张海峰　赵凯　（长城计算机软件与系统有限公司 100083）　　陆倜　（北京机械工业学院 100085）

Introduction to Technology and Application of Lightweight Certificate Authority

轻量级认证、授权技术与应用最新进展

摘要：PKI的CA体系是网络安全的一种很成熟的解决方案，但比较笨重，而且不是对所有应用都适合。因此，一些轻量级的认证与授权模式被提出作为必要的补充，本文介绍了电子令牌技术、一次性口令技术、生物识别技术和硬件识别技术。

关键词：CA　电子令牌　一次性口令　生物识别　多功能感知　硬件识别

1　引言

在Internet这样完全开放的环境里，如何认证用户的合法身份并授予其恰当的权限，是一个先要解决的安全问题。原始的解决方案是用户名和密码的方式，随着技术的发展，这种体制暴露出了严重的缺点：不佳的密码很容易被字典攻击获得，密码发送很容易被非法截获，无法保证信息的正确性、完整性和不可抵赖性。为了解决这些问题，出现了公钥(PKI)体系，以RSA为代表的非对称加密方法很好地解决了网上信息传递的安全问题。进入90年代，公钥体系的理论和实践都渐渐成熟起来，出现了很多相关的安全产品和CA认证中心，使网络安全的问题得到了比较全面的解决。

但PKI的CA体系也有它的明显不足之处。概括来说，就是过于完整，过于庞大，从而带来成本的高昂和技术的复杂性。尽管相应的规范早已制定，但几个主要的PKI CA体系的兼容性和互操作性却并不很好，还远没有达到现有的信用卡体系那样的广泛接受程度。而且随着用户数量的上升和使用时间的不断延伸，其管理的难度迅速增大，客户端的操作复杂和证书管理的困难也一直没有很好的解决方法。虽然PKI CA体系在理论上已经非常成熟和完整，在实际应用推广中，却遇到了相当的困难。中国截至目前为止建立的32家CA认证中心，无一例外地采用了PKI CA体系，但目前的营运状况都不理想。而且针对单一企业内部的一些并不复杂的应用，比如电子邮件，如果也采用一套完整的PKI CA作为解决方案的话，则更加显得笨重，巨大的开销也是不必要的。

针对以上情况，一些更“轻量级”的认证和授权方案被提出来了，根据采用的技术和依据不同，大致包括：电子令牌技术、一次性口令技术、生物识别和多功能感知技术、硬件识别技术等几类。

2　电子令牌技术

基于电子令牌的系统，是将一个物理令牌（客户令牌、智能卡，或者PalmPilot）与密码结合使用的双密系统。是目前比较成熟的技术，已经在网络安全方面有了极其广泛的应用。

IC卡（智能卡）是目前使用广泛的电子令牌，具有极高的保密性，而且方便携带，价格便宜。IC卡可以存储私有密钥，并且在卡内可以进行加密运算，也可以存储口令。IC卡使用PIN（个人识别码）保护技术，使用IC卡必须输入正确的PIN，如果连续输入错误（可设定，一般为3次），智能卡会自动锁定，防止了猜测口令式的攻击。在CA系统中，登录到控制台、签发证书、密钥管理等关键环节都强制使用IC卡登录，管理员只需有IC卡和知道PIN码，IC卡内的私钥和口令他不须也不可能知道，这比采用口令验证方法安全得多，管理员不可能将口令记载在笔记本上或与他人共享。

另外，还有诸如RSA SecurID的多种令牌的解决方案。在与RSA ACE／服务器结合使用时，RSA SecurID认证令牌在网络中的功能

与ATM卡类似，当用户获得访问权限之前，认证令牌要求其通过两个唯一系数进行身份识别。目前，已有超过5百万人利用该方案安全地收发电子邮件、访问网络操作系统、Extranet和Intranet等。RSA SecurID家族包含硬件令牌、软件令牌、智能卡以及针对掌上型计算设备的型号，为用户提供了可靠易用的认证解决方案，可以适应各种机构的需要。

3 一次性口令(OTP)技术

一次性口令的主要思路是在登录过程中加入不确定因素，使每次登录过程中传送的信息都不相同，以提高登录过程安全性。一次性口令技术有效地避免了重放攻击，解决了静态密码可能出现的在传输中被窃取和在数据库中被盗用的问题，目前密码认证仍然是非常重要的认证方式，将传统的静态密码替换为一次性口令将是密码发展的趋势。金融、证券、电子政务等领域均已广泛采用了一次性口令的技术。

