身份认证技术指南

身份认证技术指南

一次 RSA 遭攻击事件，将安全业内人员的目光吸引过来。谁能想到 RSA SecureID 会被盗？一时间，业界沸沸扬扬，各种猜测和讨论不断出现。与此同时，各大安全厂商在这个时间宣传自己的认证方案，吸引用户选择更换他们的产品。

复杂的不确定因素，眼花缭乱的产品选择，我们的认证该何去何从？如何才能实现有效的身份认证和访问管理，从而保护我们的信息不被泄漏呢？

本技术手册，将从三个部分：认证概念及认证方式，解析各认证方案的特点和风险，未来认证技术的趋势，为你详细介绍有关认证方面的知识。帮助你选择合适的安全的认证方案。

认证概念及认证方式

身份认证是在计算机网络中确认操作者身份的过程。身份认证可分为用户与主机间的认证和主机与主机之间的认证，用户与主机之间的认证可以基于如下一个或几个因素：用户所知道的东西：例如口令、密码等，用户拥有的东西，例如印章、智能卡(如信用卡等）；用户所具有的生物特征：例如指纹、声音、视网膜、签字、笔迹等。

这一部分中，我们将为你介绍各种认证工具及方式。

- ❖什么是身份认证?
- ❖ID 和密码认证：利用管理和策略保证数据安全
- ❖PKI 和数字证书：安全、认证和采用
- ❖生物认证的设备、系统和实施
- ❖安全令牌和智能卡认证

❖确保网上银行安全的多重身份认证方案

❖抗击网络钓鱼的关键：电子邮件认证方式

❖用于电子身份验证的短信双因素认证

解析各认证方案的特点和风险

面对那么多的认证方案和各大厂商提供的各种各样的认证产品，我们该如何选择？不同的认证方案之间有什么区别，又会带来哪些风险？这一部分，我们来分析一下各认证方案的特点和风险。

❖确定认证系统缺陷　抵御黑客攻击

❖密码安全库：SSO 认证更好吗？

❖数字签名和数字认证的不同

❖生物识别认证设备能与内部软件整合吗?

❖用户供应最佳实践：访问权限重新认证

未来认证技术的趋势

不管是不是炒作，我们都不得不承认，云计算的时代已经到来。当然，云计算环境还有许多问题要解决，身份认证和管理就是其中之一。那么，在云计算时代，未来认证技术会有怎样的趋势呢？

❖安全认证如何选择 软件认证或取代硬件令牌？

❖更强的双因素认证方案

什么是身份认证？

身份认证涉及判断是否是用户，也就是，他或者她想要成为谁。身份认证可以通过使用登录密码、单点登录（SSO）系统，生物认证、数字认证和 PKI（public key infrastructure）进行。

用户认证对于确保对系统和服务的合适的认证和访问很关键，特别是由于数据窃取和信息安全威胁变得越来越先进。虽然身份认证不能完全阻止信息和身份窃取，但是我们可以确保使用了几种认证方法，资源可以得到保护。

身份认证要考虑有三个因素：你知道的东西，例如用户 ID 和密码；有些你具有的东西，例如智能卡；和你的身份，这就是说身份特点，例如使用生物认证技术验证的指纹。这些因素可以单独使用，或者他们可以综合构建强大的认证策略，这就是已知的双因素或者多因素认证。以下几篇文章将介绍和这三种认证因素相关的方法。

（作者：SearchSecurity.com 译者：Tina Guo 来源：TechTarget 中国）

ID 和密码认证：利用管理和策略保证数据安全

用户 ID 和密码系统是最古老的数字认证方式。这种类型的认证系统可以简单的提示用户输入她或他的 ID 和密码以获得对系统的访问，这是实行和使用都很简单的方式，但是他们也有很大的安全风险。

密码的最大问题之一就是他们可以被共享、猜到或者滥用。企业应该在如何恰当地处理密码上对用户进行教育。在对用户的密码指南中最重要的是密码永远不应该写下来。通常员工会把密码记下来帮助他们记忆大量信任状。排除这个问题的方式之一是不要使用多个密码。如果用户在企业系统中有一个 ID 和密码——典型的是企业的单点登录——把他们记下来的可能下就大大减少了。

企业还应该对用户制定策略，说明如何选择安全的密码。用户密码应该完全和用户的 ID 无关。密码的最小长度应该是八个字符，并包含字母和数据，以及大小写的字符。如果企业运行的是微软的系统，有个简单的方法可以查看是否符合密码策略，就是 Windows Server 中的使“密码必须满足复杂性要求”的安全设置。这些设置要求用户的密码满足特别的指导原则，而如果不满足，用户将会收到错误信息，强制在企业系统激活前重设密码，以满足特殊的安全条件。

通常，攻击者通过猜测一般用户的 ID 或者密码"强力破解"获得对系统的访问。大部分的企业使用员工名字的第一个字母，然后接上他或她的姓氏最为 ID，这使得黑客可以及其简单地获取企业中所有用户的 ID。

