP) specifications [12-14], which defines comprehensive end-to-end security architecture and focuses on mobile platform identity and integrity to prove TC for ME. The generic two processors hardware architecture for TMP is depicted in Fig.1. The components darkened make up the trust boundary including 1) the application processor 2) Trusted Platform Module (TPM) 3) USIM (Universal Subscriber Identification Model) 4) Core Root of Trust for Measurement (CRTM) 5) internal flash, 6) memory controllers and 7) DMA controller. Where CRTM is stored in the ROM memory and performs the initial trust measurements for the remainder of platform on power up. While, TPM [15] is a very important tamper-resistant component in TMP who is responsible for recording the integrity measurements of TMP and works closely with the CRTM to perform trusted boot. TPM also provides security functionality, such as platform attestation, protected storage, and sealing, to measure and validate the hardware and/or software configurations of the platform. For more detail about TMP architecture, refer to [12-15].

Some key features of TMP are listed as the follows, which are beneficial to satisfy critical requirements of DRM system. Firstly, integrity measurement can provide trusted boot of ME and detect virus or attacker's malicious tamper on operating system and/or DRM Agent when ME powers up. Secondly, process separation and mandatory access control policies can resist unauthorized access on DRM Agent's process. Thus the attacker can't compromise sensitive information from the hardware resource used by DRM Agent. Thirdly, protected storage can be utilized to safeguard DRM Agent's private key and CEK so that attacker can not read them from non-volatile memory. Finally, the seal storage and mandatory access control policy can also constrain user's illegal distribution of protected content to other ones.

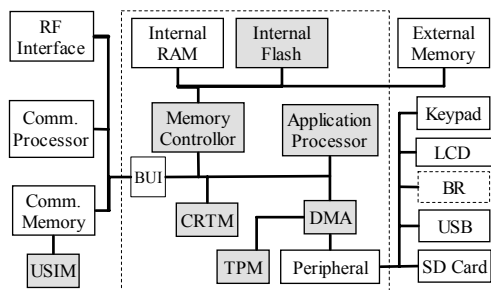


Figure 1. Generic hardware architecture for trusted mobile platform

2.2 TMP-based DRM system for mobile networks

As shown in Fig.2, TMP-based DRM scheme is proposed in compliance with OMA DRM specifications v2. In our scheme, just like OMA DRM specifications there still are four actors that interact with each other in order to provide access to protected digital content to the end-user. The CI, as the owner of digital content, firstly converts content to DCF and then negotiates Right Object (RO) with one or more RI, which describes permissions and constraints granted to the DRM Agent when accessing a specific DCF. Before selling a RO to the end-user, the RI sets up a trusted relationship with the DRM Agent, a trusted logical entity residing in the user's ME. Trust in OMA DRM v2 is based on PKI certificates issued by a Trusted Authority. In OMA DRM the right and content are logically separate entities, although being uniquely associated. Thus consumer must gain DCF and corresponding RO from CI and RI respectively for usage of the protected content. For more detail refer to [3-5].

The contribution and novelty of our scheme to the original OMA DRM are listed as the follows:

- (1) DRM Agent is embedded in TMP. DRM Agent's public-key certificate, private key and original integrity metric are stored in TMP's TPM, which can not be accessed by unauthorized user and/or process.
- (2) TPM offers trusted boot for ME with CRTM and should check the integrity of DRM Agent before the download of protected content.
- (3) Before sending the DCF to the consumer, CI should identify the consumer to resist DoS attack.
- (4) DRM Agent should authenticate the consumer via TPM and USIM to against abuse on DRM Agent.
- (5) Before responding the RO to DRM Agent, RI should check the validation of the state of TMP via TC's remote attestation (including Integrity report protocol and Validation data protocol) to against malicious tamper on mobile platform by attacker and/or virus.
- (6) The RO validation, interpretation and enforcement functions of a DRM Agent are implemented within the trusted boundary of TMP. Information inputted by user/consumer/subscriber and/or shown on screen is transferred via TMP's trusted I/O.
- (7) The CI does not deliver CEK to RI directly. Two secret key seeds (S_1, S_2) to generate CEK are issued by CI. Where S_1 is