当一个用户在服务器上首次注册时，系统给用户分配一个种子值(seed)和一个迭代值(iteration)，这两个值就构成了一个原始口令，同时在服务器端还保留有仅用户自己知道的通行短语。当用户每次向服务器发出连接请求时，服务器把用户的原始口令传给用户，用户接到原始口令以后，利用口令生成程序，采用MD4或MD5散列算法，结合通行短语计算出本次连接实际使用的口令，然后再把口令传回服务器；服务器先保存用户传来的口令，然后调用口令生成器，采用MD4或MD5散列算法，利用用户存在服务器端的通行短语和它刚刚传给用户的原始口令自行计算生成一个口令；服务器把这个口令与用户传来的口令进行比较，进而对用户进行身份确认；每一次身份成功认证后，原始口令中的迭代值数自动减1。这里要指出的是，用户主机上采用的散列算法和服务器上采用的散列算法必须是一样的。

可以看出，用户通过网络传给服务器的口令是利用原始口令和通行短语经MD4或MD5散列算法生成的密文，用户本身的通行短语并没有在网上传播；在服务器端，因为每一次成功的身份认证后，用户原始口令中的迭代值就自动减1，这样，下一次用户连接时使用的原始口令同上一次使用的原始口令是不一样的，因此，两次生成的口令也是不同的，从而有效地保证了用户口令的安全。一次性口令的使用过程示意图(见图1)。

不确定因子选择方式大致有以下几种：

(1) 口令序列(S/KEY)口令为一个单向的前后相关的序列，系统只用记录第N个口令，用户用第N－1个口令登录时，系统用单向算法算出第N个口令与自己保存的第N个口令匹配，以判断用户的合法性。由于N是有限的，用户登录N次后必须重新初始化口令序列。

(2) 挑战/回答(CRYPTOCard)用户要求登录时，系统产生一个随机数发送给用户，用户用某种单向算法将自己的秘密口令和随机数混合起来发送给系统，系统用同样的方法做验算即可验证用户身份。

(3) 时间同步(SecureID)以用户登录时间作为随机因素，这种方

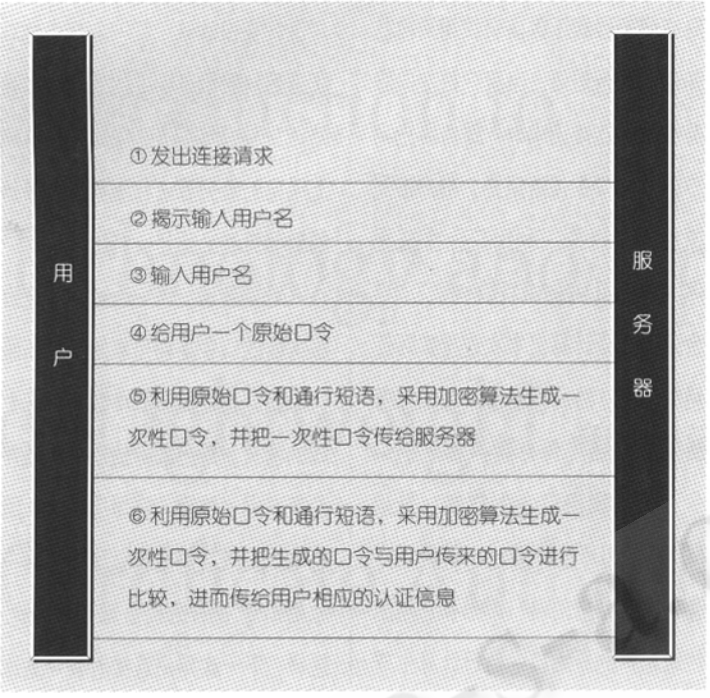


图1 一次性口令的使用过程示意图

式对双方的时间准确度要求较高，一般采取以分钟为时间单位的折中办法。在SecureID产品中，对时间误差的容忍可达±1分钟。

(4) 事件同步 (SafeWord) 这种方法以挑战/回答方式为基础，将单向的前后相关序列作为系统的挑战信息，以节省用户每次输入挑战信息的麻烦。但当用户的挑战序列与服务器产生偏差后，需要重新同步。

4 生物识别和多功能感知技术

生物特征识别技术[1]是利用人体的生物特征来进行身份验证的一种解决方案，由于人的生物特征具有人体所固有的不可复制的唯一性，因此这一生物特征密钥无法复制、失窃或遗忘。Bill Gates曾做过这样的断言，生物识别技术将成为今后几年IT产业的重要革新。利用生物特征识别技术，人们开发了指纹识别、语音识别、虹膜识别以及面部特征识别等多种系统，而且许多系统都已经发展成熟并得以应用。它的应用也越来越广，诸如税务、银行、证券、计算机系统、核电站、身份证、公安、汽车防盗、电话、会员制场所身份确认系统(俱乐部、机场)、门禁、考勤(办公室等安全、机要部门)、身份确认系统、护照、警网现场指纹认证、股民身份认证等许多方面。各种生物识别系统很好地解决了传统安全保护方式存在的隐患，提供了相对方便、快速、准确的身份识别方法，但由于技术和硬件的问题，当前的生物识别对于特征库较小的应用更实用，如果需要几百万甚至更多人的特征，则使得比对开销很大，成本也较高。而且生物识别系统也存在着各自的缺点。

