Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):491-497

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Application research and analysis based on Bitlocker-Data protection & Secure Start-up of Windows 7

Hou Rui, Jin Zhi Gang and Wang Bao Liang

School of Electronic Information Engineering, Tianjin University, Tianjin, PRC

ABSTRACT

Bitlocker is an important safety measure of Windows 7 operating system, which lays the foundation for data protection and security start over of window 7 and has a far-reaching influence on Windows 7 or even subsequent windows platform. This paper obtains some useful conclusions and potential problems for reference according to the achievement of data protection and the analysis of secure start-up flow.

Keywords: Bitlocker；Data Storage；Data Security；Secure Start-Up；Trusted Compute

INTRODUCTION

The full name of Bitlocker is Bitlocker Driver Encryption. Windows 7 inherited security strategy of Vista operating system, and embedded Bitlocker disk drive encryption and Bitlocker to Go mobile storage device encryption, and could protect security of user data storage in system disk encryption, data disk encryption and mobile storage device encryption. The function ofBitlocker encryption system boot drive can lock the normal system boot processes, and only the use of USB start-up key or system recovery key or can restart the computer in normal. If the user's computer system installed with a TPM (Trust Platform Module) trusted platform module[1],, he could also checkthe system integrity before starting to ensure the system boot disk encrypted has not been replaced or starting unit data has not been modified. This ensures that only authorized users can start and operate the computer system and use encrypted file to get the maximum of system protection. The next development direction of information security is recognized as trusted compute. The basic idea is in the computer system firstly establishing a trust root, and then setting up a trust chain. Starting from the trust root, a level measurement certificatesa level and a level trustsa level and the trust relationship are extended to the whole computer system so as to ensure that the computer system is trusted. It is very important to the start safety of Windows 7 to introduce Bitlocker drive encryption function based on trusted computing technology In Windows 7[2],. Due to the use of a series of security boot measures with focus on Bitlocker, thus it is very difficult to apply to Windows 7 of Bootkit attack that makes use of tampering with the operating system and starting up files to achieve the kernel hijacking function.

THE ACHIEVEMENT OF BITLOCKER DATA PROTECTION

A. DISK ENCRYPTION PRINCIPLE

Bitlocker uses Advanced Encryption Standard algorithm(AES) of 128-256 key, volume of each sector is encrypted alone, and a part of the encryption key is derived from the sector number. Two identical unencrypted data sectors will also be written in disk in a different encryption key, so that it increases the difficultyto try to find the key through the creating and encrypting known information. Bitlocker encrypts the whole system volume by using the full volume encryption key FVEK (Full Volume Encrypt Key) [3], FVEK itself is also encryptedby the main volume key VMK (Volume Master Key). If VMK is cracked, the system can replace the new VMK and encrypt FVEK again, so there is no need to decrypt a disk data and encrypt again. In the use of Bitlocker initialization the user need to specify the key recovery password or through the USB equipment storage to recovery key (Recovery key) in order to carry on the system data recovery when necessary. Bitlockerdoes the integrity check of system module before the start of the system through the trusted platform module TPMin order to ensure the integrity of the disk data. TPM collectsthe information of system boot module, such as the BIOS settings, to form the fingerprint of current machine. When the disk is replaced or disk boot data is modified, the machine cannot start system normallysince it cannot identify current disk correctly. When the machine does not support TPM or it has no TPM chip, the user can use the strengthened verification function of Bitlocker to protect the system boot. At this point the user must enter correct PIN code or insert the USB key and type the correct password (Startup password), otherwise the system does not start normally. Bitlocker drive encryption must use NTFS file system, it will automatically decrypt the file system when the encrypted data copy from NTFS encrypted drive to the others. The files in Bitlocker encryption driver are tha same as the ordinary files in Windows, encryption and decryption are processed automatic. The files stored in the encryption driver are stored in encrypted form so that legitimate users can visit in any way.

