I.J. Information Technology and Computer Science, **2011, 1, 54-62**
Published Online February 2011 in MECS (http://www.mecs-press.org/)

Trusted Mobile Client for Document Security in Mobile Office Automation

Xiaojun Yu
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, China
yuxiaojun@bupt.edu.cn

Qiaoyan Wen
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, China
wqy@bupt.edu.cn

***Abstract*—Mobile Office Automation is a popular application on the mobile platform. However, the mobile platform has no enough security protection in front of the open system, such as internet. The document security problem in this application has become a hot topic. This paper proposed a new solution to this problem. The solution based on the trusted computing technology, which implements the platform security by hardware. The solution also includes the transparent encryption technology that means application could run independent to the security module and keep the consistency of user experience. The trusted mobile client platform architecture and security functions process of the mobile document protection system are detailed. Related work also been introduced; the security analysis shows the proposed solution could provide well security enhancement for document protection in mobile platform.**

***Index Terms*—document security; mobile office automation; mobile trusted computing; transparent encryption**

I. INTRODUCTION

As the development of mobile communication technology , the mobile device has played a very important role in daily life. We use the mobile phone not only as a communication tools, but also a work assistant. In many company, the mobile office automation (MOA) is very popular because the staffs of company could work any time and anyplace.

However, the security status is very worrying . The mobile devices typically lack the necessary security measures like firewall, anti-virus and so on. In other side, the mobile devices are difficult to administer centrally.

With the popular of mobile devices, the mobile devices have become the new target of attackers. Thus, protect sensitive information in application of MOA from attack has become an important issue.

According to the security requirements of mobile office automation, this paper proposes a security mobile protection solution. A trusted mobile client for the document security is designed. The solution integrates the trusted computing and application transparent encryption. The idea of transparent encryption is that the application running independent on encryption procedure or the encryption and decryption don't have influence to application directly. This technology or design idea could be said a kind of filtering technology that an addition filtration layer exists in the normal data process.

The trusted computing is initially developed for protecting the pc environment based on hardware protection technology. This technology has been used in mobile devices now, which is MTM[6].with the trusted computing, many security requirements could be easily realized, such as secure document transport, remote authentication for mobile platform, secure documents storage and so on.

The paper is organized as following: part II gives the threats around the mobile platform; part III is core of this paper, the detail design of the solution and solution security analysis; related work is list in part IV. The last part is conclusion and the direction for further research。

II. THREATS TO MOBILE DEVICE

Security threats to mobile devices include the following items, which are discussed in more detail below [1]:

A. Loss, Theft, or Disposal

The size of mobile devices small that means mobile, at the same time, they are easy to be lost or stolen. If there are not proper measures, the devices could be activated, and be access straightforward, potentially exposing sensitive data that resides on the device. There are many tools that can be used to recover erased data from the flash memory.

Besides the compromise of its logical and physical data, a cell phone with active service could be used

indiscriminately to place toll and international calls and accumulate charges for the subscriber.

B. Unauthorized access

Through some methods, attackers can forging or guessing authentication credentials, or bypassing the authentication mechanism entirely.

Most mobile devices users seldom employ security mechanisms built into a device, and even using them, the settings can be easily determined or broken. If the mobile device is incorrectly configured, the devices are vulnerable.

The weaknesses in the authentication method are another avenue that can be exploited. For example, some devices may have a reserve password or master password built into the authentication mechanism, which allows unfettered access when entered, bypassing the phone lock set by the user. On certain handsets, the master security code for overriding the phone lock mechanism can be calculated directly from the equipment identifier.

Occasionally a backdoor can be found to bypass all or part of the control mechanism.

Forensic tools and procedures also exist that can be used to bypass built-in security mechanisms and recover the contents of a device. A number of GSM mobile phones allow acquisition with a forensic tool. It is also possible to create substitute SIMs for certain models of phones that fools them into treating the SIM as the original, and allowing access.

Manufacturers often incorporate built-in test facilities or other backdoors into a device that an examiner can exploit to obtain information.

