广西科学院学报
Journal of Guangxi Academy of Sciences

2009,25(4):282~283,287
Vol. 25,No. 4 November 2009

基于短信息动态口令的企业办公网双因子安全系统的设计与实现*

Design a Two-Factor Security System for Enterprise Office Network Based on SMS Dynamic Password

陈红霞[1,2],李陶深[1]
CHEN Hong-xia[1,2],LI Tao-shen[1]

(1. 广西大学计算机与电子信息学院,广西南宁 530004;2. 广西工业职业技术学院计算机系,广西南宁 530001)
(1. School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China; 2. Department of Computer, Guangxi Industrial Vocational and Technical College, Nanning, Guangxi, 530001, China)

摘要:为了进一步加强企业办公网络安全系数,设计一种基于手机短信息的一次一用动态口令+用户静态口令的企业办公网身份认证双因子安全系统,并讨论其工作流程和安全机制。该系统通过架构短信息服务器平台,由算法程序产生动态随机校验码,以短信形式发送校验码到用户手机,用户利用手机接受到的动态校验码与用户静态口令登陆办公网。该系统可以使企业在不变更原有网络架构的基础上,加强办公系统的安全性。

关键词:手机短信 动态口令 GPRS MODEM 串口 加密算法
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2009)04-0282-02

Abstract: In order to enhance the security quotiety of the enterprise office network, a two-factor security system for identity authentication which based on the SMS dynamic password and the user's static password is designed. the work flow and the ecurity mechanism are discussed. The system established a short message service platform, created randomly dynamic check code through the algorithm procedure and sended the check code as the short message to user's mobile phone. The user logins on the office network by the dynamic check code and the user's password. This system would increase the security level without changing existing system.

Key words: SMS, dynamic password, GPRS MODEM, serial port, encrypted algorithm

身份验证作为企业办公网的第一道防线,在企业办公网网络安全中起着举足轻重的作用。身份验证的任务是验证有效用户的身份合法性,按系统授予的用户权限访问办公网内部资源,将非法用户拒之门外。

常见的企业办公网大都采用简单的用户名+用户密码登陆[1],这类静态口令身份验证因其存在着静态性、固定性和长期使用性而容易被窃取、盗用或在枚举等方式下被猜测或被破解,进而造成身份冒用非法登陆办公网。

事实表明,在政府、企业、金融等领域的网络信息安全级别越来越需要加强的今天,单一的静态口令身份验证已经难以满足企业等信息安全级别较高的网络安全需求,因此,一用一变的动态口令身份验证技术得到了推广与应用[2]。

本文介绍一种基于短信息动态口令+用户静态口令的企业办公网双因子安全系统的设计与实现。

1 系统总体设计

基于短信息动态口令+用户静态口令的企业办

收稿日期:2009-07-20

作者简介:陈红霞(1974-),女,硕士研究生,讲师,工程师,主要从事网络信息安全、软件工程研究。

*广西科技创新能力与条件建设项目(桂科能 07109008-006-Z),广西自然科学基金项目(桂科自 0832056)资助。

公网双因子安全体系系统是在不变更原有网络架构的基础上，通过架构短信息服务器平台，由算法程序产生动态随机校验码，利用手机并通过串口连接到GPRS MODEM，由俗称的“短信猫”以短信形式发送校验码到用户手机，用户通过手机接受到的动态校验码＋用户名、用户密码登陆办公网。其原理如图1所示。

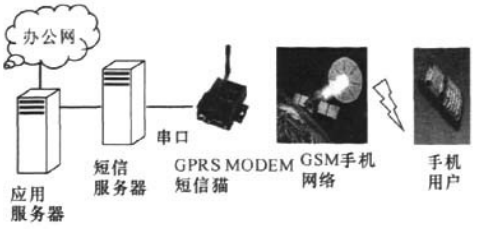

图1 短信发送原理

该系统的功能从整体上可以分为两部分：上层管理功能和下层的通信功能。上层管理功能实现办公网合法用户的管理、用户名和用户密码的静态口令验证以及动态口令随机校验码的产生与验证，进而允许合法用户登录办公网。下层通信功能则通过GPRS MODEM以手机短信息的形式实现动态口令的发送与接收。

1.1 上层管理功能模块

上层管理功能模块分为用户管理模块、动态口令生成模块、短信的发送和接收、身份验证、系统选项等模块组成(图2)。其中：

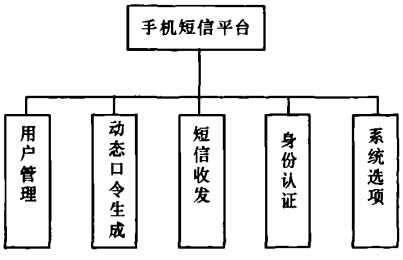

图2 上层管理功能模块

(1)用户管理模块：查看、修改、添加用户信息，实行分组管理用户名、用户密码以及用户关联手机号码。

(2)动态口令生成模块：以用户登录到系统的当前时间t为参数，包括系统当前时间(年、月、日、时、分、秒)作为明文，经过TEA加密算法后将密文发送到用户手机，通过TEA密码算法解密，核对用户身份的合法性。

