The Research on PGP Virtual Disk Password Cracking

Qingbing Ji[a], Lijun Zhang, Fei Yu

Science and Technology on Communication Security Laboratory, Chengdu, 610041, China

[a]email: lijun6918@163.com

Keywords: PGP; virtual disk; password cracking

Abstract. PGP virtual disk encryption technology is a double-edged sword, on the one hand it is helpful to prevent the user’s sensitive information on the disk from being stolen or tampered. On the other hand, some criminals take advantage of PGP virtual disk encryption to engage in illegal activities. This paper proposes an effective method to crack password of PGP virtual disk, which provides the feasibility for the judicial investigation, counter-terrorism and prevention of criminal activity.

Introduction

Personal desktop and notebook computers are becoming more and more popular since the 1980s which induces a lot of important data are stored on hard disk. But people soon find such a phenomenon that is a great many sensitive data are leaked because of the disk loss or computer stolen which involves important secret information. This is a particularly bothersome problem for relevant government agencies, enterprises and individuals. According to the result of a survey by the USA Computer Security Institute, the loss of laptop and hard disk has become the second-largest security issue besides the computer virus infection[1]. In recent years, more people realize the importance of disk data protection from the series of hard disk and laptop thievery. Therefore, many computer manufacturers and information security organizations focus on the research of data protection under the circumstance of laptop and hard disk lost.

In order to prevent the laptop being stolen, manufacturers have come up with various ways such as providing computer box similar to ordinary suitcase, inventing the alarm system, designing data encryption program to avoid unauthorized users to understand the content of the computer, etc. Moreover, Laptops even introduced fingerprint security identification system and the user only need to press the fingerprint on the inductive area, then the fingerprint information will be recorded. Later, this system will require the user to provide fingerprint for identification and only the fingerprint is matched, the operating system can enter. But all these strategies have a fatal weakness: once the thieves take out the hard disk from computer by brute force, they can immediately access the valuable data in the hard disk which may cause the leakage of confidential information.

In view of the above methods, many computer manufacturers and information security companies adopt software encryption to protect the hard disk data. All the data on the hard drive is protected by using this hard disk encryption technology which greatly reduces the risk of confidential data leakage. Disk encryption technology enables the data storage on the disk in the form of ciphertext while operating system can access and use these data in the way of real-time decryption. This technology can effectively solve the problem of data confidentiality in the case of computer stolen or lost.

Pretty Good Privacy (PGP) software is confirmed as a secure and reliable encryption software after enduring a large amount of safety testing and verification since it is announced. Utill now, no back door has been found in this software [2]. PGP Desktop encryption software contains all the functionality of PGP encryption technology and integrates the PGP disk encryption tools which provides much convenience for the security of personal data storage.

There are many versions of PGP currently and the final free available version is PGP 10.0.2[3]. Due to the effect of purchase by Symantec Corporation, PGP is no longer released separately as a stand-alone installation package after version 10.0.2 but exists in the form of integrated plug-ins

© 2015. The authors - Published by Atlantis Press

contained in other commercial security products of Symantec Norton company [4]. Hence, the majority of Internet users employ PGP 10.0.2.

Encryption protection is a double-edged sword. On the one hand, it conveniently prevents the private information to be leaked. However, the encryption mode also provides an opportunity for some criminals to engage in illegal activities, which induces that it is more difficult to implement investigation and evidence collection for those criminal activities of property infringement, corrupt transaction and even worse cases of affecting market economic order, national security and social stability.

So, the research on recovery of PGP encrypted virtual disk is greatly significant to prevent and investigate behaviors of leaking national secrets, terrorism and other criminal activities.

The Working Principles of PGP Encrypted Virtual Disk

PGP virtual disk is on the level of disk encryption, it can exploit a part of disk space to store sensitive data and this exclusive space is used to create a PGP disk encryption volume (.PGD files). The encryption volume can provide sufficient operations including files storage and application program running and so on, although the encrypted volume looks like a separate file.

When a PGP disk encryption volume is mounted, we can use the disk location of PGP Disk encryption volume specified as a normal disk. For example, a user can install software in this volume or move and save confidential documents to this volume. When we do not use the encrypted volume, it can be unmounted immediately. However, the differece between PGP disk encryption volume and other mounted disk is that it provides the passphrase to control the mount of virtual disk, one will not be able to access to it unless he knows the correct password.