C. Malware

Mobile malware is typically targeted toward mobile devices which has open SDK. Thus, It's is easy to create malware on these platform.

The malware propagation may run through the communication network or mobile storage media, some as following:

- Internet Downloads –A infected file may be download via an Internet connection. The file could be disguised as a game, security patch, utility, or other useful application posted somewhere as a free or shareware download. Even downloads of legitimate applications may pose problems if they contain vulnerabilities that can be exploited by malware.
- Messaging Services – Malware attachments can be appended to electronic mail and MMS messages delivered to a device. Instant Messaging services supported on many phones are another means of malware delivery. The user must choose to open the attachment and then install it for the malware to infect the phone.
- Bluetooth Communications – Bluetooth technology is a convenient way to connect devices and send messages or move files between them. Malware can be delivered by engaging the available connectivity services supported by a device left in discoverable mode.

With all of these delivery methods, the user usually has to give consent for the malware to install and execute. Malware writers use social engineering techniques to get users to carry out the necessary actions.

The range of malware behaviors and subsequent consequences is broad. Malware may potentially eavesdrop on user input or otherwise steal sensitive information, destroy stored information, or disable a device. Malware may also accumulate wireless communications fees against a subscriber, for example, by sending SMS messages or initiating calls to chargeable toll numbers. Propagation onto other handheld devices or even desktop computers may also be attempted by malware to broaden its effect or to perturb the entire communications network.

D. Spam

SMS text messages, email and voice messages from advertisers have begun to appear on mobile phones. Besides the inconvenience of removing them, charges may apply for inbound activity, such as a per-message charge on each SMS message received or charges for those messages above the monthly limit of a service plan.

Data downloads may also cost extra, with each image attachment further escalating costs. Mobile spam may also be used fraudulently to persuade users to call or send text messages to chargeable service numbers using social engineering techniques. Spam can also be used for phishing attempts that entice users into revealing passwords, financial details, or other private data via Web pages, email, or text messages, or to download malware attached to the message or via a Web page.

Instant messaging and multimedia messages are other possible means for malware delivery through spamming. Denial of service is also a possibility using spam techniques. For example, repeated attempts to establish Bluetooth pairing with a phone block the user from being able to initiate a call until the prompt is acknowledged.

E. Electronic Eavesdropping

The most direct way of electronic eavesdropping is for spy software to be installed onto a device to collect and forward information onto another phone or server. Such applications exist for certain phone models and are commonly advertised as a means to monitor a spouse or child's activities.

The capability to remotely turn on the microphone and listen or record conversations in the area is also a feature for some of these tools. Phones with vulnerabilities could allow the spy software to be loaded over an active communications interface.

While communications between a mobile phone handset and cell tower were designed with security in mind, apparent weaknesses exist that can be exploited. Specialized intercept equipment for law enforcement surveillance of cell phone traffic also exists. In a more targeted approach on the network fabric, cell phone switches have been surreptitiously modified to allow eavesdropping on the conversations of subscribers.

F. Electronic Tracking

There are companies now offer location tracking services for registered cell phones to allow the whereabouts of the user to be known by friends and family. The services are also touted as a means to track employees' whereabouts. Registration can take place quickly, making temporary misplaced devices or unattended devices a possible target.

Some tracking services periodically send the phone a notification for the user that monitoring is taking place, and may give the user the option to terminate the service. Other services provide no notification or indication of monitoring to the user, once registration is complete.

Early tracking service was shown to be vulnerable to the possibility of surreptitiously registering someone else's phone for tracking without having possession of the device. For example, if the scheme to complete the registration of a phone requires a positive acknowledgement from the device as confirmation, such as an SMS message reply with an authenticator code, but uses a code value that is predictable or not unique, another means such as an online SMS gateway could be used to forge the response needed to complete registration.

G. Cloning

If certain unique device identifiers built into a cell phone are reprogrammed into a second cell phone, a clone is created that can masquerade as the original. For example, monitoring the radio wave transmissions of analog cell phones allowed the factory-set Electronic Serial Number and Mobile Identification Number from those devices to be obtained easily and used to create clones.

