基于二维码的移动终端动态口令认证方案*

周立兵 朱婷婷 付 伟
(海军工程大学信息安全系 武汉 430033)

摘 要 提出了一种适用于移动电子商务中的身份认证方案,以二维码为主要认证载体,结合随机数,实现了移动终端的动态认证。该方案安全性高,运算量小,方便快捷,且实现了移动终端和服务器端的相互认证。

关键词 二维码; 移动终端; 身份认证; 动态口令
中图分类号 TP393 **DOI**:10.3969/j.issn1672-9722.2014.04.027

A New OTP Authentication Scheme for Mobile Terminal Based on 2-Dimensional Code

ZHOU Libing ZHU Tingting FU Wei
(Department of Information Security, Naval University of Engineering, Wuhan 430033)

Abstract A new authentication scheme for mobile terminal in E-commerce environment has been put forward. The scheme was based on 2-dimensional bar code and combined random number to implement one-time-password authentication. It not only provided higher security and smaller computing task, but also provided mutual authentication between the mobile terminal and service provider.

Key Words 2-dimensional bar code, mobile terminal, authentication, OTP
Class Number TP393

1 引言

随着移动通信技术的飞速发展,我们已经进入了 3G 时代,移动终端已经成为了最常用的通信工具,用户只需轻轻按键就可以得到银行、商家提供的商品和服务。人们在享受移动终端和电子商务给生活带来的便捷的同时,对其安全性也存在不同程度的担忧。

身份认证是移动电子商务安全重要的组成部分,也是移动商务交易过程中安全性的薄弱环节[1]。传统的身份认证技术采用静态口令认证机制,通过用户输入的 ID 和口令来验证合法性,由于认证信息以明文形式在网络中传输,因此易受到窃听、重放等攻击。动态口令技术是在认证信息中加入不确定因素,然后将此变长的信息输入并压缩成一个定长的值输出,再发送至系统进行验证。虽然动态认证技术是一种安全可靠、切实可行的解决方案,但其存在易受小数攻击等安全漏洞。此外,由于移动终端和无线网络性能的限制,该技术在移动商务应用中具有更高的要求。

二维码是用特定的几何图形,按一定的规律,在二维平面分布的黑白相间的图形上记录信息[2~3]。作为一种全新的信息存储、传递和识别技术,具有容量大、识别速度快、防伪效果好、抗磨损等特点。若将其应用于移动商务,则可将用户信息、定制服务信息等多项信息都集成在二维条码内,提高了移动商务的服务质量。而任何一款拥有 30 万以上像素的移动终端,下载了二维码识别软件后,就可以充当二维码识别器了。

本文结合二维码和动态口令认证技术,提出了

* 收稿日期:2013 年 10 月 4 日,修回日期:2013 年 11 月 16 日
基金项目:国家自然科学基金(编号:611100042);湖北省自然科学基金(编号:2012FFC13201)资助。
作者简介:周立兵,男,硕士,讲师,研究方向:信息安全,身份认证技术,PKI 技术等。朱婷婷,女,博士研究生,讲师,研究方向:可信计算。付伟,男,博士,讲师,研究方向:云计算。

基于移动终端的身份认证方案。该方案充分考虑了移动商务交易的安全性要求，以及移动设备和无线网络的性能限制，具有安全性高，运算量小，方便快捷等特点，并且实现了通信双方的相互认证。

2 传统动态口令认证方案

动态口令是根据用户身份信息，引入不确定因子，产生随机变化的口令[8~9]。其实现方案主要有口令序列、挑战/应答、时间同步三种技术。

2.1 口令序列(S/Key)

S/Key 方案是在初始化阶段选取一个口令 pw 和一个数字 n，及一个哈希函数 f，计算 $y=f^n(pw)$，把 y 和 n 的值存到服务器端[3]。初次登录时，用户计算 $y'=f^{n-1}(pw)$，服务器端也进行同样的计算并同用户发送的值进行比较，如果二者相同则验证通过。下次登录时，计算 $y''=f^{n-2}(pw)$，以此类推，只到 $n=1$，重新将口令初始化。通过哈希链算法，用户每次登录到服务器的口令都不相同。这种方案易于实现，且无需特殊硬件的支持。

2.2 挑战/应答方案(Challenge-Response)

在 Challenge-Response 方案中，用户端和服务器端事先共享算法、密钥和挑战/应答令牌[4]。当用户向服务器端请求服务时，服务器端随机生成一个挑战数并发送至用户，用户依据共享信息计算出相应的应答数发送给服务器进行验证，从而身份认证。

