新型双因子认证系统①

王振铎[1], 王振辉[2], 张慧娥[1], 陈绥阳[3]

[1](西安思源学院 电子信息工程学院, 西安 710038)
[2](西安翻译学院 工程技术学院, 西安 710105)
[3](西安交通大学 信息科学系, 西安 710049)

摘 要: 以传统的双因子认证技术作为研究对象, 分析了其不足之处. 提出身份标识文件(PIF)作为双因子认证中的第 2 个因子. 据此,设计了服务器端进行身份识别, 客户端进行身份认证独特的双因子认证系统. 并采用 J2EE 技术实现了该系统. 经实验表明, 与其它双因子认证技术相比, 具有易用、成本低、性能好的特点, 切实保障了身份认证的安全.

关键词: 身份认证; 双因子; 身份标识文件; 身份标识码

New Two Factor Authentication Systems

WANG Zhen-Duo[1], WANG Zhen-Hui[2], ZHANG Hui-E[1], CHEN Sui-Yang[3]

[1](School of Electronic & Information, College of Siyuan, Xi'an 710038, China)
[2](School of Technology and Engineering, Xi'an Fanyi University, Xi'an 710105, China)
[3](School of Information and Science, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: For the traditional two factor authentication technology, the paper analyzes its deficiency and puts forward using personal identity file as the second factor in the two factor authentication. Therefore, we designed the unique system which identification at server and authentication at client and realized this system by J2EE technology. Experiments show that compared with other two factor authentication technology, it has the characteristics of easy use, low cost, good performance, protect the authentication security effectively.

Key words: identity authentication; two factor; personal identify file; personal identify number

作为整个信息安全体系的基础, 身份认证是信息安全的第一道关隘. 如果缺乏有效的身份认证手段, 那么合法身份就很容易被伪造, 即使投入再多的资金, 建立再安全、坚固的安全防范体系都会形同虚设. 个人账号、密码如同开启系统的钥匙, 其安全性再度成为人们关注的焦点, 同时也是信息安全领域专家和学者研究的热点课题.

1 相关工作

双因子认证技术是指将密码以及实物(信用卡、手机、令牌或指纹)等标志结合起来, 形成两种条件对用户进行认证的方法[1]. 该技术作为传统的、行之有效的身份认证方式, 已经被金融、证券等关键行业或业务广泛采用. 据最新报道美国金融机构将加快采用双因子认证的步伐, 以便促使消费者习惯这一方法, 同时提高客户对静态口令安全的重视程度. 最近, 网易邮件系统, 也采用手机动态验证码和二维码方式实现了双因子认证. 为了更好地加强双因子认证的安全, 国内外许多学者做了大量的研究工作, 取得了不少成果. 如文献[2]的动态令牌技术、文献[3]智能卡技术、文献[4]的 UKEY 方式, 文献[5]生物特征识别方式, 文献[6]的手机密令方式. 经过实际应用和研究发现, 动态令牌方式属于一次性密码, 通过多重认证对用户身份进行鉴别, 安全性好. 但不同的网站需要用到不同的令牌, 当要访问很多公司的网站时, 可能并不想携带一大串的令牌. 智能卡和 UKEY 方式不利于随时携带,

① 基金项目:陕西省教育厅自然科学研究课题(14JK2087)
收稿时间:2015-04-10;收到修改稿时间:2015-05-12

并且使用时需要安装不同的驱动程序, 容易丢失, 需要进行妥善保管. 生物特征识别的认证方式, 虽然具有不易遗忘丢失, 防伪性能好, 随时随地可用, 不易伪造或者被盗等优点. 但是它还有一系列暂时不能克服的缺点. 主要表现在技术不完全成熟, 识别的准确性和稳定性急待提高, 研发成本高, 产量小和识别设备成本高, 现阶段难以推广和大规模应用, 对识别正确率没有确切的结论, 难以做到真正的唯一性和安全性[7]. 笔者查阅了大量文献, 新的双因子认证方式朝着智能穿戴方式发展. 比如, Nymi 公司采用的心电图穿戴技术, 利用独特的心跳节奏识别个人身份. 当人触摸穿戴式手镯时, 会产生一种模式用于鉴别用户. 但该技术仍处于试验阶段. 并且其成本和准确性等原因, 应用推广还有待时日[8].

