

文章编号:1001-9081(2005)10-2428-03

基于位图验证码方法的 Web 认证系统及其应用

李 辉¹, 牛 悅²

(1. 北京化工大学 信息科学与技术学院,北京 100029; 2. 中国图书进出口(集团)总公司,北京 100020)
(lili555@263.net)

摘要:引进验证码可增强 Web 认证系统的安全性,验证码基于位图格式,由系统随机产生,图像识别环节的引入是增强安全性的关键。已在多个实际工程项目中成功应用,该原理同样适用于其他端到端即时通信的认证系统。

关键词:验证码;位图;认证;散列函数

中图分类号: TP393.08 **文献标识码:**A

BMP validation code based Web authorization system and its applications

LI Hui¹, NIU Yi²

(1. School of Information Science and Technology, Beijing University of Chemical Technology, Beijing 100029, China;
2. China National Publications Import & Export (Group) Corporation, Beijing 100020, China)

Abstract: A validation code based method which can enhance the security of web authorization system was introduced. Validation code was based on bitmap and created at random, and the image identification was the key to enhance the security. Web authorization system was applied to practice successfully in several projects, and it's also applicable in other authorization systems for peer-to-peer communication.

Key words: validation code; bitmap; authentication; Hash function

0 引言

根据 ISO/IEC 7498-2、GB/T 9387.2 和 YD/T 1163-2001 的基本定义,安全服务包括认证、数据保密性、数据完整性、防抵赖性和访问控制五个基本部分^[1]。所谓认证是指“通过信息交换鉴定一个实体身份的机制”,认证的目的是为通信实体和数据源提供认证服务。

基于 Web 方式的认证已广泛地应用于各种 Internet 应用服务系统,如电子商务、电子政务等等。近年来,小区宽带接入、校园网宽带接入等系统也出现采用 Web 方式认证、计费的趋势^[2]。

以往的 Web 方式认证系统主要通过用户名、口令这种简单的静态口令机制进行身份验证。在这种情况下,存在以下安全问题^[3]:

1) 网络侦听:由于口令明文在网络上传输,攻击者可以通过网络侦听获得用户名和口令。

2) 截取、重放攻击:即使在网络上传输前对口令进行简单加密,攻击者仍然可通过截取、重放来假冒合法用户。

3) 暴力破解:如果攻击者获得了用户名和口令密文,就可对口令密文离线实施穷举暴力破解。

针对此安全问题,可以通过 HTTPS 的机制来建立端到端的安全通道,保证用户名、口令的安全传输^[4],但是此方法实现起来较为复杂,且效率不高。

动态口令方法不失为一种较好的解决方案,每次登录使用不同的动态口令^[5]。主要包括两种实现方式:挑战/响应(Challenge/Response)方式^[6]和时钟同步方式^[7]。与静态口

令相比,这种机制的安全性大大提高。但是在客户端产生动态口令时,还需要附加对称密钥,这就产生了另一个安全隐患。而且,动态口令的实现需要认证服务器进行大量运算,势必造成相当大的系统开销。

为了解决单一口令机制存在的问题,还可将静态口令机制和动态口令机制结合起来,形成双因素的身份认证方案^[8]。在双因素身份认证方案中,需要服务器端生成验证码(或挑战码),然后尽可能安全地发给客户端。大多数情况下,验证码是以数字方式直接从服务器端发送到客户端,因此该环节上也存在安全隐患。

将验证码的传送内容由数字变成表示数字的图像可使系统更加安全,客户端接收到以位图方式传送过来的验证码后,通过人工识别出来,然后反馈给服务器完成除用户名、口令之外的辅助认证。由于验证码随机产生,且不是以显式方式在网络上传输,攻击者只有通过图像识别才能对系统安全构成实时的威胁。

1 基本原理

基于验证码方法的 Web 认证系统包括位图的存储、随机生成验证码、身份认证等环节。

1.1 验证码位图的存储与生成

位图(BMP)格式的图像文件最初由美国微软公司为 Windows 环境应用而设计,目前已经成为一种通用的图像标准。位图文件的主要特点是文件结构简单,每个文件中可存放一幅静止图像,数据顺序存放,支持的彩色模式从 16 色到 32 位真彩色。因此,与其他图像格式相比,在生成、显示校验

