Send Orders for Reprints to reprints@benthamscience.net

34 *The Open Electrical & Electronic Engineering Journal,* 2014, *8,* 34-41

Open Access

Trusted License Distribution System Based on IPSec VPN for Mobile DRM

Jian Wang*, Zhiyong Zhang, Fei Xiang and Weihua Yu

College of Electronics Information Engineering, Henan University of Science and Technology, Luoyang, 471023, China

Abstract: With the rapid development of mobile applications, DRM systems used for mobile terminals and wireless environment become popular. However, the present DRM schemes are not fit for mobile applications because of the new security problems in wireless environment and the limitations of mobile terminals. In this paper, a trusted license distribution system based on IPSec VPN and its correlative issues are presented. This system supports DRM clients to build IPSec VPN connection based on trusted authentication with DRM license server, and obtains license through secure tunnel. Implementation and testing indicate that the security and efficiency of the proposed scheme can reach the requirement of the mobile DRM.

Keywords: DRM, IPSec VPN, multi-factor authentication, trusted authentication.

1. INTRODUCTION

Digital Rights Management (DRM) is a technology that protects content owner rights when selling and distributing content online in a digital form [1]. DRM also introduces new ways of selling, distributing and consuming content that can be considered as important as the prevention of piracy. With the rapid development of mobile access networks and popularization of mobile devices such as intelligent phone and PDA, digital content usage and distribution on mobile terminals become more and more popular, which leads to the mobile DRM becomes a research hotspot. There have been various DRM schemes [2-9] proposed. However, these schemes are not suitable for mobile DRM, because mobile DRM systems and its protocols usually face more problems than common DRM do. Firstly, for the opening of wireless network and the mobility of the terminals, mobile DRM is confronted with more serious threats than DRM in fixed-IP networks. The manifestations include: (1) The data transmitted through wireless networks has more possibility of suffering interception, modification and replay attack. (2) Mobile terminals are easier to be stolen or suffer virus invasion, which makes them to be easily used by people with ulterior motives. Secondly, some of the limitations arise from the mobile devices themselves: have limited processing power, memory, and data transmission capabilities and thus cannot use as strong and complicated encryption technologies as PCs connected to the broadband Internet. So, the design of the mobile DRM system must consider the characteristics of mobile terminals.

Some schemes [10-14] were specially designed for mobile DRM, but these schemes only tried to reduce the computational cost, without enough consideration about mobile terminals security. Relatively, some other schemes did researches on trusted computing based DRM system to avoid dangers from malicious terminals. Stamm *et al.* [15] and Yu *et al.* [16] presented TPM-based DRM architectures separately, and Yan *et al.* [17] presented a remote authentication protocol based on integrity attestation. However, these schemes are not suitable for mobile applications. The Open Mobile Alliance (OMA) [18] has been working on mobile DRM to introduce and promote open standards and specifications for the application and services over mobile networks. Its version 2.0 specifications [19] is thought to be more secure than version 1.0, which 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. Nevertheless, only identity authentication cannot guarantee DRM agents or terminals are trusted for the unsecure mobile operating system or malicious software. What's more, version 2.0 requires the DRM terminals have the abilities of hash, signature, generating nonce, and encrypt/decrypt. Most smart mobile terminals in market cannot support it, which makes it difficult to be generalized.

This paper presents a trusted license distribution system for mobile DRM according to the OMA DRM 2.0 architecture and its implementation. The scheme supports trusted authentication based on remote attestation extended IPSec between the mobile client and the DRM license server.

2. RELATED LITERATURE

2.1. Trusted Computing Enabled DRM System

The typical architecture of a DRM system is consisted of three main modules: content server, license server, and DRM client. The DRM client usually includes DRM agent and digital content usage tool. The difference between the DRM system based on trusted computing and the common DRM