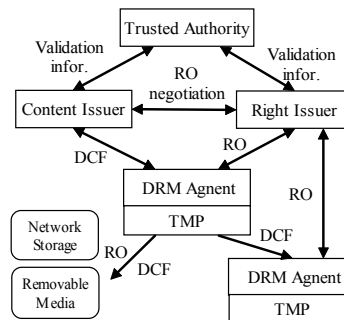


Figure 2. TMP-based OMA DRM functional architecture

encrypted by DRM Agent's public key and sent to DRM Agent within DCF. While S_2 is firstly encrypted by RI's public key and sent to RI. Then RI retrieves S_2 and encrypts S_2 with DRM Agent's public key and delivers it to DRM Agent in RO. Thus neither the RI nor consumer can capture or construct the CEK individually in order to decrypt the corresponding DCF.

As shown in table I our TMP-based DRM is compared with the original OMA DRM v2. All expected security feature in the left row will be achieved in our scheme which can improve the security and robust of DRM systems for mobile networks.

TABLE I. COMPARISON BETWEEN OMA DRM AND OUR TMP-DRM

Expected security features	OMA DRM	TMP-DRM
Integrity protection on DRM Agent and mobile platform	No	Yes
Confidentiality of DRM Agent's sensitive information	No	Yes
Mutual authentication between user and ME	No	Yes
Resist compromised ME's attack or illegally distribution.	No	Yes
Consumer identified by CI to resist DoS attack on CI	No	Yes
Resist compromised/malicious RI's attack or piracy	No	Yes

2.3 Authentication in TMP-based DRM system

As shown in Fig.3, according to the critical requirements of TMP and OMA DRM v2, in our scheme we argue that five kinds of possible authentication should be offered in sequence as the follows in order to provide a robust platform for mobile DRM systems. Where USIM is used to store user/owner/subscriber/consumer's public-key certificates, private key and other sensitive information that can prove their identities, e.g. password and biometric template.

- (1) Mutual authentication between user/owner and ME via USIM and TPM.
- (2) Mutual authentication between subscriber and network operator via USIM.
- (3) DRM Agent identifies consumer via USMI and TPM.
- (4) Content provider/CI authenticates consumer via USIM.
- (5) Mutual authentication between DRM Agent and RI with the help of TPM.

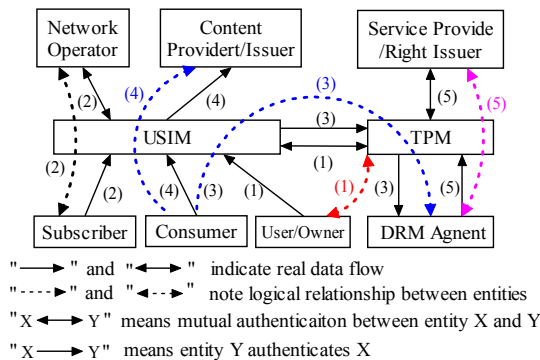


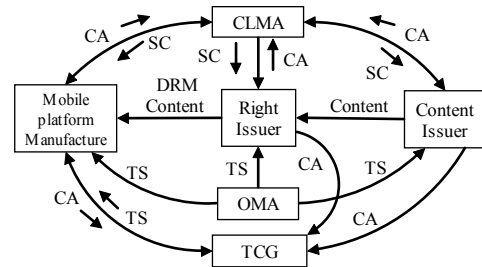
Figure 3. Authentication in TMP-based DRM system

2.4 Compatibility and interoperability between TC and DRM

Our scenario of solution to offer compatibility and

interoperability between TCG and OMA DRM is depicted in Fig.4. Where Content Management License Administrator (CMLA) [16] is a licensing and compliance entity formed to provide a full solution implementation of the OMA DRM v2 interoperability specification.