1)Bitlockerkey system

Bitlocker protects the safety of the system by using various keys，the key system structure ofBitlockeris as shown in the figure 1.

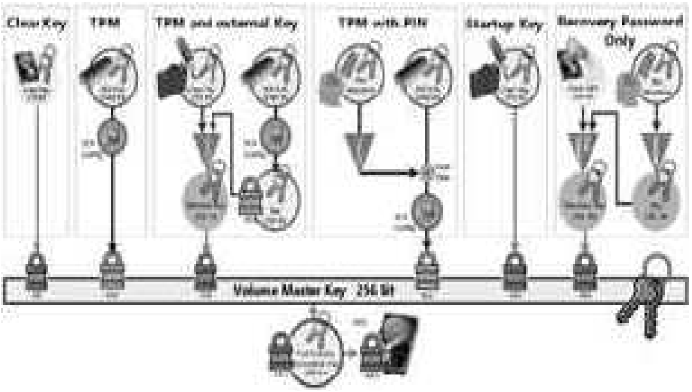

Figure 1.key system structure ofBitlocker

The computer system With TPM1.2 trusted platform module product system startup key (StartupKey) and system restore key (Recovery Password)in the use of Bitlocker encryption system boot disk. The startup key is of encrypted form, system restore key is of non-encrypted form. Each key has a corresponding label which provide to the user to find the corresponding key when needed by the system. The function of main keys:

- Startup key: startup key is stored in the USB device,and it must be inserted into the computer to start up (or return from hibernation). There are two cases thatneed startup key: the first is when the BitLocker is configured to use TPM + as the startup key and the other is Bitlocker is configured with the boot key start onlywhen in the absence of TPM.
- Recovery key: recovery key is stored in a USB device that is used in recovering data system and restarting the computer when the startup key could not be in normal use.
- All encryption key: the disk data encryption in unit of sector.
- Primary key: used to protect the whole disk encryption key. The primary key is protected by TPM module.
- Password recovery: users input manually when the startup key and recovery key cannot be used, start the computer encryption system disk data.
- The file form of recovery key: BitLocker recovery key XXXXXA26-A4BA-4DF9-9FA1DAC7F3EF27A0.TXT
- The file of system startup key: 78089CFC-792F-46D7-82B9-6446DEFC6EBE.BEK.It should be noted thatin Bitlocker encryption system the system uses the FVEK (full volume encryption key) key encrypt the entire disk sector, FVEK is used by the system, users can not access. When the system boot disk encrypted by Bitlockerstart up, TPM decrypts SRK (Storage Root Key) and storage root key,VMK is decrypted by SRK, FVEK is decrypt by VMK and the disk data is decrypted by FVEK to complete the system startup.Bitlocker encryption system startup process is shown in figure 2.

