中国农业大学学报 2006,11(2):85-87
Journal of China Agricultural University

B/S结构银行业务系统中三重身份认证的设计与实现

杨丽丽 张 莉
(中国农业大学 信息与电气工程学院,北京 100083)

摘 要 针对独立于Internet网络的企业电子业务处理系统普遍采用的静态的"用户名+密码"的二元身份认证方法抗攻击能力弱的问题,并从方便、可靠,尽可能降低成本的设计思想出发,设计并实现了基于三重认证技术的系统身份认证方法:利用IP认证方法防止非法客户端的访问;利用服务器用户认证方法防止非法角色的访问;通过随机码认证和操作员号/密码认证,防止利用程序对用户密码的分析破解。在混合结构电子联行系统中的应用结果表明,该方法简单有效,实现了设计要求。本研究可为其他基于B/S结构的系统提供参考。

关键词 系统安全;身份认证;三重认证技术
中图分类号 TP 393.08 **文章编号** 1007-4333(2006)02-0085-03 **文献标识码** A

Design and realization of triple identities of authentication in a bank electronic business system based on B/S structure

Yang Lili, Zhang Li
(College of Information and Electrical Engineering, China Agricultural University, Beijing 100083, China)

Abstract Originated from identity of authentication in a bank electronic business system based on B/S structure and a combination of practical techniques in most systems, the triple identities of authentication scheme was designed in a new system. In the new system, the fundamental structure and specific technique of the scheme were introduced and realized the identity of authentication of the EIS system. The operation of this new system showed that the method was simple and available. The triple identities of authentication scheme developed here can also be applied to the similar systems.

Key words system security; Identity of authentication; triple authentication techniques

身份验证技术是网络安全的重要环节,对于很多行业来说,它是解决网络安全问题的首要问题。目前针对身份认证问题国内外已有多种技术和方法:纯软件认证开发成本高,硬件认证则需要增加额外设备;单因子认证容易被仿冒,双因子认证提高了安全性但也增加了成本;动态身份认证方法在国外应用较广,但在国内应用还不普及,主要原因是国内令牌技术的发展还不够充分,并且系统中应用令牌的成本也比较高[1]。

目前独立于Internet网络的企业电子业务处理系统普遍采用静态的"用户名+密码"的二元身份认证方法。这类技术操作简便,实现成本低,但抗攻击能力很弱。笔者针对B/S结构银行电子业务处理系统所遇到的身份认证的实际情况,结合目前国内外身份认证技术,提出一种基于IP认证、Web服务器用户认证、随机码认证和操作员号/密码认证的三重认证方法。设计方案的主要思想是身份认证要尽可能方便可靠,并尽可能降低成本。

1 系统身份认证问题描述

某银行电子业务处理系统采用二级业务处理结构和独立于Internet的金融地面网络,其系统示意图见图1。其中的业务分中心系统采用B/S模式实现,服务器端采用Tomcat或Websphere,任何可与

收稿日期:2005-05-11
作者简介:杨丽丽,讲师,主要从事计算机网络技术应用和数据库理论研究,E-mail:llyang@cau.edu.cn

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

服务器连接的 Windows 系统的 IE 浏览器都可作为 Web 客户端。银行内部业务操作人员使用操作员号/操作员密码的方式进行认证,认证通过即可进行各种操作。

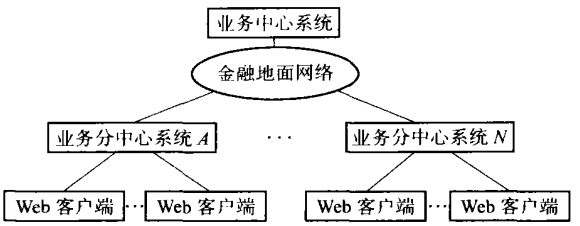

图 1 电子业务处理系统示意图

Fig. 1 Sketch map of an electronic business system

这种模式存在以下问题:

1)系统通过独立的基于 TCP/IP 协议的金融地面网络进行连接,该网络中任意节点间可以互通,故可能出现 *A* 节点业务分中心系统的浏览器连接到 *B* 节点业务分中心系统的现象。

2)业务分中心系统采用 Windows 系统的 IE 浏览器,使用 HTTP 协议与 Web 服务器连接,这种情况下,可能出现"破坏者"编写程序模拟 BROWSER 发送 HTTP 请求的现象,或出现使用程序如 WebZip 下载服务器端页面和应用程序的现象。

3)业务分中心系统采用操作员号/操作员密码的方式进行认证,系统安装时有默认的操作员号和操作密码,如果 *A* 节点和 *B* 节点不修改默认密码,则会出现 *A* 节点操作员号/操作员密码与 *B* 节点的一致的情况,如果再同时出现 1)中问题,则可能出现 *A* 节点操作员可以进入 *B* 节点业务分中心系统进行操作的现象。

银行电子业务处理系统存在的这 3 个问题,其实质都是系统身份认证问题,也就是如何正确鉴别合法用户身份的问题。

2 现有身份认证方案分析

1)纯软件安全认证方式。如采用公开密钥基础设施(PKI)。PKI 中引进了一个可信任的第三方,即交易双方共同信任的签发其数字证书的证书签发机构(CA)。PKI 采用数字证书和 CA 信任的机制,服务方和客户方必须获得 CA 签发的证书,并在 Web 服务器上配置服务器端证书,设置所有可以信任的客户端证书,在客户端配置客户个人证书,设置服务器端的可信任证书。操作员通过客户端向服务器出示客户个人证书以证明自己的身份而非伪装的系统;也可以验证服务器端证书以确定服务器是否为自己本段的业务分中心系统而非其他系统[2-3]。此技术认证手段的安全性超过基于静态或动态口令的认证方式,但需要增加额外软件和证书验证等功能,开发成本较高。

