文章编号:1001 - 9081(2008)07 - 1810 - 02

一种基于三因素认证的网络支付安全认证模式

程 亮,刘 辉
(华中科技大学 信息与系统技术研究所, 武汉 430074)
(chengliang. price@163. com)

摘 要:在目前流行的双因素认证的网络支付安全认证模式的基础上,引入动态验证码认证,提出了一种基于三因素认证的网络支付安全认证模式。文中给出了具体的认证协议实现过程,并对其安全性进行了分析,结果表明本认证模式能提高网络支付的安全。

关键词:网络支付;三因素认证;安全认证
中图分类号: TP309 **文献标志码**:A

Three-factor authentication mode of network payment

CHENG Liang, LIU Hui
(*Institute of Information and System Technology, Huazhong University of Science and Technology, Wuhan Hubei* 430074, *China*)

Abstract: This paper introduced a three-factor authentication mode of network payment which added an authentication code factor on the basis of the traditional dual-factor authentication. The realization method of the authentication protocol was also given, followed by an analysis on its security. The analysis verifies that this mode can enhance the security of the network payment.

Key words: network payment; three-factor authentication; security authentication

0 引言

随着网上银行业务及计算机技术的快速发展,保障网络支付的安全成为网上银行支付系统应用的关键,而安全的认证模式又是保障网络支付安全的关键。目前国内外的网络支付系统都是采用 SSL 协议或 SET 协议作为基本的底层安全认证协议来构建安全的网络支付认证模式[1-2]。Visa 公司推出的 Visa 3D Secure 安全认证模式[3]和 MasterCard 公司推出的 MasterCard SecureCode 安全认证模式[4],他们的技术内核都嵌入了 SSL 协议;而 3D SET 三域认证模式[5]则是 SET 开发商对 SET 协议进行改善后得到的安全认证模式。这三种安全认证模式都是针对信用卡用于互联网支付,但在一些非信用卡为主体交易工具的国家中,网上支付还是主要依靠其他支付工具如中国。目前国内网络支付安全认证模式的技术内核都是基于 SSL 协议的,其主要有以下两种模式:一种是基于第三支付平台的认证模式[6],另一种是基于"口令 + 硬件加密设备"的双因素认证模式[7],其中最常用的硬件加密设备就是 USBKEY(智能密码钥匙)。由于后者的安全性要高于前者,因此广泛被应用于国内的网上银行业务。

在基于"口令 + USBKEY"的双因素认证的安全认证模式中,用户必须拥有正确的口令以及属于自己的 USBKEY 才能进行认证及支付等相关操作[8]。但这种认证模式也存在安全隐患,有些用户习惯于将 USBKEY 长期插在 USB 口上,这就使黑客有机会利用黑客工具在用户不知道的情况下对 USBKEY 进行操作,伪装成用户与服务器通信进行仿冒攻击。目前有两种方法能防止这种情况发生,一种是在 USBKEY 上增加一个液晶显示器[9],每次进行 USBKEY 操作的动态密码通过显示器显示,这样黑客就无法获得动态密码,就不能非法操作 USBKEY。另一种是使用基于生物特征的 USBKEY[10]如用户的指纹,在 USBKEY 上增加一个指纹采集器,每次对 USBKEY 进行操作时必须在指纹采集器输入用户的指纹,黑客无法获得用户的指纹也就无法操作 USBKEY。这两种方法都是通过硬件实现防止仿冒攻击,这样就是使得 USBKEY 的成本大大的提高,普及使用有一定的困难。基于这个事实本文在使用普通 USBKEY 基础上,引入验证码认证,通过软件实现防止仿冒攻击。不仅具有很高的安全性同时具有很好的实用性。

1 验证码认证

验证码认证是当前各大门户网站应用的认证方式其基本原理[11]:验证码生成器随机产生验证码并存储下来,然后以图片文字的形式告知用户,用户照着图片文字手动输入然后提交,服务器对提交的验证码与先前存储下来的验证码进行逐位对比看是否吻合,从而完成验证。根据目前使用的 USBKEY 的计算处理能力,完全有能力进行验证码的生成和识别算法,因此在 USBKEY 中进行验证码的认证是可行的。

目前的图片识别技术能识别简单的验证码,因此必须在验证码中加入干扰来增大验证码的识别难度,如使验证码随机变色或变换大小,这样的验证码要想通过图片识别技术进行识别几乎不可能。

