基于手机令牌的动态口令身份认证系统的实现①

叶　晰　叶依如　岑　琴 (温州医学院 计算机系 浙江 温州 325035)

摘　要： 随着网络技术的普及，传统的静态密码方案已不能满足电子商务中的身份认证的要求。描述了动态口令技术的基本原理，分析了其软件和硬件实现的利弊，设计了一种基于挑战/应答模式的动态口令认证协议，并在此协议基础上设计实现了基于手机令牌的动态口令身份认证系统，论述了系统的总体设计、认证过程、安全性措施和具体的实施步骤，最后进行了系统的安全性分析。分析表明，该系统具有安全性高、适用面广，使用方便，系统成本低的特点。

关键词： 动态口令；手机令牌；挑战/应答

Implementation of a Dynamic Identity Authentication System Based on Mobile Phone Token

YE Xi，YE Yi-Ru，CEN Qin

(Department of Computer, Wenzhou Medical College, Wenzhou 325035, China)

Abstract: With the development of Internet technology, the traditional static password based authentication solutions are no longer an adequate protection scheme to serious enterprise applications. In this article, the principle of dynamic password technology is described, and the pros and cons of implementing dynamic password technology by software and hardware are analyzed as well. A dynamic password authentication protocol based on challenge/response mechanism is designed. The system's design authentication processes, and safety measures are described, and its security is analyzed as well. The analysis indicates that this system features high security and wide application. It can be conveniently used and implemented at a low cost.

Keywords: dynamic password; mobile phone token; challenge/response

随着电子商务的普及，人们已经习惯于网上购物，网上银行和电子支付等新兴事物，然而网络安全始终是制约电子商务发展的一个主要瓶颈。由于所有的个人和交易信息要在一个开放的网络(如 Internet)进行传输和交换，故我们需要身份认证技术去验证客户的身份[1]。身份认证一般基于客户拥有什么(如令牌，智能卡或者 ID 卡)，客户知道什么(如静态密码)，客户有什么特征(如指纹，虹膜和脑电波等)[2]。在众多的身份认证方案中，静态的用户名和口令方案至今仍是使用最广泛的方案，特别是针对那些安全性要求不强的应用场合，如论坛，BBS 和电子信箱。由于静态的密码方案不能抵御重放攻击，字典攻击且密码容易忘记，所以其安全性是很低的，不能满足电子商务中的身份认证的要求，而动态口令技术的发展和流行很好的弥补了传统静态密码方案的不足。

1　动态口令技术

1.1 动态口令技术的基本原理

动态口令又称为一次性口令 OTP(One - Time - Password)，其特点是用户根据服务商提供的动态口令令牌的显示数字来输入动态口令，而且每个登录服务器的口令只使用一次，窃听者无法用窃听到的登录口令来做下一次登录，同时利用单向散列函数(如 SHA-1 算法等)的不可逆性，防止窃听者从窃听到的登录口令推出下一次登录口令[3]。选取动态口令认证这种方案的商用系统采用的是静态密码与令牌相结合

① 收稿时间:2010-02-04;收到修改稿时间:2010-03-09

的方式进行身份鉴别。这种方式在检查用户静态密码(知道什么) 的同时，验证用户是否持有正确的令牌(拥有什么)[4]。

1.2 动态口令技术的硬件和软件实现

随着电子商务和网络游戏的盛行，网络身份认证技术越来越受到重视，银行和各种大型电子商务网站大多采用了提供动态口令令牌或动态口令卡来加强网络身份认证系统的安全性,如中行的电子口令牌、盛大密宝、网易将军令等。硬件口令令牌的成本较高，以中国银行免费提供给客户的 RSA SID700 型号的电子口令牌为例，根据其口令位数和有效期，价格为 900 至 1548 元不等。虽然硬件实现动态口令其安全性要高于软件实现，但对于中小型的电子商务网站来讲，硬件实现成本太高，显然是不现实的。软件实现动态口令技术的方法虽然简单易行，而且无需购买任何新硬件，只需一次编程就可解决所有问题，但攻击者可以通过假冒用户进行注册申请，从而获得服务器发送的用于生成动态口令的可执行文件。由于该可执行文件中包含了生成动态口令的算法，因此其口令生成机制容易被攻击者通过软件跟踪或其他方式予以破译[5]，这将在很大程度上降低软件实现动态口令系统本应具备的高安全性，违背了动态口令系统部署的原则。故开发一种低成本，高安全性的动态口令技术，可以解决中小型电子商务网站的身份认证问题。

