计算机三级国内网上银行USBKey安全评测计算机等级考试
 2009年下半年全国计算机等级考试时间是2009年9月19日至23日。更多优质资料尽在百考试题论坛 百考试题在线题库 USB Key是一种USB接口的硬件存储设备。USB Key的模样跟普通的U盘差不多，不同的是它里面存放了单片机或智能卡芯片，USB Key有一定的存储空间，可以存储用户的私钥以及数字证书，利用USB Key内置的公钥算法可以实现对用户身份的认证。目前USB Key被广泛应用于国内的网上银行领域，是公认的较为安全的身份认证技术。 USB Key在网上银行中，被用作客户数字证书和私有密钥的载体，在网络上鉴别用户身份处于极其关键的地位。而网上银行首要的关键问题就是安全，安全是所有一切的基础，没有安全的网银还不如没有网银。一些新闻报道的国内某某银行几十万资金通过网银被盗，都给网上银行带来巨大的负面影响，让人对于USB Key的网上银行认证的安全性产生怀疑和顾虑。 本文将从技术的角度出发，详细论述一下目前中国网上银行使用的USB Key的安全性以及可能存在的风险和漏洞。当然，一个网银系统的安全，涉及到的理论知识非常多，不仅仅要懂得大学课程《密码学》的全面知识，还要知道最新加密锁和USB Key的产品动态，进行全面的网银评测并不是那么简单的事情。本文也仅仅起个抛砖引玉的作用，欢迎各方高手继续补充和讨论。 行业安全专家基本都公认USB Key是安全可靠的，那么USB Key为什么是安全的呢？目前有几个重要的性能指标能够说明USB Key的安全性。 1、

硬件PIN码保护 黑客需要同时取得用户的USB Key硬件以及用户的PIN码，才可以登录系统。即使用户的PIN码被泄漏，只要用户持有的USB Key不被盗取，合法用户的身份就不会被仿冒；如果用户的USB Key遗失，拾到者由于不知道用户PIN码，也无法仿冒合法用户的身份。 2、安全的存储介质 USB Key的密钥存储于安全的介质之中，外部用户无法直接读取，对密钥文件的读写和修改都必须由USB Key内的程序调用。
从USB Key接口的外面，没有任何一条命令能够对密钥区的内容进行读出、修改、更新和删除。 3、公钥密码体制 公钥密码体制和数字证书从密码学的角度上保证了USB Key的安全性，在USB Key初始化的时候，先将密码算法程序烧制在ROM中，然后通过产生公私密钥对的程序生成一对公私密钥，公私密钥产生后，公钥可以导出到USB Key外，而私钥则存储于密钥区，不允许外部访问。进行数字签名时以及非对称解密运算时，有私钥参与的密码运算只在芯片内部即可完成，全过程中私钥可以不出USB Key介质，以此来保证以USB Key为存储介质的数字证书认证在安全上无懈可击。 4、硬件实现加密算法 USB Key内置CPU或智能卡芯片，可以实现数据摘要、数据加解密和签名的各种算法，加解密运算在USB Key内进行，保证了用户密钥不会出现在计算机内存中。 以上几点是USB Key在理论上安全性的技术保证，但是从技术角度分析，这些安全性能指标往往也存在一些容易被忽视的漏洞。 1、硬件PIN码就绝对安全吗？ 目前的大多数银行使用的USB Key的PIN吗都是从电脑上输入的，因此黑客可以通过木马程序直接拦截到USB Key的PIN码，这也是目前大多数USB Key存在的一个漏洞。知道了PIN码后，如果用户忘记将USB Key

从电脑上取出，那么黑客还可以进一步通过PIN码来操作USB Key。一个非常极端的情况，当个人用户的电脑已经完全被黑客远程控制，并且所有键盘和屏幕的操作都会被拦截的时候，目前的USB Key是否还能保证安全交易呢？我看未必，因为此时USB Key的PIN码已经完全可能会被黑客拦截，当用户操作完一次USB Key后，假如没有立即拔出USB Key，那么黑客完全可能在这个间歇期伪造一次交易，而此时USB Key以及PIN码都可以验证通过。 2、外部真的无法读取Key内部的密钥吗？ USB Key的密钥从“ 理论 ”上讲是无法从外部直接读取的，这个“ 理论 ”上指的是设计上要绝对安全，如果设计和编写USB Key操作系统COS的人在COS上留了后门，那么这个人就可以从外部读取Key内部的密钥。 3、数字证书 公钥密码体制的确是很安全的，通过复杂的证书管理体系来增加破解的难度，但是数字证书是否是第三方CA机构发放的呢？有些银行的数字证书竟然是银行自己发放的，这就让PKI安全认证大打折扣了。 4、如何保证通讯安全 虽然USB Key内置CPU或智能卡芯片可以完成加密运算，但是数据从电脑上传入USB Key的过程中还是有可能被拦截和修改，USB Key内置的CPU只能保证自身的运算安全，却难以保证数据传入前不被修改。 那么，理想中安全的USB Key应该是什么样子的呢？ 1、针对现有USB Key的键盘输入PIN码的漏洞，可以使用生物技术（例如个人指纹）来替换键盘录入PIN码。 也就是说，交易时候接入USB Key，我们不需要再到键盘录入PIN码来验证身份，我们只需要在USB Key的设备上按一下指纹，就能自动验证个人身份，这种身份验证机制带来的安全性和实用性是一种跨时代的提高，用户不可能再忘记密码了，只

需要验证指纹即可，指纹的验证实在外部设备上进行的，电脑即使被黑客完全控制也无法截取到用户的指纹，从而保证了PIN码的唯一性和安全性。 2、通过管理或者审计防止COS在设计上留有后门。 3、数字证书应该由独立于用户和银行以外的权威的第三方安全认证机构CA发放，不能由银行自己发放。 4、交易金额从USB Key上录入，以防止数据在传入USB Key之前被篡改。 如果采用了以上我所说的这些安全措施，那么USB Key的安全就可以说达到了“ 无懈可击 ”的地步了，实际的安全性可以得到本质上的提高。 当然我也知道，更加安全的USB Key必然会导致其成本的上升，不利于大规模的推广应用，目前智能卡的USB KEY成本已经超过50元，商业银行发布给最终客户的USB Key的价格则会更高，比如招商银行的USB Key需要88元的费用，而工商银行的USB Key需要76元的费用，增加这些新的安全措施带来的成本还是相当大的，在实际应用中需要低成本的替代方案才是现实可行的。 那么，对于现有USB Key，如何更安全的操作呢？我的建议如下： 1、和银行确认存在USB Key中的数字证书是唯一的，用户应该把USB Key随身携带。 2、经常扫描一下电脑是否有木马病毒或者被远程控制。 3、没事不要在电脑接入USB Key，只有在交易的时候接入。 4、交易的时候接入USB Key，输入PIN码交易完成后，立即取走USB Key。 如果用户使用招行和工行的USB Key时候能够像我建议的这样操作，那么也可以在现有的硬件基础上，安全性会得到进一步提高。 总而言之，目前的USB Key的主要优点是具有CPU，类似加密锁或加密狗，能够进行RSA等加密算法运算，私钥无法读取，成本上有一定优势，因此在网络认证等领域得到广泛的应用，

越来越多的人将会采用USB Key作为日常理财或进行其它网络交易的工具，而作为国内在此领域应用最早、最成熟且最具潜力的网上银行应用，在技术和应用方面都应该先人一步，及时找到USB Key潜在安全漏洞的补救方法。 特别推荐：
2009年9月全国计算机等级考试时间及科目预告 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com