1874-1290/14

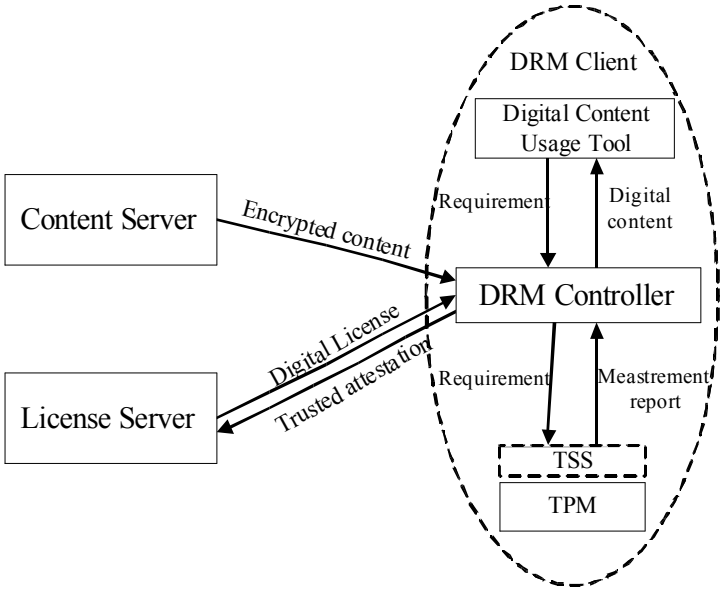

Fig. (1). Architecture of trusted computing enabled DRM.

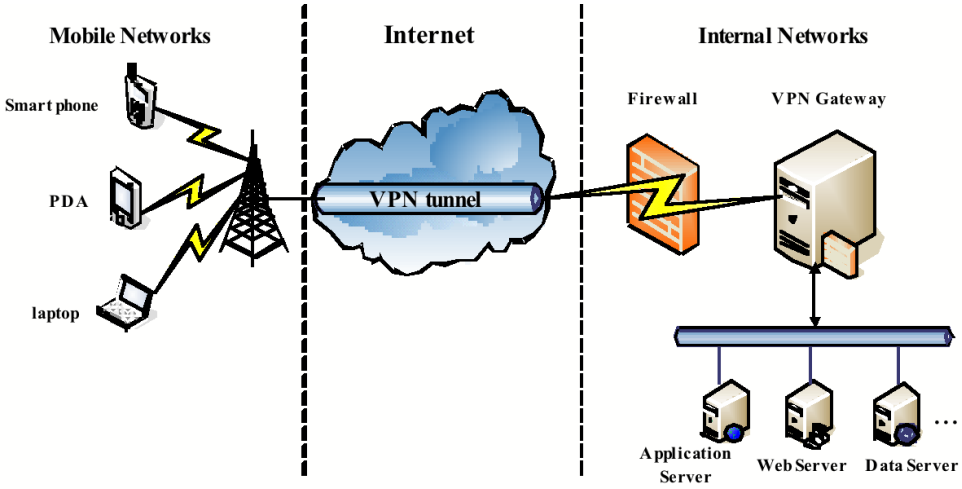

Fig. (2). Mobile VPN network topology.

system is the former's client contains a TPM chip, and implement trusted authentication using TPM (Trusted platform Module) and TSS (TCG Software Stack) [20]. The architecture of DRM system based on trusted computing is illustrated in Fig. (**1**).

The content server is responsible to generate the digital content and the corresponding license for the owner or creator. The content distributed by the content server is encrypted and can only be used with digital license. The license server manages the license on behalf of the owner and distributes it to the consumer. So, the security of the license decides the usage security of digital content, and the license distribution is a key scenario that the DRM system must control.

2.2. Mobile VPN

A mobile virtual private network provides mobile devices with access to network resources and software applications on their home network, when they connect via wireless networks. It integrates standards-based authentication and encryption technologies to secure data transmissions to and from devices and to protect networks from unauthorized users. The functioning of an effective mobile VPN is transparent to the end user without compromising security or privacy. A typical mobile VPN network topology is illustrated in Fig. (**2**). In this environment, a VPN client uses a mobile terminal to build connection with the internal information system through the public mobile networks (CDMA/GPRS/3G). The typical information exchanging process is described as following:

(1) The mobile terminal originating the request to access Internet; the mobile network gateway receives the request and allocates a public IP for the terminal after the identity authentication.

