

基于认证授权的文件安全保险箱技术研究与实践

董晓宁¹, 吴晓平², 李洪成²

(1. 海军驻北京地区通信军代室, 北京 100000;
2. 海军工程大学信息安全系, 湖北 武汉 430033)

摘要: 针对现有的文件保险箱缺乏文件管理机制和在线身份认证的问题, 设计并实现了基于认证授权的文件安全保险箱系统。系统首先对文件保险箱的用户进行在线身份认证, 避免非法用户登录, 并利用服务器收集客户端上对机密文件的敏感操作行为事件, 进而对用户操作进行细粒度集中授权管理, 避免了内部用户的非法操作和误操作。通过测试表明, 系统实现了预定的功能, 具有良好的通用性和适用性。

关键词: 文件保险箱; 在线认证; 授权管理; 远程控制

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00054

Research and implement of file safe deposit box based on authentication and authorization

DONG Xiao-ning¹, WU Xiao-ping², LI Hong-cheng²

(1. Naval Communications Army Generation Room in Beijing, Beijing 100000, China;
2. Department of Information Security, Naval University of Engineering, Wuhan 430033, China)

Abstract: Considering that the existing file safe deposit boxes lack online authentication and server authorization, a file safe deposit box based on authentication and authorization was designed and achieved. This system firstly identified the users of the file box online, thus avoiding the illegal users to login. Moreover, the master collected the operation events exerted on the files in the clients, and the master provided a granular authentication for the operation of users, thus avoiding the illegal operation and incorrect operation. The test of this system proved that it can be able to achieve the preset functions and can be widely used in many conditions.

Key words: file safe deposit box, online authentication, authorization management, telnet control

1 引言

近年来, 伴随着全球信息化的大潮流, 整个社会的运转越来越密切地依赖于信息技术, 然而随着信息技术的发展和越来越广泛的应用, 计算机和网络已成为行政部门、军队和企业日常办公的必备工具和途径, 数据存储安全逐渐成为应用

计算机系统的一个首要问题^[1~3]。解决这个问题的一种方式就是数据加密, 文件安全保险箱系统作为其中一种工具应运而生^[4,5]。

文件保险箱的安全性关系到用户文件的安全性, 如果系统本身存在任何安全漏洞都会给用户带来不可估量的损失^[6~8]。企业中与业务相关的内部机密文件分布在各个内部局域网计算机中, 常

收稿日期: 2016-04-02; 修回日期: 2016-05-05。通信作者: 董晓宁, yztzyb2b@yahoo.com

基金项目: 国家自然科学基金资助项目 (No.61100042); 湖北省自然科学基金资助项目 (No.2015CFC867)

Foundation Items: The National Natural Science Foundation of China (No.61100042), The Natural Science Foundation of Hubei Province (No.2015CFC867)

面临以下安全隐患^[9]。

1) 缺乏强制性保护措施。无法防范工作人员故意或无意的泄密。

2) 缺乏对用户身份的认证。如果没有对用户身份的认证,任何用户都可以加载文件保险箱,给系统的安全性带来了极大的隐患。

3) 缺乏基于角色的用户权限管理措施。没有建立文件使用权限和用户角色之间的对应关系,无法实现细粒度访问控制。

针对以上不足,本文设计并实现了一种基于认证授权的文件安全保险箱系统。该系统的优势主要体现在以下方面。

1) 基于角色的用户权限管理。通过建立员工、角色、权限之间互相对应的关系,为不同级别的员工建立各种不同的功能权限。

2) 文档应用权限细分。针对企业文档使用级别、使用范围不同进行权限上的细分:修改属性、移出、打印、拷贝、删除、拷屏、刻录、权限传递以及可设置所有可执行操作的可打开具体时间、次数,为用户提供更加科学的权限管理机制。