2 认证系统体系结构

本认证系统体系由客户端、客户端代理、认证代理、认证服务器、安全管理服务器和管理控制台、用户信息和授权策略数据库等部分构成,如图 1 所示。其各部分功能如下。

客户端(包含 USBKEY,用户的私钥和证书存储在其中):完成身份令牌信息读取、对支付命令进行数字签名、产生动态密码及进行图像认证。

收稿日期:2008 - 01 - 14;**修回日期**:2008 - 03 - 24。

作者简介:程亮(1985 -),男,江西乐平人,硕士研究生,主要研究方向:电子商务、信息安全; 刘辉(1969 -),男,湖北武汉人,副教授,博士,主要研究方向:电子商务、信息安全。

客户端代理:用来截获用户的访问请求,利用从 USBKEY 中取出的密钥加密用户信息、访问请求并发送给认证服务器端代理,然后接收应用服务器的响应消息,并与认证服务端代理建立安全通道。

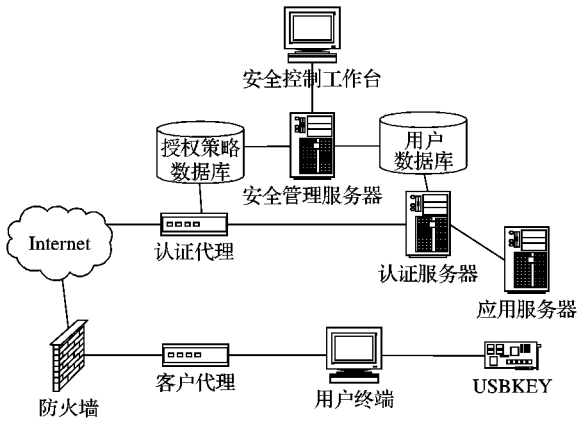

图 1　认证体系系统结构

认证代理:用来连接有身份认证请求的客户端和认证服务器。

认证服务器:凭借用户的身份信息和服务端代理的身份信息,查询用户注册数据库看二者是否一致,从而进行用户的身份认证。

安全管理服务器和管理控制台:从管理控制台上可以管理注册用户信息和授权策略数据库。

应用服务器:响应用户的支付请求,并完成支付。

用户数据库:存储用户的信息,如密钥信息等。

授权策略数据库:存储注册的受保护资源的各项信息,如位置、端口号及授权策略模板等。

3　认证协议实现流程

本认证协议包括身份认证和支付认证两个阶段。

3.1　符号描述和定义

表 1　符号描述和定义

符号	定义	符号	定义
C	客户终端	K_s	认证服务器的公钥
S	认证服务器	K_a'	应用服务器的私钥
A	应用服务器	K_a	应用服务器的公钥
ID_c	客户标识	K_c	用户 USBKEY 的公钥
T_c	客户终端当前系统时间	K_c'	用户 USBKEY 的私钥
A_c	客户登录的账号信息	$F_c(T_c,H_c)$	USBKEY 产生随机数的算法
T_s	认证服务器当前系统时间	$F_s(T_s,H_s)$	服务器产生随机数的算法
$H_c()$	USBKEY 的 HASH 算法	B	USBKEY 产生的验证码
$H_s()$	认证服务器的 HASH 算法	B'	用户输入的验证码
T_a	应用服务器当前系统时间	$H_a()$	应用服务器的 HASH 算法
COM	终端发出的支付命令	P	用户密码
REQ	客户端发出的支付请求	N_{ci}	用户产生的随机数
‖	级联符号	N_{si}	认证服务器产生的随机数
K_s'	认证服务器的私钥	⊕	异或符

3.2　身份认证阶段

身份认证阶段其数据交换过程如图 2。

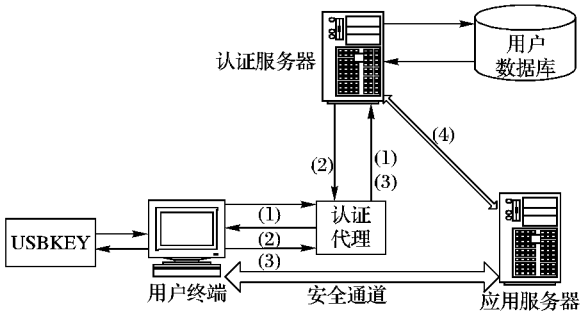

图 2　身份认证阶段数据交换过程

1)用户登录客户终端 C,插入手中的 USBKEY,客户端软件提示用户输入 PIN 码 P。在验证 P 正确后,客户端软件获取 T_c、A_c、ID_c 等信息,并将他们写入 USBKEY 内存。USBKEY 调用 $F_c(T_c,H_c)$ 生成 N_{c1} 并存储 N_{c1},再调用 $H_c()$ 计算 $H_c(T_c \| A_c \| ID_c \| P \oplus N_{c1})$,用 K_c' 签名后向认证服务器发送认证请求。表述为:

$$C \rightarrow S: K_s\{T_c \| A_c \| ID_c \| P \oplus N_{c1} \| H_c(T_c \| A_c \| ID_c \| P \oplus N_{c1})\}$$