Though not as prevalent today with the rise of digital networks, analog networks may still exist in some rural areas. Technology used in digital cell phone networks improved security during device authentication by using cryptography to thwart device identifiers from being recovered. However, with physical access to a device, cloning of some early generation equipment is possible.

III. DETAIL DESIGNE

A. Design Idea

There are different Mobile platform operating systems, the top OS including window mobile series, symbian series, and open-source Linux series. This paper focus on the open source Linux system

Two problems should be solved in Mobile document protection. One is which security measures should be added, the other is how to achieve transparent encryption protection effective. According to the idea of trusted computing and transparent encryption, we propose the solution as following:

For the first problem: use the MTM based technology to provide related security functions for mobile document security. Before touching the document, the application must be checked integrity status by using the integrity verification, ensuring the application is not modified. When downloading the document from the server, the mobile platform firstly attests to the remote server and supports safe file transmission procedure. In addition, MTM can be used to encrypt the key that used to document transparent encryption and protect the key storage and update.

For the second question: The document encryption module was installed in the VFS layer. The VFS layer is in the kernel, which achieves not only transparent encryption and decryption, but also higher security and efficiency, thus the existing applications don't need modification.Fig.1 shows security module position in Linux platform:

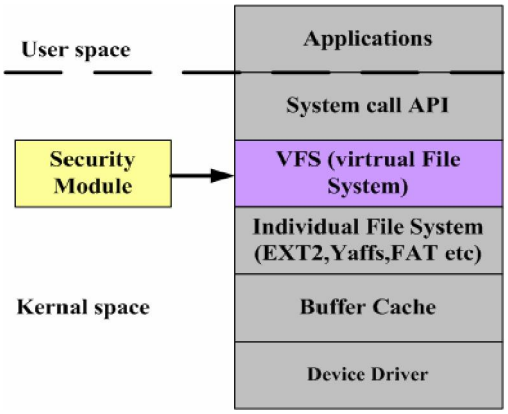

Figure 1. Security module deployment

Although there is many layers could be used to add the document encryption module, the difficult and affecting is different, the more low-level, the more difficult and more dependent on the concrete file system. We think that the document encryption module in the VFS layer could be suitable, because of less modification, supporting different file systems and keeping transparent encryption.

B. Model of Mobile Document Protection System

The whole mobile office system can be viewed as a C/S mode structure, which can be expressed in the following fig. 2:

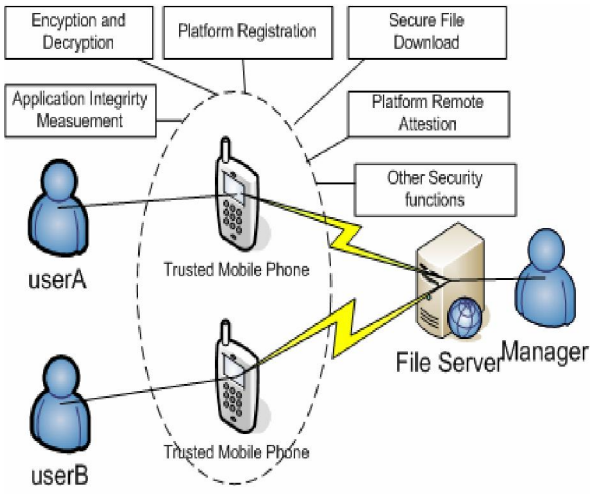

Figure 2. The model of mobile document protection system

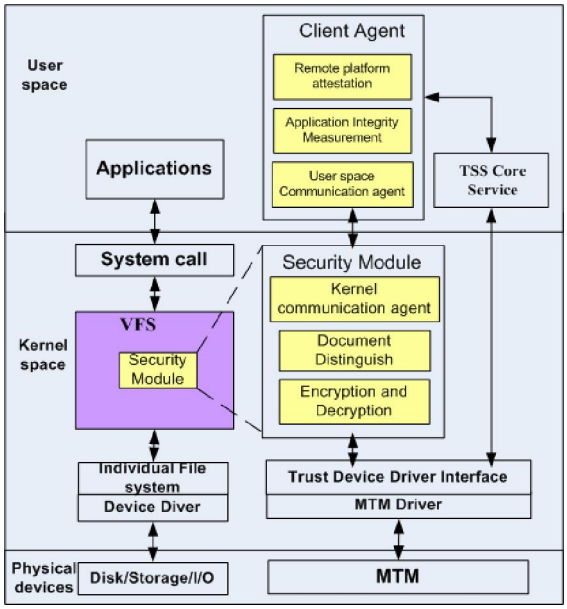

Figure 3. Trusted mobile client platform

Description: The system consists of a file server and many trusted mobile client component.

The file server is responsible for user management, key and certificate management, document management and so on. Trusted mobile client is enhanced by a MTM security chip and is responsible for protecting the document in the mobile platform.

The trusted mobile client has many security functions: Remote Attestation, transparent encryption and decryption, application Integrity verification, platform registration, security file download and so on. These functions will be described in section C and D.

C. Trusted Mobile Client Platform

As a whole security system, the file server security is also very important but its problem will not be considered in its paper.

The trusted mobile client is proposed and its architecture as fig.3:

Description: The Trusted mobile client is security enhanced in two parts:

on one hand, the VFS is changed that a security module is added to it; the module consists of the security document distinguish, document encryption and decryption and kernel communication agent;

on the other hand, a MTM based client agent is added, which consists of several security functions, including platform remote attestation and application integrity measurement;

In order to improve the document key security, the key for document encryption and decryption are stored in the MTM. The user space communication agent, which links to the kernel communication agent, could be used to manager the key, encryption algorithms, authorization data and access control management policy and so on.

D. Security Functions and Process

In this part, we give the description of security function and some in detail by process. The mobile document protection solution is achieved through different security stages or functions. For convenient, related concepts are described here in abbreviation:

Platform Information: I ; Message: M ; File: F . Public key pair: (K_{pub}, K_{pri}) ;Session Key: k ; Encryption function: $E_k(M)$;Decryption function: $D_k(M)$;Signature function: $S = Sig_k(M)$;Verify function: $V = Ver_k(M, S)$;Radom number : R ;Attestation Identity Key Pair : AIK = (AIK_{pub}, AIK_{pri}) ; Root Key of Store: SRK ; Identity of Entity : ID ; Hash Function: $H(M)$; Time : T ; Trusted Mobile Client: TMC ; File Server: FS ;

M_1 combine with M_2 : $M_1 \| M_2$; Error Check function: $Check(M)$.

1) Mobile Platforms Registration:

This function is to register the phone platform information, including the identification key, platform configurations and other information, to file server. Thus, when executing the file download function, the registered key could be used to find invalid platform which caused by out of date or broken and also could be use to encrypt the document encryption key.

a) Trusted mobile client send Mc to file server

$$M_C = \{K_{pubc} \| Sig_{AIK_{pri}}(K_{pubc}) \| AIK \| R_c \| ID_c \| I_c\}$$

$$TMC -> FS : M_C$$

The trusted mobile client measure state information I_c of platform first, then generate a public key pair (K_{pubc}, K_{pric}) ,the K_{pubc} is signed with private key part of the AIK , which is an asymmetric key pair and authenticated by the trusted third part; then the trusted mobile client sends the public key K_{pubc} , a random number R_c , the platform state information I_c , customer identity ID_c to the server together.

b) file server verifies Kpubc

$$Ver_{AIK_{pub}}(Sig_{AIK_{pri}}(K_{pubc}), K_{pubc}) \rightarrow \{success, failure\}$$

file Server verifies the correction of K_{pubc} :if success The Public key Kpubc and other related information are stored in the file server database.

c) file server response to client

$$FS \rightarrow TMC : M_s$$

$$M_s = \{E_k(ID_s, T, R_s, Sig_{K_{pris}}(H(ID_c, T, R_s)))E_{K_{pubc}}(k)\ \}$$

File server responses to the client in M_s, including public key valid period T .