企业应该要求员工定期更改密码，大部每 60 到 90 天改一次。使用密码允许访问极端敏感的数据的时期应该更短。用户不应该可以重新使用他们的旧密码，并且要保证所有的密码都和用户 ID 完全不同。

遵守密码的最佳做法，不仅可以改善企业安全，还可以帮助企业遵守一些法规最访问控制的要求，例如 HIPAA， SOX(the Sarbanes-Oxley Act)和支付卡行业数据安全标准(PCI DSS)。

密码破解

密码破解的程序和工具有很多，他们也被叫做密码破解器，企业可以用于对他们目前的密码系统进行风险评估。对自己的系统进行黑客行动的方法可以帮助企业认识安全风险，并在恶意攻击发生前清除不安全的密码。它还可以帮助通过处理法规问题在问题被审计原或者黑客攻击消费者信息之前就解决可能的法律纠纷。流行的密码破解工具包括 John the Ripper 和微软基线安全分析器 (MBSA)。

决定使用道德黑客的人必须首先获取密码将被暴露的终端用户和企业管理的许可。在运行了软件并获得了结果后，企业可以决定目前密码系统的风险等级。这可以帮助评估新的认证形式时候需要实施，或者是否需要对员工进行关于如何恰当地使用和创建密码的简单培训。

（作者：SearchSecurity.com 译者：Tina Guo 来源：TechTarget 中国）

PKI 和数字证书：安全、认证和采用

公钥基础设施(PKI)是可以处理数字证书的公共密钥的创建的一组服务器。PKI 系统可以维护数字证书，根据需要创建和删除证书。这种系统允许用户在公共网络上通过公共和私有的密码键安全地交换信息，而这些密码键的获取和访问是通过认证授权（CA）实现的。PKI 提供了数字认证，这就是电子"信用卡"，包括认证授权的名称、用户名和有效期以及用户的公共密钥。数字证书是用于在在线交易中建立用户证书的。所有的证书都是数字授权发布的，而且包括证书发布的数字签名来验证接受者的授权。

当用户想要进入和用户或者系统的安全的交流时，他或者她只需向那个用户或系统发送他或者她的证书，然后这些用户或者系统使用 CA 的公共密钥来认证 CA 的私人密钥特征。这个过程可以验证发送者的公钥是否是真实的，而接受然后可以使用公共密钥进入于证书发送者的安全地交流。

虽然发送者的私人密钥不是用于认证的，但是它要求解密发送者的信息。交流只有在原始信息被解密后才能完成；这只能使用私人密钥，而只有用户可以访问。

在使用数字证书前，需要选择企业策略的终止日期。在选择终止日期时，需要考虑的两个因素是成本和安全。终止日期越久，就越贵，但是这不应该是做决定时考虑的唯一因素。证书的终止日期还可以影响 PKI 基础设施的安全性，而是意识到这一点很重要。

证书的生命周期越长，它所使用的公共和私人密钥也越长，而这会增加攻击的可能性。如果企业使用生命周期长的证书，例如两年，他们就需要在证书到期前更改公共和私人密钥。

PKI 的实施和管理

PKI 系统的一些最大劣势是他们很复杂而且很贵，要求相当细致的计划，而且维护、安装和实施也很难。

实施过程需要广泛的 IT 人员的参与，考虑 PKI 系统要求专门的个人硬件和服务器的全面工作。用户需要为系统的复杂的安全措施上挣扎。安全意识培训应该要求调解用户的问题或者关心的地方并确保系统合适的使用。这些培训应该指导用户如何通过一些最佳的安全实践保护他们的私人密钥，例如安全存储、站外笔记本保护，以及如何选择强大的登录密码和反恶意软件程序。

PKI 可以被用于双因素认证的一种。这种技术可以和其他认证设备上一起使用，然后单一的认证方法的安全性就会增加了。

个人数字证书

为了缓解实施 PKI 的金融负担，有些企业为内部访问在内部系统中配置这种技术，而不在外部配置。外部实施要求企业获得从成本较高的 CA 中获取公共数字证书。当在内部配置 PKI 时，数字证书不需要来自已有的 CA；他们可以通过企业的 PKI 自己标识，这是一种成本效益比较高的方法。

对于那些决定从公司获得数字证书的人来说，它应该只是为了内部访问。个人数字证书不能被外部识别，因为他们不是 CA 注册的。在一个大型企业中，个人证书可以被用于在员工中进行网络访问或者用于在远程部门中的文件或者系统的用户验证。

(作者：SearchSecurity.com 译者：Tina Guo 来源：TechTarget 中国)

生物认证的设备、系统和实施

什么是生物认证

生物认证是使用指纹或者面部扫描和虹膜或者声音识别辨认用户的认证方法。生物扫描设备可以提取用户的生物数据，例如虹膜类型或者指纹扫描，并转化成电脑可以解读并验证的数字信息。因为恶意黑客很难获得一个人的生物数据，而用户也不太可能把他或她的生物数据放错位置或者滥用，这种形式的技术比起他的认证方法可以更强大。

