

使用 USB Key 完善 PKI 体系

随着网络的发展,互联网成为了人们生活的一个延伸。人们将越来越多的社会活动搬到了网络上进行。例如即时交流用的 MSN、QQ 等,在线购物的 eBay、淘宝等,在线进行金融活动的如电子支付平台、网上银行等等。

其中,网上银行是银行系统在互联网上的一个有力的延伸,将人们的金融活动直接转移到网络上进行。人们可以不用为了转帐而专程到银行柜台去排队,每个月都要缴纳的水电费、上网费、话费等等也可以直接从自己的银行帐号上划出,并且随时可以在网络上查询具体细节,这一切,自己都可以舒舒服服的坐在家里的电脑前面,通过网络来完成。

然而,作为现实生活的一个延伸,网络环境也一样充满了危机。

如同现实生活一样,网络骗子可以假借银行的名义来骗钱,例如所谓的“钓鱼网站”,就是使用欺骗手法的典型案例:不法分子开设一个网站,设计得跟真正的网络银行一样的外观,用户如果没有察觉,那么输入的帐号和密码就轻易的被不法分子获取。

此外,网络小偷利用一些黑客技术,在用户的计算机上安装木马或者后门程序来监控用户的键盘输入,当用户使用自己的帐号后,木马程序监控到的用户的银行帐号和密码被发送到网络小偷的计算机上,“网银大盗”就是利用这样的手段来非法获取用户信息的。

用户对于网络环境下的这些伎俩的认识往往不如现实生活中那么清楚,这样很容易造成信息的丢失,导致经济上的损失。而且,这样的负面报道越多,普通用户越是对网上银行的安全性持怀疑态度,不敢使用网上银行来进行自己的日常活动,非常不利于网上

银行业务的开展。

事实上,网上银行已经越来越多的采用 PKI 体系来解决认证的问题。一方面是网上银行服务器需要认证登录的用户是否是银行帐号的真正持有人,另一方面,也让进行登录的用户能够分辨当前登录的网络银行是否真的是自己打算登录的银行,而不是什么“钓鱼网站”。

20 世纪 80 年代,美国学者提出了 PKI 的概念。PKI 是 Public Key Infrastructure (公开密钥基础设施)的缩写,是一种普遍适用的网络安全基础设施。PKI 通过延伸到用户本地的接口为各种应用提供安全服务,包括认证、身份识别、数字签名、加密等。

数字证书是 PKI 中最基本的元素,所有安全操作都主要通过证书来实现。PKI 的部件还包括签署这些证书的认证机构(CA)、登记和批准证书签署的登记机构(RA)以及存储和发布这些证书的电子目录。除此之外,PKI 中还包括证书策略、证书路径、证书的使用者等。所有这些都是 PKI 的基本部件,它们有机地结合在一起就构成了 PKI。

我们平时使用的密码,例如登录计算机所用的密码,或者在银行提取现金时需要输入的密码,基本上都是对称算法的密码,同一个密码,可以把明文数据加密成密文,也可以把密文解密成为明文。因为对称算法的这种特性,我们不能使用它来作为身份鉴别的依据,试想一下,双方都需要知道这个密码,才能够互相发送信息,那么,如果其中一方不小心泄漏了密码,对方根本无从得知,仍然还会与之联系。

数字证书的认证基础建立在非对称密码算法之上,目前广泛使用的非对称密码算法有 RSA 算法、DSA 算法、椭圆曲线算法等。我们以 RSA 算法为例来说明非对称算法在证明身份时的特点。

RSA算法的密钥由两部分组成，称之为RSA密钥对，一般我们称之为公钥和私钥。用公钥加密的数据，只能用与之对应的私钥才能够解密，公钥本身也无法解密自己加密的数据。反过来也一样，用私钥加密的数据只能能够用公钥才能够解密。一般的，我们称用私钥加密为“数字签名”。数字签名比现实生活中的签名更难以假冒，因为只有签名者才能够使用其自己的私钥，私钥是绝对不能泄漏的。需要验证签名者的身份时，就用签名者公开的公钥来进行解密，如果解密成功，说明该数字签名的确是来自于签名者，我们一般将公钥解密称之为“数字验证”。这里，签名者的公钥(以及一些附加信息如姓名、工作单位等等，组成一个证书)需要由一个专门的机构来保证是该签名者的，这样的机构我们称之为CA，即证书认证中心。

有了这样的基础，我们就可以很容易实现网络上的身份识别了：A、B两个用户分别取得对方的公钥，例如从证书认证中心下载，或者由对方发送证书(其中包含发送者的公钥)，然后将收到的证书提交到证书认证中心进行验证，确保得到期望的公钥。

当A想要验证B的身份时，由A发送一些数据给B，由B进行数字签名。然后B将数字签名结果发送给A，A用B的公钥进行数字验证，从而能够验证B的身份。

反过来，如果B想要验证A的身份，也可以使用上面的方式。

PKI体系已经在世界范围内广泛使用，经过长期的实际验证，证明了其安全性。但是我们仍然经常能够看到一些用户的银行帐号被窃取，导致经济损失等等的报道，经过分析，绝大部分都是因为没有能够满足使用PKI体系的一个先决条件造成的。回顾一下前面所说的，要把保证PKI体系的安全，一个先决条件是：私钥只能自己持有，绝对不能泄漏。但是在实施PKI体系时，一般都是将自己的私钥保存到本地硬盘或者软盘中，当需要进行数字签名时，私钥会被读取到计算机内存中进行签名运算。即使私钥是被加密存放在本地计算机中，当要进行签名运算时，也会被解密为明文，然后才能够运算。

注意，这里“私钥会被读取到计算机内存中进行签名运算”是一个很大的漏洞，因为病毒、木马等恶意程序会监控计算机的运行，可以将计算机中的私钥截取到，并悄悄发送给网络小偷，这样，网络小偷就可以假冒用户的身份，将其帐号上的资金转移到别的地方，从而导致用户的经济损失。

那么，只要我们能够保证私钥不会泄漏，就能够很好的利用PKI体系的优点，完全解除安全的后顾之忧。要想防止泄漏，私钥必然不允许被保存在计算机本机上，只能保存到特别的外置设备中。而且，为了防止病毒、木马程序从计算机内存中截取私钥，绝不能能够将私钥读取到计算机的内存中，所以保存私钥的设备还必须能够完成数字签名的工作。

USB Key就是这样的一种设备，能够保存私钥，能够完成数字签名。

引入USB Key来配合PKI体系，就能够很好的解决上述问题，打造一个完美的解决方案。USB Key内置智能卡芯片，能够存储私钥和其他私密数据，并可以内置密钥算法，在智能卡内部完成数字签名所需的工作。当需要进行数字签名时，计算机给USB Key发送签名的命令，USB Key内部进行签名，然后将签名结果返回给计算机，私钥永远不会暴露在USB Key外部，网络小偷也永远不可能得到用户的私钥，更无法假冒用户的身份。

特别的，在使用USB Key之前，还必须输入正确的USB Key的个人识别码，这样，即使USB Key丢失了，也不会被非法使用。可以这样认为：USB Key就是一个可以随身携带的超微型安全计算机，一个受保护的私人电子印章。

目前，很多银行已经注意到USB Key的对PKI体系的有力支持，在开办网上银行时纷纷采用USB Key来作为网上银行认证的“身份证”。但是出于安全性方面的疑虑，用户接受度还不是很理想，如何让“使用USB Key的网上银行是安全的”这一理念深入人心，我们还任重而道远！