2 系统设计

2.1 设计思想

双因子认证中, 密码是其中一个重要的因子, 而另一个关键因子, 主要是以下三类:

1) 被认证的人所知道的某个秘密, 比如, Passwords 或者 PIN;

2)被认证的人所拥有的某个东西, 比如, 数字证书, UKEY、智能卡等;

3)被认证的人所固有的生物特性, 比如, 指纹, 相貌, 声音, 耳廓等等.

双因子认证均属于配合用户名和密码验证方式的增强方式, 即上述 1+2 或者 1+3 模式. 而 1+2 的模式更容易做系统的迁移和维护.

在安全性要求高的系统中, 多采用 UKEY 和手机短信验证码、二维码的双因子方式. 即被认证人所拥有的某个东西及附属物. 这样就造成了需要额外的硬件设备. 能否不依赖于这些硬件, 实现双因子认证, 需要考虑的关键是怎样识别用户的身份. 日常生活中, 公安机关颁发的居民身份证就是最好的身份证明, 可以设计一个“电子身份证”, 作为双因子认证中的身份识别因子. 这个思想符合上述认证因素 1)和 2)的双重特性, 即用户所知道的秘密和拥有的物品. 故系统设计由个人身份标识文件(Personal Identify File 以下简称 PIF)和用户密码构成的双因子认证. PIF 用于用户身份真实性的识别, 该文件存放在客户端, 其中存放的数据称为身份标识码(Peronal Indetify Number 以下简称 PIN). 用户密码存放在服务器端, 但并非直接显示存放, 而是将用户的账号、密码加密形成的 PIN 存放在数据库中, 防止黑客“暴库”操作, 有效保护核心数据不外泄.

2.2 数据库设计

系统数据库设计关键是用户数据表的设计, 该表中主要存放以下用户数据, 见表 1, 从中可以看出该数据表, 并没有直接存放用户的敏感数据“账号”、“密码”信息, 原因见 2.1 节设计思想, 这里不再赘述.

表 1 用户信息表(tbl_user)

字段名	类型	长度	主键	备注
tu_pin	varchar	50	是	PIN 码
tu_name	varchar	20		姓名
tu_sex	char	2		性别
tu_zy	varchar	20		职业
tu_birthday	date	3		出生日期
tu_pn	char	11		手机号码
tu_mail	varchar	20		电子邮箱
tu_reg	datetime	8		注册时间

2.3 功能设计

系统采用 ssh 架构[9], 功能主要包括:

1)用户注册: 对系统中的用户信息进行采集.

2)用户登录: 用户身份核对.

3)密码修改: 用户更改密码.

4)密码找回: 忘记密码时, 密码找回功能.

5)重新索取 PIF 文件: 对于更换计算机的用户, 需要向服务器索取原来的 PIF 文件, 该项操作前, 有严格的身份确认.

系统关键功能是用户注册和用户登录, 用户注册时产生 PIF, 登录期间对 PIF 和密码两个因子按顺序进行认证, 下面主要介绍 PIF 和认证过程的设计思路.

2.3.1PIF 的产生

PIF 文件在用户注册时产生, 包括以下几个步骤:

1)用户填写个人信息, 客户端向服务器发送该信息;

2)服务器检测用户个人信息的有效性, 主要是账号的唯一性, 若已存在, 服务器提示用户重新输入账号;

3)否则, 将用户个人信息存储到用户表中, 同时在客户端输出个人 PIN 码(这个 PIN 码由用户账号和密码经严格加密组成), 用户自行拷贝 PIN 码到一个文件(PIF 文件)中, 比如 Key.kss 中. 如图 1 所示.

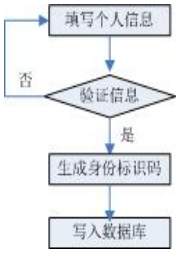

图 1 用户 PIF 产生过程

2.3.2 身份认证过程

系统认证过程分为两步. 首先进行用户身份识别, 其次进行用户认证. 包括以下几个步骤:

1)初次登录系统, 需要进行系统设置. 需要设置用户身份标识文件存放的位置及文件的名称(该名称前面举例为 key.kss, 用户也可以自行命名).