2 基于手机令牌的动态口令系统的总体设计

现在某些大型企业(如中国移动)应用了基于无线传输的动态身份认证的系统，该类系统使用数字物理噪声源产生完全随机变化的动态(验证)密码,并通过无线通信方式将该动态密码发送到用户的无线通信终端(寻呼机或移动电话等)上。由于该认证系统的实时性和稳定性在很大的程度上依赖于无线通信网的状态。当网络出现拥塞时将导致动态密码传输会有较大的时延,甚至将使系统无法正常完成身份认证过程[6]，而且由于短信的发送会产生大量的短信费用，对中小型电子商务网站来说仍然是不小的开销。据赛迪网报道，到 2010 年中国手机用户数量将近七点四亿[7]，而基于手机令牌的身份认证技术利用用户已有的手机作为软件的运行载体，无需购买任何其他硬件，只需一次编程就可解决所有问题，并且在验证用户身份时手机无须接入 GPRS 网，不产生网络数据流量，这也减低用户的负担。

2.1 硬件的设计

一个常用的令牌(Token)需要解决：输入设备、输出设备、CPU、存储设备、电源、通信端口、晶振以及二进制和十进制的互相转换等问题[6]。如果应用于手机，那么输入设备(键盘)、输出设备(显示屏)、通信端口(串口)、晶振、存储设备、二进制和十进制的互相转换就可以借助手机的已有部件来实现。

2.2 手机程序运行平台的选择

手机程序运行的几种主流平台包括[8]：

1) Java 2 Micro Edition (J2ME)

2) Binary Runtime Environment for Wireless

3) Symbian

4) Windows Mobile Smartphone

由于 Java 语言广泛的网络支持和它的平台无关性特点，只要安装了 Java 虚拟机的手机都可以运行 Java 程序， 真正实现了“一次编程，到处运行”的理念，故选择 J2ME 作为手机令牌的开发平台。

2.3 动态口令技术模式的比较和选择

根据不确定因素的选择方式，动态口令可以分为：时间同步机制、事件同步机制和挑战/应答机制，其特点如下[9]：

(1)基于时间同步的令牌，一般每 60 秒产生一个新口令，但由于其同步的基础是国际标准时间，则要求其服务器能够十分精确的保持正确的时钟，同时对其令牌的晶振频率有严格的要求，从而降低系统失去同步的几率。

(2)基于事件同步的令牌，其原理是通过某一特定的事件次序及相同的种子值作为输入，在算法中运算出一致的密码。由于其算法的一致性，其口令是预先可知的，通过令牌，你可以预先知道今后的多个密码。同样，基于事件同步的令牌也存在失去同步的风险。

(3)基于挑战/应答模式的令牌属于异步令牌，由于在令牌和服务器之间除相同的算法外没有需要进行同步的条件，故能够有效的解决令牌失步的问题，降低对应用的影响，同时极大的增加了系统的可靠性。异步口令使用的缺点主要是在使用时，用户需多一个输入挑战值的步骤，对于操作人员，增加了复杂度。

基于时间同步的令牌的技术实现比较容易，但由于手机的时间精度不是很高，失去同步的机率较大，事件同步的令牌也存在失去同步的风险，所以我们最

终采用基于挑战/应答模式的异步令牌。

3　动态口令认证协议的设计

3.1 手机令牌（客户端）动态口令的产生过程

动态口令的产生和验证过程如图 1 所示。为了方便描述，对图中采用的符号做如下定义：A 为用户；S 为认证服务器；IDA 为 A 的标识；KA 为 A 用户密钥；PA 为动态口令；手机 IMEI 码 (International Mobile Equipment Identity),是国际移动设备身份码的缩写，是由 15 位数字组成的"电子串号"，它与每台手机一一对应，而且该码是全世界唯一的。