生物认证可以用于对企业大楼的物理访问和企业电脑系统的内部访问。生物认证最常被用于更广泛的双因素或者多因素认证系统中的一种认证方式，因为大部分生物认证的进行还是需要员工输入用户 ID 和密码。

生物认证设备和系统

可用的生物认证设备特别多——包括指纹扫描器、面部和声音识别、虹膜扫描和击键特征——而对企业来说，选择适合并解决特殊需要的设备是很重要的，而这些特殊需要包括业务架构、系统漏洞和用户访问。下面是一些流行的生物认证设备和系统的简要介绍，可以帮助安全经理们了解赞成和反对的理由，以及怎样知道他们是否适合企业。

指纹扫描器时最早的生物认证方式，而且是最可靠的认证方式。这些系统很容易使用，而且很受用户的赞许，但是和所有的认证产品一样，他们也存在不足。指纹可以从一个用户的计算器或者杯子上提取，例如用于恶意访问。如果用户的指纹被破坏或者改变（例如被切断或烧伤的手指），他们还可以造成以下麻烦。

面部和声音识别系统和指纹扫描器类似。他们的易用性使之很受欢迎，但是用户的声音可以被录音，而面部可以从照片上复制，在有些情况下可能导致对系统的第三方恶意访问。

虹膜和视网膜扫描被认为是更安全的生物认证方式，因为复制一个人的视网膜比复制指纹复杂多了。

使用**击键特征**的认证系统是另一种选择。这种技术可以测量用户的击键特征和速度——每妙的自述、常见的错误、字符顺序——并且把这些信息存储到系统目录中，用于以后认证用户。BioPassword Inc.、Aladdin Knowledge Systems Ltd.和 Deepnet Security Ltd.是可以提供击键特征产品的三家厂商。

生物认证的实行

实行生物认证很复杂，而且成本很高，要求企业在硬件和软件上的花费巨大。不同生物认证的实行和配置过程也不相同，所以企业必须首先慎重考虑配置哪种系统，然后小心策划这一过程。

生物认证是一种用于保护极端敏感数据的先进技术，所以应该考虑高等的敏感资料。任何其他类型的数据使用生物认证都是对时间何资源的浪费。企业应该对他们的系统进行全面的风险分析，并决定哪些信息需要生物认证技术的保护，例如用户的信用卡信息。

企业还必须保证生物数据的传输和存储的安全性。虽然生物认证系统被认为是最先进的认证方式，但是他们也有一些漏洞。例如，有些人认为复制用户的生物信息是不可能的，但是当生物信息被转换成数字数据后，它就可以在不安全的网络中被黑客窃取并重设。

就像前面说过的，企业可以通过更难以复制的数据的使用，减小黑客通过对用户生物认证信息的可能性，但是风险依然存在。考虑一下，企业采用一些防范措施保证数据的可以适当地传输、收集和存储很重要。

企业必须保证所有从生物读取器传输到认证服务器上的信息都汇集到了安全的设备上，而且在加密的信道中传送，并存储到加密数据库中。Active Directory 和 LDAP 都可以执行这些动作。最后，任何运行生物应用的系统都必须打补丁并加固。

最后，企业要决定采用哪些产品，有一点很重要就是首先在测试环境中运行产品，以除去在使用过程中可能出现的缺陷，并指出如何使用户接受的问题最小化。

(作者：SearchSecurity.com 译者：Tina Guo 来源：TechTarget 中国)

安全令牌和智能卡认证

智能卡是一张小小的塑料卡片，和信用卡大小差不多，包含的内置微芯片可以存储特定用户的认证信息。智能卡的芯片可以存储特定用户的多种认证因素（例如密码和指纹）。当用户在智能卡读卡器上刷卡的时候，智能卡就可以进行多因素认证，使得智能卡系统可以进行双因素或者多因素认证。

缺点是，只有有限的信息可以被存储在智能卡的微芯片上。出于这个原因，智能卡加密的选择也很有限。短小的加密密钥很有必要，而这提高了数据受到攻击的可能性。

一次性密码（OTP）智能卡，也被叫做密钥卡（key fob），是认证的另一种方式，它要求有两种因素：你所知道的和你所拥有的。这些令牌的设计是为了在特定的时段内产生和显示新密码。为了访问一个系统，用户必须输入她或他的用户名或者 ID，，这是认证的第一个因素（你所知道的），然后提供令牌上的 PIN，这就是你所拥有的认证因素。

令牌提供的 PIN 是不断变化的——大约每 30 到 60 秒一次，这取决于程序的设计——这就使黑客很难使用那个 PIN 获取访问。即使攻击者成功窃取了 PIN，在他或者她把 PIN 输入到系统中时，它就已经改变了。

虽然双因素或者多因素认证系统要比单因素认证方法好得多，但是不是可以混乱设置的。有一种方法黑客可以破解两种形式的认证——例如用户 ID 和密码以及 OTP——就是通过人在中间攻击（man-in-the-middle attack，MITM）。在 MITM 攻击中，黑客可以截取服务器和认证系统之间的信息。黑客盗取了证书，然后使用证书重设用户 ID 和密码并获取新的 OTP。现在黑客使用自己的密码和 OTP 就获得了完全的帐户权限。