(3)短信发送和接收模块：将系统生成的动态口令以短信息的形式，通过串口连接的GPRS MODEM发送到用户手机。

(4)身份验证模块：用户以用户名、用户密码、手机短信息接收到的动态口令登录，当短信息服务器将用户输入的动态口令与系统保留的动态口令想比对，若两者相同，则该用户为合法用户，允许其登陆。

(5)系统选项：进行GPRS MODEM串口选择、短信息中心号等系统设置。

1.2 下层通信功能模块

下层通信功能模块以底层的串口通信为基础，由串口通信、AT指令、PDU编解码等模块组成。它是利用串口通信的API函数实现计算机和GPRS MODEM的通信；利用AT指令通过串口完成对“短信猫”的控制，实现短信的发送、读取和系统设置等功能；通过实现对各种目标手机号码、短信中心号码、短信内容的正确编码，形成可发送的PDU串；实现对收发的各种短信PDU串的正确分解和正确解码。

2 系统工作流程

基于短信息动态口令＋用户静态口令的企业办公网双因子安全体系系统的工作流程如下：

(1)用户请求接入办公网应用服务器；

(2)应用服务器请求短信服务器对用户的身份的合法性和真实性进行认证；

(3)用户终端弹出身份认证对话框；请求用户输入手机号码；

(4)用户手机号码核对无误，短信服务器发送动态口令到用户手机；

(5)用户将用户名、静态口令、动态口令键入终端的身份认证对话框；

(6)用户终端将帐号和口令通过网络传输给短信服务器进行身份认证；

(7)短信服务器调用客户信息，产生与客户信息和时间相关的随机序列，并与客户输入的口令进行比对，判别客户身份的合法性和真实性；

(8)短信服务器将认证结果报告给应用服务器；

(9)应用服务器根据客户身份的合法性和真实性反馈给客户终端，并决定是否可以提供服务或拒绝服务。

用户的身份认证过程如图3所示。若明文e＝明文m，则用户身份合法，允许其登录办公网；否则，用户身份不合法，拒绝服务。密文的加密和解密过程

(下转第287页)

点:(1)网络授权接入访问。采用网络接入认证技术措施,杜绝电脑随意接入网络和访问网络资源的现象,保障网络和信息安全。(2)杜绝内网非法外联和移动存储介质"摆渡"。通过部署内网安全管理审计系统,对内网电脑操作行为实施实时监控,杜绝电脑以任何形式非法外联。通过对移动存储介质进行注册管理,禁止移动存储介质非授权访问,杜绝"摆渡"。(3)病毒有效隔离,避免对全网攻击,造成网络堵塞瘫痪。采用第三层网络交换技术和OSPF路由协议,有效地将病毒和网络广播限制在一个特定区域内,抑制病毒和广播风暴扩散,保护网络安全。(4)事先预防、事中监控、事后审计。对接入网络的电脑实施实时监控,对非法外联、端口流量异常及时报警和阻断,并可以对电脑的端口和外设进行控制,电脑所有操作都留下痕迹,便于事后审计。

广西发改委网络信息安全系统应用实践证明,网络受到病毒、木马的攻击明显减少,杜绝了内网非法外联、移动存储介质"摆渡",很好地解决了内/外网数据安全交换问题,符合网络信息安全保密要求,能够确保信息安全。

参考文献:

[1] 孙玮,何兴高.内网安全监管审计系统的架构设计[J].计算机应用,2008,12(28):267-270.

[2] 蒋明华,李声,李俊.入侵检测系统与防火墙系统联动平台的设计[J].网络安全技术与应用,2009(7):39-41.

[3] 朱海龙,张国清.基于802.1x的以太网接入技术[J].计算机工程,2003,29(18):130-132.

(责任编辑:韦廷宗)

(上接第283页)

由TEA算法[1]来完成。

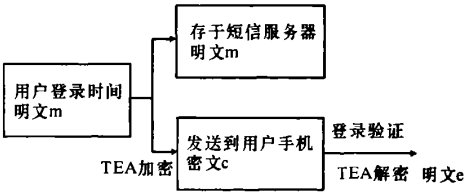

图3 用户的身份认证

3 结束语

为了消除当前企业办公网普遍采用的静态单一口令身份认证机制存在的安全隐患,本文设计一种基于手机短信的一次一用动态口令+用户静态口令的企业办公网身份认证双因子安全体系,并讨论其工作流程和安全机制。手机的普及使该系统具有较高的安全性和使用上的方便性,并且系统通过GPRS MODEM来发送短信息,实现成本低,可与基于互联网的各种应用服务商结合,为其提供安全的用户认证服务,替代传统单一静态口令用户认证方式。同时,在动态口令上采用了TEA加密算法,将密文以短信息的形式发送到用户手机,即使被第三方截获,因其不知道密钥,也无法破解得到相关明文,从而杜绝了非法用户登录办公网的可能,能够极大地提高企业办公网络安全性,可以在企业内进行技术推广和应用。

参考文献:

[1] 杨本臣,张全贵.基于短信息平台的高校办公网络的研究[J].中国科技信息,2007(3):96-98.

[2] 张文.动态口令身份认证系统的设计与实现[J].微计算机信息,2005,21(3):232-233.

(责任编辑:尹 闯)