2) S 通过认证代理截获认证请求后,用 K_s' 解密用户的认证请求。通过用户发来的 ID_c,在用户数据库中查找用户的数据,如果用户为注册用户则在数据库中调用用户的 K_c,验证用户的数字签名从而验证用户的身份。用户身份通过认证后,S 调用 $F_s(T_s,H_s)$ 生成 N_{s1} 并存储 N_{s1},再调用 $H_s()$ 计算 $H_s(T_s \| N_{s1})$,用 K_s' 加密后作为挑战数应答用户的认证请求。表述为:

$$S \rightarrow C: K_c\{T_s \| N_{c2} \| P \oplus N_{c1} \| H_s(T_s \| N_{s1})_{K_s'}\}$$

3)USBKEY 接收到应答加密包后,用 K_c' 解密然后用 K_s 验证服务器的数字签名从而验证服务器的身份。再验证服务器发来的 $P \oplus N_{c1}$ 是否与自己存储的相同,相同说明服务器响应了自己这次的认证请求。这时 USBKEY 便向服务器请求与应用服务器建立安全通道,为支付做准备。表述为:

$$C \rightarrow S: K_s\{T_c \| N_{c2} \| H_c(T_c \| N_{s1})_{K_c'}\}$$

4) S 在接收到用户建立支付安全通道的请求后,先解密再验证用户发来 N_{s1} 与自己存储的 N_{s1} 相同,就在应用服务器和用户终端之间建立安全通道。

3.3　支付认证阶段

支付认证阶段其数据交换过程如图 3。

1)在 C 和 A 之间的安全通道建立后,C 获取用户的支付信息如用户账号、支付金额、商家的账号等信息,将这些信息综合生成支付请求 REQ 并调用 $H_c()$ 计算 $H_c(T_c \| REQ)$,用 K_c' 签名后向 A 发送支付请求。表述为:

$$C \rightarrow A: K_a\{T_c \| REQ \| H_c(T_c \| REQ)_{K_c'}\}$$

2) A 在接收到 C 发来的支付请求,解密后从 REQ 中提取

(下转第 1822 页)

进一步具体细化、主动通信平台的开发、具体的信息建模、业务主动应用的开发、具体业务管理算法、管理原型系统的开发,等等)奠定基础和提供设计与实现指导,同时也为其他的研究者提供技术参考。

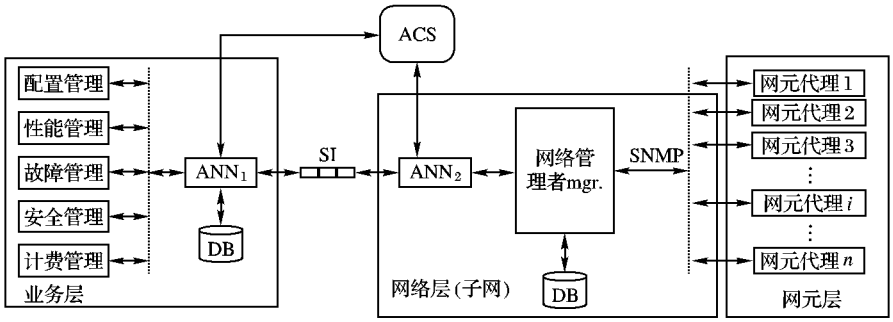

图 7 基于主动网络技术的业务管理模型

参考文献:

[1] 郭健,吴伟明,张爱霞. 面向业务的 NGN 综合网管系统的研究[J]. 数据通信,2005(3):9-12.

[2] MITRA D, SAHIN K E, SETHI R, *et al*. New directions in services management[J]. Bell Labs Technical Journal, 2000,5(1):17-34.

[3] Common information model core model version 2.4[R]. White Paper, Distributed Management Task Force,2000.

[4] TINA-C, Management architecture Version 2.0, TINA Baseline TB_GN010_2.0_94 [S]. 1994.

[5] Tele Management Forum. Telecom Operations Map. Approved Version 2.1 GB910[S]. 2000.

[6] TENNENHOUSE D L, SMITH J M, SINCOSKIE W D, *et al*. A survey of active network research[J]. IEEE Communications Magazine, 1997,35(1):80-86.

[7] CALVERT K L. Directions in active network[J]. IEEE Communications Magazine,1998,36(10):72-78.

[8] 王建国,李增智,韩冬,等. 主动代码插入机制研究[J]. 计算机研究与发展,2001,38(7): 68-72.