安全令牌的执行

那么企业如何决定安全令牌是否是正确的选择呢？这个决定应该基于这项技术和现有的认证系统之间的配合程度。用户的赞同和维护也是很重要的因素。如果这项技术在使用中出现混乱或很难使用，而且如果管理员需要投入大量的时间来维护它，它就不会受欢迎。

在实施令牌系统时，加密对于避免攻击很必要，而且可以最大程度地进行保护。确保用户 ID、密码、OTP 和 PIN 都已经加密了。当说到 OTP 的时候，物理窃取是重大的问题。如果

攻击者可以物理窃取你的 OTP，你的运气就太不好了，所以物理安全和适当的分配对于安全的认证也很重要。

员工意识培训有助于教育用户恰当地使用他们的令牌。应该说清楚令牌永远不应该被无意地丢在员工的桌子上。

应该对那位员工接受了令牌进行记录，而且应该实行验证确保每一个令牌都给了合适的员工。

(作者：SearchSecurity.com 译者：Tina Guo 来源：TechTarget 中国)

确保网上银行安全的多重身份认证方案

今年夏天，法院首次开庭受理了印第安纳州花旗金融银行的一位客户的案件，该客户控告其网上银行保障措施中缺少足够的多重身份认证。这起案件的法官指出，在 2007 年该客户帐户被盗的时候，银行只提供了单重身份认证保护，这很明显违反了美国联邦金管会 FFIEC 2005 的规定，该规定指出金融机构要采取多重身份认证来确保网上银行的安全。

随着网上金融交易的增长，网上银行欺诈行为也逐渐增多，用户要求银行能够提供更高级别的保护措施，包括 FFIEC 要求的多重身份认证。把这些控制工作做到位，是减少金融数据盗窃以及虚假帐户活动的关键一步，这样做还可以让银行避免因网上欺诈而要担负的潜在赔偿责任。

按照多重身份认证的要求，在进行用户认证时，须同时提交下面的两个身份验证：一是你知道什么（比如密码）；二是你持有什么（比如一个动态的 PIN 码或令牌码），或者你个人独有什么（比如指纹）。让我们来看看几种银行已经实施的、比较常用的多身份认证系统，以及一些比较新的、确保网上银行安全以及符合 FFIEC 规则要求的选择。

其中，最常用的一种方法是使用传统的、带动态 PIN 生成器的硬件令牌（hardware token）。这些硬件令牌效果明显且容易扩展，但是部署困难，价格也很昂贵。对于许多大公司来说，这显然不是一个可行的方案。在某些情况下，金融机构倾向于使用“软件令牌（soft tokens）”，或者使用基于软件的 PIN 生成工具，用户能够进行下载然后安装在手机上。经过一个简单的注册过程以后，用户可以在他们的移动设备上生成 PIN 密码，其实质上把它们变成了个人的硬件令牌。这种方法性价比更高，而作为硬件令牌的替代方案，这种“软件令牌”也迅速得到了人们的认可。

另外一种传统的办法是使用一次性密码(OTP)，有时也把它叫做交易认证数字（TAN）。在这种系统中，金融机构会发给每个用户一张特别的卡片，上面印有一次性密码或者密码短语列表。用户每次进行身份认证时，需要使用其中的一个密码或者短语（按顺序），然后把使用过的密码从表格中划掉。金融机构建立并维护着一个用户数据库及其相应的密码列表，还能追踪哪个 OTP 正在被使用。这个系统的性能很好，维护费用也不贵，因为它只需要利用软件就可以使服务器端和用户端的密码列表同步。唯一的缺点是，当用户丢失他们的密码列表或者双方列表不同步的时候，维护成本会增加。

还有一种与此类似的系统是使用特殊的"宾果卡（bingo cards，类似填字图）"。这些卡片由 Entrust Inc. (IdentityGuard)和 TriCipher Inc.这样的公司提供，它们上面有一个网格，网格的一个轴上印有数字，另外一个轴上印有字母，在网格内部还印有一些数据。当用户要登陆银行应用程序时，首先需要输入用户名和密码，然后根据提示输入一系列在网格上的数据（举个例子，D2）进行认证。每个卡片都是独一无二的（像 OTP 一样），如果卡片丢失，进行替换也很方便，而且价格便宜。除了用户丢失卡片时不能提供技术支持外，这种系统几乎没有缺点。其他的系统能够生成 OTP，并且把它们通过带外(OOB)的方法（比如 SMS、电子邮件和电话等）发送给用户。

另外一种传统的、实施多重身份认证的另类方案是利用用户登陆时使用的电脑作为多认证的一个因素。通过在系统中放置一个已经成功注册的 cookie，用户就能通过输入用户名和密码进行登陆，通常还需要回答一些在注册时事先设定好的"个人"问题。当用户试图用不包含这些 cookie 的电脑进行登陆的时候，他们或者会被拒绝登陆，或者需要回答更多的、更严厉的、事先设定好的一系列问题才能通过认证。