When creating a new PGP disk encryption volume, system will require the user to select the file storage location, volume size, disk drive name and password of protecting this virtual volume. A PGD file is generated after volume creation. The mounted virtual disk will be protected by the password and it is encrypted in the state of unmounted. PGD files can also perform operations of deleting, copying or moving. Generally, PGP disk encryption volume exists in the form of a partition, but also can be used as a directory on NTFS partitions.

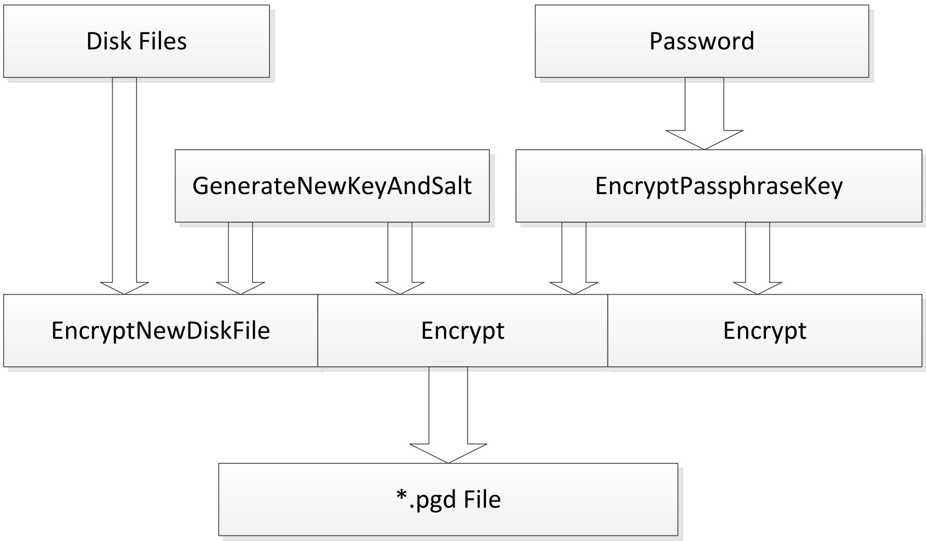


Fig. 1． The implementation of PGP disk encryption based on password

The specific procedure of creating encrypted volume and function implementation is as follows:

(1) generate a new session key, every session key is unique corresponding to every encryption operation. A new session key data and salt is created from the random data and used for symmetric key encryption algorithm. Concretely, function entrance named "GenerateNewKeyAndSalt" calls function "GetRandomBytes" to generate key data "KeyData", salt "Salt" and random number of malicious tampered data "MungeData". Function "GenerateNewSymmetricKey" makes use of the above data to generate a new key of a symmetric key algorithm according to the different algorithms where PGP Disk supports symmetric algorithms including AES-256, CAST5-128,

Twofish-128.

(2) user enters the password and this password is directly used as key of a symmetric encryption algorithm to encrypt random generated session key. After the user input password, system calls function entrance "EncryptPassphraseKey" to complete processing of password and session key encryption. Function "HashSaltSchedulePassphrase" adds salt value and hashes the password to protect the security of the password, then calls function Encrypt to encrypt the session key with encrypted password and calculate the checksum value of password used for decryption verification, where algorithm include AES-256, CAST-128, Twofish-256.