On one hand, CLMA issues security certificates (SC) to RI, CI and DRM Agent to establish trust relationship. OMA offers technical specifications (TS) e.g., OMA DRM v2, to RI and CI as well as mobile platform manufacture. Mobile platform manufacture also conforms the TMP specifications provided by TCG to support TC in ME. On the other hand, CI, RI and mobile platform manufacture provide compliance assurance (CA) to TCG and CLMA separately. The compliance assurance provided by RI and CI to TCG is mainly shown in support on TMP's remote attestation.



Mobile Platform includes hardware and software

Figure 4. Compatibility and interoperability between TCG and OMA DRM

III. BASIC DOWNLOAD PULL MODEL

As shown in Fig.5, we take basic download pull model, which is the mainstream method of content distribution in mobile DRM system, as a specific example to describe how trusted computing is combined with OMA DRM in our scheme. The first two authentication phases presented in subsection 2.3 will not be discussed again within this scope on the premise that subscriber has accessed the mobile network successfully. Here we only focus on depicting the difference between our download pull model and the original scheme. The detail information isn't mentioned hereafter can be regarded in compliance with the original scheme (see section 5.1 in [5]). The detail procedure is described as the follows:

- (1) USIM checks the integrity and validation of TMP. Then TPM verifies the integrity of DRM Agent.
- (2) DRM checks the identity of consumer is valid via USIM and TPM. The digital signature could be utilized as a specific method.
- (3) Consumer selects content from website he wants to purchase and then will be identified by CI before he download the DCF. A lightweight unidirectional authentication scheme should be designed here as specific method to resist QoS attack.
- (4) If the consumer is authenticated, the protected DCF accompanied with ROAP trigger is sent to DRM Agent. Where S_1 encrypted with DRM Agent's public key is

embedded in DCF. Meanwhile, CI negotiates RO with RI in which S_2 encrypted by RI's public key is embedded.

- (5) On receipt of ROAP trigger, DRM Agent launches the registration phase in accordance with OMA DRM v2. The mutual authentication between DRM Agent and RI should be enforced during this phase with the help of online certificate state protocol (OCSP).
- (6) If the received registration response is valid DRM Agent initiates the RO acquisition phase and transfers its integrity metrics to RI via Integrity Report Protocol (refer to section 5.5 in [14] for detail). Before responding the RO to DRM Agent, RI should turn to trusted authority to verify the validity of the integrity metrics via Validation Data Protocol (see section 5.4 in [14]) so as to check the current state of DRM Agent and TMP is valid. Then S_2 encrypted by DRM Agent's public key and embedded in RO is sent to ME.
- (7) DRM Agent retrieves two key seeds from CDF and RO separately and computes $CEK=KDF(S_1, S_2)$. Where KDF is a key derivation function shared between CI and DRM Agent. Then DRM Agent can decrypt DCF with the CEK and enjoy the downloaded content.

3 CONCLUSION

With the steady increase of digital media distribution over wireless networks, digital rights management is becoming a required system component in the mobile industry. The currently issued OMA DRM v2 specifications are expected to provide a controlled consumption of digital content to protect the intellectual property rights in mobile networks. However, they have been facing the following potential risks according to our analysis in this paper:

- (1) Current mobile platforms including its software and hardware are insecure.
- (2) OMA DRM systems don't provide a way to protect digital content from the RI.
- (3) The uncontrolled download may result in possible DoS attack on CI and wireless network operator.

The concepts and features of OMA DRM associated with TC are presented in this paper to provide a new way for mobile DRM system. How to offer interoperability and compatibility between TC and OMA DRM are also discussed so as to support more feasibility of mobile DRM in real market. Then a TMP-

based DRM scheme is proposed for mobile networks to solve the existing security flaws in current OMA DRM system. Since some key features of TC are beneficial to satisfy critical requirements of DRM system, we argue that the TMP in conjunction with OMA DRM may offer a considerably more robust DRM system for future mobile networks.

ACKNOWLEDGMENT

This work was partially supported by the National Laboratory for Modern Communication Foundation of China under Grant No.51436050404QT2202.