2.3 时间同步方案(Time Synchronization)

Time Synchronization 方案事先也须共享算法、种子密钥等信息，把时间戳作为不确定因子加入到认证信息中，利用时间戳的实时性(通常 60s 变化一次)达到安全认证的目的。该方案可以保证很高的安全性，但也对时间戳有较高精确度的要求。

2.4 传统动态口令认证的缺陷

上述三种动态口令方案都比较安全和方便，但在安全性方面也存在隐患，将其应用于移动终端也存在相关不足，主要体现在以下几个方面：

1) 易受小数攻击。动态口令技术都采用 Hash 函数，输出定长且具有雪崩效应。目前，广泛应用的 Hash 函数有 MD4、MD5 和 SHA 系列等。但是这些方案存在着易受小数攻击等安全漏洞。

2) 没有实现双向认证。传统动态口令方案都只是对用户身份的合法性进行单方面验证，而没有对服务器端的真实性进行鉴别。攻击者采用中间人攻击的方式，可以轻易地冒充服务器窃取用户的信息。

3) 移动终端和无线网络的限制。在移动环境下，认证方案必须考虑设备性能的限制，此外无线网络也更容易被监听。Challenge-Response 和 Time Synchronization 都需要方案具备特殊的硬件支持，而要求每个移动用户都额外配置该硬件不切实际，降低了方案的可行性。

3 二维码技术

二维码是用计算机软件编码技术形成的平面几何图形，能够在横向和纵向两个方位同时表达信息，可以存储数字、汉字和图片[5,7]。它是一个不含电子芯片的存储器，而且这个图形可以通过打印、印刷、屏显等形式出现，其成本远远低于电子存储器。在代码编制上巧妙地构成计算机内部逻辑基础的“0”、“1”比特流的概念，使用若干个与二进制相对应的几何形体来表示文字数值信息，通过图像输入设备或光电扫描设备自动识别以实现信息自动处理。

二维码应用非常广泛，特别是在高科技行业、储存运输业、批发零售业等需要对物品进行廉价快捷的表示信息的行业用途广泛。二维码具有以下几个方面的特点：

1) 信息容量大：二维码比一维码的容量增大几十倍，例如 QR 码可以放入 1817 个汉字，或 7089 个数字，或 4200 个英文字母。

2) 编码范围广：可以表示图片、声音、多种文字、签字、指纹、数据等信息。

3) 容错能力强：具有纠错功能，因穿孔、无损等引起局部损坏时，只要损毁面积低于 50%，照样可以正确得到识别。

4) 防伪性能好：相比传统的一维码，二维码有着强大的防伪功能，通常有软件加密、指纹识别、照片等方式进行防伪，安全性能较高。

5) 尺寸可改变：条码符号形状、尺寸大小比例可变。

此外，还具有成本低、易制作，持久耐用及易识别等特点。

4 基于二维码的动态口令认证方案

本方案采用移动终端的唯一标识码 IMEI(International Mobile Equipment Identity Number)作为身份认证的主要认证因素，利用二维码技术进行认证信息的二次加密，并且实现了移动终端盒服务器的双向认证。

4.1 注册过程

用户获得相关服务前,需首先向服务器端进行注册,步骤如下:

1) 用户的注册信息包括移动终端唯一标识码 IMEI、用户 ID、定制的服务类型,将此注册信息使用双方共享的对称密钥加密后发送给服务器。

2) 服务器端接受信息后首先进行解密,然后生成服务器端随机数 $SerM_1$,连同提取的相关信息存储在服务器端数据库中。然后将服务器端随机数 $SerM_1$,以及将用户 ID、服务类型 SerType、服务提供商名称等信息生成二维码 $2\text{-}DCode_1$ 发送给用户。

3) 移动终端接收后,通过内置的解码器解码,核实服务提供商名称及定制服服务类型 SerType。确认无误后,将确认信息且发送给服务器端,同时保存收到的 $2\text{-}DCode_1$。

4) 服务器端将该用户账户激活。

4.2 身份认证

用户在获取其定制的服务之前,必须先访问服务器,并通过服务器的身份认证,在此过程中,用户也需要对服务器进行身份认证,步骤如下:

1) 用户第 i 次访问服务器时,将最新的二维码 $2\text{-}DCode_i$ 发送给服务器。

2) 服务器端收到后与保存的二维条码相比较,相关信息无误,则发送 $f_{S2C}(\text{SerType}|\text{SerM}_i)$ 给用户。其中 f_{S2C} 函数为双方共享的 Hash 函数,实现服务器向用户的身份认证。

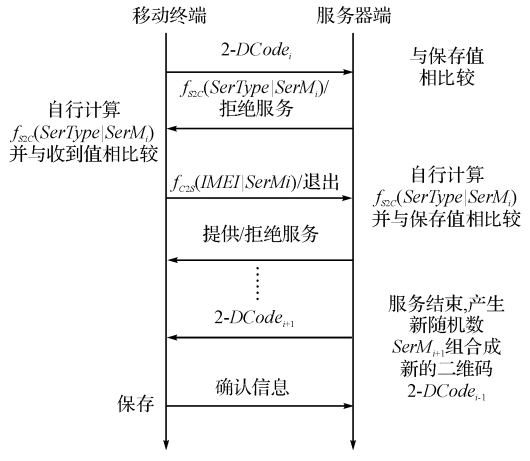

图 1 身份认证与信息更新

3) 用户接收后,自行计算 $f_{S2C}(SerType|SerM_i)$,并将二者进行比较。若相等则对该服务提供商认证通过,然后发送 $f_{C2S}(IMEI|SerM_i)$ 至服务器端;否则拒绝下载服务。其中 f_{C2S} 函数也是双方共享的 Hash 函数,是想用户向服务器的双方认证。

4) 服务器接收后,自行计算 $f_{C2S}(IMEI|SerM_i)$,并将二者进行比较。若相等则承认该用户的合法身份,为其提供服务。

5) 服务提供结束后,服务器端重新生成新的随机数 $SerM_{i+1}$,并且与之前生成的 $i+1$ 个随机数比较,确认无重合。然后将 $SerM_{i+1}$ 和相关信息重新组合的二维码 $2\text{-}DCode_{i+1}$ 发送给用户。

整个过程实现了移动终端与服务器之间的双向认证,并产生了新的二维码 $2\text{-}DCode_{i+1}$,供下次登录用。具体流程如图 1 所示。

4.3 安全性分析

本方案具有较高的安全性,具体分析如下:

1) 实现了双向认证:不同于传统的动态口令,本方案实现了移动终端对服务器的认证,提高了系统的安全性。

2) 抵御中间人攻击:在用户与服务器端通信的过程中,若攻击者截获了二维码并冒充用户与服务器进行通信,当服务器端需要确认用户身份时,由于攻击者无法获得用户的 IMEI,无法计算 $f_{C2S}(\text{IMEI}|\text{Ser}M_i)$,因此攻击者不可能冒充合法用户;同样,如果攻击者冒充服务器,由于其无法获得服务类型编码 SerType,同样无法计算 $f_{S2C}(\text{SerType}|\text{Ser}M_i)$,因此冒充失败。

3) 抵御重放攻击:由于每次服务结束后都重新生成新的服务器端随机数 $\text{Ser}M_i$,因此攻击者截获的消息不可重用。

4) 抵御小数攻击:本方案利用 Hash 函数产生一次性口令,与口令序列(S/Key)方案的产生原理不同,所以不存在小数攻击的漏洞。

5) 二维码的二次加密:f_{S2C} 与 f_{C2S} 是由一次性的信息压缩而成的,其在网络上传输即使被截获也不能还原得到内部参数信息;此外,二维码的编码复杂性和防辐射、抗磁性又增加了本方案的安全性。

5 结语

本文提出了一个基于二维码的移动终端动态口令认证方案,其结构简单,在实现上不需要额外的第三方,注册和认证过程均能快速完成。本方案能够抵御中间人攻击、重放攻击、小数攻击等安全威胁,且实现了移动终端和服务器端的双向认证,具有较高的安全性。

参 考 文 献

[1] 吴晓波,陈小玲. 移动商务与电子商务的比较研究—基于价值创造视角[J]. 情报杂志,2010,29(8):19-21.
WU Xiaobo, CHEN Xiaoling. Comparing mobile-com-

merce with E-commerce — Based on angle of view create value[J]. Information journal,2010,29(8):19-21.

[2] 王波. 手机二维码技术及业务发展[J]. 通信世界,2007(30):33-35.
WANG Bo. Mobile telephone 2-D code technology and business development[J]. Communication world,2007(30):33-35.