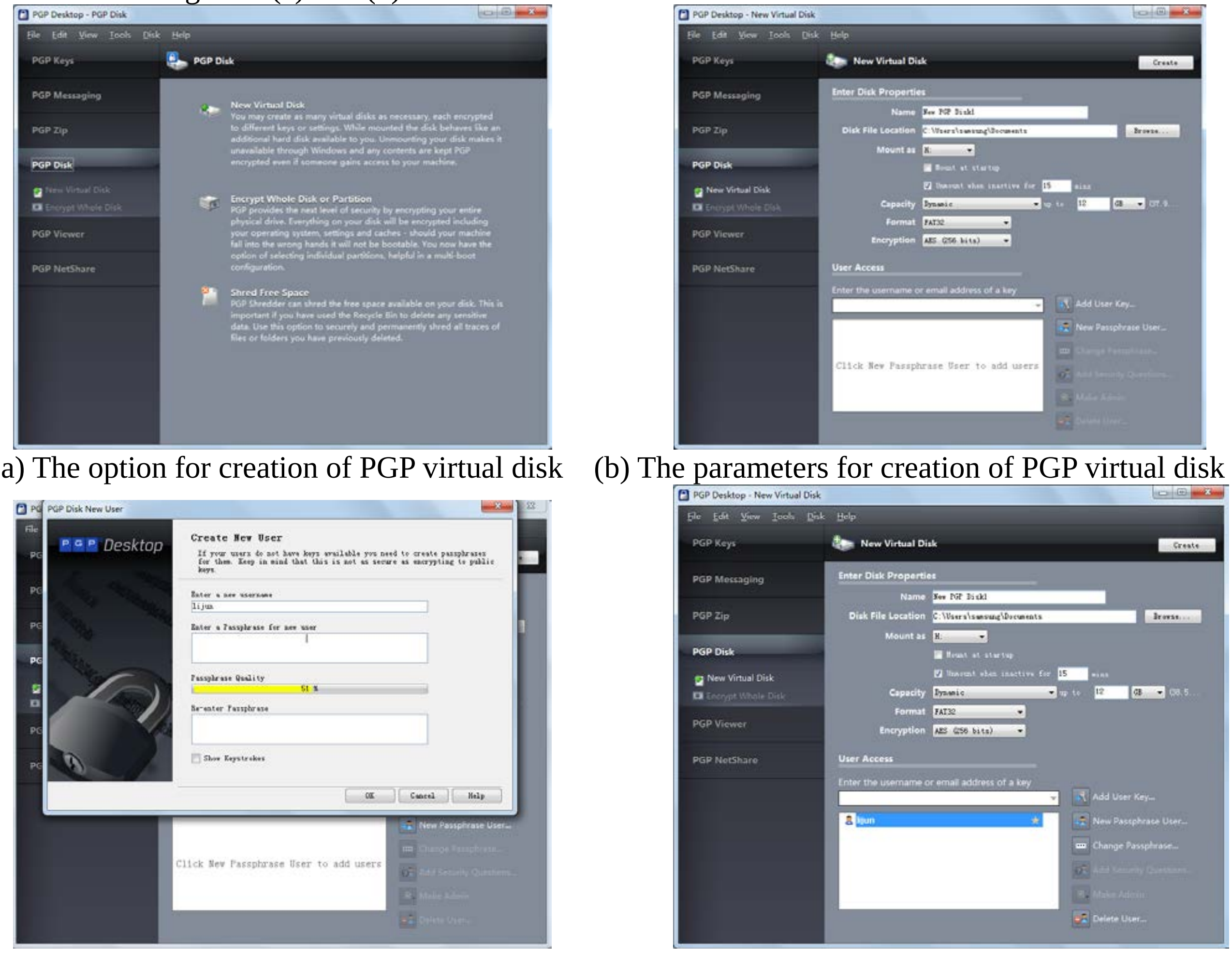
(3) Function "EncryptNewPGPdiskFile" uses the session key as the key of symmetric cryptographic algorithm to encrypt disk files. First, it will calculate the disk size that is required to encrypt, then encrypt the disk by using the chosen encryption algorithm in CFB operation mode and finally generate PGD file. The optional algorithms are AES-256, CAST-128, Twofish-128. The implementation of PGP encryption is described in Figure 1.

The Creation and Mount of PGP Disk Volume

A. *The Creation of PGP Disk Volume*

The creation process of PGP virtual disk volume is as follows.

(1)First, open the PGP desktop software and click the new virtual disk PGP disk options to start creation as in Figure 2 (a) and (b).



New Virtual Disk
You may create as many virtual disks as necessary, each encrypted to different keys or settings. While mounted the disk behaves like an additional hard disk available to you. Unmounting your disk makes it unavailable through Windows and any contents are kept PGP encrypted even if someone gains access to your machine.

Encrypt Whole Disk or Partition
PGP provides the next level of security by encrypting your entire physical drive. Everything on your disk will be encrypted including your operating system, settings and caches - should your machine fall into the wrong hands it will not be bootable. You now have the option of selecting individual partitions, helpful in a multi-boot configuration.