(2) The mobile terminal then originating a request to the VPN gateway to build a VPN connection with corresponding certificates. Then, the VPN gateway verifies the identity and credibility of the mobile terminal. After certifying the client

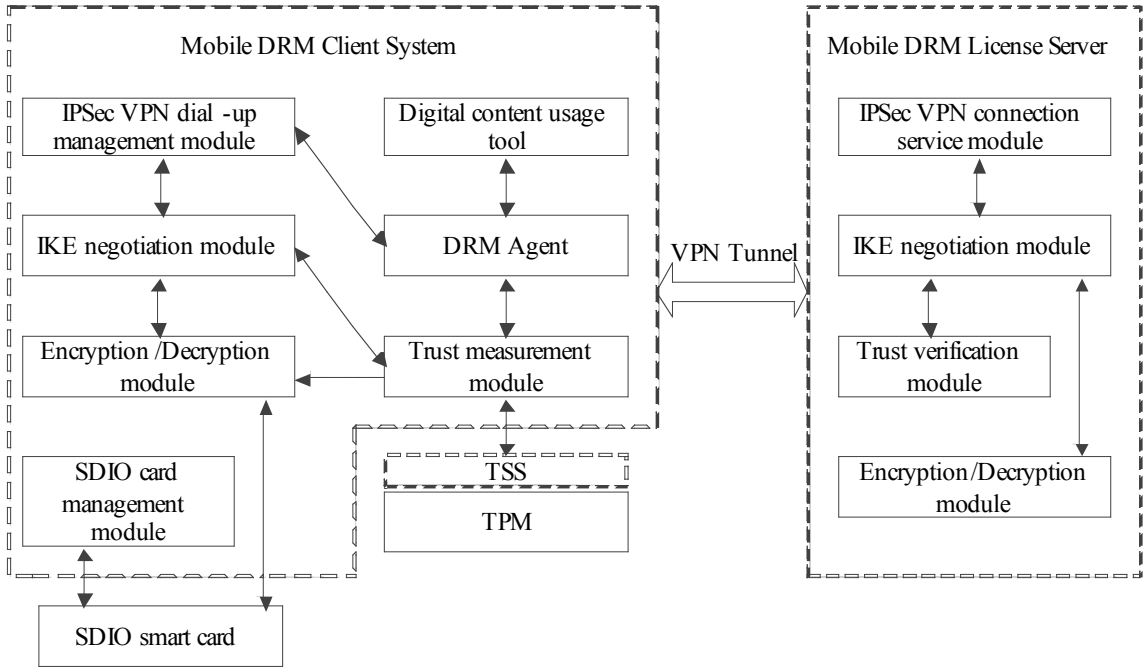

Fig. (3). Architecture of trusted authentication enabled mobile DRM based on IPSec VPN.

is legal, the gateway permits the access and provides services to the client.

(3) The application server in the internal network returns the processing result to the client through the Internet and mobile network in encrypted way. And then, the results are displayed on the mobile terminal.

During the information exchanging between the mobile terminals and the VPN gateway, the data is transmitted through a complicated network environment consisting of mobile networks, Internet and home networks. All kinds of probable threatening from servers, communication links and mobile terminals make the mobile VPN faces more serious security problems [21, 22].

VPN technology can be implemented by several security protocols on different network layers, including PPTP and L2TP on data link layer, IPSec on network layer, SOCKS on session layer, and SSL on application layer. IPSec (IP Security Protocol) becomes the main solution scheme to build mobile VPNs for its characteristics such as high flexibility, excellent extensibility and strong independence for applications. And some researches [23, 24] presented schemes for mobile VPN based on IPSec.

2.3. Remote Attestation Extension for IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Usually, IPSec is a good choice to build mobile VPN between server and a mobile terminal to realize the secure wireless access. The IP security architecture uses the concept of a security association as the basis for building security functions into IP. Security associations are established using the Internet Security Association and Key Management Protocol (ISAKMP), which is implemented by manual configuration with pre-shared secrets, or Internet Key Exchange (IKE and IKEv2), and the latter is thought to be more secure way to implement identity authentication.

However, in 2011, we [25] argued that standard IPSec does not provide any guarantees about the integrity of the endpoints when an IPSec linkage is established. Then, we presented the method of remote attestation extension for IPSec, introducing TCG remote attestation into IKE negotiation of IPSec, to avoid terminal security vulnerability. The extended IPSec protocol can complete double authentications including identity and system integrity to ensure an end-to-end secure linkage. Besides, the extended protocol can guarantee not only confidentiality, integrity and freshness, but also endpoints' privacy. So, in the proposed mobile DRM system, we use remote attestation extended IPSec to build mobile VPN between the DRM client and the server when the digital license is distributed.