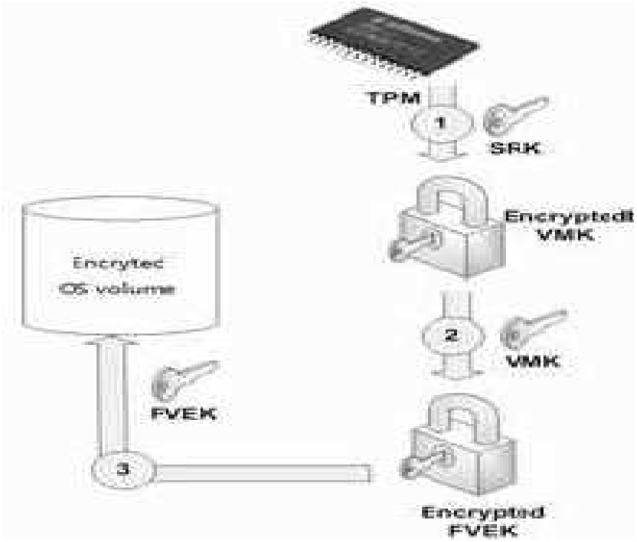

Figure 2. Bitlocker encryption system startup process

2)The use of user key
When usingBitlocker encryption system disk, system generates a startup key and a recovery key. Recovery key is a password file in the way of document, there are 48 plaintext passwords thatare divided into 8 groups, each group of 6 numbers, you can view and print save. Compared with password, Bitlocker is holding the recovery key, while the corresponding one is the startup key. When necessary, the user can use recover key decrypt the encrypted disk copy. If the disk protected by Bitlockeris transferred to another computer, the user can use recovery key open the encrypted file. Both system startup key and recovery key can be copied and saved.

B. THE ANALYSIS OF ENCRYPTIONALGORITHM

Bitlocker use AES-CBC+Elephant Diffuser algorithm [5],The requirements of Bitlocker encryption algorithm are disk sectorsof size of encryption and decryption of 512102420484096 or 8192 bytes. Bitlocker in sectors as unit (512-8192 bytes) is as the input of the algorithms, each sector of a diffuser, the advantages of such design is when any change and disturbance in the ciphertext bits will pass through the whole sector[4], because the algorithm is based on the entire sector as the processing unit and it has strong protective capability.Because of prior treatment to the key of the entire sector which brought the performance overhead the processing speed is affected. For the AES-CBC+ElephantDiffuser algorithm adopted by Bitlocker, it is used in wide block design and AES-CBC mode, the key of each sector and the construction of CBC pattern initial value has the system overhead.Bitlocker is the encryption of sector levelwhich can protect not only the driver in the operating system, but also the data disk. Bitlocker encrypted the drives of the whole Windows system to protect the user data on a computer to prevent unauthorized users from destroying the Windows system files and system protection whichcould offline checkthe information in protecteddrive. Bitlocker drive encryption system can also prevent other users to start a plug-in operating system such as Winpe or by running the software to bypass the Windows system protection which could offline obtainthe files in protected driver. When the user does not insert USB startup key Bitlocker drive encryption lock the normal startup process on the computer until inserting the USB startup key or inputting recovery key, system can start normally. If the computer system is equipped with TPM1.2 of the trusted platform module to protect user data, it can protect the computer maximumfrom breaking in the system offline. If there is no TPM 1.2 security modules, Bitlockercould still protect the hard disk data, but it would not execute system integrity verification
.

C. EXPERIMENT RESULT AND ANALYSIS

Experiments use portable computer equipment without TPM trusted platform module, the operating system is Windows 7 ultimate, and useBitlocker disk encryption to encrypt the Windows system disk and data disk to test the time and reliability of encryption process and the encryption process and stability.

1) System disk encryption
Windows 7 use TPM 1.2 trusted platform module as the defaulting setting in the use of Bitlocker encryption system disk. The computer system which has not installedtrusted platform module of TPM1.2 version, need to modify the local group policy to allow the system to support the use of Bitlocker encryption system disk by using the USB disk storage startup key to start up Bitlocker encryption[5]. Select the computer configuration, management templates, Windows component, Bitlocker drive encryption, operating system driver, double-click " in the startup requires additional authentication" in the settings of the operating system driver tab open the corresponding window, in the

option selected "allows Bitlockerisas without compatible TPM", confirm exit from the local group policy editor, then Windows 7 operating system uses of Bitlocker encryption system boot disk in the case of without installingtrusted platform module of TPM1.2 version. Encryption started, open the desktop icon, select the system disk (C:), click the right key and chooseBitlocker (B), requires the startup key when started every time (S). Then the system is required to insert the USB disk save startup key, insert a prepared USB disk, select the disk, click the Save button, save the key in the USB disk, save the USB disk, it is startup key of this computer. The next step is to save recovery key that can be saved in the USB disk and also in other places in the file. After the completion of the above work, the system provides direct access to the encryption key or inspection to startup keyand recovery key so as to ensure that the system can correctly read and use. Choosing to restart the system the encryption is officially began on Windows 7 system disk. The process of Bitlocker encryption is stable and reliable, it would not interrupt because of the system operating in other program, even shut down the computer system, interrupt the encryption process that is performed, after the restart, encryption can still continue.