3) 全面的日志审计功能。通过记录终端用户操作过程的记录以及对突发安全事件的详细记录、分析,对企业数据信息进行全面审核,为企业内部泄密事件提供强有力的追踪依据。

2 文件安全保险箱系统设计

本文件安全保险箱系统的主要功能应包括以下几个方面。

1) 基本功能:主要实现文件的保密存储和加解密功能。

2) 安全功能:主要实现文件保险箱系统的使用安全,包括在线身份认证、文件及消息的保密传输等功能。

3) 管理功能:主要实现用户保险箱的集中管理功能,包括密钥分发管理、生成审计日志、特殊操作管理、用户权限管理、共享文件传输等功能。

为实现以上功能,本系统主要分为2个模块:在线认证模块和文件操作授权管理模块。下面分别对这2个模块的设计原理进行具体介绍。

2.1 在线认证模块设计

用户文件保险箱上密文的解密密钥存放在服

务器端,该解密密钥是本系统的重要机密信息。在线认证模块是保证文件解密密钥信息机密性和完整性的基础,同时为C/S间文件传输提供认证。

本系统采用基于散列函数的口令认证方式,使用口令和用户信息经过多次执行散列运算得到认证信息。这种认证方案的优点是:1) 利用散列函数对口令、密钥等短消息加密简单高效且安全性较高,有效防止信道上的窃取攻击;2) 用户的身份信息和登录凭据经过散列处理后,存储在服务器数据库中,避免了机密信息以明文形式存储在数据库中所带来的对安全性的损害。

文件安全保险箱系统在线认证流程如图1所示。

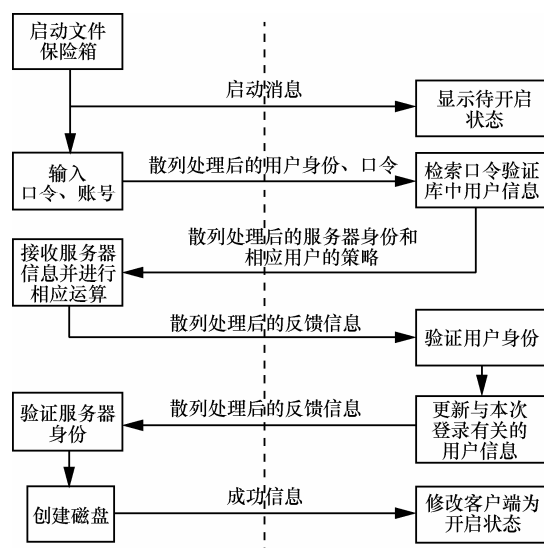


图1 文件安全保险箱系统在线认证流程

2.2 文件操作授权管理模块设计

文件操作管理模块是文件保险箱系统安全性的一个关键部分,主要防止非授权用户窃取文件以及减少因用户误操作而带来的损失。

文件操作管理主要是针对可能造成信息泄露的某些特殊操作,这些特殊操作会对系统的安全性造成很大的安全隐患。具体操作类型如下。

1) 从保险箱移出文件操作

文件从保险箱移出就不再具有保密性,被移出文件的安全性将无法得到任何保障,可被随意窃取。

2) 打印文件

非法用户如果打印文件就能直接窃取到机密文件,这一操作对系统的安全性造成了极大的威胁。

3) 多次登录失败

如果某一用户连续登录失败,则很可能是非

法用户对系统进行口令猜测攻击。

4) 异常时间登录

若有用户在 0:00~3:00 之间执行开启文件保险箱操作, 则极有可能是非法用户登录。

5) 长时间无操作

如果用户长时间没有进行任何操作, 很可能用户有事离开或者用户忘记关闭, 这会给非法操作者可乘之机。

针对以上安全隐患, 本系统对文件操作进行如下控制。

1) 当用户进行移出操作时, 系统管理员根据用户移出的文件和用户的级别来判断是否允许其进行相应的操作, 并发送相应操作指令; 对于打印、删除等操作控制策略与移出基本相同。

2) 当用户连续登录失败时, 如果次数达到 5 次, 系统 1 h 内不允许该用户进行登录, 并且在服务器端弹出警告, 通知管理员该用户连续登录失败。

3) 当用户成功登录后, 如果 5 min 没有对文件进行任何操作, 系统就强制关闭文件保险箱, 退出到登录界面, 要求用户输入口令, 防止因用户离开, 其他操作者对文件进行非法操作。

