



享受便捷的安全

1 引言

随着互联网的不断发展,越来越多的人开始尝试在线交易。然而病毒、黑客、网络钓鱼以及网页仿冒诈骗等恶意威胁,给在线交易的安全性带来了极大的挑战。据调查机构调查显示,去年美国由于网络诈骗事件,使得银行和消费者遭受的直接损失总计达24亿美元,平均每位受害者付出了约1200美元的代价。另据香港明报消息,香港去年由于网络诈骗导致的直接损失达140万港元。

层出不穷的网络犯罪,引起了人们对网络身份的信任危机,如何证明“我是谁?”及如何防止身份冒用等问题又一次成为人们关注的焦点。

2 主要的身份认证技术分析

目前,计算机及网络系统中常用的身份认证方式主要有以下几种:

2.1 用户名/密码方式

用户名/密码是最简单也是最常用的身份认证方法,是基于“what you know”的验证手段。每个用户的密码是由用户自己设定的,只有用户自己才知道。只要能够正确输入密码,计算机就认为操作者就是合法用户。实际上,由于许多用户为了防止忘记密码,经常采用诸如生日、电话号码等容易被猜测的字符串作为密码,或者把密码抄在纸上放在一个自认为安全的地方,这样很容易造成密码泄漏。即使能保证用户密码不被泄漏,由于密码是静态的数据,在验证过程中需要在计算机内存中和网络中传输,而每次验证使用的验证信息

都是相同的,很容易被驻留在计算机内存中的木马程序或网络中的监听设备截获。因此,从安全性上讲,用户名/密码方式一种是极不安全的身份认证方式。

2.2 智能卡认证

智能卡是一种内置集成电路的芯片,芯片中存有与用户身份相关的数据,智能卡由专门的厂商通过专门的设备生产,是不可复制的硬件。智能卡由合法用户随身携带,登录时必须将智能卡插入专用的读卡器读取其中的信息,以验证用户的身份。智能卡认证是基于“what you have”的手段,通过智能卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的,通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息,因此还是存在安全隐患。

2.3 动态口令

动态口令技术是一种让用户密码按照时间或使用次数不断变化、每个密码只能使用一次的技术。它采用一种叫作动态令牌的专用硬件,内置电源、密码生成芯片和显示屏,密码生成芯片运行专门的密码算法,根据当前时间或使用次数生成当前密码并显示在显示屏上。认证服务器采用相同的算法计算当前的有效密码。用户使用时只需要将动态令牌上显示的当前密码输入客户端计算机,即可实现身份认证。由于每次使用的密码必须由动态令牌来产生,只有合法用户才持有该硬件,所以只要通过密码验证就可以认为该用户的身份是可靠的。而用

户每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。

动态口令技术采用一次一密的方法，有效保证了用户身份的安全性。但是如果客户端与服务器端的时间或次数不能保持良好的同步，就可能发生合法用户无法登录的问题。并且用户每次登录时需要通过键盘输入一长串无规律的密码，一旦输错就要重新操作，使用起来非常不方便。

2.4 USB Key 认证

基于USB Key的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key是一种USB接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用USB Key内置的密码算法实现对用户身份的认证。基于USB Key身份认证系统主要有两种应用模式：一是基于冲击/响应的认证模式，二是基于PKI体系的认证模式。

3 技术的回归

传统的身份认证技术，一直游离于人类体外，有关身份验证的技术手段一直在兜圈子，而且兜得越来越大，越来越复杂。以“用户名+口令”方式过渡到智能卡方式为例，首先需要随时携带智能卡，其次容易丢失或失窃，补办手续繁琐冗长，并且仍然需要你出具能够证明身份的其它文件，使用很不方便。

直到生物识别技术得到成功的应用，这个圈子才终于又兜了回来。这种“兜回来”，意义不只在技术进步，站在“体验经济”和人文角度，它真正回归到了对人类最原始生理性的贴和，并通过这种终极贴和，回归给了人类“绝对个性化”的心理感

受，与此同时，还最大限度释放了这种“绝对个性化”原本具有的，在引导人类自身安全、简约生活上的巨大能量。

生物识别技术主要是指通过可测量的身体或行为等生物特征进行身份认证的一种技术。生物特征是指唯一的可以测量或可自动识别和验证的生理特征或行为方式。生物特征分为身体特征和行为特征两类。身体特征包括：指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和DNA等；行为特征包括：签名、语音、行走步态等。目前部分学者将视网膜识别、虹膜识别和指纹识别等归为高级生物识别技术；将掌型识别、脸型识别、语音识别和签名识别等归为次级生物识别技术；将血管纹理识别、人体气味识别、DNA识别等归为“深奥的”生物识别技术。

与传统身份认证技术相比，生物识别技术具有以下特点：

- (1) 随身性：生物特征是人体固有的特征，与人体是唯一绑定的，具有随身性。
- (2) 安全性：人体特征本身就是个人身份的最好证明，满足更高的安全需求。
- (3) 唯一性：每个人拥有的生物特征各不相同。
- (4) 稳定性：生物特征如指纹、虹膜等人体特征不会随时间等条件的变化而变化。
- (5) 广泛性：每个人都具有这种特征。
- (6) 方便性：生物识别技术不需记忆密码与携带使用特殊工具(如钥匙)，不会遗失。
- (7) 可采集性：选择的生物特征易于测量。
- (8) 可接受性：使用者对所选择的个人生物特征及其应用愿意接受。

基于以上特点，生物识别技术具有传统的身份认证手段无法比拟的优点。采用生物识别技术，可不必再记忆和设置密码，使用更加方便。

4 展望

就目前趋势来看，将生物识别在内的几种安全机制整合应用正在成为新的潮流。其中，较为引人注目目的是将生物识别、智能卡、公匙基础设施(PKI)技术相结合的应用，如指纹KEY产品。PKI从理论上，提供了一个完美的安全框架，其安全的核心是对私钥的保护；智能卡内置CPU和安全存储单元，涉及私钥的安全运算在卡内完成，可以保证私钥永远不被导出卡外，从而保证了私钥的绝对安全；生物识别技术不再需要记忆和设置密码，个体

的绝对差异化使生物识别树立了有始以来的最高权威。三种技术的有机整合，正可谓是一关三卡、相得益彰，真正做到使人们在网上冲浪时，不经意间，享受便捷的安全。

参考文献：

- 1 “身份认证与管理 下一个安全部署重点”，徐远航，宋丽娜
- 2 “生物识别：回归的力量”，杜杜
- 3 “生物识别技术对比浅析”，杨强，谭礼俊