2)Data disk encryption
Bitlocker is very simple on data disk encryption, in the computer window selecting a logical disk drive that needs to be encrypted, right-click the option to enable Bitlocker (B). Choose to use the password to unlock the drive, input unlock password, save or print recovery key generatedby system automatic, choose the next step, Bitlockerstart up the encryption process for this disk. Bitlocker encryption process is very slow that the encryption speed is about 5M per second in a portable notebook computer and is about 10M per second in commercial desktop computers asBitlocker encrypt system disk or logical disk. Because Bitlocker encryption algorithm is the encryption for the whole sector, it is not important whether there is a data in sector, and storingdriver encryption with data and without data required the same time.

D. EXISTENT PROBLEMS

It is very slow for Bitlocker initializes encryption disk process. It will take about 30 minutes to encrypt a logical disk of 10G, and it is difficult to encryptthe large capacity drive. Windows7 cannot restore the original state very well whenit cancels the system disk of Bitlocker encryption.When Bitlockeris on the system disk encryption, it will automatic create an unencrypted startup key to check. When system activitiespartition (about 290M)decrypted operating system disk eliminate the system disk usingBitlocker encryption, it cannot uninstall and delete small boot partition created[6].The mobile disk and USB diskencrypted by Bitlockerto Go mobile device can only from the use of the Windows XP system while can't modify, edit and store in the encryption state.

IMPLEMENTATION OF SECURE SECURE START-UP

A. WINDOWS 7STARTUP PROCESS

The main startup module of Windows 7 include BIOS, the master boot record, Bootmgr, Winload.exe and kernel file Ntoskrn1.exe. The BIOS is a small operating system of charging of basic input and output, and is mainly responsible for the hardware initialization. The control flow is transferred to the master boot record (Master Boot Record, MBR) after the BIOS executing the function. MBR is constituted by the boot code and primary partition table[7], its main function is locate and store the main partition of operating system, and read the operating system loading module into memory, finally hand control to partition boot record (Partition Boot, Record, PBR), load module by PBR operating system. After PBR operating system, it will go into the initialization phase.In the phase boot module to get control right is Bootmgr firstly. Bootmgr consists of 16 boot code and 32 PE file section. The boot code is mainly responsible for the parameter settings, opening the protection mode and other functions. The PE file is usually named OSloader, this module is mainly responsible for memory initialization and obtaining the parameters from the startup manager. If openingBitLocker protection, OSloader will be responsible for obtaining key and decrypting Winload.exe. The Bootmgrcontrol power will hand to Winload.exe. The function of the module includes loading the operating system kernel module[8], setting part of kernel structure, loading device driver etc. The last step to start up the operating system is done by the kernel file Ntoskrn1.exe, this module will establish all environments needed by the system operation, and create a system thread and process. The startup process of Windows 7 is shown in figure 3