3. THE PROPOSED MOBILE DRM SYSTEM ARCHITECTURE AND DESIGN ISSUES

3.1. The Architecture of Mobile DRM Client and License Server

The client and license server architecture of the trusted authentication enabled mobile DRM based on IPSec VPN is illustrated in Fig. (**3**). The mobile DRM client system is

Table 1. IPSec dial-up policy.

Policy	Condition	Method
IPSec	No NAT or Firewall	Standard IPSec
IPSec+NAT-T	Only NAT exists and the communicating peer supports NAT-T	UDP encapsulation to ESP packets Medium
Improved IPSec + NAT-T	Both NAT and firewall (or ISP proxy) exist	Port transformation: UDP500↔UDP53 UDP4500↔UDP80

software designed based on SDIO smart card and TPM chip, consisting of seven main modules as shown in the above figure. ***DRM agent*** is responsible for enforcing permissions and constraints associated with DRM content, as well as controlling access to DRM content. Besides, it initiates the connection to the server through invoking ***IPSec VPN dial-up management module*** when the client requests license. The dial-up module is responsible for connection building/deletion, configuration, status query/management, and so on. When building VPN connection, ***IKE negotiation module*** will be invoked to complete the mutual authentication and key agreement with the communicating peer. Here, the IKE negotiation protocol has been remote attestation extended to realize trusted authentication. The trust measurements used in IKE negotiation comes from ***Trust measurement module***, which collects PCRs value from TPM and SML (Stored Measurement Log) from the system. To further strengthen access security, user's private key is designed to be a hard key which is stored in a SDIO intelligent card with the certificate for VPN building as soon as it is generated and can't be taken out for ever. And the ***SDIO card management module*** provides an interface to access or manage the smart card. ***Encryption/ Decryption module*** calls the digital certificates, signature private keys, and encryption interfaces provided by the smart card when encryption or decryption operations occur during trusted authentica-tions. ***Digital content usage tool*** is same as it ever is in common DRM client systems.

The mobile DRM license server is consisted of the corresponding modules to support the building of VPN based on remote attestation extended IPSec. Here, it acts as not only a DRM server, but also an IPSec VPN gateway. So, it includes at least four modules as ***IPSec VPN connection service module***, ***IKE negotiation module***, ***Trust verification module***, and ***Encryption /Decryption module***.

3.2. Adaptive VPN Dial-up Connection

NAT and firewall traversal is a traditional problem that IPSec VPN faces. Besides, ISP limit is a new possible trouble in mobile networks. Considering intelligence and flexibility, the system adopts an adaptive policy, voluntarily detecting and intelligently choosing VPN connection way. This function is provided by ***IPSec VPN Dial-up Management module*** in the mobile DRM client. The policies and the corresponding web environment are listed in Table **1**.

Policy (1) carries out standard IPSec with the lowest cost. Policy (2) is aiming at NAT traversal, resolving it through UDP encapsulation to ESP packets. This method decreases the actual load, and increases cost. Policy (3) is mainly designed for the condition that there is packet-filter firewall or ISP proxy which closes IPSec normal communication port (UDP500 and UDP 4500). In this policy, the UDP encapsulated packets by policy (2) are intercepted in NDIS (Network Driver Interface Specification) layer and forwarded after transforming their ports to UDP53 and UDP80 separately which are not closed generally. Then, at the DRM server, they will be contrarily transformed. In this way, no more additional load than policy (2) is produced, but the cost is raised further.

To implement the policy, the IPSec VPN dial-up management module in DRM client sends UDP detective packets through normal ports to identify whether the IPSec communication UDP ports are open. Locations of NAT devices and whether the communicat-ing peer supports NAT-T can be acquired through phase 1 in IKE negotiation [26]. The flow chart of the system's adaptive dial-up policy implementation is shown in Fig. (**4**).

3.3. Multi-factor Trusted Authentication

Considering efficiency and security, the proposed system combines the multi-factor identity authentication based on SDIO smart card with integrity authentication based on remote attestation in trusted computing. The DRM client user will be issued a SDIO card with his certificates in it when he successfully registers to the DRM system, and define his PIN to approve he is the legal owner of the card. When the DRM user requires building VPN connection with the DRM license server, he must insert the smart card into his mobile device, and input PIN. Only if the PIN is correct, he can call the dial-up program through visual interface and use the certificates in card to perform IKE. The registration information includes mobile phone number, IMEI (International Mobile Equipment Identity), and IMSI (International Mobile Subscriber Identity), which constitute the initiator identity load used in IKE.

