

网上银行 安全无间道

中国金融认证中心(CFCA)联合金融时报发布的《2006中国网上银行调查报告》中的数据显示,2006年国内网上银行的使用人数已将近4000万,但是仍有61%的非网上银行用户由于安全顾虑而不使用网上银行,不难看出,安全成为阻碍网上银行健康发展的最大障碍。

谈到网上银行的安全,首先我们要弄清一个问题,什么样的网上银行才算安全呢?也许有人会说,最安全当然是资金绝对不会被盗。没错,能做到这一点,网上银行肯定是安全的。但是,如何能做到这一点,还需要慢慢道来。

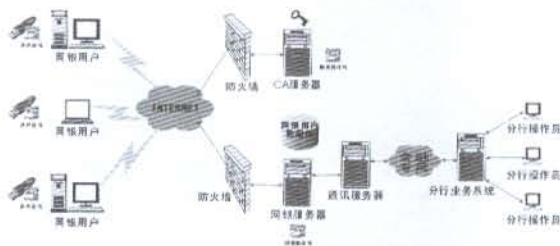


图1 网上银行拓补图

我们知道,网上银行大多是对现有银行专用网的延伸和对银行传统业务方式的补充,银行通过增加一些软、硬件设备,使得用户可以通过家用电脑连接到互联网,再通过互联网连接到网上银行系统,完成某些银行业务。网上银行拓补图如图1所示,通过拓补图可以看出,银行端系统安全保障措施比较齐全,安全问题不大,但是,网上银行的客户端——家用电脑却存在较大安全隐患。据公安部门统计,家用电脑的安全状况不容乐观,所有家用电脑中,有近80%是不安全的,非常容易受到病毒、木马、黑客的攻击,有的甚至已经被黑客挟持,成为受黑客控制的“僵尸”电脑。另外,互联网在为我们提供方便的同时,也成为了藏污纳垢的场所,充斥着病毒、木马、不良信息等,甚至在互联网的背后,形成了谋取不正当利益的黑色产业链。

网上银行还有一个特点,就是所有的信息,包括用户信息、确认信息、通讯信息、交易信息等,都是数码形式,可以说网银系统是“只认数码不认人”。所有网上银行资金被盗事件,都是不法份子,冒用合法用户的数码身份,欺骗网银系统造成的。

综上所述,要保证网上银行的安全,其实就是要在客户端不安全、不可信的情况下,如何保障合法用户的数码身份不被盗用。

下面,我们一起看一看各家银行,针对网上银行系统采取的一些安全措施。

帐号+密码

大众版的网上银行,一般采用这种方式。因为密码的使用由来已久,用户认知度高,使用方便,容易被广大用户接受。但是,据有关部门统计,目前90%以上的网银案件发生在“大众版”网上银行。原因很简单,前面已经提到,多数的家用电脑不安全,很容易受到木马攻击。木马一般都具备键盘记录的功能,我们在输入帐号密码的同时,网络中潜藏的“牧马人”通过木马,也就获得了你的密码,就可以冒用合法用户的数码身份进行非法交易了。发展到后来,出现了更加智能、更具针对性的“网银大盗”木马病毒,利用病毒技术,大量非法获取用户密码信息,给网上银行带来了巨大危害。所以我们可以得出结论:帐号+密码方式,是目前网上银行最不安全的一种方式。

为了解决键盘被记录的问题,网上银行纷纷推出了密码输入控件。这些控件使用了很多系统底层的驱动技术,可以在键盘按下的第一时间将键值捕获,并伪造一个虚假键值传给系统,从而使键盘记录木马失效。这听起来不错,但不幸的是,并非只有银行才拥有这种驱动技术,黑客往往是一些技术上的天才、怪才,只要他们愿意,完全有可能将木马的优先级提到比银行控件还要高。

基于密码方式的大众版网银,其脆弱的安全性已引起了各方的注意,但由于大众版网银开通方便、使用简单,目前仍拥有大量用户。业内曾有人呼吁取消大众版的网上银行,其实我们没有必要因噎废食,对于只是想进行信息查询的用户,不存在安全性问题,可以使用大众版网银,同时,银行还可以进一步采取一些安全措施,提高大众版网银的安全性。目前比较好的方法是使用手机短信验证。手机短信验证是一种比较有中国特色的认证手段,每次交易前,由系统产生一次性的验证码,以短信的形式发给用户,用户输入验证码,才能完成交易。这样,黑客就算获得帐号、密码和验证码,但由于验证码每次都不一样,每个验证码只能使用一次,所以黑客不能冒用用户的数码身份进行非法交易,大大提高了安全性。