d) client deals with response:

$$D_{K_{pric}}(E_{K_{pubc}}(k)) \rightarrow k$$

$$D_k(E_k(ID_s, T, R_s, Sig_{K_{pris}}(H(ID_c, T, R_s)))) \rightarrow \{ID_s, T, R_s, Sig_{K_{pris}}(H(ID_c, T, R_s))\}$$

$$Ver_{K_{pubs}}(Sig_{K_{pris}}(H(ID_c, T, R_s))) \rightarrow \{success, failure\}$$

Trust Client Decrypt the M_s, first decrypt the session key k, then use k to decrypt the other part of message M_s, then verify the server signature. If success, then the K_{pric} is encrypted with the SRK_c, which is the public key part of an asymmetric key pair stored in MTM and is used to encryption other keys. Then stored encrypted K_{pric} in the MTM; the K_{pubc} is packaged with the valid time T and some authentication data, and stay outside the MTM.

2) Mobile platform Attestation Service:

When connecting to the file sever, the client need to prove that it has a valid identity and integrity status. In our solution, this function is used in many stages, such as security file download, platform register, and platform key update and so on.

a) file server send remote platform authentication request Ms to the client;

$$FS \rightarrow TMC : M_s$$

b) trusted mobile client send Mc to file sever

$$M_C = \{Sig_{AIK_{pric}}(ID_c, I_c) \| ID_c \| I_c\}$$

$$TMC -> FS : M_C$$

Client measures platform information Ic, return the Ic and platform identity ID_c , a signature in M_c to file Server.

c) File server verifies the Mc and send back check result Ms to client.

$$Ver_{AIK_{pubc}}(Sig_{AIK_{pric}}(ID_c, I_c)) \rightarrow \{success, failure\}$$

$$M_s = Check(I_c) = \{success, failure\}$$

$$FS \rightarrow TMC : M_s$$

File Server verify the signature, if success, and the Ic meet expected condition, then the trust relation is established and returns the authentication result M_s. Or else, an error will send back to the client.

3) Document Security Download:

The mobile document is stored in file server and the procedure of transporting file between the mobile client and file server not always security. This function can ensure the security by using the encryption technology and remote platform attestation.

a) Trusted mobile client send file download request to file server

$$M_C = \{Sig_{AIK_{pric}}(ID_c, I_c) \| ID_c \| I_c \| F\}$$

$$TMC -> FS : M_C$$

Mobile client send the file download request Mc to the server, include the mobile platform information, user ID and other information related to target file.

b) File server check request and return result.

$$Ver_{AIK_{pubc}}(Sig_{AIK_{pric}}(ID_c, I_c)) \rightarrow \{success, failure\}$$

$$Check(I_c) \,\&\, Check(ID_c) \rightarrow \{success, failure\}$$

The file server verifies the integrity of platform first. if meet the condition, then the server return back the encrypted document and encryption key in M_s.

$$M_s = \{E_K(F) \,\|\, E_{K_{pubc}}(k) \,\|\, H(E_k(F)) \,\|\, E_{K_{pubc}}(k)\}$$

$$FS \rightarrow TMC : M_s$$

c) The trust mobile client received the Ms and stores the encrypted file and encrypted key k in platform.

4) Applications Integrity Verification:

Before using the document, application is checked to find whether it is tempered. This principle is to compare the hash value of the application with the one stored in some PCR of MTM. If in the same state, the application continue executing and operating the protected file or refuse to run.

5) Document Transparent Decryption:.

a) application send request for access file

This action is received by system call and transport to the security module in VFS

b) Identify the protected file:

The decryption function is called by the VFS. Before the real document decryption action, the protected file should be discerned. There must be set some character for the protected file. One method is to add a unique string into the encrypted file. Thus, if there is no such string in the current file, then the file will no need to decrypted, or else the current file is a protected file and need to be decrypted.

c) To obtain the decryption key:

The decryption key k is needed before decrypting the protected file. Because k is encrypted by the mobile public key, and the mobile private Key is stored in MTM, so in the first, the current process gets the private key to decrypt the file encryption key.