4) 当服务器检测到审计日志文件中接收到的审计消息中用户登录时间为 0:00~3:00 之间时, 管理者界面弹出警告窗口, 提示该异常操作。

文件操作授权管理的流程如图 2 所示。

3 文件安全保险箱系统实现

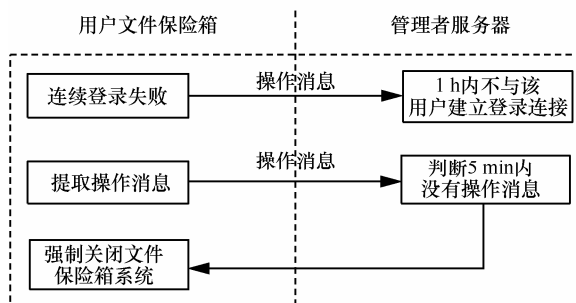
3.1 系统环境与开发平台

系统的开发环境是 Microsoft .NET Framework 4.0, 文件保险箱服务器需要安装 SQL Sever 2008 Express 或更高版本。

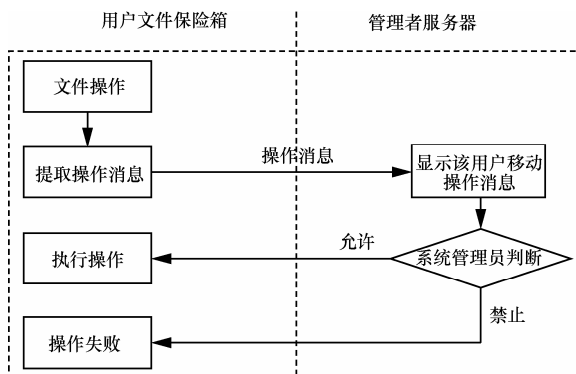
开发平台: Microsoft Visual Studio 2010 旗舰版。本系统采用 C# 语言编写, 运用面向对象技术, 基于 .NET 框架开发, 继承了自动内存管理和垃圾回收的机制, 使程序本身的构造与析构都更加方便容易, 在具体编写程序时不需要为释放空间而费心^[10]。

3.2 在线认证模块实现

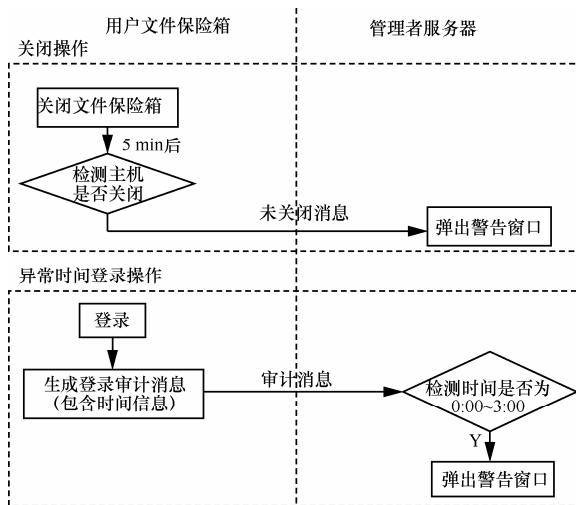
在线认证模块中, 运用了散列运算, 建立了用户信息库。部分代码如图 3 所示。



(a) 集中管理服务工作流程1



(b) 集中管理服务工作流程2



(c) 集中管理服务工作流程3

图 2 集中管理服务工作流程

```

private void Send(string uid, string pwd)
{
    Md5_uid = getMd5Hash(uid);
    Md5_pwd = getMd5Hash(pwd);
    Login(Md5_uid, Md5_pwd);
}
...
public void Login(string userName, string password)
{
    WriteTokens("LOGIN", userName, password, SubjectName);
}
  
```

图 3 在线认证部分代码

本用户信息库存储在本项目所用数据库中, 本系统设计过程中使用 SQL Server 2008 数据库。存储用户信息的用户信息表 dbo.user 设计如图 4 所示。

列名	数据类型	允许 Null 值
用户ID	nvarchar(10)	
用户密码	nvarchar(10)	
用户名	ntext	
用户级别	char(10)	
单位	ntext	
职务	ntext	
计算机名	nvarchar(30)	
Mac地址	nvarchar(30)	
用户手机	float	
用户状态	char(10)	
账户状态	char(10)	