The remote attestation extension for IPSec is actually the extension for IKE through introducing the integrity attestation into its process. The information flow of the extended IKE is related to the four entities: The mobile DRM client system, the SDIO card, TPM, and the DRM server. It is

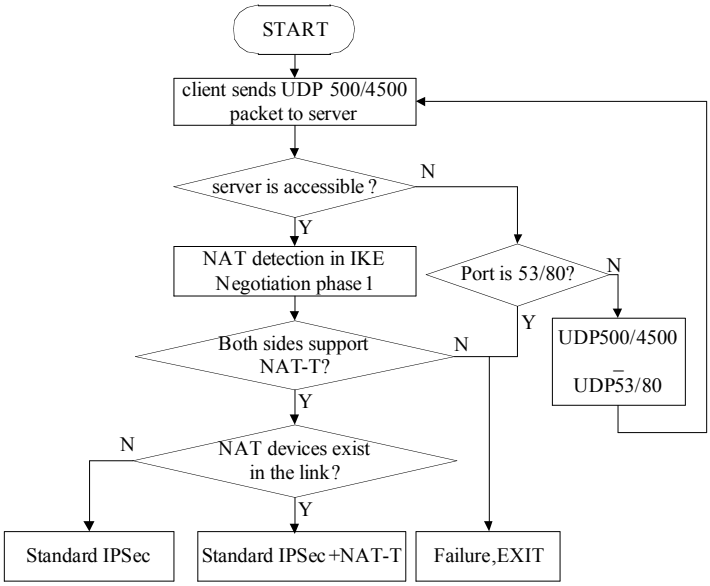

Fig. (4). Flow chart of adaptive dial-up policy.

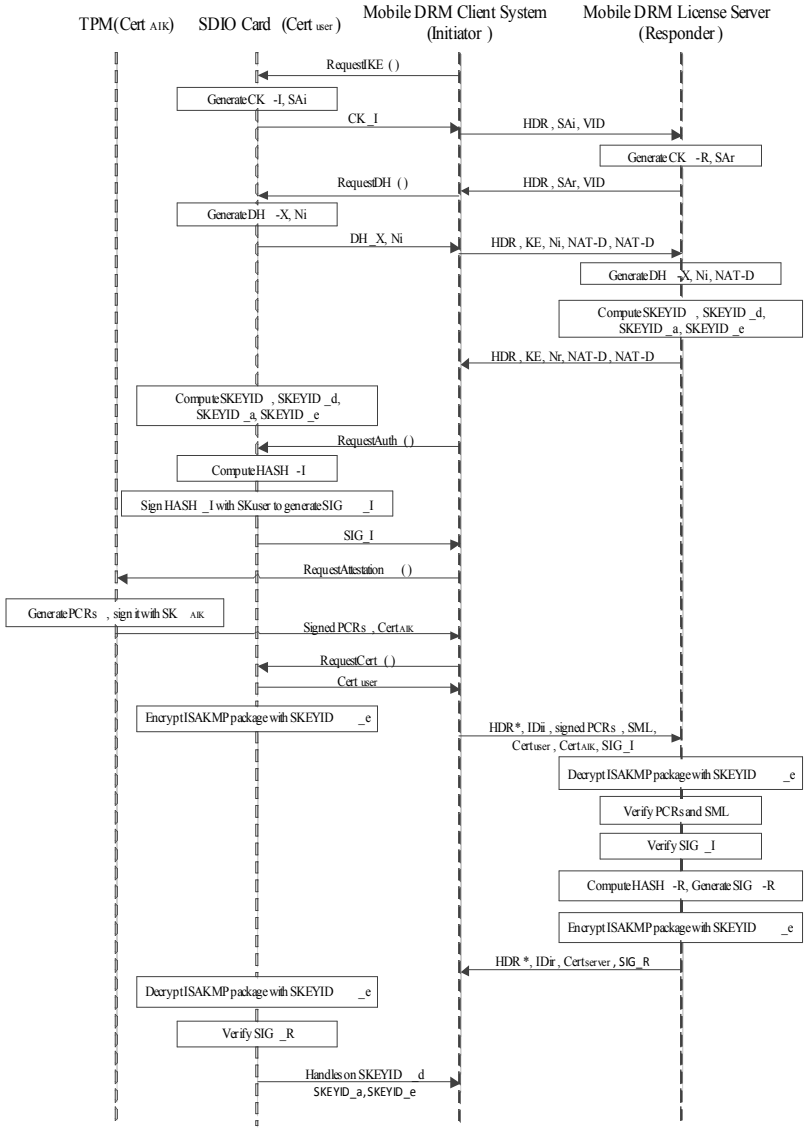

Fig. (5). Flow chart of remote attestation extended IKE.