Shred Free Space
PGP Shredder can shred the free space available on your disk. This is important if you have used the Recycle Bin to delete any sensitive data. Use this option to securely and permanently shred all traces of files or folders you have previously deleted.

(a) The option for creation of PGP virtual disk

Enter Disk Properties
Name: New PGP Disk1
Disk File Location: C:\Users\samsung\Documents
Mount as: H:
□ Mount at startup
☑ Unmount when inactive for 15 mins
Capacity: Dynamic up to 12 GB
Format: FAT32
Encryption: AES (256 bits)

User Access
Enter the username or email address of a key
Click New Passphrase User to add users

(b) The parameters for creation of PGP virtual disk

Create New User
If your users do not have keys available you need to create passphrases for them. Keep in mind that this is not as secure as encrypting to public keys.
Enter a new username: lijun
Enter a Passphrase for new user
Passphrase Quality: 51 %
Re-enter Passphrase
□ Show Keystrokes
Click New Passphrase User to add users

(c)Set the password for virtual disk volume

Enter Disk Properties
Name: New PGP Disk1
Disk File Location: C:\Users\samsung\Documents
Mount as: H:
□ Mount at startup
☑ Unmount when inactive for 15 mins
Capacity: Dynamic up to 12 GB
Format: FAT32
Encryption: AES (256 bits)

User Access
Enter the username or email address of a key
lijun

(d) The successful creation of virtual disk volume

Fig. 2． The Creation of PGP Disk Volume

(2)Change the attribute of virtual disk according to the requirement and click "New PassPhrase User…" button to add user and passphrase. Then input user's password as shown in Figure 2 (c).

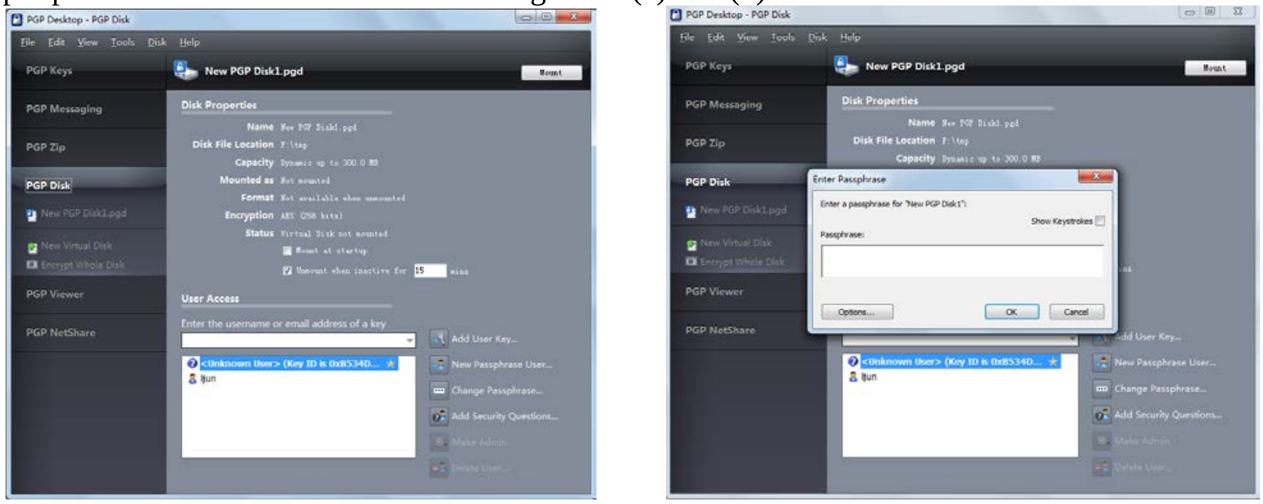
(3)After click OK button, the virtual disk encryption volume will be created successfully as shown in Figure 2 (d).

B. *The Mount of PGP Disk Volume*

The mount process of PGP virtual disk volume is as follows.

(1)Open the PGP desktop software, click on "open" option in the "file" menu.

(2)Double-click the selected virtual disk encryption volume file, then click "mount" button and input password and confirm as shown in Figures 3 (a) and (b).