基于 cookie 认证方案主要的问题是 cookie 容易损坏或者丢失。另外，如果 cookie 难以获得或者一个系统无法被识别的话，这种方案就会退化成一些安全系数不高的方案，需要用户回答一系列个人问题。大多数情况下，这些 cookie 是加密的，即使被人通过跨站点脚本攻击以及其他的方式获得的话，也没有多大的用处。

一些银行正倾向于使用另外一种技术，在普通多重身份认证方案的基础上添加一个新的认证因素：基于位置的因素。尽管在一定程度上跟"你持有什么"的方案相关，但是这个较新的双因素模型（有时也被称作设备指纹（device fingerprinting））依靠的是把地理位置的 IP 地址、ISP 连接以及其他位置信息跟提前设置好的用户总体信息联系起来。提供这个技术的厂商包括 41st Parameter Inc.、ThreatMetrix Inc.和 Iovation Inc 等公司。尽管这个方法越来越流行，但是因为大家对将它用于实际的多重身份认证方案还缺乏信心，所以它并没有被广泛采用。许多金融结构和用户认为，这个方法与其他的方法相比缺少移动性和灵活性，如果终端机器被恶意软件感染的话，安全还会受到威胁。

最后，我们将介绍另一种方法，尽管被金融机构使用的非常少：生物辨别系统（biometrics）。然而，由于高成本和维护的复杂性（包括需要给用户提供指纹阅读器或者类似的东西），这种方案在大规模部署操作时不太现实。

总而言之，银行和其他金融机构需要采取行动，实现安全的多重身份认证系统，这对保护用户的账户安全是至关重要的。市面上有许多不同的方案可供选择，即使最大的金融机构也能够添加额外的认证因素，从而验证使用网络银行和其他应用的用户是否合法。如果不采取这些

措施，银行将面临因不遵守相关规定而被惩罚的风险，并需承担相应的赔偿责任，同时这还会使得消费者对他们的网上银行缺乏信心。

（作者：Dave Shackleford 译者：Sean 来源：TechTarget中国）

抗击网络钓鱼的关键：电子邮件认证方式

在旧金山召开的 2010 RSA 会议中，安全专家们在周三的一次小组讨论中提到，越来越多的公司需要采取电子邮件认证方式来有效阻截越发频繁和复杂的网络钓鱼及垃圾邮件问题。

“以前拼写和语法错误曾是垃圾邮件的特征之一，现在这种情况正在渐渐消失。” Todd Inskeep 这样说道，他是美国银行的资深副总裁，他的工作内容专注于认证，客户保护和社会空间方面。

“由于现在坏人们变得越来越老练，我们真的需要技术解决方案来保护我们所有的客户，这个问题非常紧迫。”他在一个关于如何通过对抗网络钓鱼和欺诈以保护电子邮件安全的小组上这样说道。

“很多用户的电脑系统受网络钓鱼的攻击感染病毒，这使得降低非法邮件数量这个问题变得非常紧迫。”Paul Smocer 这样说道，他是 BITS 的安全副总裁，BITS 是金融服务业论坛的一个部门，是一个关注最佳实践和技术基础结构的金融服务领导人的论坛。他另外补充道，由于网络钓鱼现象的存在，金融产业由于品牌信誉受损而遭到沉重打击。从声誉的角度来看，存在这样的情况对我们的产业一点好处也没有。

小组成员说，电子邮件认证方式和协议在对抗网络钓鱼问题上还有很长的路要走，去年，BITS 发表了一篇用于实施 DKIM 和 SPF（通过域钥鉴别的邮件和发送者策略框架）的指导性文章。SPF 的目标是通过提供一个可供邮件发送者认证的框架来防止邮件的滥发，DKIM 允许组织对外发的邮件的邮件头上增加上一个加密的签名，以证明这封邮件是从这个域中发送出来的。

从小组讨论中所给出的统计数据来看，从 18 个月前只有 20%的邮件带有 SPF 记录，到现在已经有 51%的邮件带有 SPF 记录。在相同时期，通过 DKIM 认证的邮件比例从 2%上升到 16%。

雅虎邮件的资深产品管理总监 Mark Risher 说：“我们希望鼓励更多的公司来认证他们的邮件，那样他们就不会成为薄弱环节。”

Smocer 说，如果将电子邮件认证和信任推进到一个更高的阶段，那将允许金融机构使用电子邮件来为客户提供更多的服务，而不只是提供警报。如果我们可以保证安全问题，那么将有很多机会可以用来加强金融机构通过电子邮件可以提供的服务。

但是小组成员说，电子邮件认证方式和技术是有限制的。Smocer 说，拥有多种业务的大机构经常会有超过几十个并没有通过中央管理的域。同时，小机构可能缺乏擅长电子邮件认证的人员。还存在制定机构和多家 ISP 在他们所创建的关于 SPF 和 DKIM 的规则集上达成一致的问题。

