学校编码：10384　　分类号____密级____

学号：23320141153248　　UDC_____

厦门大学

硕 士 学 位 论 文

PGP Desktop 加密磁盘口令恢复技术的研究与实现

Research and Implementation of Disk Passphrase Retrieve Technology on PGP Desktop

胡军

指导教师姓名：洪景新 高级工程师

专 业 名 称：电子与通信工程

论文提交日期：2017 年　　月

论文答辩时间：2017 年　　月

学位授予日期：2017 年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2017 年　　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

无论是在传统的通信时代，还是在现在的互联网时代，信息安全的重要性从来都没有改变过，特别是在信息泄露事件和网络诈骗事件频发的今天，每个人都应该比以往更注重保护个人信息和隐私。PGP Desktop 所具备的诸多功能就可以为我们的重要数据和个人信息保驾护航。但是无论用户使用 PGP Desktop 加密哪种类型的数据，都需要用户设置一个口令，这个口令可以在解密数据时起到验证用户合法性的作用。如果用户在一段时间后遗忘了加密数据时使用的口令，那么用户将无法再使用这些加密的重要数据。本文所做的研究就是为 PGP Desktop 用户提供一系列方案解决遗忘加密磁盘时使用的口令的问题。

磁盘加密功能是 PGP Desktop 的几大重要功能之一。PGP Desktop 中的磁盘加密功能又可以分为对虚拟磁盘加密和对物理磁盘加密两种类型，这两类磁盘加密功能都支持两种类型的用户，即密钥环用户和普通用户。密钥环用户是指使用非对称加密算法保护会话密钥的用户，而普通用户是指使用对称加密算法保护会话密钥的用户。这两类用户口令的作用是有区别的，密钥环用户口令的作用是保护用户的私钥，而普通用户口令的作用是直接保护会话密钥。本文研究的重点就是如何恢复虚拟磁盘以及物理磁盘的密钥环用户和普通用户的口令。目前针对这方面的研究工作非常少，并且还没有关于如何恢复物理磁盘上普通用户口令的研究工作。

本文使用的研究方法是分析磁盘的结构和 16 进制数据，寻找与验证用户口令的相关的参数，然后根据 PGP Desktop 早期开源的一些代码，理清这些参数的含义，再根据这些已知的参数，研究两类磁盘中不同用户口令验证的步骤，最后使用字典枚举的方式在可能的解空间中寻找用户的口令。为了验证方案的可行性和性能，使用 Visual Studio 2015 编码实现这套方案。最终本文会给出三套方案，分别是通用的密钥环用户口令恢复方案、虚拟磁盘中普通用户口令恢复方案以及物理磁盘中普通用户口令恢复方案。其中方案一与现有方案相比，可以支持更多类型的密钥；方案二和方案三是目前公开发表的唯一能够解决此类问题的方案。

关键字：PGP 磁盘；口令恢复；密码破解.

Abstract

Whether in the traditional communication era, or in the current Internet age, the importance of personal information security has never changed. In particular, taking into account frequent information disclosure incidents and cyber scams, everyone should pay more attention to protecting personal information and privacy than ever before. PGP Desktop has a number of features that can protect our important data and information. However, no mater what kind of data that user want to encrypt by using PGP Desktop, a passphrase should be set when encrypting the data. This passphrase can be used to verify the legitimacy of the user when decrypting the data. If the user forgets the passphrase used for encrypting the data after a certain period of time, these encrypted important data will never be decrypted again. What we have done in this research is to help the PGP Desktop users resolving problem that they may forget the passphrase which they have used to protect their data or information.

Disk encryption is one of the most important features of PGP Desktop, which can encrypt two types of disks, vitraul disks and physical disks. Each kind of disk supports two types of users, key ring users and passphrase users. The difference between the two types of users is that the key ring user protect the session key by using asymmetric encryption algorithms while the passphrase user using symmetric algorithms. Furthermore, the passphrase of key ring user is used to protect user's private key while the passphrase of passphrase user is used to protect session key directly. What we focus on in this research is how to retrieve the passphrases of both two types of users in virtual disks and physical disks. At present, there is very little work on this area, and no one has studied how to retrieve passphrase of passphrase user from physical disk.

In order to achieve the purpose of the research, we firstly analyze the structure of the disk and its hexadecimal data, and then find the parameters that are related to the user's authentication. Secondly figure out the meaning of these parameters according to source code of PGP system and study the procedure of different user passphrase verification in different disk. Finally search the user's passphrase in possible passphrase sets by way of enumerating. In order to verify the feasibility and performance of this research, a program will be developed by using Microsoft Visual

Studio 2015. At last, there are three schemes proposed in this paper, the universal key ring user's passphrase retrieve scheme, the passphrase retrieve scheme of passphrase user in virtual disk and the passphrase retrieve scheme of passphrase user in physical disk. Respectively, comparing with the similar scheme, the first scheme can retrieve both of RSA and DH key ring user's passphrase. In addition, the third scheme are proposeed for the first time, and no one else has proposed.

Key Words: PGP Disk encryption; Passphrase retrieve; Brute-force.

目 录

Table of Contents