多通道混合身份认证系统中安全策略设计①

Design of security policy in Hybrid Person Identity Authentication System

徐 洁 杜鹏英 方志刚 鲍福良 （浙江大学城市学院信电分院 310015）

摘要：将生物认证技术与传统认证方法结合起来，针对不同安全等级需求，构建了一个基于密码、人脸和语音的多通道混合身份认证系统。提出了一种安全策略的栅栏模型，并设计了一个针对 ATM 银行柜员机的身份认证系统的安全策略。

关键词：生物认证 多通道 安全策略

1 引言

传统身份认证方法存在着与生俱来的缺陷，主要表现为有形物品容易丢失、被盗窃、被伪造，而口令和密码等容易遗忘、记错或被盗取，这是因为上述标识物品和被认证人之间无法建立牢固的直接联系。目前，大多数用户认证系统无法区分真正的用户和取得用户标识的冒名顶替者，假冒事件时有发生。因此，用户身份认证应当考虑人的因素，可以采用生物认证（Biometrics Authentication）技术[1]。

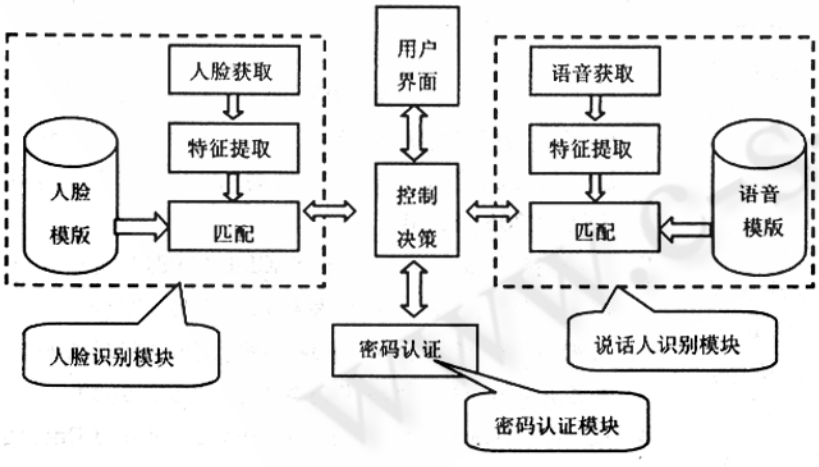

图 1 多通道混合身份认证系统框图

尽管与传统的认证方法相比，生物认证在安全性和保密性上的优势显而易见。但是，生物认证技术一般也不具备传统认证方法具有的认证过程简便、认证结果精确、成本低等优点。生物认证技术通常会对用户造成一定的侵入性（Intrusive），使用户在个人习惯和公共卫生（如留取指纹时）、身体安全（如获取虹膜特征时）以及个人隐私方面产生顾虑[2]。这种顾虑对于反恐和刑侦等应用领域也许不是主要问题，但是对于银行之类的应用却必须考虑用户是否接受、是否配合以及使用成本等因素。另一方面，由于生物认证本质上依赖模式识别和数据融合技术，识别结果必然存在一定的模糊性，故而存在虚警（即错误地拒绝真实用户）和漏警（即错误地接受虚假用户）的问题[3]，应用系统往往很难权衡安全性与方便性的矛盾，从而限制了生物认证技术的推广使用。为解决这一矛盾，应当将生物认证技术与传统认证方法结合起来，针对不同安全等级需求，实现多通道混合用户身份认证系统。

2 系统介绍

传统用户身份认证和生物特征认证技术具有不同特点，这要求仔细权衡两者的安全性和方便性指标，发挥各自的优势。本文针对不同安全等级需求（如 ATM 取款金额），研究一种混合用户身份认证体系，以满足数字化交易对用户身份认证的安全性、可靠性和灵活性要求。系统框图如图 1 所示。

① 基金项目：浙江省科技厅项目（2006C31006）、浙江大学城市学院教师科研基金（J52207001）

人脸识别模块完成用户面部图像的获取，图像预处理，人脸检测和定位，人脸识别等任务。说话人识别模块完成用户说话语音的获取、语音信号预处理（噪声消除、预强调、语音检测、分帧和加窗等）、语音信号特征提取和分类识别等任务。密码认证模块完成传统的密码认证任务，本系统中简化了这一模块的设计，没有采用复杂的密码加密技术，只进行简单输入密码与真实密码的比对工作。