The procedure will be checked by the security policy, including the application integrity measurement and valid of registered public key .If the check progress is success, then the document encryption key is returned to the encryption module, or else a special error code is returned.

d) The security module decrypt the protected file:

With the document encryption key k, the security module decrypt the cipher text of protected file and copy the data to the user space. Application process reads plain text from the of user space.

6) Document Transparent Encryption:

The application modifies the protected document. The modified data of protected document are written to user space

a) Identity the protected file

The encryption function is called when the file in writing status. Before this action, the security module also need to distinguish the normal file and protected file. Because there is no any unique code which is removed in decryption stage, so the distinguish policy must be designed in other way. Our method is that the security module needs to record the protection file name when in decryption stage and name change. This method is easy to realized and effective.

b) Get the encryption key

Before the encryption function, the document file key must be ready. The procedure of access key is like the one in decryption stage.

c) The modified data are encrypted and encode into protection file format.

The modified data in user space data is encrypted and encoded into protection file format that there is an unique string in file data. There may two methods to update the protected file. One is to delete the original protected file and create a new file with the same name of original file. The other is to directly update original file with the new data.

7) Public key update:

public key generated with MTM, the key used to encrypt the document, in order to increase security, you can only use public key on the validity period to decrypt the document, once expired, platform have to re-registration a pair of public key.

a) Trusted mobile client send Mc to file server

$$K_{new} = (K_{pubc-new}, K_{pric-new})$$

$$M_c = \{ID_c, K_{pubc}, K_{pubc-new}, Sig_{AIK_{pric}}(K_{pubc-new}), R_c\}$$

$$TMC -> FS : M_C$$

Trusted Client public key is time out. Client creates a new public pair Key K_{new}, and send the request M_c to file server.

b) File server check Mc and return result.

$$Ver_{AIK_{pubc}}(Sig_{AIK_{pric}}(K_{pubc-new}), K_{pubc-new}) \rightarrow \{success, failure\}$$

$$M_s = \{ID_s \,\|\, K_{pubs} \,\|\, Sig_{K_{pris}}(K_{pubc-new} \,\|\, T_{new} \,\|\, ID_c \,\|\, R_s) \,\|\, E_{K_{pubc-new}}(k) \,\|\, E_{K_{pubc-new}}(T_{new}) \,\|\, R_s\}$$

$$FS \rightarrow TMC : M_s$$

File server verify the client request, if success, the server delete the old public key in storage and add a

new public key to storage. Then sends the M_s back to client .

c) Client update the public key

$$Ver_{K_{pubs}}(Sig_{K_{pris}}(K_{pubc-new} \| T_{new} \| ID_c \| R_s) \rightarrow \{success, failure\}$$

$$D_{K_{pubc-new}}(E_{K_{pubc-new}}(k)) -> k$$

$$D_{K_{pubc-new}}(E_{K_{pubc-new}}(T_{new})) -> T_{new}$$

The clients verify the return massage, and get the encryption K and a new valid time. The encrypted k is been packaged with some authentication information, and stored into MTM. The new public key $K_{pubc-new}$ is also packaged with new time T_{new} .

E. Security Analysis

One security problem of mobile office document is the confidentiality of document data. In our solution, the protected document is always saved as a cryptograph in mobile platform; it can't be decrypted without the encryption document key, which is binding to the mobile platform so that the document can't be decrypted in other platform. At the same time, the document also is transmitted as a cryptograph in file download stage, preventing a network eavesdropper to obtain plaintext.

Another security problem is how to realize the access control that only the trust entity can use the document. Because the application and even the platform system may be tampered by the malicious software, which means the application or platform couldn't be trusted always. The simple precaution is to find the modification action before executing the target code. In our solution, TC technology is used for the integrity verification of application, and platform, ensuring that document only is used by expected entity.

In addition, the mobile platform must register a public key to the server. The public key is used to encrypt and decrypt the session key K and security control. When the security module visits the MTM, it firstly checks whether the current public key is expiration or not. If the key is out of date, the platform needs to register again, or it will not execute.

IV. RELATED WORK

The security status in mobile device arise many attention. There are many researches on how to secure the mobile devices.