指纹识别系统充分利用了两个人的指纹完全一样的几率是十亿分之一这一特性，通过图像扫描设备将指纹图案扫描下来，利用计算机视觉理论、图像分析算法和模糊逻辑算法将指纹图像特征转化为点或线构成的图，并计算出一些距离值和角度值，然后将转化后的图片及数值储存到数据库中以备查询匹配之用。这使得无论怎么按指纹，这些图片及数值都不会发生变化，以此作为识别特征几乎可以保证万无一失。但这种技术要求在按指纹时手指保持洁静、光滑，脏东西或者疤痕都会给识别带来困难。

语音识别技术是利用每个人的声音如同指纹一样彼此相异这个特点，利用人们语音特征的不同，对特定人进行判断。然而说话语气的变化，甚至当您感冒时嗓音发生了变化，都可遭到识别系统的拒绝。

虹膜识别系统利用世界上没有两个人的眼睛虹膜是一样的这一特征来进行身份鉴别，即使是双胞胎，虹膜也各不相同，而且人的虹膜在一岁之后不再发生变化。系统利用一台标准摄像机对用户的眼睛进行扫描，然后将扫描图像转化成数字信息与数据库的资料核对，以对用户的身份进行验证。但目前虹膜识别系统的价格还比较昂贵。

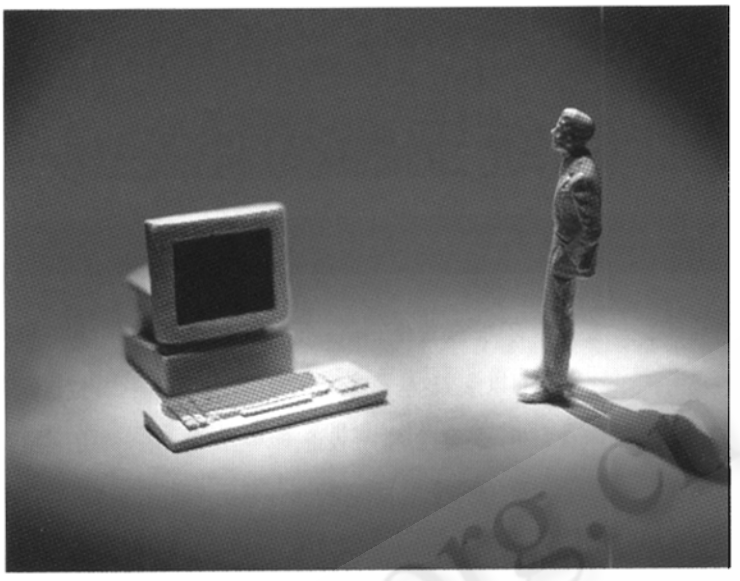
面部特征识别系统是人们最早使用的生物特征识别技术。该技术通过比较面部某些特征部位的大小和关系，例如鼻子的长度和两眼之间的距离，或是对面部区域周围的几十个点进行分析，将这些点排列成一幅图案，并与数据库中储存的图像进行比较。但是这种系统的抗干扰性差，对双胞胎的鉴别仍然无能为力，发型、肤色的变化甚至胡子或是体重的变化、是否戴眼镜都会影响到系统的识别。

不同于上面提到的几种单一的生物特征并需配合特定硬件使用的识别系统，应运而生了多功能感知技术。多功能感知机是集自然语言-语音、文字与非自然语言-手语、人脸、表情、唇读、头势、体势等多通道为一体的,并对这些通道信息进行编码、压缩、集成、融合的计算机智能接口系统，包括图象、音频、视频、文本等多媒体信息，它的目的在于改善人机之间的交互方式，改变目前计算机的盲、聋、哑的状态，达到能够看、听、说的水平，使计算机能够与人自然交互，是计算技术向人类社会全面渗透的重要手段。

5 硬件识别技术

硬件识别技术是通过计算机本身唯一的硬件特征来标识使用者的身份，结合PIN码的使用，可以实现一种高强度的双因子认证。它的基本假定就是：对于固定的用户，其使用的电脑也是相对固定的(在公用的电脑上是不应该执行任何涉及个人机密的操作的，否则安全根本得不到任何保障)，那么，通过对这台电脑的识别，加上对当时使用电脑的使用者的识别，就可以实现