REFERENCES

- [1] Digital right management for mobiles. <http://www.tml.hut.fi/Opinnot/T-109.551/2004/reports/DRMforMobiles.doc>.
- [2] Yu Hong Heather. "On content protection for mobile consumer multimedia applications," In proc. IEEE International Conference on Multimedia and Expo, Taipei, Taiwan, vol.1, pp.439-442, 2004.
- [3] Open Mobile Alliance. <http://www.openmobilealliance.org>.
- [4] OMA DRM Specification v1.0. http://www.openmobilealliance.org/release_program/drm_v10.html.
- [5] OMA DRM Specification v2.0. http://www.openmobilealliance.org/release_program/drm_v20.html.
- [6] Tobias M., Heiko R. "How secure are current mobile operating systems," <http://sec.isi.salford.ac.uk/cms2004/Program/CMS2004final/p2a2.pdf>.
- [7] Stephen P., Reinhardt B. "An Investigation into Access Control for Mes," <http://www.infoseca.co.za/proceedings2004/035.pdf>.
- [8] Zheng Yan. "Mobile Digital Rights Management," <http://www.iprsystems.com/whitepapers/Mobile-DRM-WP.pdf>.
- [9] Trimeche M., Chebil F. "Digital rights management for visual content in mobile applications," In proc. International Symposium on Control, Communications and Signal Processing, pp.95-98, 2004.
- [10] TCG. <https://www.trustedcomputinggroup.org/>.
- [11] Reid, Jason F and Caelli. "DRM, Trusted Computing and Operating System Architecture," In proc. Workshop on Information Security, Newcastle, Australia, 2005.
- [12] Trusted Mobile Platform Hardware Architecture Description. http://www.trustedmobile.org/TMP_HWAD_rev1_00.pdf.
- [13] Trusted Mobile Platform Software Architecture Description. http://www.trustedmobile.org/TMP_SWAD_rev1_00.pdf.
- [14] Trusted Mobile Platform Protocol Specification Document. http://www.trustedmobile.org/TMP_Protocol_rev1_00.pdf.
- [15] TPM Main Part 2 TPM Structures TCG PUBLISHED. https://www.trustedcomputinggroup.org/downloads/tpmwg-mainrev62_Part2_TPM_Structures.pdf.
- [16] CMLA. <http://www.cm-la.com>.

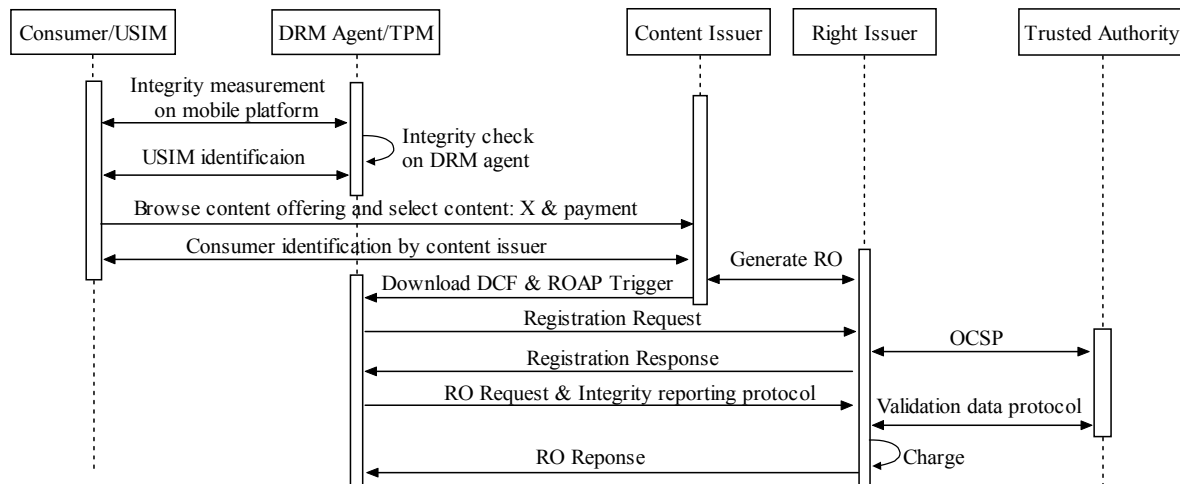


Figure 5. Basic download pull model in our proposed TMP-based DRM system