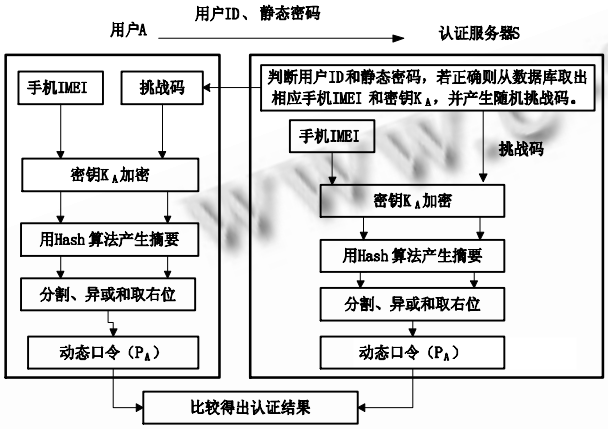

图 1　基于挑战应答模式的动态口令的产生和验证流程图

用户登录时首先在网站输入用户 ID 和静态密码，如果正确，网站会产生随机的 6 位挑战码并等待用户输入相应的动态口令。手机客户端 Java 软件首先直接从手机主板中读取本手机的 IMEI 码，然后使用保存在软件里的用户注册时生成的密钥 KA 分别加密手机 IMEI 码和用户输入的挑战码，然后用 HASH 算法(如 Sha-1 算法)对加密结果进行单向散列计算(相当于第二层加密)，产生两个等长的 40 位十六进制摘要。把这两个摘要分别平均分割为 8 段并转换为十进制，最后把两组 8 段的十进制数分别进行异或运算并取每段最右边位得到最终的 8 位动态口令。

3.2 动态口令的验证

验证服务器接收到用户输入的用户 ID 和静态密码后，先验证两者是否正确，如正确则在数据库中读出该用户的密钥 KA 和注册时用户登记的手机 IMEI 码，并产生随机 6 位数作为挑战码。密钥在发布动态口令客户端软件时应该已确定，并存放在验证服务器端数据库内。使用密钥 KA 对手机 IMEI 码和挑战码进行同客户端相同的处理，最终产生验证服务器端的动态口令，并与客户端传来的动态口令进行比较，一致则通过验证。

3.3 提高安全性的措施

(1)将用户密钥 KA 和手机 IMEI 码用服务器公钥经公钥加密算法(如 RSA 等)加密后保存在用户数据库中，这样就能防止对服务器用户数据库的攻击造成用户密钥和手机 IMEI 码的泄露。

(2)对于手机客户端软件设置特定的使用密码，只有用户本人才能使用手机令牌软件，实现双因素认证。

(3)为了防止攻击者通过输入假冒的手机 IMEI 码进行注册申请，从而获得服务器发送的用于生成动态口令的可执行文件，我们可以编写一个验证手机 IMEI 码的 Java 程序。该 Java 程序可直接读取存储在手机主板上的 IMEI 码信息，然后进行计算 H’(IMEI),其中 H 是一种安全的杂凑算法。用户下载该验证程序，运行并把得到的 H’(IMEI)值提交到服务器，同时用户可在本手机上通过输入“*#06#”得到 IMEI 码并提交到服务器。服务器计算 H（IEMI），然后比较 H（IEMI）和 H’(IMEI)，如果相等则认为用户输入的手机 IMEI 码是合法真实的。由于该 Java 程序是直接从手机主板读取 IMEI 码，且安全的杂凑算法的理论不可逆性决定了破坏者无法根据密文推出明文[10]，故攻击者是无法根据 H’(IMEI)推算出 IMEI 码的，这样一来攻击者就无法通过假冒手机 IMEI 码进行注册申请了。