控制决策模块在系统中的作用类似大脑在人体中的作用，它负责协调各个模块的工作，各种控制、数据信息都在它的控制之下，由它负责统一调度。控制决策模块和其它模块进行交互，完成接受用户界面的输入，进行用户安全策略读写，向各个身份认证模块发出认证指令，接收各个认证模块的身份认证结果并分析处理，反馈给用户界面认证结果等工作。该模块根据系统设置的安全等级（具有可伸缩性），生成相应的多通道生物特征融合算法，实现混合用户身份认证功能。

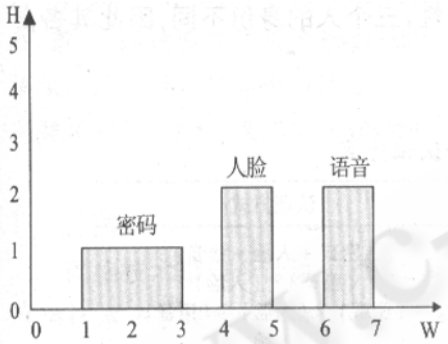

图 2　H－ATM 三种认证方式各自的栅栏形状

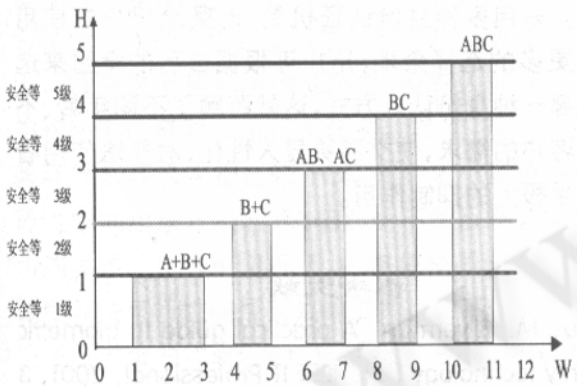

图 3　5 种安全等级的栅栏

3　系统安全策略设计

3.1　栅栏模型

设认证系统由 $A_1, A_2, \cdots, A_i, \ldots, A_{n-1}, A_n$ 共 N 种认证方式，A_i 的栅栏模型表述如下：①由于各种认证方式的安全性不同，给每一种认证方式赋予一个安全权值 H，用这个 H 来代表该种认证能提供的认证安全水平，H 值越大表示安全水平越高，设这 N 种认证方式的安全权值分别为 $H_1, H_2, \cdots, H_i, \cdots, H_{n-1}, H_n$；②由于各种认证方式的成本、可操作性和用户接受度等性能参数不同，给每种认证方式设置一个参数 W，W 是这种认证方式的成本、可操作性和用户接受度等性能参数的函数。W 值越大表示成本、可操作性和用户接受度等性能参数合性能越好，设这 N 种认证方式的参数 W 参数分别为 $W_1, W_2, \cdots, W_i, \cdots, W_{n-1}, W_n$；③认证方式 A_i 独立工作时，用一个栅栏 F_i 表示它，栅栏的高度是 H_i，它表示 A_i 能提供的认证安全等级；栅栏的宽度是 W_i，它表示了 A_i 因的一些其它性能参数的幅度。因此每一个认证方式都可以用一个矩形栅栏表示。

在系统中，考虑三种认证方式密码、人脸和语音三种栅栏存在，由于人脸识别和说话人识别在使用方便性、用户接受度上和密码差别不大，人脸识别所需的摄像头和说话人识别所需的话筒两种输入设备也可以很廉价地得到，因此可以认为它们各自的栅栏宽度是相同的，我们给它们的 W 参数都赋值单位宽度 1。我们将密码的安全等级参数 H 赋值为 1，由于人脸识别和说话人识别都是生物认证，其安全性要比密码高，我们认为人脸识别和说话人识别的安全性是相同的，它们的 H 都赋值为 2。这样就得到了所有三种认证方式的栅栏，见图 2 所示。