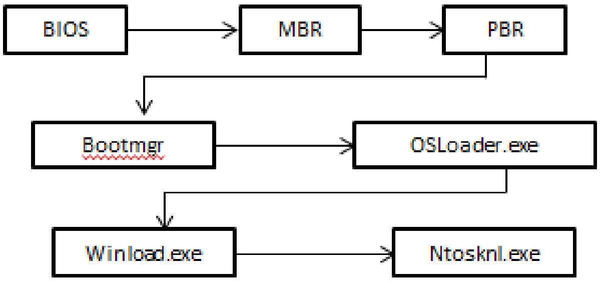

Figure 3 The startup process of Windows 7

B. TECHNOLOGYREALIZATION OF WINDOWS 7SECURE START-UP

1) Bitlocker technology realization

Bitlocker is the most important safety boot technology introduced in Windows 7, and it could realize its full protection function with TPM v1.2.chip supporting by computer. Opening the Bitlocker will encrypt the entire Windows volume, and at startup time check whether the integrity of the system boot module is destroyed. Once monitoring tamper with the behavior of the module, the system terminates the startup, and warns the user there has something changed. The Bitlocker generates full volume encryption key (Full VolumeEncrypt Key, FVEK)in the initialization and uses the key encrypt the disk, FVEK is protected by volume master key (Volume Master Key, VMK) of another key volume, VMK itself is protected by the TPM. When the system starts, BIOS, MBR, PBR andBootmgretc. starting modules will be measured in turn, metric value is stored in the PCR register. Finally, the Bootmgr requests TPM using the PCR value of the register to decrypt VMK. Only when all the metrics and measurement results of VMK package are in agreement, can VMK be successfully decrypted, and then decrypts the entire operating system. Startup process of operating system after Bitlocker opening is shown in Figure 4.

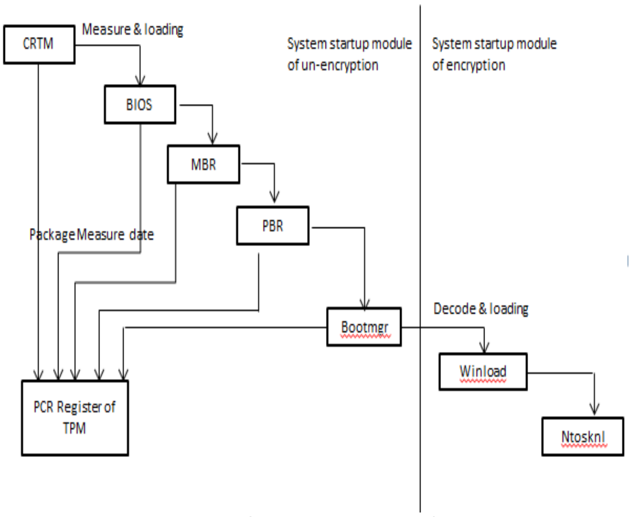

Figure 4. Startup process of operating system after Bitlocker opening

2) Random distribution technology of starting module load address

Address space randomization techniques of ASLR (Address Space Layout Ran domization) is introduced to randomly distribute load address of memory module of the system, rather than the previous fixed memory segment [9], which can prevent the behavior of malicious software attacking in search of a specific system code.

3)Bootmgr protective measures

In addition to Bitlocker will protect the integrity of Bootmgr, Bootmgr itself will take some protective measuresincluding static files Coding, digital signature and verification and inspection of the module. Static file encoding is defined in Windows 7BootmgrOSloader 32 will be stored in the form of code on disk. The encoded part is decodedby Bootmgr boot code as starting up.Then malicious code could not attack on BootmgrOSloader through the method of searching feature code, and the attacker could not do static disassembly of OSloader stored on disk, greatly improving the difficulty of reverse analysis. Digital signatures and module verification and inspection are all the functions of integrity check of Bootmgr for its own.

C. ANALYSIS OF SECURE START-UP MEASURES OF WINDOWS 7

1)Analysis of safety hidden trouble of Bitlocker

- Existing key management concerns

In order to enable users to measure the startup file that be legally modified, in the Bitlockerwe define a disable (disable) state. When BitLocker is disabled disk will form a clear text clearkey J. When the system is booted next time it will decryptdirectly with clearkeywhile no longer by TPM. Because clearkey lacks enough protection, if an attacker obtains the clearkey through special means it would be a threat to the data protectedby Bitlocker.

- The lack of authentication protection to disableBitlocker

Bitlocker does not validate user who disable it. This means that once the attacker gain executive powerof system by the method of leak exploiting, he will be easily completed the operation of disable Bitlocker, which is a prerequisite to obtain clearkey.