动态令牌

动态密码也称一次性密码(one time password),

它指用户的密码按照时间或使用次数不断动态变化,每个密码只使用一次。

动态密码采用一种称之为动态令牌的专用硬件,如图2所示。动态令牌内置电池、密码生成芯片和显示屏。这种产品的密码生成芯片内置专门的密码算法,根据当前时间或者使用次数生成当前动态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。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,所以只要密码验证通过,系统就可以认为该用户的身份是可靠的。而且用户每次使用的密码都不相同,即使黑客截获了一次性密



图2 动态密码

码,也无法利用这个密码来仿冒合法用户的身份,因为下一次登录必须使用另外一个动态密码。另外,动态令牌硬件不可复制,一旦丢失可立刻向银行挂失,从而保证资金安全。

动态令牌比传统密码方式,安全性有大幅提升,而且使用方便,因此在国外银行中有大量应用。但我们也应该看到动态令牌方式存在的一些安全问题。首先,动态令牌是单向认证,即只能是用户向网银系统证明身份,用户没办法验证网银系统是否可信,这就为代理攻击提供了条件。黑客可以建一个代理网站,用户连接网上银行,其实是连接到代理网站上,代理网站显示与真正的网上银行一样的页面,诱使用户输入动态密码。等用户输入后,黑客就可以使用此动态密码,登录真正的网上银行进行非法交易。其次,动态令牌由于同步的需要,每次产生的动态密码存在一个很短的有效期(通常是一分钟),只要在有效期内,动态密码都是有效的,可以用来证明身份。这样,只要黑客动作足够快,他完全可以使用截获的动态密码,冒用用户数码身份进行非法交易。

USB Key

USB Key是一种USB接口的硬件设备,外形如图3所示。它内置单片机或智能卡芯片,有一定的存储空间,



图3 USB Key

可以存储用户的私钥以及数字证书,利用USB Key内置的公钥算法实现对用户身份的认证。由于用户私钥保存在硬件中,理论上使用任何方式都无法获取,因此保证了用户认证的安全性。

USB Key的硬件本身和PIN码构成了可以使用私钥的两个必要因素。如果用户PIN码被泄漏,只要USB Key本身不被盗用,仍然是安全的,这就是“双因素认证”。

USB Key目前在网上银行应用十分广泛,大家看到一些银行的U盾、优KEY等都是这种产品。USB Key的

使用比较简单,当登录网银系统的时候,在电脑上插入USB Key,然后输入PIN码,如果验证通过,则可以进行相关交易。这种加密方式使用了PKI技术,私钥安全地保存在Key硬件中,即使在不安全的在网络应用的环境下,也可以实现客户与网银系统身份的双向识别、交易的保密性、数据的完整性和交易的不可否认性。

业界认为,目前解决网银安全问题的最佳方案就是使用USB Key,利用第三方的数字证书机制保证交易的安全。在这种机制下,银行与上网用户通过数字证书相互确认身份,交易信息则在证书机制实现的加密通道内传输,电子签名保障交易的真实。USB Key的强双因素认证,保证用户私钥不会泄露。到目前为止,还没有发现一例使用USB Key的用户发生网银资金被盗案件。另外,作为数字证书的签发机构,C F C A则承担第三方安全责任,对因数字证书出现问题造成的损失负责并进行2~80万元相应的赔偿。

当然,USB Key虽然是目前解决网银安全问题的最佳方案,但也不是无懈可击。我们设想一种场景,用户在已经中了木马的电脑上使用USB Key进行网银交易。由于PIN码是在用户电脑上输入的,因此黑客可以通过木马截获用户PIN码,如果用户不及时取走USB Key,而是让USB Key一直插在电脑上,那么黑客可以通过截获的PIN码来取得USB Key的使用权,在后台,假冒用户进行一些非法交易。尽管这个场景实现起来有较高的难度,但毕竟在理论上存在这样的安全隐患。我们必须居安思危,防患于未然。

进一步提高USB Key的安全性,方法有几种,一种是改造现有的USB Key,增加输入键,使其PIN码可以在USB Key上输入,这样就不会被电脑上的木马拦截。但这样做,USB Key的体积会增大,影响便携性。另外,这种方法也不是绝对安全,理论上还存在黑客抢在用户的正常交易之前,进行非法交易的可能;还有一种方法,也是改造现有的USB Key,增加显示屏和确认键。将要被签名的交易信息,通过显示屏显示出来,让用户自己确认,用户确认后,通过确认键进行确认,完成交易。这种安全的USB Key,如图4所示。通过将关键信息显示出来,并让用户自己确认,可以让后台进行的所有非法交易无处遁形,让黑客对网上银行的资金再也无能为力。



图4 安全USB Key

如果把黑客和网银比喻为攻守两方的话,他们之间一直就是在魔高一尺道高一丈,道高一尺魔高一丈的博弈状态。所以说,安全是相对的,不安全是绝对的,黑客与网上银行的这场“魔道”博弈还将一直持续下去。