图 4 用户信息表设计

用户信息表中存储的示例用户信息，如图 5 所示。

用户ID	用户密码	用户名	用户级别	单位	职务	计算机名	Mac地址	用户手机	用户状态	账户状态
1	123	66666	武大	A	董事长	PC-20110123U0ES	00-23-5A-74-47-E3	18900000000	在线	存在
2	456	123456	武二	B	纳管部 经理	PC-20110115U0ES	00-23-5A-74-47-C5	13600000000	离线	存在

图 5 示例用户信息

3.3 文件操作授权管理模块实现

若客户端对所存储的机密文件进行了非法操作（如非法拷贝到 U 盘或其他盘符下等）时，系统将会对此类操作进行监控管理。若要对客户端上存放的机密文件进行监控，需要设计一个文件监控管理守护模块，该模块与文件保险箱中的所有机密文件进行关联，一旦机密文件遭到非法操作时，监控管理守护模块将自动向服务器端触发一条消息，提示服务器客户端对机密文件进行非法操作，一些善意的文件操作动作（如合法客户端需要拷贝某个文件）时，只有得到服务器端的许可才允许执行，否则禁止。

其监控管理守护模块中的主要函数为

```
Void MoniorFile(string strFileName; string strFilePath; UNIT uFileState; string strMessage);
```

其中，strFileName 为文件名称；strFilePath 为文件路径；uFileState 为文件状态（如是否执行拷贝）；strMessage 为向服务器提交的告警消息内容。

文件共享传输也是文件操作的主要功类型之一。本系统中的文件传输利用 Socket 协议来实现，其服务器端示例代码如图 6 所示。

```
private void Receive(Socket socket)
{
    NetworkStream ns = new NetworkStream(socket);
    FileStream fs = new FileStream("c:\\file.txt", FileMode.OpenOrCreate);
    bool isRead = true;
    ...
    this.txtFile.Text = "文件传输成功";
    fs.Close();
}
```

图 6 文件共享功能服务器端示例代码

Socket 协议的客户端示例代码如图 7 所示。

```
private void btSend_Click(object sender, System.EventArgs e)
{
    if (this._isConnect)
    {
        _ns = _tc.GetStream();
        string path = this.txtPath.Text.Trim();
        FileStream fs = new FileStream(path, FileMode.Open);
        ...
        fs.Close();
    }
}
```

图 7 文件共享功能客户端示例代码

4 系统功能及性能测试

4.1 测试环境

1) 硬件环境

联想 Y450, Intel Core2 双核, CPU T6600 主频 2.2 GHz, 内存 2.0 G, Windows7 操作系统; 宏基 4 740 G, Intel Core2 双核, CPU i3 主频 2.13 GHz, 内存 2.0 GB, Windows7 操作系统。

2) 软件环境

Windows 7 操作系统, Windows XP 操作系统, Microsoft Visual Studio 2010, SQL Server 2008 Express Edition。

4.2 认证及授权功能测试

通过用户认证功能测试发现，用户可以及时准确地通过认证并登录文件保险箱系统，认证后在服务器端的显示结果如图 8 所示。



图 8 认证功能测试结果界面

通过用户认证功能测试发现，服务器可以实现对用户角色的分类管理，并分配相应的权限，其管理界面如图 9 所示。



图 9 用户角色管理界面

此外,服务器可以对用户已进行的各类操作进行审计,便于管理员事后查看,文件操作管理审计界面如图 10 所示。



图 10 用户操作授权管理审计界面

4.3 服务器负载性能测试

服务器是整个网络系统和计算平台的核心,许多重要的数据都保存在服务器上,很多网络服务都在服务器上运行,因此服务器性能的好坏决定了整个应用系统的性能。通过模拟多个用户实施并发负载及实时性能监测的方式来测试服务器的负载性能是必不可少的。对服务器的测试如下:运行服务器端并开始监控网络;多个客户端同时运行,当听到口令时进行登录;查看客户端登录成功率;多个客户端同时连续进行多种不同文件操作;查看服务器端登录日志记录是否与客户端登录情况和用户操作匹配。