2)软硬件结合的安全认证方式。如采用 USB KEY 认证模式。使用 USB KEY 或其他类似的 ePass ID,首先要在服务器端创建允许登录的用户列表,只有授权的用户才能访问服务器,从而防止非法入侵。客户信息全部存放于 USB KEY,客户不必记忆繁琐的用户信息,只需把 USB KEY 插入服务器或客户机就可完成登录(有些类型 USB KEY 为带 PIN 码的双因子认证,登录时则需要输入 PIN 码)。服务器上运行的网络登录服务程序,通过接收客户端 USB KEY 中存储的网络登录信息,调用相关网络登录验证过程对其进行确认,以完成网络身份认证,从而保障网络信息的安全性。

此技术可靠、简便和安全,缺点为需要增加额外的硬件设备[4-5]。

3 三重认证方案及其实现

3.1 三重认证方案

该银行电子业务处理系统采用独立的金融地面网络处理业务,因而可防止网络黑客的攻击和破坏,同时建立了严格的规则和制度,建有详细的系统运行日志;需要解决的仅是系统内部工作人员的合法访问问题[6]。

比较上述几种技术方案,根据系统的实际情况,在该银行电子业务处理系统中设计了 IP 认证、Web 服务器用户认证、随机码认证和操作员号/操作员密码认证的三重认证的方案。

第一重:IP 认证。通过指定合法的访问服务器的 IP 来防止异地或非法客户端的访问,在服务器端配置合法的 IP 表进行 IP 认证。将客户端的 IP 与网卡的 MAC 地址绑定,防止 IP 被盗用。

第二重:Web 服务器用户认证。此认证方式通过指定合法的访问服务器的用户角色来防止非法的用户利用合法客户端访问服务器[7],同时可防止用户使用程序如 WebZip 类下载服务器端的页面和应用程序。

第三重:用户名/密码认证和随机码认证。传统的"用户名+密码"的二元认证方式,容易被恶意程序暴力破解,而用户名/密码认证和随机码认证方式

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

除要求用户输入用户名和密码之外,还要求手工输入随机生成的随机码,有助于防止自动化的程序填写登陆;同时限制错误登录次数和使用"扩展动态密码",密码错误超过限制次数,即封欲登陆者 IP 或 ID,以降低恶意程序访问服务器的频率。页面中的随机码为数字或字符,用图形显示,每个随机码对应的图形不止一种,以防止非法程序的分析破解。以下为生成随机数字图像认证码的主要代码:

```
//取随机产生的认证码(4 位数字)
String sRrand = "";
for(int i = 0;i < 4;i + +){
  String rand = String.valueOf(random.nextInt(10));
  sRand + = rand;
  }
session.setAttribute("rand", sRrand);
g.setColor(Color.black);
g.setFont(new Font("Times New Roman", Font.PLAIN,18));
g.drawString(sRrand,10,15);
//随机产生 100 个黑点干扰,使图像中的认证码不易被其他程序探测到
Random random = new Random();
for (int i = 0;i < 100;i + +)
{
    int x = random.nextInt(width);
    int y = random.nextInt(height);
    g.drawLine(x,y,x,y);
}
```

3.2　三重认证方案的实现

首先,在服务器端定义合法客户端的 IP 表,此表可使用数据库表或 XML 文件方式。当有 Web 客户端连接到服务器端时,服务器使用定义的客户端 IP 表来检查其合法性,若是合法的客户端 IP,则进行下一步;否则,返回错误响应,并中止连接。XML 文件格式合法客户端 IP 表如下:

```
< ?xml version="1.0"encoding="GB2312"? >
< UserIP >
    < IP > 10.1.254.10 < / IP >
    < IP > 10.1.254.11 < / IP >
< / UserIP >
```

其次,在服务器端的 Web 服务器中设置基于表单的认证模块:

1) 设置可以访问服务器的用户角色和用户;

2) 配置服务器端应用配置文件 Web.xml,设置基于表单的认证模块,同时设置允许访问的用户角色[8];

3) 建立服务器端认证页面和出错页面。

最后,通过第一重 IP 认证和第二重 Web 服务器用户认证,进入正式业务处理系统用户登录界面。在此设置用户名/密码认证和随机码认证,同时限制错误登录次数。

4　结束语

本文中提出利用三重身份认证方案解决 B/S 结构银行电子业务处理系统内部人员合法访问问题,并给出了方案的技术实现。此方案已在基于混合结构的电子联行系统中应用实现,并通过多次测试。三重身份认证方案符合简单、有效的设计原则,代码开发所需费用较少,无需增加额外硬件设备。此方案可为其他相似系统提供参考。

参　考　文　献

[1] 郭代飞,杨义先,李作为,等. 数字认证技术的现状与发展[J]. 计算机安全,2003,7:1-4

[2] Brayton J, Finneman A, Turajski N, et al. PKI[ED/OL]. [2005-10-30]. http://searchsecurity.techtarget.com

[3] 谢冬青,冷健. PKI 原理与技术[M]. 北京:清华大学出版社,2004

[4] 冯世力,李鹏飞,张海峰. USB 安全钥在电子政务系统中的应用[J]. 计算机安全,2006,2:31-32

[5] 徐远航,宋丽娜. 身份认证与管理:下一个安全部署重点[J]. 网络世界,2004(11):021

[6] 驹宝平. 如何构建无贼内网[J]. 电子商务,2005,11:78-80

[7] 宋善德,郭翔,戴路. 基于 XML Web 服务的企业应用集成系统身份认证技术研究[J]. 计算机工程与科学,2004,26(10):5-7,18

[8] 孙卫琴,李洪成. Tomcat 与 Java Web 开发技术详解[M]. 北京:电子工业出版社,2004

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net