New PGP Disk1.pgd

Disk Properties

Name New PGP Disk1.pgd

Disk File Location F:\tmp

Capacity Dynamic up to 300.0 MB

Mounted as Not mounted

Format Not available when unmounted

Encryption AES (256 bits)

Status Virtual Disk not mounted

□ Mount at startup

☑ Unmount when inactive for 15 mins

User Access

Enter the username or email address of a key

<Unknown User> (Key ID is 0x8534D... ★

ljun

Enter Passphrase

Enter a passphrase for "New PGP Disk1":

Show Keystrokes □

Passphrase:

(a) Select the PGP virtual disk volume to mount (b)Enter the correct password of disk volume

Fig. 3. The Mount of PGP Disk Volume

If the mount is successful, then there will be a disk partition named "New PGP Disk1 (H:)" in hard disk of "my computer".

The Cracking of PGP Encrypted Virtual Disk

According to the encryption principle of PGP virtual disk in Figure 1 and reverse engineering technology[5], we are able to crack the virtual disk encryption. Now we give the main process of cracking.

Step 1. Acquire the algorithm identification "PGPpgdEn -Algorithm", random number "PGPpgdSALT", checksum value "PGApgdCheckData" and hash iteration times "PGPpgdHash -Reps" from the virtual disk encryption file. Go to step 2.

Step 2. Calculate the hash value "HashedPassphrase" of password by SHA-1 algorithm. Go to step 3.

Step 3. Generate the hash value "Key" by using SHA-1 algorithm to deal "PGPpgdSALT" and "HashedPassphrase" with times " PGPpgdHashReps". Go to step 4.

Step 4. If PGPpgdEnAlgorithm = 3 then go to step 6; otherwise use SHA1 algorithm to get the hash value " HashedPassphrase" of "Key||PassPhrase" and go to step 5.

Step 5. Generate the hash value "HashValue" by using SHA-1 algorithm to deal "PGPpgdSALT" and "Hashed-Passphrase" with times " PGPpgdHashReps", then combine some bytes of "HashValue" and "Key" to form a new value "Key". Go to step 6.

Step 6. Calculate the ciphertext value "CheckData" of "Key" by the encrytion algorithm corresponding to "PGPpgd-EnAlgorithm", and go to step 7.

Step 7. If the value "CheckData" and "PGApgdCheckData" matches, then output this correct password, otherwise go to step (2).

The whole cracking process is described in Figure 4.