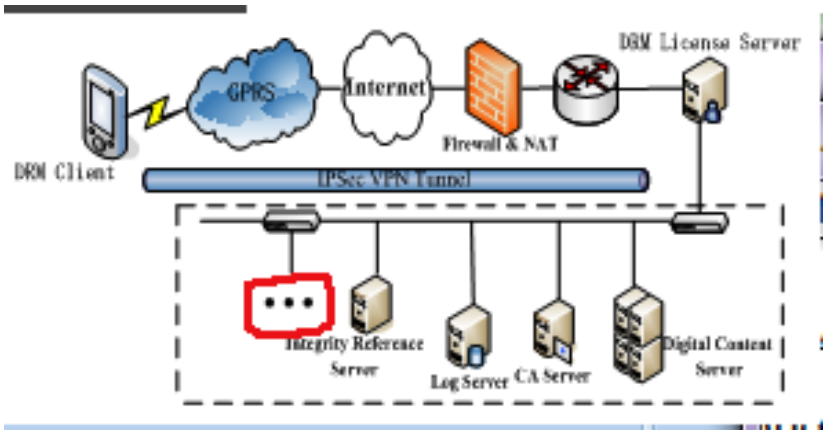

Fig. (6). Test network topology.

illustrated in Fig. (**5**) and the correlative denotations are shown as below.

HDR: ISAKMP head, * shows the load after ISAKMP head is encrypted;

CK-I: the initiator's cookie in ISAKMP head;

CK-R: the responder's cookie in ISAKMP head;

SA: Security Association load with one or more suggested load;

VID: vendor ID (an IKE load, shows whether the negotiating party supports NAT-T);

DH-X = g^x mod p: initiator's Diffie-Hellman public value;

DH-Y = g^y mod p: responder's Diffie-Hellman public value;

Ni/Nr: 20/16 bytes nonce;

IDx: identity load, x is ii or ir，ii is ISAKMP initiator，ir is ISAKMP responder;

<P>_b: the body of load <P>, it's a load without ISAKMP head;

SKEYID = PRF (Ni_b | Nr_b, g^xy);

SKEYID_d = PRF (SKEYID, g^xy | CKY-I | CKY-R | 0) (used to generate IPSec SA key);

SKEYID_a = PRF (SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1) (the key used to authenticate the succeeding ISAKMP information);

SKEYID_e = PRF (SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2) (used to encrypt keys exchanged in ISAKMP);

HASH_I = PRF (SKEYID, DH-X| DH-Y | CKY-I | CKY-R | SAi_b | IDii_b);

HASH_R = PRF (SKEYID, DH-Y | DH-X | CKY-R | CKY-I | SAi_b | IDir_b);

SIG_I: the signed HASH_I load;

SIG_R: the signed HASH_R load.

4. EFFICIENCY AND SECURITY

A real network environment has been built to test the availability and performance of the trusted mobile DRM system. The DRM client terminal (Sharp PDA) firstly builds connection to GPRS mobile networks and acquires a public IP (192.168.0.102). Then it can establish IPSec VPN connection with DRM license server when it requires digital license. Once VPN connection is built, it will be allocated a private IP as fixed-IP from the internal IP address pool (10.199.199.1-10.199.199.254) by the DRM License Server. Then, the DRM clients can securely access the DRM license server to get digital license. The test environment is shown in Fig. (**6**), and Table **2** presents the system configuration information.

4.1. Function Evaluation

Through black-box testing, it's validated that the proposed system supports DRM clients to build IPSec VPN connection with DRM license server, and implements the following functions:

(1) The proposed system provides multi-factor authentication combined with trusted authentication. Only if the DRM client owes both SDIO card distributed by the DRM server and PIN, he can use the mobile terminal to dial. Meanwhile, only if the identity certificate and the AIK certificate are valid and the terminal integrity passes the verification, the IKE can be completed.

(2) The proposed system is able to adjust dial-up policy to establish connection according to different conditions. It can support NAT traversal and firewall/ ISP proxy traversal.