3.2　安全策略设计

三种认证方式，按照与和或的组合方式，一共能构成 17 种组合。按照安全性相同时，方便性尽可能大和方便性相同时，安全性尽可能高的选取原则，并且只考虑 H 等级的连续性，允许 W 不连续，对 H 和 W 进行分级选取有代表性的认证方式，得到安全等级的认证组合，栅栏模型如图 3 所示。

3.3　建立资源 R 和安全等级的联系

假定资源就是 ATM 上任何需要保护的服务，例如

取款、转账、查询等。建立资源和安全等级的联系有两种方法：

第一种是银行设置。由银行给某种服务规定安全等级。比如取款，取 100 元只需通过安全等级 1 的验证，取 1000 元则要通过安全等级二的验证，取 10000 元则必须通过最高等级的认证。这个办法的好处是可以方便统一管理，可以根据情况随时调节。缺点是缺乏灵活性和人性化，因为不同客户的需求是不同的，对于一个没有固定收入的学生来说 100 元，他也许也觉得是很大的一个数字，他或她可能不会介意认证过程的繁琐，愿意接受最高等级的认证，因为这样可以确保他或她的 IC 卡和密码丢失而可能带来的损失；而对于一个有较高收入的人来说，他可能会忙于各种事物，没有精力去记忆密码，他也许觉得如果取 100 元只需要一张 IC 卡就可以了，无需任何其他认证。

第二种办法用户自定义。认证安全等级由客户在银行账号时自己定义，他或她根据自己的意愿规定自己的等级。这种做法灵活好；由于充分尊重了客户的意见，因而会受到欢迎。当然这种策略施行之前银行和客户之间应该先签署认证协议，规定各自的权利和义务，以便出现纠纷能够很好地进行解决。

表 1 显示了 3 个人在银行注册时各自的安全策略，比较具有代表性，三个人的身份不同，因此其各自的需求也不一样。

表 1 三个典型的客户选择的不同金额时的身份认证方式

客户姓名	账号	职业	取款金额(元)	认证方式
张三	001	学生	100 – –300	密码 + 人脸 + 语音
			400 – –600	(密码)? (人脸)
			700 以上	(密码)? (人脸)? (语音)
李四	002	某公司职员	100 – –1000	人脸
			1100 – –3000	(人脸)? (语音)
			3100 以上	(密码)? (人脸)? (语音)
王五	003	某公司经理	500 元以下	只需银行卡
			600 – –3000	人脸
			3100 以上	(人脸)? (语音)

客户张三是学生，由于其经济来源主要靠父母，因此他比较重视自己的钱安全性，他不介意每次取钱时要通过层层认证；李四作为公司职员，他有一定的经济实力，日常消费可能也比较多，数额一般会在 100 – 1000 元，因为工作比较繁忙，他不愿意记忆密码，因此在 3000 元以下的取款时他都采用生物认证的方式；王五是一位公司的经理，平时经常要进行各种社交活动，他经济实力很强，他选择了银行提供的“一键通”服务，即只要他插入智能卡，就无需认证其他认证，他就可以进行一定的交易额度。

4 结束语

结合生物认证技术与传统认证方法，本文构建了一种可伸缩安全等级的多通道混合用户身份认证系统。系统中提出了一种安全策略的栅栏模型，该模型对于设计混合型身份认证系统的安全策略具有普遍的指导意义，认证方式组合灵活多变，能实现可伸缩的安全等级。采用多种身份认证机制，无疑给用户的使用带来了更多的选择余地，用户可根据自己的意愿来选择使用哪一种身份认证方式，这就照顾了不同年龄、不同层次客户的需求，使交易更显人性化，对非法使用者也会产生极大的抑制作用。

参考文献

1 S. Liu, M. Silverman. A practical guide to biometric security technology [J]. IEEE IT Professional, 2001, 3 (1):27 –32.

2 A. K. Jain, A. Ross, S. Prabhakar. An introduction to biometric recognition[J]. IEEE Trans. Circuits and Systems for Video Technology, 2004, 14(1):4 –20.

3 L. Hong, A. Jain, S. Pankanti. Can multibiometrics improve performance[c]. Proc. AutoID'99, 1999: 59 –64.