Sokhumi[2] design and implement an flash cryptographic file systems based on YAFFS(Yet Another Flash File System).all the files are encrypted by different keys, but user managers only one master key. This solution suite the embed systems such as mobile device that used the flash file system YAFFS. Charles [3] proposed a cryptographic file system named NCryptfs based on stack file system which can suite to any kinds of file systems. This solution balancing four conflicting aspects: security, performance, convenience, and portability. It achieved security by including support for many ciphers and authentication methods. It also considers the key timeouts and performance issues. It achieved high performance by designing NCryptfs to run in the kernel.

Xu[4] proposes a differentiated user access control model named DiffUser to enhance smart phone security and user privacy. Differentiated user access control model to enhance smartphone security and user privacy. DiffUser classifies Smartphone users based on certain sets of user access privileges. The evaluation results show that the proposed solution is lightweight and flexible.

Wu [5] proposed a security software download framework and the protocol based on mobile trusted computing . It aim to resolve the security threats exiting in software download. The framework and the protocol can be not only used for the download of software, but also can be widely used for the download of other contents.

Zhen[8] discuss the mobile DRM issue using the TC technology. Based on the new characters provided by trusted computing platform, the authentication scheme in mobile DRM can be simplified, which is safe enough to increase the security of latest mobile DRM framework and promote its interoperability and compatibility. LIU [9]also discuss on how to build user authentication mode about content protection system based on TCM, which is a TC standard from china. They proposes a new application for the trusted computing in the filed of mobile terminal.

Luigi [10] mainly research the security of mobile storage. They present an extension of the TVD architecture to incorporate the usage of Mobile Storage Devices. It discusses three major issues: coherent extension of TVD policy enforcement by introducing architectural components that feature identification and management of transitory devices; transparent mandatory encryption of sensitive data stored on mobile devices; and highly dynamic centralized key management service.

These security technologies have its advantage. This paper combines some advantage of these technologies. And the solution could be another choice when design the security solution for mobile document in mobile office automation.

V. SUMMARY

Given the security requirements of mobile platform document protection and the current technology, this paper proposed a new document protection solution based on TC technology. Compared with the existing security solution, the solution can be seen as an improved version of the existing document protection technology. It achieved not only common security requirement, but also the transparent encryption requirement.

The security advantage of TC technology is fully applied to provide strong platform security, including the remote platform authentication, key storage and so on.

The transparent encryption scheme in the VFS layer can maintain the independence of the application program to the security module.

Although the proposed solution has some security advantage, there are some points need to further consider:

- Ø Platform Revoke: When a user change his mobile device or lost the mobile, the system must stop the old mobile client platform to download file or use protected file in the mobile platform.
- Ø Security policy change: for different requirements, some changes need to support, including encryption algorithm, access control rule, and so on.
- Ø It is also necessary to study the performance aspects and the realization of document protection on other operating systems

APPENDIX A TRUSTED COMPUTING

The aim of Trusted Computer (TC) is to protect platform security of computer system. The principle of TC is to add a trusted root in computer systems. Based on the trusted root, a complete trust relationship from the system hardware to the application could be created, and then a trusted running environment could be established. Trusted Computing is a hardware-based security technology. The key hardware called Trusted Platform Module (TPM) is a security chip with rich cryptographic functions. Thus the TC could be used to develop kinds of security applications. A typical TPM structure as shown below:

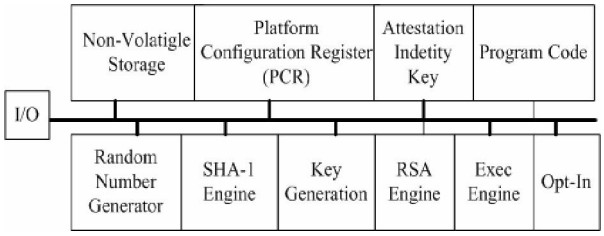

Figure 4. Structure of TPM

TPM is a hardware specification for PC platform. Given the mobile platform development, TCG published another specification named MTM, which has the similar security functions of TPM. The major difference from TPM is that a MTM platform could have different trusted roots for different shareholders [7]. Meanwhile, whether the MTM implemented by hardware is optional. This paper presumes that the hardware–based MTM is used.