(上接第 1811 页)

支付信息,,生成支付命令 COM 并将它发送给 C,要求 C 对 COM 签名。表述为:

$$A \rightarrow C: K_c\{T_a \parallel \mathrm{COM} \parallel H_a(T_a \parallel \mathrm{COM})_{K_a'}\}$$

3)USBKEY 在接收到支付命令 COM 后,通过验证码生成器生成验证码 B,并在用户端显示。用户输入验证码 B',USBKEY 接收到 B',验证与 B 是否相同。如果,则验证用户身份合法,可以进行安全操作。此时 USBKEY 会对支付命令签名,并将它送往认证服务器。表述为:

$$C \rightarrow A: K_s\{T_c \parallel H_c(T_c \parallel \mathrm{COM})_{K_c'}\}$$

4) A 在接受到用户签名后的支付命令之后,就进行交易。

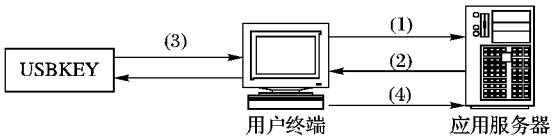

图 3 支付认证阶段数据交换过程

4 安全性分析

本文在双因素认证的基础上引入验证码认证,除了可以防止双因素认证可以防止的攻击如拒绝服务攻击、字典攻击、网络侦听、跟踪地址攻击和口令字猜测攻击等,还可以具有双因素认证不具备的如下所述的安全性。

1)双向认证。在身份认证第 2 阶段中完成了 S 对 C 的认证,S 通过 ID_c 在数据库中获得 K_c,在验证 C 发来的 $H_c(T_c \parallel A_c \parallel ID_c \parallel P \oplus N_{c1})_{K_c'}$ 就可以认证 C 的身份。而在第 3 阶段中完成了 C 对 S 的认证,C 通过验证 S 的 $H_s(T_s \parallel N_{s1})_{K_s'}$ 和核对 S 发来的 $P \oplus N_{c1}$ 就能验证 S 的身份。通过双向身份认证可以防止 S 的冒充。

2)重放攻击。每次 C 向 S 发送认证请求是,都会将 T_c 发送给 S,S 会将 T_c 保存。如果攻击者重放认证请求来冒充 C,S 就可以提取 T_c,如果提取的 T_c 与自己保存的 T_c 相同,则说明是重放攻击,S 就拒绝服务。同理,攻击者也不能重放以前的数据冒充 S。

3)仿冒攻击。本认证模式最大的特点就在于可以防止原有方案不能防止的仿冒攻击。引入验证码认证也是出于这个目的。在支付认证第 3 阶段中要对 USBKEY 进行安全操作时,USBKEY 会产生 B 要求用户输入。由于验证码中加入干扰增大验证码的识别难度,攻击者不能通过图片识别技术识别 B,也就无法仿冒用户输入验证码,就不能对 USBKEY 进行安全操作。

5 结语

近几年,随着网上银行的兴起,网络支付的应用越来越受到人们的关注,如何保障安全性成为其发展的关键因素。本文在现有的双因素认证的基础上,引入验证码验证并给出了具体的认证和支付协议。它能防止目前网上银行支付系统不能防止的仿冒攻击,提高网上银行支付系统的安全性。

参考文献:

[1] 赵著,胡运发,李丽燕. 电子商务中网上购物的安全协议: SSL 与 SET[J]. 计算机工程,1999,25(12):16-19.

[2] RFC 2401, Security architecture for the Internet protocol[S]. 1998.

[3] Copyright 1996—2007, Visa international service association, 3-DSecureTM System Overview[S]. 2001:5-10.

[4] 骆絮飞. 银行卡网上支付安全认证模式分析[J]. 信息安全与通信保密,2005(5):20-22.

[5] 危刚. 一种安全的网上支付及安全认证模式的分析与设计[D]. 长沙: 中南大学,2007.

[6] 李二亮. 第三方支付平台研究[J]. 电子商务,2005(9):91-94.

[7] 郑绮萍. 电子商务安全支付策略分析[J]. 华南金融电脑,2007(8):50-52.

[8] 魏永禄,朱红,邱兵. 基于双因素特征的信息安全身份认证技术研究[J]. 山东大学学报: 理学版,2005,40(3):76-79.

[9] 黄智. 基于 Z32U 带动态密码显示 USBKEY 的实现[D]. 武汉: 华中师范大学,2007.

[10] 王同洋,李敏,吴俊军. 基于多因素的身份认证[J]. 计算机应用与软件,2005,22(6):100-103.

[11] 洪伟铭. 验证码的原理及实现方法[J]. 武汉科技学院学报,2007,20(4):17-19.