2)系统设置信息保存在 cookies 中, 为了防止黑客及病毒软件获取其中的信息, 提高安全性, 将文件名和目录名以字节方式按一定的规律加密存放在 cookies 中[10].

3)非首次登录, 系统自动从 cookies 中解密获取 PIF 文件目录及文件名, 读取用户的 PIN 码, 若未获得 PIF 文件, 则用户身份识别失败; 反之, 系统将 PIN 码发送到服务器, 与用户表中的 PIN 码进行逐一比对, 若一致的则用户身份识别成功, 反之身份识别失败.

4)身份识别成功, 立即进行用户身份认证. 传统的身份认证是将账号、密码发送到服务器端进行验证, 而本系统的这个工作仅在客户端进行. 客户端将 PIN 码解密得到账号、密码与用户输入的账号、密码进行比对, 若一致, 则认证成功, 否则认证失败. 认证过程如图 2 所示.

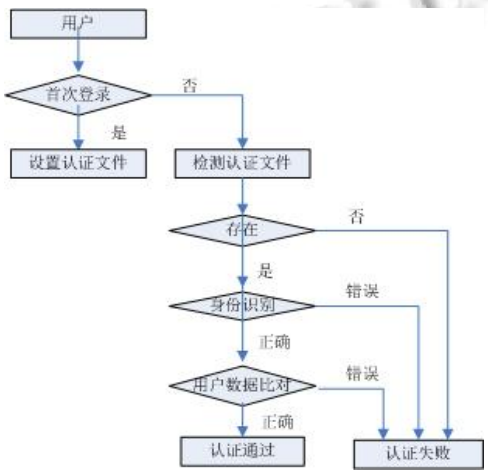

图 2 登录认证流程

修改密码、密码找回、重新索取 PIF 文件三个功能使用时, 也需要首先进行用户身份的识别, 这比其它系统的同样功能安全性高, 其中身份识别过程与用户登录认证过程相同, 这里不再赘述.

3 关键技术

系统利用 Jsp 技术实现, 包括两个页面: 注册(reg.jsp)、登录页面(login.jsp)、修改个人信息及密码(editinfo.jsp)、重新索取 PIF(regetpif.jsp)以及四个 JavaBean 组件: kss_helper.java, md5_helper.java, sql_helper.java, txt_helper, 分别实现 PIF 的生成, PIF 的加密, 个人身份的数据库验证以及文件操作. 系统中关键技术包括以下内容:

3.1 数据加解密

PIF 文件作为第 2 个认证因子, 其安全性至关重要, 也是本文认证的关键所在. 对于密码等少量数据的加密常采用单向加密算法. 单向加密算法主要有 MD5、SHA 等. 单向加密的特点是: 将明文生成密文, 而无法由密文生成明文; 相同的明文每次加密都生成相同的密文, 由明文无法猜测密文. 对账号、密码等信息的加密, 多采用 MD5 算法[11].

虽然王小云教授成功破解 MD5Life_of_rent 使用了量子碰撞原理[12]. 宣告该算法不再安全, 但是对于公司以及普通用户来说, 从算法上来破解 MD5 非常困难, 因此 MD5 仍然算是一种安全的算法.

为了避免 MD5 加密的碰撞攻击及破解[13], 采用数据加盐技术[14]. 目前, MD5 密码数据库的数据量已经非常庞大了, 大部分常用密码都可以通过 MD5 摘要反向查询到密码明文. 为了防止内部人员和外部入侵者通过 MD5 数据库反查密码明文, 更好地保护用户的密码和个人帐户安全(用户可能会在多个系统中使用同样的密码, 因此涉及到用户在其它网站和系统中的数据安全), 需要对 MD5 摘要结果掺入其它信息, 称之为加盐. PIF 文件中的 PIN 码有账号、密码、用户的注册时间的二进制编码(作为随机数盐)构成, 确保同样密码的 PIN 码是完全不同的.

论文在加盐技术的启发下, 针对 MD5 算法进行了改进, 以 Java 语言为例, 首先利用 Java 语言中安全类中的 MD5 加密方法对明文进行加密, 形成密文, 对密文加以改变, 在密文中截取一段数据并丢弃, 然后使用 Java 数学类中的随机函数(加盐技术的应用)填充被

丢弃的数据, 且整个过程不改变 md5 加密后的位数. 加密过程用算法描述如下:

(1)对明文 PIN 码进行 md5 加密, 获得密文 md5(PIN).