收稿日期:2005-04-25;修订日期:2005-06-28

作者简介:李辉(1975-),男,北京人,副教授,博士,主要研究方向:计算机安全、计算机图形学;牛悦(1977-),女,北京人,工程师,主要研究方向:图书馆学、信息管理。

码这类特殊应用中位图文件格式优势明显。

位图格式的文件结构分为文件头、调色板数据以及图像数据三部分,如图 1 所示,当图像采用 24 位真彩色模式或更高模式时,调色板数据无效。



图 1 位图文件结构

校验码是由若干个随机数字或字母构成的图案,通常数字或字母的个数固定选为 4 个或 4 个以上。由于每次出现的校验码都不相同,因此将所有位图都存储下来将消耗大量的存储空间,比较合理的方法是在程序中动态产生位图。

可以将校验码位图文件分为固定部分和可变部分。固定部分由文件头构成,文件头依次包括以下信息:

位图的类型;整个文件的大小;从文件开始到位图数据开始之间的偏移量;位图信息头的长度、位图的颜色、压缩方法;位图的宽度;位图的高度;位图的位面数;压缩说明;位图数据的大小;水平分辨率;垂直分辨率;位图使用的颜色数;重要的颜色数。

以上所有的字段信息都可以根据数字或字母的点阵大小和数量来确定,当校验码发生变化时,该数据保持不变。

校验码位图文件的可变部分由数字或(和)字母的点阵信息构成。为了正确地将数字显示在浏览器中,可以将所有数字或(和)字母的点阵信息按顺序存放在一个文件中,以便动态生成校验码位图时读取。

为了增加图像识别的难度,建议在位图表达的数字或(和)字母中采用非印刷体的数字或(和)字母,因为识别非印刷体比识别印刷体更加困难^[9]。

1.2 身份认证

图 2 是基于位图校验码方法的 Web 认证系统的认证流程示意图。

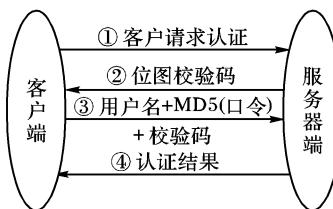


图 2 身份认证流程

带校验码的 Web 认证系统按以下几个步骤实现身份验证:

- 1) 当客户端需要访问由服务器提供的某些资源时,向服务器提出认证请求。
- 2) 服务器弹出认证界面,包括用户名、口令、校验码输入框以及校验码的位图图像,要求客户端如实提交认证信息。其中校验码位图生成的过程是:由系统产生一个随机数字或(和)字母串,作为校验码;将当前进程的进程标识与校验码关联起来,该进程标识在当前的连接状态下保持有效。
- 3) 客户端向服务器提交用户名、口令和校验码。
- 4) 系统需要对用户名、口令和校验码进行确认。针对错误的用户名、口令和校验码进入相应的出错处理流程;如果用户名、口令和校验码完全正确,则根据用户的权限、角色进入相应的界面。

用户名和口令存储在服务器端的数据库中,口令可加密存放。校验码随机产生,并与当前会话关联。

为避免反复进行身份认证,还可以在系统登录时将认证信息以 Cookie 的方式保存在客户端,通过设置 Cookie 的有效时间确定必须再次身份认证的时间间隔。

在口令认证中,先通过 MD5 散列函数对口令做数字摘要(见图 3),然后与数据库中的口令(往往经过同样的 Hash 函数处理)进行比对。

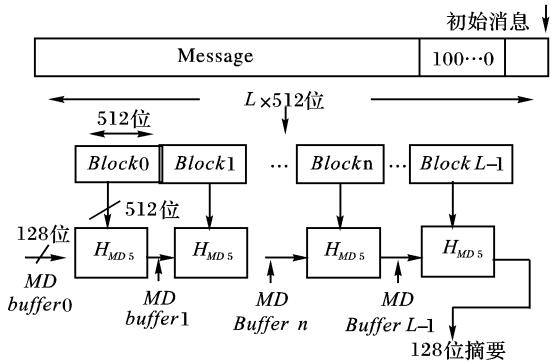


图 3 MD5 散列函数的流程

校验码是以位图的方式从服务器端发送到客户端的浏览器中,攻击者要获得具体的校验码,必须截获位图后,通过图像识别的手段才能破解。由于每次登录的校验码都是不相同,因此即使校验码在网络中被破解,也不会对系统安全造成真正的威胁。