- The risks in Starting upand transferring module control

During Bitlocker system startup, just by a higher startup module submitted to the next level metric measurement module value while not to verify the correctness of the metric value, until the control passes to Bootmgrit verifies the integrity of the startup module. That is before the verification of Bootmgr startup module tampered with malicious software still can obtain of executive power.Thusthe correlation function of BitlockerinBootmgr will likely be tampered with which may provide the possibility for the malicious softwarebypass Bitlocker protection.

2)Analysis of safety hidden trouble of Bootmgr
OSloaderin Bootmgr is initially interruptedby INT13 and read into memory of the code, such malicious software even gains control of BIOS or MBR, are still unable to effectively control the OSloader. From OSloader is decodedby 16 boot code ofBootmgr toOSloader gains control the code of the 2 processes is likely to be the springboard of attack as the attacker.Because this code can be attackeddirectly by the malicious code from the bottom, and as the code is executed OSloader in memory has been decoded, an attacker as long as obtain the control when this codeexecutes, can be used to attack on OSloader[10]. Bootmgr itself does integrity checking with Digital signatures and module verification and inspection which is a part of Bootmgr, itself may be attacked. As long as the attacker tampers with approximate function of the 2 functions can bypass protection.

D. EXPERIMENTAL VERIFICATION SCHEME

To verifythe harm of safety hidden trouble described in above, we can design bypass the scheme for the various safety measures, and according to the scheme design and adapt existing Bootkit, thus verifying the feasibility of the scheme.

1)Bootkit
Bootkit is a kind of Rootkit that could tamper with the boot file of operating system to realize its function. After Bootkit is embedded operating system, it will tamper with a startup file with special means in which to insert malicious code. In the next system start up, once control is passed to the startup files modified by Bootkit, the attacker's malicious code will be executed and tamper with the boot file of next level. This modification process will be in accordance with the transfer direction of the control from the bottom to the top during system startup process is repeated several times until the Bootkit finally gets permission to modify the system kernel.

2)Bitlocker bypass scheme
In embedding Bootkit using a command line tool in Windows 7 disable Bitlocker, then extract clearkey from the disk, after the extraction reopen the Bitlocker protection. The next time you start Bootkitwill force to submit the extracted clearkey to Bitlocker, so the Bitlocker mistakenly think that it is in the disabled state[11].. Soany changes Bootkitdoes to start module will not alert Bitlocker. After completed the startup the system will display Bitlocker is still in openprotect state.

3)Bootmgr bypass protection scheme
For Bootkit, the ability to tamper with Bootmgr is a prerequisite for bypass BitLocker protection[12]. If Bootkitconsiders BIOS or MBR as attacking starting point, it needs to bypass the static file encoding mechanism, namely it must first find a springboard in 16 boot code of Bootmgr. After debugging Windows 7 start-up, the function transferring control toOSloaderin Bootmgr boot code is in memory 20A5Ah to 20A98h, as the code is in the implementation OSloader has been decoded. So, as long as the hook of the function, the attacker will have the opportunity to tamper with the attack on Bootmgr. The function in Bootmgrwhich is responsible for the digital signature is BmFwVerifySelfIntegrity, as long as tampering with the return value of the function you can skip the check of the digital signature. Skipping verification and check you only need to modify IC instruction in memory 20E2Ch of Bootmgr boot code to a JMP instruction, the system will not act on tamper alarm.

4)Address space randomization solution scheme
Bootkitmust obtain loading base ofpart of the kernel module if it wants to achieve the kernel hijacking. Because of the application of ASLR Bootkit must dynamic obtain loading base of module during the execution process[13]. The scheme designsa method of obtaining loading base of the specified module by calling ZwQuerySystemInformation function, Figure 5 shows how to get loading base ofBitlocker driver fvevo1.sys in the kernel through the method.