(2)使用截取方法截取加密后的密文, 从第 startIndex 位置开始截取到 endIndex, n 位数值, 得到密码 X, 其中 X= md5(PIN).substring(int startIndex,int endIndex).

(3)使用截取方法截取加密后的密文的 n 位数后的值 Y, 其中 Y= md5(PIN).substring(n,endIndex).

(4)使用随机函数 rand(n)填充被截取的 n 的值.

(5)变换后的密码值为 afteren =X&rand(n)&Y

变量说明:

PIN: 客户端提交的帐号、密码的连接值

afteren: 经过改进处理后的密码

startIndex: 对原始密码开始截取的位置

endIndex: 对原始密码结束截取的位置

32: MD5 采用的位数(有 16 和 32 位两种, 本文采用 32 位)

解密过程跟加密过程类似, 先对输入的明文进行加密, 接着从 startIndex 处截取前半部分得到 X′, 后半部分得到 Y′, 然后从数据库中读出 PIN 码中的 X 和 Y 部分, 最后如果 X=X′并且 Y=Y′, 则认为用户输入的密码是正确的.

同时, 文中认证方案的 PIF 文件名、存放位置可变, 这样同样可以加大破解难度. 加密后产生的 PIN 码如下图 3 所示.

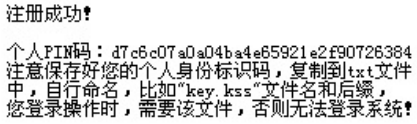

图 3 用户注册及 PIN 码产生运行结果图

3.2 PIF 文件读取及登录认证

此功能是系统的核心, 完成用户身份认证工作, 由于需要操作客户端的认证文件, 采用客户端技术实现, 本系统采用的是 JQuery 技术, 它是 AJAX 技术的一种[15]. 优点是可以进行客户端和服务器端代码的执行. 其中, PIF 文件读取属于客户端的操作, 身份识别在服务器端, 身份认证在客户端. 在客户端及服务器端程序通信的过程中, 传递的都是密文, 确保系统的安全. 部分关键代码:

```
 txt_helper b= new txt_helper();
//读取 Cookies 读出 key.kss 文件到变量 filepath
 String fg=b.r_txt(filepath+"\\key.kss");//读取文件内容
 String sql="select tu_pin from login_info
 where tu_pin ='"+fg+"'" ;//查找数据库对应的 pin 码
     sql_helper a=new sql_helper();
     ResultSet rs=a.Query(sql);
     String userpin=null;
     while(rs.next())
     {userpin=rs.getString(1);
     }
     if(sign==true)
     {     if(userpin==null)
     {//当 kss 证书不存在时执行
out.println("<script>window.parent.callback3()</script>"
);
     }else
     {//当 kss 证书存在时执行
         session.setAttribute("key_id",fg);
out.println("<script>window.parent.callback('"+fg+"','"+u
serpin+"')</script>");
          }
     }else
{out.println("<script>window.parent.callback2()</script>
");
}
```

4 实验结果及分析

为了验证该系统的实际效果, 我们在真实环境中进行了测试. 实验环境: 客户端计算机采用处理器 AMD Phenom(tm)II*4 955 4 核处理器, 4GB 内存, 安装 Windows7 旗舰版 32 位操作系统; 网络为联通的 6MB 宽带, 服务器注册了美国 EATJ 提供的免费空间, 该空间适合应用系统的测试, 支持 JSP、PHP 技术, 提供 MySql5.1 数据库.

实验 1 安全性测试, 其目的是验证认证文件的安全性, 我们在著名的 MD5 和 CMD5 网站上注册了用户, 输入认证文件中的密文, 均无法获得原文. 如下图 4 所示.

图 4 MD5 解密测试结果

该实验结果表明, MD5 算法破解有难度, 再经过方案中对 MD5 算法进行的变化, 破解难度更大, 表明方案的加密强度足够, 认证文件本身是安全的.