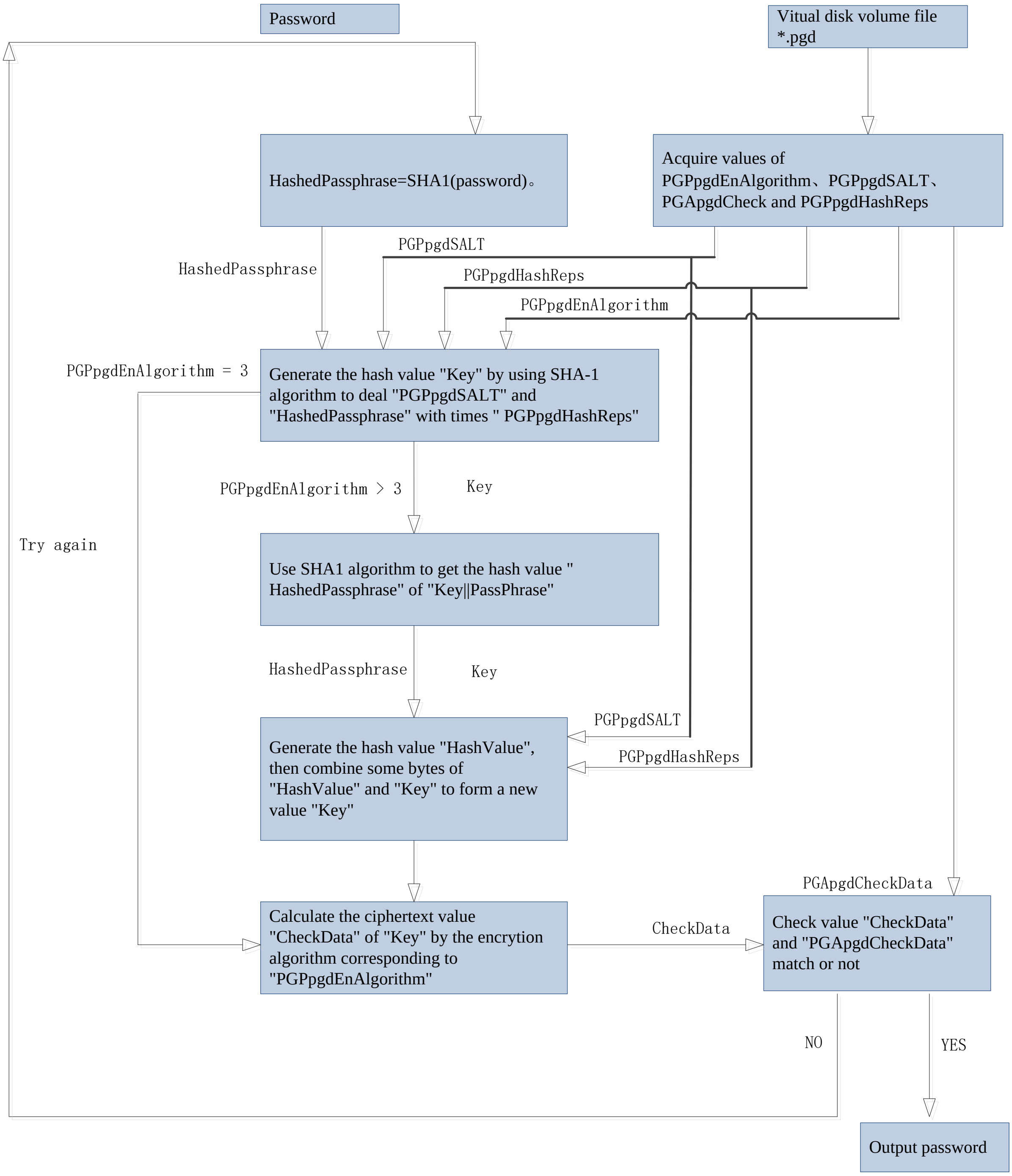

Password
Vitual disk volume file *.pgd
HashedPassphrase=SHA1(password)。
Acquire values of PGPpgdEnAlgorithm、PGPpgdSALT、PGApgdCheck and PGPpgdHashReps
HashedPassphrase
PGPpgdSALT
PGPpgdHashReps
PGPpgdEnAlgorithm
PGPpgdEnAlgorithm = 3
Generate the hash value "Key" by using SHA-1 algorithm to deal "PGPpgdSALT" and "HashedPassphrase" with times " PGPpgdHashReps"
PGPpgdEnAlgorithm > 3
Key
Try again
Use SHA1 algorithm to get the hash value " HashedPassphrase" of "Key||PassPhrase"
HashedPassphrase
Key
PGPpgdSALT
PGPpgdHashReps
Generate the hash value "HashValue", then combine some bytes of "HashValue" and "Key" to form a new value "Key"
PGApgdCheckData
Calculate the ciphertext value "CheckData" of "Key" by the encrytion algorithm corresponding to "PGPpgdEnAlgorithm"
CheckData
Check value "CheckData" and "PGApgdCheckData" match or not
NO
YES
Output password

Fig. 4. The cracking process of PGP disk volume

Conclusion

This paper proposed a method of cracking PGP encrypted virtual disk volume and the effect of cracking will be better if combining with the dictionary cracking technology based on social engineering. This cracking method is of great significance for the prevention and investigation of leaking national secret, terrorism and other criminal activities.

References

[1]LIU Jing jing , YI Qing song, DAI Zi bin, Application of Hard Disk Encryption System in Information Security, Modern Electronic Technology, 2007, 256(17) : 101- 104.

[2]Philip R Zimmermann. No Back Doors. [2010-04-06]. http://www.philzimmer mann.com

/EN/back ground/index.html.

[3]PGP Corporation Home Page[Z].http://www.pgp.com/.

[4]http://www.symantec.com/business/theme.jsp?themeid=pgp.

[5]Deng Huijie, PGP Cracking Research and Implementation against Passphrase, thesis, Shanghai Jiaotong University, 2011.