Smocer 说，"我们正在尝试创建一个核心服务，它可以提供一个流程，通过这个流程金融机构可以创建他们自己的规则集，而且 ISP 们可以对它们进行检查。"

Inskeep 说，"同样，问题也存在于发送邮件的商业合伙人上，美国银行有很多合伙人，他们会以美国银行的名义发送电子邮件，所以很紧迫的一点是，要和你的商业合伙人建立一个联盟，并把他们包括进来。"

Steve Jones 是美国银行的副总裁兼架构师/战略家，他说："实施电子邮件认证的第一步是建立从所有业务线上买进的策略，你需要全组织的支持。"

小组成员注意到电子邮件认证并不是最终的解决方案，而只是一层安全保护。CISCO 公司的首席安全研究员，讨论会的主持人 Patrick Peterson 表示："即使它通过了认证，也并不意味着它是可信赖的。"但随着行业推进电子邮件认证进程的深入，以及大公司越来越多地鼓励厂商去支持这样的协议，那么对于小公司来说，就更容易采取这样的解决方案。

Smocer 说："你可以从对你来说最重要的区域开始着手。"另外他补充道："欺骗性电子邮件问题将会随着电子邮件认证在整个行业的采用而得到解决。"

（作者：Marcia Savage　译者：陈运栋　来源：TechTarget 中国）

用于电子身份验证的短信双因素认证

大家都知道用户名和密码这样的身份验证方式不是特别的安全，相对于一些你知道和拥有的身份验证方式来说，一些有安全意识的管理员更希望使用强双因素身份验证（2FA）。但如果要使用 2FA 系统，则需要一个硬件令牌。象这样基于令牌的系统，通常是一个会显示一次性密码的设备，而用户必须把密码做为身份验证的一部分提供给系统进行验证，这样的系统在实施和维护的时候需要许多的资源和精力。

这种令牌对大多数用户来说很昂贵，而且不便于企业外的用户管理，比如顾客和合同制员工。这是因为为了要使用这些设备，公司必须先采购硬件令牌，把它们配置好（以便随时使用），并且还要教用户它们的物理保护和使用方法，处理粗心用户丢失他们设备的问题。

但是最近在双因素身份验证上的一个创新可以缓解这些问题：无令牌双因素身份验证（T2FA）。T2FA 不使用专用的硬件设备来传递一次性密码，相反，它使用用户已经拥有的并且很熟悉的设备，可以是用户的移动电话、家用电话、传真机、上网本或笔记本电脑、掌上电脑、智能手机或任何其他通讯设备。

无令牌双因素身份验证入门

为了使用 T2FA 服务，用户需要注册该服务，这可以通过一种自助式应用程序或 Web 门户网站完成。首先，用户根据 T2FA 服务管理员的要求输入他（或她）的个人信息以及其他附加数据来开始他（或她）的注册过程。在确认了用户的身份之后，组织可以根据他（或她）的角色或他（或她）希望访问的信息来验证用户是否需要高强度的身份验证。

如果用户需要高强度的身份验证服务，应用程序会要求用户输入他（或她）首选的通讯渠道信息，比如移动电话，这样就可以通过手机给他们发送密码。由于 T2FA 系统不需要用户在设备上安装任何软件，这就意味着通过 T2FA 实现的高强度身份验证与众多终端用户设备是兼容的，因此可以为公司在管理费用、用户培训以及技术支持上节约开销。

在成功完成注册流程后，每当用户使用用户名密码方式进行身份验证时，一次性密码会实时地通过短信、电话交互式语音应答（IVR）、传真或电子邮件服务自动发送到用户的首选通讯设备上。组织也可以选择另一个方案，即预先发送一次性密码到用户设备上，这样可以解决由网络延时造成的短消息延时和网络覆盖损失，比如，如果用户在一幢没有手机信号覆盖的大楼里工作，用户可以把这个预先发送的密码输入给系统验证服务来进行身份验证。这样的方案

允许公司通过终端用户自己拥有并操作的设备而不是公司提供的设备，来使用高强度凭证验证用户的身份。

未来认证：双因素认证 vs 无令牌双因素认证

那么这难道意味着 2FA 正在走向灭亡吗？不是，在组织内部，这两种保护机制都有发展的空间。但在组织中，要根据使用者的角色和他（或她）的访问需求来决定使用的机制。对于那些需要频繁访问不同应用程序和门户网站（需要强身份认证）的用户来说，如 IT 管理员或系统工程师、全职远程员工、出差的员工、商业人士、医务专业人员和其它人员，如果通过他们自己的设备来等待接收密码，可能会太复杂或过于费时。但对于偶尔使用的用户来说，如合同制员工、顾客或一个因意外事件或坏天气而在家工作的员工，T2FA 是一个更好的选择。