通过表 1 的测试结果可以看出服务器运行良好,没有出现错误,可以较好负载整个文件保险箱系统的运行。

表 1 服务器负载性能测试结果

客户端数量	登录成功率	服务器日志记录匹配情况	耗时
20	100%	记录完整,没有漏记情况	10 min

5 结束语

目前,政府公文失窃、军事机密泄露、商业秘密外泄等一系列问题成为电子文件的一大弊端,如何高效安全地实现电子文件的保密存储成为众多部门的一大难题。本文件保险箱系统可以在远程认证用户身份,并对用户的文件操作在线管理。因此,本系统在政府行政机关、军队保密部门、企事业单位等需要保密的部门具有良好的应用前景。

参考文献:

[1] 李成东,徐飞.一种基于 USBKEY 的文件保险箱系统设计与实

现[J].软件学报,2013,10(5):11-15.

- LI C D, XU F. A USBKEY based file system design and implementation of safe[J]. Journal of Software, 2013, 10 (5): 11-15.
- [2] 熊厚仁,陈性元,费晓飞,等.基于属性和 RBAC 的混合扩展访问控制模型[J].计算机应用研究,2015,34(9):29-33.
- XIONG H R, CHEN X Y, FEI X F, et al. The mixed extent access control model based on attribute and RBAC [J]. Computer Application Research, 2015, 34 (9) : 29-33.
- [3] 叶重阳,庄毅.一种基于多维信任度的动态 RBAC 模型[J].计算机与现代化,2015,19(8):20-24.
- YE C Y, ZHUANG Y. A dynamic RBAC model based on multi-dimensional trust[J]. Computer and Modern, 2015, 19 (8):20 -24.
- [4] 戈泉月,车力军.基于多因素认证的网络安全支付模式研究[J].信息网络安全,2015,(12):48-59.
- GE Q Y, CHE L J. Network secure payment mode study based on multi-factor authentication [J]. Information Network Security, 2015, (12): 48-59.
- [5] 戈泉月,车力军.基于 SELinux 强制访问控制的进程权限控制技术研究与实现[J].信息网络安全,2015,(12):34-42.
- GE Q Y, CHE L J. Research and implementation of the process of access control technology based on SELinux mandatory access control[J]. Information Network Security, 2015, (12):34-42
- [6] 白辉.在线授权认证平台的设计与实现[D].广州:华南理工大学,2010.
- BAI H. The design and implementation of online authorization certification platform [D]. Guangzhou: South China University of Technology, 2010.
- [7] 张悦,郑东,张应辉.支持动态授权和文件评价的访问控制机制[J].计算机应用,2015,32(4):127-131.
- ZHANG Y, ZHENG D, ZHANG Y H. Access control mechanism which support dynamic authorization and file evaluation[J]. Journal of Computer Applications, 2015, 32(4): 127-131.
- [8] 沈洋.安全文件服务系统的研究与开发[D].武汉:武汉理工大学,2014.
- SHEN Y. The research and development of the security file service system[D]. Wuhan: Wuhan University of Technology, 2014.
- [9] 张红林.分布式文件系统中集中安全管理服务器设计与实现[D].武汉:华中科技大学,2011.
- ZHANG H L. Design and implementation of centralized safety management server in distributed file system [D]. Wuhan: Huazhong University of Science and Technology, 2011.
- [10] 马骏,郑逢斌,沈夏炯.C#网络应用高级编程[M].北京:人民邮电出版社,2006:59-67.
- MA J, ZHENG F B, SHEN X J. High-level programming of C# network application [M]. Beijing: People's Posts and Telecommunications Press, 2006:59-67.

作者简介:



董晓宁(1964-),男,河北唐山人,海军驻北京地区通信军代室高级工程师,主要研究方向为信息系统安全防护。

吴晓平(1961-),男,山西新绛人,博士,海军工程大学教授、博士生导师,主要研究方向为信息安全、密码学。

李洪成(1991-),男,河南商丘人,海军工程大学博士生,主要研究方向为信息安全、密码学。