可通过以下办法进一步增强认证的安全性:将输入口令和校验码组合后做 MD5 数字摘要,然后与数据库中口令及 Session 中校验码的散列值进行比对。此外,在选择散列函数方面,MD5 并非唯一选择,其他 hash 函数也都适用,如:SHA-1、SHA-256、SHA-384 和 SHA-512 等等,选择更高强度的散列函数也能提高认证的安全性。

2 应用系统的实现

下面以一个正在运行的实际系统为例,来说明基于校验码方法的 Web 认证系统的实现过程。

校验码的位图由 4 个 0~9 的数字构成,每个数字用 10×10 的点阵表示。

于是,校验码位图的头文件(vc. head)包括以下 54 个字节:

```
42 4D E8 04 00 00 00 00 00 00 36 00 00 00 28 00
00 00 28 00 00 00 0A 00 00 00 01 00 18 00 00 00
00 00 B2 04 00 00 12 0B 00 00 12 0B 00 00 00 00
00 00 00 00 00 00
```

校验码位图的图像数据文件将数字 0~9 的位图数据按顺序存放在一个文件(vc. body)中,该数据文件的总字节数是:(10×3+2)×10×10=3200 字节。之所以加 2 是因为行尾有 2 个字节“00 00”的行结束标志。

整个 Web 认证系统通过 ASP 程序来实现,认证信息存放在 SQL Server 数据库中。

以下程序生成一个随机数串 validation_code,串长为 4,随机数被赋予“SetCode”的会话变量中:

```
Randomize timer
validation_code = cint(8999 * Rnd + 1000)
Session("SetCode") = validation_code
```

根据 validation_code 中 4 个数字的大小,从 vc. body 中读

取相应的位图点阵信息,按数字顺序组合起来:

```
Ados1. LoadFromFile( Server. mappath( "vc. body" ))
for i = 0 to 3
    Ados1. Position = (9 - cint( mid( cstr( validation_code) , i + 1, 1 )))
    * 320
    Ados2. Position = i * 320
    Ados2. write Ados1. read(320)
next
```

按数字先后顺序组合起来的位图数据(占 320×4 字节)与需要显示出的 40×10 点阵图数据并不一致,需要进行内部重新排列(如图 4 所示):

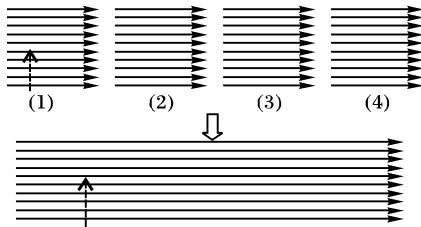


图 4 数字串位图信息的内部重新排列过程

```
Ados1. LoadFromFile( Server. mappath( "vc. head" ))
LenHead = lenb( Ados1. read() )
Ados1. Position = lenb( Ados1. read() )
for i = 0 to 9 step 1
    for j = 0 to 3
        Ados2. Position = i * 32 + j * 320
        Ados1. Position = LenHead + 30 * j + i * 120
        Ados1. write Ados2. read(30)
next
```

在生成完整的校验码位图后,将位图在浏览器中显示出来:

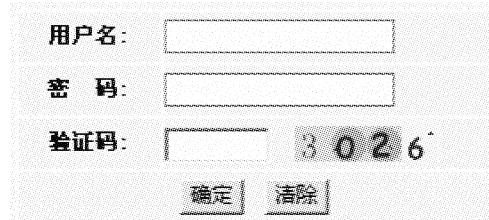


图 5 登录表单

```
Response. ContentType = "image/BMP"
Ados1. Position = 0
Response. BinaryWrite Ados1. read()
Ados1. Close: set Ados1 = nothing
Ados2. Close: set Ados2 = nothing
显示在浏览器中带校验码的登录表单如图 5 所示。
用户在输入登录信息后,先除掉口令字段的空格,然后进行 MD5 处理:
```

```
username = trim( Request. Form( "username" ))
password = md5( trim( Request. Form( "password" )))
```

按输入的用户登录信息从数据库中取出用户名、口令的 hash 值以及角色,若用户名或口令出错,则没有符合条件的记录。接下来,将输入的校验码与 Session("SetCode")进行比对,若不一致,则显示出错信息,若一致,则根据用户信息设置相应的 Cookie 值。

程序如下:

```
Set rs = conn. execute( "select user, password, role from users where
user = '&username&' and password = '&password&'")
```

```
if ( rs. bof and rs. eof) or ( int( request( "Validation_code" )) < > int
(Session( "SetCode" ))) thenResponse. Write "用户名、口令或验
证码不正确!"
else
    if rs( "password" ) = password then
        Response. Cookies( "username" ) = username
        Response. Cookies( "password" ) = password
        Response. Cookies( "role" ) = rs( "role" )
        Response. Cookies( "login" ) = "Y"
        session( "user" ) = username
        Response. Redirect "user_welcome. asp"
    else
        Response. Write "relogin. asp"
    end if
end if
```

3 结语

基于 Web 方式的认证在各种 Internet 应用服务系统中应用广泛,但仅通过用户名、口令比较作为认证手段不够安全,尤其是在公网上。通过引进位图校验码的方式,可以显著增强认证系统的安全性,而且这种方法易于实现,简单实用。

安全性的增强建立在位图生成的基础之上,巧妙地利用了人工交互中的肉眼识别环节。要对认证系统发起攻击,必须具备对位图进行快速自动识别的能力,这对于图像的识别准确度和识别时间是很高的要求。增加校验码的数量和避免使用印刷体的数字和字符可增强系统安全性。

目前,该系统已在某大型图书在线服务系统中得以应用,运行稳定。

严格地说,位图校验码是服务器端与客户端之间共享的实时保密信息,因此位图校验码不仅可以简单地作为认证的辅助手段,还可以用作双方即时通信的对称密钥。也就是说,校验码认证的原理还可以应用到除 Web 应用之外的其他网络即时通信应用中。

当然,位图校验码方法仅仅是一种简便易行的辅助手段,要建立高强度的身份认证系统,还必须结合密码学的其他理论。

参考文献:

- [1] 李辉. 计算机安全学 [M]. 北京: 机械工业出版社, 2005. 146 – 148.
- [2] 邢小良. 宽带网接入认证的发展方向——Web 认证 [J]. 通信世界, 2002, (12): 23 – 24.
- [3] 童永清. 口令攻击与防范 [J]. 计算机安全, 2004, (1): 66 – 67.
- [4] 薛文卿. 使用 https 编写客户端程序 [J]. 计算机周刊, 2001, (31): 25 – 26.
- [5] CHANG Y-F, CHANG C-C. A secure and efficient strong-password authentication protocol [J]. ACM SIGOPS Operating Systems Review, 2004, 38(3): 79 – 90.
- [6] BICAKCI K, BAYKAL N. Infinite length hash chains and their applications [J]. Proceedings of the 11th IEEE International Workshops on Enabling Technologies, 2002, (6): 57 – 61.
- [7] 张宏, 陈志刚. 一种新型一次性口令身份认证方案的设计与分析 [J]. 计算机工程, 2004, 30(17): 112 – 113.
- [8] 汪同庆, 鲁军, 华晋, 等. 基于 MD5 算法和 Schnorr 协议的双因素身份认证系统 [J]. 计算机应用研究, 2004, (12): 137 – 139.
- [9] 刘春阳, 梁德群, 宋焕生. 带有手写干扰的印刷体数字识别 [J]. 西安交通大学学报, 1998, 32(1): 21 – 24.