对用户的远程认证。其难点和重点，在于识别电脑的唯一硬件特征。每张使用的网卡都有一个全球唯一的MAC地址，这是网卡生产商都遵循统一的规定，它们按照统一的分配来给自己生产的网卡指定MAC地址。同样的，对于CPU，硬盘，主板等其他计算机部件，都存在着相应的协议和规范。正规的生产厂商所生产的产品一定是遵循这些规范的，因此这些部件都有一定的参数可以作为自身的标识，而这些参数的联合，足够构成一个全球唯一的硬件标识号码。因此，如果首先对合法用户的电脑进行硬件特征采集，在实际的使用过程中，通过对于该号码的实时获取，可以实时地认证一台具有唯一特征值的电脑是否是已经注册的合法使用者。而认证的另外一个过程发生在认证开始之前，用户要启动认证过程，首先要输入自己的PIN码，这样，通过对用户口令（在本地识别，不必与认证服务器进行口令传送的交互）和计算机硬件特征值的联合识别，可以以相当高的安全性来确认用户的身份（由于使用的加密技术与PKI CA体系完全一致，完全可以认为这样的身份认证系统具有与PKI CA



体系一样好的安全性），而且由于没有作废列表查询更新等问题，认证是相当快速的，这样的系统与现有的业务和网络系统的整合也相对简单，它本身是相对独立的系统，其实现也并不复杂，非常容易整合到现有的网络体系之中。

这样的一个认证系统，通过Internet来完成对业务受理点的接入者的认证，从而杜绝业务信息可能的外泄，是一个相当理想的方案，而且这样的一个系统经过拓展，可以实现网上出版物的版权保护这个世界性的难题。以往，网上知识产权的保护是基本上无能为力的，同一本书的拷贝可以在任何一台计算机里面复制，被阅读；同一段音乐或影像也可以毫无障碍地予以复制。这是网络媒体和传统媒体的先天区别。通过识别特定计算机的硬件特征，如果以这种硬件特征值来对经授权的拷贝进行签名或加密，那么这个拷贝就带有了与某一计算机的硬件相关的唯一标识。这样，可以通过一定的手段来限定这样的拷贝只能在该计算机上解密后使用；这样即使被复制，复制品在别的（因此硬件特征值一定不同）计算机上也不能使用。这就达到了版权保护的初衷。

6 小结

当今Internet越来越壮大，也越来越庞杂，基于网络的应用种类也越来越多，在这种情况下，很难有一种安全机制可以一劳永逸地解决全部的安全问题，或者对于全部应用都是最佳的选择。所以，虽然PKI CA的体制可以说非常完善了，但不同的认证和授权模式的研制还是十分必要的。

本文介绍了几种"轻量级"的认证和授权方案，它们是PKI CA体制很好的补充。下表是几种认证方法的比较：

本文介绍的认证方法可以结合起来使用，比如将一次性口令技术使用在智能卡的认证过程中，而电子令牌又可以为一次性口令提供不确定因子，通过针对具体应用的"量身定做"，合理使用其中一种技术或者结合使用几种技术可以提供更灵活、更适当的安全保障，这样可使得许多的网络应用开发变得更加简单、快捷，成本也更低廉了。

参考文献

1 王波涛，蔡安妮，孙景鳌．生物图像识别技术及其应用 [J]．计算机工程与设计，2001,22(4)，

2 BruceSchneier.应用密码学协议、算法与C源程序（第二版）[M]，吴世忠等，机械工业出版社，2000。

表 几种认证方法的比较

认证方法	安全性	优势	目前缺点	应用领域	发展趋势
PKI CA	极高	安全性高，被广泛接受	技术复杂，比较笨重，需要第三方	电子商务、电子政务等	对高安全性领域将是主流技术
电子令牌	一般	技术成熟，成本低	容易损坏，物理尺寸限制，硬件性能提高较慢	证券、银行、门禁、签到、电子钱包等	将成为认证信息携带的主要载体
一次性口令	高	算法实现简单	通常需要和其他技术结合使用	证券、银行、企事业单位	将是未来密码认证的必然发展趋势
生物识别	高	不会丢失、遗忘，可以唯一确定某人	技术不够完善，识别正确率不能达到100%	个人身份确认、身份 证、银行、门禁等	随着技术成熟，将成为个人认证方式的主流趋势
硬件识别	一般	可以唯一确定某机器，可以实现版权保护	硬件变化可能很频繁，变更需要人工确认	机器相对固定的企事业、网点，版权保护等	将成为唯一识别机器、版权保护技术的主流趋势