(3) Through sniffing and interception test, it is verified that all the communication data is encapsulated in ESP mode and transmitted in encrypted form.

4.2. Efficiency Evaluation

To a wireless secure access system, the time performance is an important target. As illustrated in the Fig. (**5**), all the encryption/decryption or signature operations are completed in SDIO card or TPM. It's designed for not only security, but

Table 2. Trusted Mobile DRM System Configuration Information.

Entity	Hardware Parameter	Software Parameter
mobile terminal (Sharp Zaurus SL- 5600 PDA)	Processor: Intel PXA-250 , 400 MHz; Memory: 32M SDRAM, 64M ROM; Intelligent card: SD/MMC, supports SDIO.	Linux 2.4 Embedix kernel; Qtopia; TPM Emulator; GUN MP 4.1; TrouSerS TSS 1.2;
mobile networks (China Mobile GPRS)	Upload speed: 26.8kbps; Download speed: 53.6kbps.	None
DRM license server	Processor: P4 3.0G dual-core processor; Memory/Hard Disk: 1G/160G.	Linux Kernel 2.6.23; MySQL4.0.14; Openswan 2.4.7; L2TP 1.1.09;

also the efficiency, because of the limited computational ability of the mobile terminals.

For efficiency analysis, we tested the time from the DRM clients sending connection request through mobile terminals to the connection being built successfully, and compared it to the corresponding time of the common IPSec VPN system. In GPRS environment, the average connection/ disconnection time for VPN of 20 tests in the proposed trusted mobile DRM system is 13.5 s/0.8 s. And the comparison of the average connection building time between the presented system and a common IPSec VPN indicates that it needs about 1 more second to build the trusted connection than a common VPN connection. The time cost will not affect the users' experience; meanwhile, the security is improved largely.

4.3. Security Analysis

The proposed system is designed for mobile terminals and wireless application environment. The security of the system can be concluded as the following aspects:

(1) The proposed system reaches all the security performance of IPSec VPN. The system has all the basic security functions including data source identity authentication, secure data transmission, data integrity protection, resisting replay attack, and so on.

(2) The proposed system provides trusted authentication combined with multi-factor authentication. The DRM client must own the SDIO smart card and have its PIN to login the system, and when he builds connection with the DRM server, the identity and integrity of the mobile terminal will be checked. If any factor does not match, the DRM license server cannot be accessed. So, the authentication mechanism is an all-around scheme combining software and hardware, identity and integrity. It improves the security of the mobile DRM system greatly.

(3) The proposed system provides secret protection for mobile terminals. The SDIO card is a hard key to store DRM client's private key and certificates, and the private key never appears outside the SDIO card. During the IKE, all the encryption/decryption and signature happen in the card or TPM chip. The mobile terminal doesn't take part in any computation or keep any keys, thus, even if it is stolen, the keys and certificates cannot be obtained by others.

5. CURRENT & FUTURE DEVELOP-MENTS

Aiming at the security problems of mobile DRM system used for wireless environment and the mobile terminals, we presented a trusted DRM license distribution system for mobile DRM system. The architecture and the correlative issues of the system are described in detail. The system supports DRM clients to build trusted connection with the license server and obtain digital license through secure tunnel. Besides, the adaptive VPN dial-up policy guarantees the connection can be built whatever the network condition is. What's more, we implemented the system in a real wireless network environment, and test its function and efficiency. It's verified that the system can improve the security of mobile DRM significantly with relatively smaller time cost. Computational cost can be improved for proposed scheme as future works.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was sponsored by National Natural Science Foundation of China Grant No.61003234, Key Program for Basic Research of The Education Department of Henan Province Grant No.13A520240 and No.14A520048, Plan for Scientific Innovation Talent of Henan Province Grant No. 134100510006.

REFERENCES

[1] Z.Y. Zhang. Security, "*Trust and risk in digital rights management ecosystem*", Beijing: Science Press of China, 2012.

[2] B. Wouter, K.F.L.A Johannes, L.P. Johannes, and S. Lukasz, "*DRM system*", U.S. Patent 20080229387 A1, September 18, 2008.

[3] C. David, and L. Paul. "File system operation and digital rights management", U.S. Patent 8640256, Jan. 28, 2014.

[4] Q.l. Huang, Z.F. Ma, J. Mo, X.X. Niu, Y.X. Yang, "Design and implementation of a novel general format multimedia digital rights management system," *J. Comm.*, vol. 34, pp. 153-161, 2013.