还有另一种情况，跨越经常使用和偶尔使用的用户的界限：就是员工使用虚拟终端服务的情况，"终端服务"是微软的瘦客户端终端服务器的实例，其中的应用程序或者整个电脑桌面，都可以通过一个远程客户机来访问。其它的选择方案包括 Citrix 系统公司的 GoToMyPc 和赛门铁克公司的 pcAnywhere。这些服务变得越来越流行，因为很多公司合同雇佣第三方来远程开发和维护应用程序、服务器以及网络设备。由于和终端服务相关联的权限很大，而且事实上，一旦通过了身份验证，用户就可以访问敏感的内部应用程序和数据，因此需要使用高强度身份验证服务来保证它们的安全。通过使用 T2FA，远程员工只需要通过手机接收密码短信，就可以在登陆到终端服务的时候，确保他们是被授权访问公司内部资源的。

那么 T2FA 存在的问题是什么呢？那就是，当使用电话和掌上电脑的时候，T2FA 服务只有在每个移动设备的网络覆盖情况良好时才能正常工作。此外，为了接收到密码，象手机这样的设备必须有电而且可以正常运行。而且，手机上的服务并不都是免费的，使用频率高的用户可能因为在手机或掌上电话上请求密码而很快用完短信费用。由于公司并不管理终端用户的设备，所以它必须创建可以允许用户修改指定首选通讯渠道的应用程序或服务，有时候这种情况特别多，尤其是在用户无法访问他（或她）的普通设备的时候。组织还应该牢记这点，电话和一次性密码设备等并不只是在公司内部使用，而是随着用户到他们的家里、购物中心、海滩或是其它一些地方。由于存在潜在的丢失风险，组织必须创建和培训关于报告丢失和转移这些设备服务的流程。

因此，尽管部署 T2FA 存在挑战，能够在组织内部混合使用 2FA 和 T2FA 意味着为了满足特定需求、预算和工作模式，高强度认证要求可以进行定制。对于那些不具备支持一种或两种高强度身份验证方式技术或基础设施的组织来说，厂商也可以向他们提供了主机托管服务，如 Signafy 公司、Positive 网络公司和 Authentify 公司。使用基于云技术的服务意味着组织可以享受两个方案的好处，并根据特定用户的需求来选择合适的身份验证。但最终，除了降低

管理硬件令牌所需的成本和时间外，随着创新商业模式对联合劳工和设施进行远程工作的需求的增加，对 T2FA 的需求也会增加。

（作者：Randall Gamby　译者：陈运栋　来源：TechTarget 中国）

确定认证系统缺陷　抵御黑客攻击

啊，好古老的登录界面。没有这个界面，安全系统还能算得上完善吗？不管是网站登录界面还是 Unix 登录提示符，大多数系统的安全都完全依靠一个有效的用户名和密码来证明用户的身份。由于这通常是唯一的访问条件，所以很值得把你的身份验证安全系统放在放大镜下测试一下，看看能不能找出一些身份验证的弱点并看看他们如何拦截好奇的黑客。

黑客通过猜测常用的用户名和密码的方法来暴力进入一个系统是非常普遍做法。最好避免使用"admin"、"test"、"user"和任何默认的用户名。需要避免的常用密码有用户 ID、"password"、"pass"和任何预设的密码。有些系统在登录失败时显示的信息让用户更容易发现一个有效的用户名。这些信息可能会说，“无效的用户 ID”。这告诉黑客，他或她应继续猜测用户名。当一个有效的用户名被发现，恶意黑客就可以看到另一个提示信息，如，“密码无效。”理想的情况下，无论失败的原因，系统的登录失败的信息应该是通用的，如“无效的用户名和密码”。否则，黑客可以列举出有效的用户 ID，并开始猜测密码，寻找到薄弱的一个。我们在下面要讲到的正是密码。

弱密码是认证系统的一个重要的安全弱点。如果可能的话，强制网络上的每一个系统，特别是网络边界上的系统遵循密码规则。密码和帐户的规则应至少需要混合字母和数字，并应指定最小密码长度，提供密码历史，帐户锁定和密码到期。如果可能的话，设置密码规则，不允许密码和用户名或者用户的名或姓相同，因为这些都容易猜到。我目标是迫使用户选择强密码。

要真正加强你的认证机制，你应该建立双因素或三因素认证系统。多因素验证意味着，用户身份验证必须提交至少两种不同类型的证书。有三类验证因素：“你拥有的”，“你知道的”，“你是什么”。认证机制的每个因素应来自不同的类别。换句话说，用户 ID 和密码仍只是单因素认证，因为这两个件事情都属于"你知道的"。一些有效的组合应是这样的：一个电子密钥和个人身份号码（PIN）配合，指纹识别和密码配合或者视网膜扫描仪和你的声音配合。

通过改善你的认证机制，黑客想暴力进入你的系统变得更加困难。除了多因素认证系统，上述建议的采用并不会让你增加太多成本，如果有的话。

（作者：Vernon Haberstetzer　译者：Sean　来源：TechTarget 中国）

密码安全库：SSO 认证更好吗？

问：作为小企业，我正在考虑像 1password、Roboform 或 lastpass 这样的程序。对于提供 PC 与 Mac 程序的兼容性，你有什么建议吗？这些程序能否保证敏感信息的安全？以及，如果可能的话，是否能为多个用户提供服务，并且允许某些人访问特定的密码和信息？这些程序是否可以在多台计算机上和网络上使用？