(4)认证服务器端设置账户锁定关键字 FinalLock 和 TempLock。FinalLock 的值要求是一个整型数字(如 10)，如果用户连续输入动态口令的次数超过 FinalLock 的值以后仍没有通过验证，那么服务器端该用户就被锁定了，无论输入什么口令都不起作用了，只能通过注册中心人工办理解锁业务；TempLock 也是整型数字(如 3)，但是比 FinalLock 的值要小：当用户连续输入口令的次数超过 TempLock 值(但没有超过 FinalLock)以后仍没有通过验证，那么用户会进入一个延时(一般是几分钟到几十分钟)状态，在这个状态中，用户输入任何口令都是不起作用的，当这段时间过去之后，用户又可以输入口令进行验证了。·

3.4 系统碰撞性测试

不同的明文如果经过加密后密文是一样的，则我

们称这种现象为碰撞。窃听者在截取了大量老的动态口令后，可能组成一个口令字典，然后对认证系统进行攻击，故碰撞率的高低直接决定了动态口令系统的抗攻击性。具体测试方法为:

编程让 6 位挑战码从 0 每次递增 1 直至 999999，并依次产生相对应的动态口令并存入文本文件中，产生的口令总数为：999999-0+1=1000000 个。通过编程逐个两两比较这个文本文件中所有口令，找出相同的口令个数（即下表中的碰撞数），然后碰撞数除以总的口令数即为最终的碰撞率。测试结果数据如表 1 所示。

表 1　碰撞数据表

手机序列号	Key	口令数	碰撞数	碰撞率
357070001976258	12	1000000	4112	0.4112%
357070001976258	122	1000000	4001	0.4001%
359338014941875	189	1000000	4056	0.4056%
359338014941875	119	1000000	4043	0.4043%
353906010402237	255	1000000	4088	0.4088%

从上表中我们可以看到：遍历所有可能的挑战码，相应产生的动态口令的碰撞率大约为 0.406%，即平均连续输入 246 个挑战码可能会出现一次碰撞，总体碰撞率不高，而且实际应用中我们只是在需要登录时才会根据当时随机产生的挑战码得到相应的动态口令，之后即关闭程序，而不会连续运行程序。故实际应用中碰到相同动态口令的机率是很低的。

4　动态口令技术的具体实施步骤

(1)新用户在网站上先注册会员，得到自己的用户 ID 和静态密码，并要求提供动态口令服务。

(2)新用户被审核通过后，网站产生一个随机整数(或者用户自己输入一个整数)作为密钥 KA 并存放于数据库用户登录信息表中。同时用户输入自己手机的 IMEI 码，并使用下载的验证手机 IMEI 码的 Java 程序进行验证。 服务器通过验证后，把用户手机的 IMEI 码也保存在服务器数据库中。

(3)网站根据用户的密钥 KA 生成一个 Java 安装文件，并发放给用户(可通过蓝牙下载、网页直接下载和短信通知等多种方式)，用户安装生成手机令牌软件。当用户登录网站时，首先输入用户 ID 和静态密码，如正确则网站页面显示 6 位挑战码。用户运行令牌并输入挑战码，得到相应的 8 位动态口令。

(4)用户在网页上输入动态口令，如果正确即可登陆成功。系统运行模拟效果如图 2。

图 2　动态口令系统运行模拟效果图

5　系统的安全性分析

(1)本系统基于挑战/应答机制，采用异步的方式，不存在同步的问题。

(2)由于每次认证使用不同的随机数作为不确定因素，避免了小数攻击。

(3)能有效抵抗截获/重放攻击，即使攻击者可以通过一些软件或其他手段窃听到用户的动态口令，但是由于动态口令是一次性的，且我们限制同一账户同时只能一人在线，故窃听到的口令即使发送给认证服务器也不能通过认证。而且由于每个动态口令之间是不相关的，不能从这个动态口令推出下一个动态口令，所以攻击者得到了动态口令也没有用。

(4)所谓的字典攻击是指窃听者在截取了大量老的动态口令后，可能组成一个口令字典，然后对认证系统进行攻击。从上面的碰撞性测试的数据中我们得知窃听者平均连续截获了 246 个以上动态口令后，再在验证服务器上连续输入这些动态口令，可能会有一次成功的机会。实际应用中窃听者很难窃听 246 个连续动态口令，且认证服务器端我们设置了账户锁定关键字 FinalLock 和 TempLock，只要用户连续几次输入错误的动态口令后，该用户即被锁定了。故该系统可以抵抗字典攻击。