[5] M. Dheerendra, and M. Sourav. "Towards a secure, transparent and privacy-preserving DRM system," *Comm. Comp. Inform. Sci.*, vol. 335, pp. 304-313, 2012.

[6] G. Francisco, Jr. Shrum, and V. Edgar, *"Content protection and digital rights management",* U.S. Patent 20100058485 A1, March 4, 2010.

[7] T. Ta Minh, and I. Muneroshi. "A proposal of digital rights management based on incomplete cryptography using invariant Huffman code length feature," *Multimedia Syst.*, vol. 20, pp. 127-142, 2014.

[8] C.L. Chang, and J.H. Yang. "A group-oriented digital right management scheme with reliable and flexible access policies," *Int. J. Net. Sec.*, vol. 5, pp. 471-477, 2013.

[9] Q. Qin, Z. Tang, F.H. Li, and Y.Y. Yu. "A personal DRM scheme based on social trust," *Chinease. J. Elect.*, vol. 21, pp. 719-724, 2012.

[10] D.R. Jason., E.M. John, and A.N. Jarrod, *"Digital rights management for mobile devices",* U.S. Patent 7812854, Oct. 12, 2010.

[11] R.W. Shane., B.C. Warren, and Mc.C. Von, *"Application digital rights management (DRM) and portability using a mobile device for authentication"*, U.S. Patent 8353048, Jan. 8, 2013.

[12] C. Yi, B. Luis, and N. Karl, *"Method for digital rights management in a mobile communications network",* U.S. Patent 8417952, April 9, 2013.

[13] S.L. Yang, and J.P. Hu, "Research on ECC-based mobile internet digital rights management," *Lect. Notes. Elect. Eng.*, vol. 1, pp. 515-520, 2014.

[14] L. Wang, and R. Zhang, "An improved authentication approach for mobile DRM systems," *Adv. Info. Sci. Serv. Sci.*, vol. 4, pp.198-206, 2012.

[15] S. Sid, P.S. Nicholas, and S.N. Reihaneh, "Implementing trusted terminals with a TPM and SITDRM," *Electron. Notes. Theo. Comp. Sci.*, vol. 197, pp. 73-85, 2008.

[16] A. Yu, D.G. Feng, and R. Liu, "TBDRM: A TPM-based secure DRM architecture," *Int. Conf. Comp. Sci. Eng.*, pp. 671-677, 2009.

[17] J. H.Yan, X. G. Peng, "Security strategy of DRM based on trusted computing," *J. Comp. Inform. Sys.*, vol. 7, pp. 3226-3234, 2011.

[18] Open Mobile Alliance. Available at: [http://www.open mobilealliance. Org]

[19] OMA DRM Specification v2.0. Available at: [http://sec.isi.salford.ac.uk/cms2004/Program/CMS2004final/p2a2.pdf]

[20] Grawrock D. TCG Specification Architecture Overview Revision 1.4.
Available at: [EB/OL].https://www.trustedcomputinggroup.org/-groups/TCG_1.4_Archiecture_Overview.pdf.

[21] C.N tantofian, and C. Xenakis, "A security protocol for mutual authentication and mobile VPN deployment in B3G networks," In: *the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1-5, 3-7, Sep. 2007.

[22] A.V. Uskov, "Information security of mobile VPN: Conceptual models and design methodology", in The IEEE International Conference on Electro/ Information Technology, pp. 1-6, 6-8, May 2012.

[23] V. Uskov, Uskov, Alexander U.V, "Information Security of IPsec-based Mobile VPN: Authentication and Encryption Algorithms Performance", In: *11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1042-1048, 2012.

[24] W. Qu, S. Srinivas. "IPSec-based secure wireless virtual private network", in 2002 MILCOM, California, pp. 1107-1112, 7-10, Oct. 2002.

[25] J. Wang, H.H. Wang, J. Yang. "Remote Attestation Extension for IPSec", *Comp. Sci.*, vol. 38, No. 6, pp. 49-53, 2011.

[26] T. Kivinen, B. Swander, A. Huttunen, *et al*. RFC 3947. Negotiation of NAT-Traversal in the IKE. RFC Editor, Jan 2005.

Received: June 09, 2014 Revised: June 22, 2014 Accepted: July 24, 2014