[3] 林玮,王晓峰. 基于非齐次线性方程组的一次性口令认证协议[J]. 计算机工程,2010,36(13):154-158.
LIN Wei, WANG Xiaofeng. One-time password authentication protocol based on non-homogeneous linear equations[J]. Computer Engineering, 2010, 36(13): 154-158.

[4] 范玉涛,苏桂平. 一种双向一次性口令身份认证方案的设计[J]. 计算机应用,2008,28(6):71-75.
FAN Yutao, SU Guiping. Design of a two-way one-time-pass-word authentication protocol[J]. Computer Applications,2008,28(6):71-75.

[5] 李媛. 复杂系统二维信息处理方法及其应用研究[J]. 北京理工大学学报,2002(8):95-101.
LI Yuan. Management means and application researching of complex system based on 2-D code[J]. University journal of Beijing science and engineering,2002(8):95-101.

[6] 薛素静,孔梦荣. 基于单向哈希函数的远程口令认证方案[J]. 计算机应用究,2008,25(2):512-515.
XUE Sujing, KONG Mengrong. Scheme of long-distance authentication based on Hash function[J]. Research of computer application,2008,25(2):512-515.

[7] 杨军,刘艳,杜彦蕊. 关于二维码的研究和应用[J]. 应用科技,2002,29(11):11-13.
YANG Jun, LIU Yan, DU Yanrui. Research and application of 2-D code[J]. Application technology,2002,29(11):11-13.

[8] 吴建武. 开放式网络中一种新的远程用户认证机制[J]. 计算机工程,2007,33(13):153-157.
WU Jianwu. A new authentication of long-distance user inopen network[J]. Computer Engineering,2007,33(13):153-157.

[9] 王娟,何琪,严飞,等. 一种以用户为中心的移动互联网身份管理及认证系统[J]. 山东大学学报,2102,47(11):12-17.
WANG Juan, HE Qi, YAN Fei, et al. A user-centric identity management and authentication system for mobile Internet[J]. Journal of Shandong University(Natural Science),2102,47(11):12-17.

[10] 吴应良,徐学军,孙东川. 电子商务的安全机制与体系结构模型[J]. 计算机工程与应用,2001,37(8):27-29.
WU Yingliang, XU Xuejun, SUN Dongchuan. Security mechanism and framework of E-commence[J]. Computer engineering and application, 2001, 37(8): 27-29.

(上接第 626 页)

LU Haitao, HOU Tongpu, LI Jian. Embedded Automobile Positioning System Terminal Development Based on GPS and GPRS[J]. Computer & Digital Engineering,2010,38(6):150-153.

[5] 苏永红. 基于物联网的物流车辆监控系统的设计与实现[J]. 计算机与数字工程,2011,39(7):75-77.
SU Yonghong. Design and Implementation of Logistics Vehicle Monitoring System Based on the Internet of Things[J]. Computer & Digital Engineering,2011,39(7):75-77.

[6] 王洪德,张俊. 基于角改进的城市交通网络实时最短路径算法研究[J]. 安全与环境学报,2009,9(3):166-169.
WANG Hongde, ZHANG Jun. Study on the real-time shortest path algorithm on the angle-modified basis in the urban trans-portation network[J]. Journal of Safety and Environment,2009,9(3):166-169.

[7] 程焱. 基于 USB 接口的 CAN 总线控制系统的设计[D]. 成都:西南交通大学,2005:1-2.
CHENG Yan. The design of USB control system based on CAN bus[D]. Chengdu: Southwest Jiaotong University,2005:1-2.

[8] 孙慧贤,张玉华,罗飞路. 采用 USB 和 CAN 总线的电力监控数据采集系统[J]. 电力系统机器自动化学报,2009,21(1):99-103.
SUN Huixian, ZHANG Yuhua, LUO Feilu. The electric power supervisory control and data acquisition system USB and CAN bus[J]. Power system automation Sinica,2009,21(1):99-103.

[9] 欧微,焦丽萍. 突发事件下车辆路径问题的动态规划算法[J]. 计算机仿真,2011,8(28):354-357.
OU Wei, JIAO Liping. Dynamic programming algorithm of vehicle routing problem under emergency, 2011,8(28):354-357.

[10] 张渭军,王华. 城市道路最短路径的 Djkstra 算法优化[J]. 长安大学学报(自然科学版),2005,25(6):63-65.
ZHANG Weijun, WANG Hua. Djkstra optimization algorithm for the shortest path of the cityroad[J]. Journal of Chang'an University(Natural Science Edition),2005,25(6):63-65.