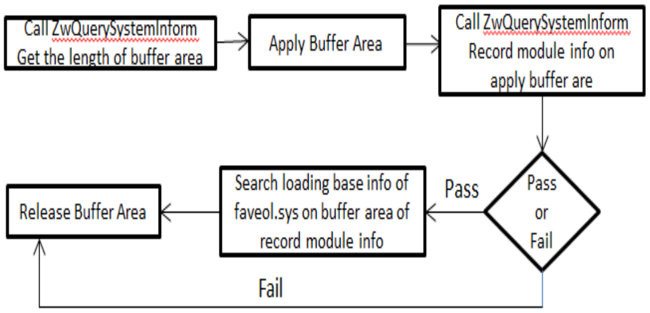

Figure 5 Get loading base of Bitlocker driver fvevo1.sys

CONCLUSION

Bitlocker is one of the best encryption methods that can be directly used with advanced algorithm and strong practicability. Users can directly use Bitlocker encryption technology embedded in Windows 7, encryption system boot disk and logical disk, reliable protection of their critical data will not be leaked. AlthoughWindows 7 based on Bitlocker has been greatly improved in the aspects of system security startup, make Bootkit and other malicious software difficult to mount effective attacks, there are still some vulnerability of these safety measures.If these weaknesses are combined to be comprehensive utilization, it is possible to make Windows 7 startup module be attacked without being foundby system and user. Thereforeit needs further study to how to protect the boot module of operating system and better apply the idea of trusted computing to system secure startup.

Acknowledgment
This paper was partially supported by my wife and make sure all translation .I would like to thank Professor .Jin Zhi Gang giving me possibility suggestion & productive discussion.

REFERENCES

[1] Gao Wei. *Research of disk date secure protect technology*[D].Shanghai Jiao Tong University,**2008**.

[2] Gao Wei,Gu Da Wu,Hou FangYong,Song NingNan. *Computer application &research*,**2008**,(5).

[3] Zeng MengQi. Research of self secure disk、Design & Implemention [D]. *Shanghai Jiao Tong University*,**2009**.

[4] Tom Olzak.Recipe for Mobile Data Security:TPM,Bitlocker, Windows Vista andActive Directory[DB/OL].[**2007**.10]. http://www.infosecwriters.com/text_resources/pdf/TOlzak_Mobile_Data_Security.pdf

[5] Niels Fe rguson.AES-CBC+Elephant diffuser A Disk Encryption Algorithm for Windows Vista[EB/OL].[**2006**-08].

[6] BitLocker Drive Encryption [EB/OL].**[2010**.4.10]. http://www.microsoft.com/windows/windows7/features/bitlocker.aspx.

[7] TrustedComputing Group. TCG Specification Architecture 0Verview[EB/OL] (**2009**—04—01). http://www.trustedcompufinggroup.org.

[8] MicrosoR Corporation ． BitLocker Drive Encryption Technical Overview[EB/OL] (**2010**—02—131)．http://technet.microsoft.colrden—us/library/cc732774.aspx．

[9] Chen Fei，Zhu YuFei,Mei Qiang． *Computer Engineering*，**2008**，34(22)：182—183．

[10] Kumar N，Kumar V．Vbootkit：Compromising Windows VistaSecurity[C]//*Proc.ofBlack Hat Europe Conference.Amsterdam*,**2007**

[11] Kumar N，Kumar V BitLocker and Windows Vista[EB/OL](**2008**-05—19)．http://www.nvlabs.irduploads/p-rojects/nvbit/nvbit_bitlocker_white_paper.pdL

[12] Jing Zhang, XinGuang Li. Cross-platform Transplant of Embedded Smart Device. JSW *Vol 5, No 10 (2010): Special Issue: Information Security and ApplicationsKaushik Deb, Hyun-Uk Chae and Kang-Hyun Jo. Vehicle License Plate Detection Method Based on Sliding Concentric Windows and Histogram. JCP* Vol 4, No 8 (**2009**): Special Issue: Trends in Hybrid Intelligent Systems