(5)认证服务器的帐户锁定功能使得蛮力攻击和猜测攻击难以成功，一个攻击者要在有限次数内猜中 8 位动态口令值的概率极小。

(6)物理安全可以保证。使用双因素身份认证，即使用户的手机丢失或者被盗，如果不知道用户设置的令牌软件的使用密码，也不能打开手机令牌软件，无法得到动态口令和通过认证。

(7)考虑到手机平台的运算能力有限，手机程序的

运算量不能太大。本手机令牌的产生只需要进行两次 Hash 计算，一次异或计算以及其他几个简单操作，总体运算量很小。

(8)该系统没有实现双向认证，故不能抵抗中间人攻击。由于认证协议的单向性，即服务器可以验证用户的身份而用户不能验证服务器的身份，若攻击者冒充服务器，就可以得到用户的口令，并可以将此口令发送到合法的认证服务器，通过认证，从而接入系统。要解决这个问题，必须采用公钥技术设计新的密码协议，但这会增加令牌设备的计算量，从而降低认证速度。当用户量较大时，还会使认证服务器产生巨大的计算负荷[11]。

(9)验证手机 IMEI 码的 Java 程序可以防止假冒的 IMEI 码的输入，但如果攻击者使用特殊仪器直接重刷手机的 IMEI 码，则本系统仍然无法防止此类攻击者的恶意注册。

6 结束语

文中提出的基于手机令牌的动态口令身份认证系统可以为各类中小型商务网站，企业用户远程登录内部网等服务平台提供安全的身份认证。该系统解决了硬件实现动态口令高成本和软件实现动态口令低安全性的不足之处，用户只需利用随身携带的手机就可以获得动态口令，不必携带额外增加的硬件设备，使用非常方便。动态口令的获得无需连入 GPRS 或 3G 网，节省了用户网络流量费。相对于传统的基于短信的身份认证系统，该系统可以为企业节省大量的短信通信费用，而且即使手机通信网络拥塞或手机无信号，该系统也不会受到任何影响。同时该系统相对独立，接口简单，易于与现有的应用系统连接，对正在运行的应用系统仅需做极小的改动即可，具有广阔的应用前景。

参考文献

1 Li Y. Research on e-business identity authentication system based on improved one-time password, 2008 nternational Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2008.

2 李传目.一次性口令技术的研究.集美大学学报(自然科学版), 2003,8(2):160－163.

3 胡天麟,刘嘉勇,陈芳,隋喆.基于 MD5 的 OTP 认证系统的原理及实现.信息技术, 2005,9:140－142.

4 Li FY, Liu PY, Ju HW. Realization of a New Scheme of Improvement on OTP Authentication Technology, Computer Systems & Applications, 2003(04).

5 Li XJ, Tong HQ. Improvement of OTP Authentication. Computer Development & Applications, 2004(9).

6 曾伟国,胡汉平,王祖喜,孔涛.基于手机令牌方式的动态身份认证系统.计算机与数字工程,2005,9:21－24.

7 天虹. IEMR:2010 年中国手机用户数量将达 7.38 亿. [2008-01-30].http://news.ccidnet.com/art/1032/20080130/1358247_1.html.

8 Morrison M, 李强.J2ME 手机游戏编程入门.北京:人民邮电出版社, 2005.8－10.

9 吴佩萱.基于时间同步机制的动态密码认证系统.长江大学学报(自然版), 2005,2(7):256－257.

10 Hu TL, Liu JY, Chen F, Sui Z. Principle and realization of OTP authentication system based on MD5. Information Technology, 2005(09).

11 Kim HC, Lee HW, Lee KS, Jun MS. A Design of One-Time Password Mechanism using Public Key Infrastructure. Proceedings 4th International Conference on Networked Computing and Advanced Information Management, NCM 2008, 2008.18－24.