The MTM has the following four basic functions:

- Ø Integrity verification: applications are often tempered by malware. This function could ensure only the integrity application to run. applications carry out integrity measurement before running and compare with the measurement value of these applications stored in PCR of MTM to find whether exists modification or not .
- Ø Safe Boot: during the boot procedure, every entity will be carried out integrity verification. Every entity's measurement is compared with the one stored in PCR of MTM. If the result is consistent, then the entity can run, otherwise there is the risk of tampering. Thus, this entity can be processed according to security policy, or report an error, or restore the tampered entity using backup. As a result, only when all entities passed the measure verification, the system is safely boot.
- Ø Remote attestation: before communication, the service requester could ask the remote service provider to attestation its platform. Remote service provider which equipped with MTM or TPM will first conduct the platform measurement and sign these measurement with AIK (Attestation Identity Key), then in some security way, it sends back this measurement to the service requestor. Thus, the requestor could judge whether the remote service provider's platform status is meet the security policy and whether the trusted relation is need to established.
- Ø Binding technology: The binding means that the important information is packaged with some special information, such as the environment status or the PCR value of MTM, So that this important data could be used only when the running environment status meets to original binding character. This function could implement some access control ability.

ACKNOWLEDGMENT

This work is support by Natural Science Foundation of China (Grant Nos. 60873191 , 60903152, 61003286, 60821001)

REFERENCES

[1] Wayne Jansen and Karen Scarfone .Guidelines on Cell Phone and PDA Security. Recommendations of the National Institute of Standards and Technology 2008 NIST Special Publication 800-124

[2] Seokhyun Kim, Yookun Cho The Design and Implementation of Flash Cryptographic File System based on YAFFS . ICISS. 2008.23 p62-65

[3] Charles P. Wright, Michael C. Martino, and Erez Zadok NCryptfs: A Secure and Convenient Cryptographic File System. USENIX 2003 Annual Technical Conference ,in pp197-210 of the Proceedings http://www.usenix.org/event/usenix03/tech/full_papers/wright/wright_html/

[4] Xudong Ni, Zhimin Yang, Xiaole Bai, DiffUser: Differentiated User Access Control on Smartphones. Mobile Adhoc and Sensor Systems, 2009. IEEE 12 Oct. 2009 pp1012 - 1017

[5] Wu Jun-jun, Fang Ming-wei, Yu Peng-fei, A Secure Software Download Framework Based on Mobile Trusted Computing WCSE.2009.167 p171-176

[6] TCG Mobile Trusted Module Specification Specification version 1.0Revision 6,26 June 2008

[7] Andreas U. Schmidt On the deployment of Mobile Trusted Modules WCNC 2008. IEEE pp3169- 3174

[8] Zhen YANG, Kefeng FAN, Yingxu LAI. Trusted Computing Based Mobile DRM Authentication Scheme.

2009 Fifth International Conference on Information Assurance and Security
pp7-10.

[9] LIU REN, Niu-Dongxiao Content Protection based on Trusted computing in Mobile Terminal. 2009 International Conference on Information Management, Innovation Management and Industrial Engineering. pp192-195

[10] Luigi Catuogno, Hans L¨ohr, Mark Manulis et al.Transparent Mobile Storage Protection in Trusted Virtual Domains. LISA'09 Proceedings of the 23rd conference on Large installation system administration 2009

Xiaojun Yu, He got master degree in computer application technology from Beijing information science & technology University in 2007, Beijing, China. He is a doctor candidate in cryptography of Beijing University of Posts and Communication, Beijing, China.

His interests include network security, cryptography, trusted computing and cloud computing. He is the member of Association for Computing Machinery.

Qiaoyan Wen, She own doctor degree in information processing from xi'dian university, Xi'an,China. She is the professor of Beijing University of Posts and Communication, Beijing, China.

She interested in information security, quantum cryptography and security protocol.