实验 2: 性能测试, 其目的是验证本系统的执行效率, 我们利用 EATJ 空间提供的 Mysql5.1 作为测试数据库, 利用 DataFactory 数据库数据自动生成工具, 产生模拟数据. 通过执行程序, 得出以下实验结果, 如下表 2 所示:

表 2 登录验证程序执行时间对比

记录数	PIF 文件	Mysql5.1	
		密码未加密	密码加密
100	172ms	2729ms	2845ms
1000		2835ms	2924ms
10000		2863ms	3439ms

从表 2 的实验数据可以看出, 认证文件针对每一个用户, 登录时, 身份识别需要与服务器进行通信, 身份认证只在客户端进行, 不受用户记录数的影响, 登录效率明显优于手机、Ukey、生物识别等方式.

通过以上两个实验, 可以看出本系统不管是在安全性方面, 还是在效率方面, 均好于传统的双因子认证方式.

5 系统特点

论文讨论的双因子身份认证系统具有以下优点:

1)安全性、易用性明显提高. 与其它双因子认证的区别是, 即使非法用户获得该文件, 也无法直接使用, 仍需要进行身份识别, 比常用的双因子认证更安全.

2)身份认证效率有所提高. 由于采用了 PIF 文件以及客户端的身份认证, 比其它双因子认证方式效率高.

3)方案通用性. 此方案适合 C/S 和 B/S 结构的应用系统.

4)私有数据专属性增强. 账号、密码这两个关键的用户私有数据, 并未直接存储在数据库中, 能够有效保证了用户对于个人私有数据的保管和知情权.

6 结语

论文提出并实现了一种强加密文件方式的双因子认证系统, 通过在应用系统中测试, 证明该认证方式, 有效降低了认证的成本、简化了认证过程, 增强了信息系统的安全、防止了个人私有数据的泄露. 但任何一种安全方案或技术都不能尽善尽美地解决所有安全问题. 单纯从身份认证方面, 只能保证是合法的用户, 但不能保证其做了符合其身份的事情. 所以下一步研究工作, 充分利用新的客户端技术, 扩展认证系统的功能. 即解决用户权限的动态审核, 同时结合数据库层次的安全, 让应用层安全与数据库底层安全贯通, 只有这样才能全面保障信息的安全.

参考文献

1 龙丽萍,陈伟建,杨拥军,文光俊.基于双因子认证技术的 RFID 认证协议的设计.计算机工程与应用,2013,34(11):3726–3730.
2 郭建昌,郭茂文,黎艳.一种电信级手机令牌动态口令系统的架构设计及其实现.电信科学,2012,(10):94–98.
3 付青琴,昂正全,徐平江.一种改进的智能卡认证方法的实现.计算机工程与科学,2014,36(1):95–97.
4 薛凯,李海霞,杨树国.一种针对云计算登陆问题的认证技术.科学技术与工程,2011,25(6):1375–1377.
5 汤宁,李勇平,王靖琰,郝新宇.多模式生物特征识别的身份验证系统.计算机工程与设计,2012,(6):317–321.
6 张丽,赵洋,史丽敏. 基于 0TP 的增强型身份认证系统的研究与设计.计算机工程与科学,2008,30(6):112–115.
7 马宏利.基于手机的身份认证技术研究.科协论坛(下半月),2010,(5):44–45.
8 斯里达尔.艾杨格.可信平台的新范式.中国计算机学会通讯,2014,(12):61–63.
9 刘斌,王最龙.Struts,Spring,Hibernate 框架在 OA 开发中的应用.计算机技术与发展,2010,(1):151–154.
10 王昆,沙瀛,谭建龙.基于 Cookie 劫持的 Deep–Web 用户数据安全性分析.计算机研究与发展,2012,(s2):17–22.
11 罗江华.基于 MD5 与 Base64 的混合加密算法.计算机应用,2012,(A01):47–49.
12 杨婕.基于量子计算的 Hash 碰撞安全性研究[硕士学位论文].南京:南京航空航天大学,2011.
13 毛熠,陈娜.MD5 算法的研究与改进.计算机工程,2012,(24):111–114.
14 王振辉,王振铎,张敏,王艳丽.Web 数据库安全中间件的设计与实现.科学技术与工程,2012,13(22):1335–1340.
15 李炳练.基于 jQuery 框架的无刷新技术设计与实现.电脑编程技巧与维护,2011,(6):5,19.