答：我要说的是，我并不非常热衷于密码安全库（password security vaults）。许多用户想用一个简单的方法来创建和维护许多系统的验证信息，我理解你们这种心情，但这些工具都仅仅只是对错误进程和非集成系统的本地认证起到一个"创可贴"的作用而已。密码库是来减轻严格密码政策的负担的，严格的密码政策要求很复杂的密码，以至于用户无法记住或者必须要把它们写下来。这个密码库也可以用来解决密码过多的问题，这是由每个商业应用程序都要存储自己的证书而造成的。

在执行一个密码库时，我建议你再看一遍你的组织策略。如果他们由于过期时间短或者密码很长而过于繁琐的话，那么它们会造成更多的安全风险，而不仅仅是没有集成。如果是后一种情况，即应用程序没有被集成，那么我会寻找一个单一登录（SSO）的产品，而不是一个密码库来解决这个问题。SSO 允许用户提供一个密码来访问多个系统，并且不必对基础设施进行过大改动。

在重要的身份管理过程中，SSO 比保持一个密码库并要求用户保持多个密码要容易实现得多，风险性也会更小。此外，两者之间的成本差异不大，因为两者都需要整合、维护和管理支持。不过，如果你还想深究密码库这条路线的话，我想你已经发现了一些更好的为小企业准备的产品，而我很可能会看 lastpass，之后是 RoboForm 程序，不过这还需要更多的信息来进行选择。

除此之外，仍然还有许多问题需要搞清楚：你的用户将要登入的是什么样的终端系统和操作系统？用户要存储多少密码？你在问题中提及的"某些人"指的是谁？你的预算是多少？不管你做什么，请你记住，当你在走向一个更加一体化的认证基础设施时，密码库只是其中的一小步而已，你不应该把它视为一个长期的解决方法。

（作者：Randall Gamby　译者：Sean　来源：TechTarget 中国）

数字签名和数字认证的不同

问：数字认证和数字签名是两个不同的东西吗？

答：是的，数字认证和数字签名很不同。数字认证是用来验证网站的可信度的，而数字签名是用来验证信息的可信度的。说到数字认证，组织可能只信任这种网站，即该网站数字认证是由组织自己发布，或者是由信任的认证组织发布（如 Verisign 公司）。但是，这也并不意味着网站的内容是可信的；一个可信任的网站也可能会被黑客侵入，并修改网站的内容。

数字签名为对象中的信息创建校验和，这样接收者就可以验证收到的信息有没有被修改。例如，如果你在邮件中发送了一个签名的 Word 附件，发送途中发生了中间人攻击（黑客通过一些方法获得了传输途中的附件，并且插入了一些恶意代码），当接收者在打开附件之前检查它时，内容校验和与修改的 Word 附件不符，它就会警告接收者接收的内容已经被修改。

还有其它的一些事情需要考虑：使用数字认证的企业不需要与远程站点建立关系；他们只要能识别该网站所使用的数字认证授权并验证它即可。但是，说到数字签名，接收者必须与发送者或托管网站建立一定的关系。这种关系需要确定校验和信息被发送的地点和方式，通过通信渠道而不是内容传输的方式，来减少被修改的风险。你也不希望黑客同时具有修改内容和数字签名校验和的能力吧。理想情况下，在一个不信任的环境中，如互联网上的企业对企业（B2B）交易，你可以连接使用可信任数字认证的网站，并且该网站的任何传输内容都具有数字签名（保证信息未被修改）。

（作者：Randall Gamby　译者：曾芸芸　来源：TechTarget 中国）

生物识别认证设备能与内部软件整合吗?

问：我们已经建立了我们自己的内部时间和出席软件（time and attendance software）。请问市场上有哪些生物识别设备可以整合到我们的内部软件中呢？我们运行的操作系统是 Windows 2000。

答：最简单的答案是：市场上所有的生物识别设备都可以使用。但是我猜你是对设备的条件有要求。生物识别认证设备（从 USB 指纹识别器到具有识别器的键盘）都可以作为输入设备（和鼠标、键盘一样）被软件识别。另外，除了设备，你还要设置你的操作系统驱动以使系统能够在设备插入时能识别它。

我研究过一些生物识别设备，发现它们很容易使用，并且很容易整合到我的软件模块中。既然你已经开发了自己的软件，那么你需要确保你的软件能够调用这个设备，并能够连接到资料库（生物识别凭证被存放的地方）中。就如我上面所提到的，它们很容易被整合；比较难的部分是你软件中的认证模块的灵活度。

（作者：Randall Gamby　译者：曾芸芸　来源：TechTarget 中国）

用户供应最佳实践：访问权限重新认证

企业自身的供应系统（provisioning system）在加入并运转后，就开始在多个主要商业应用中进行用户账户的添加、修改和删除。这一工作流程需要创建运作良好的访问参数，并使得各项工作都能按计划进行。但是，实际情况真是这样的吗？企业如何知道自己所使用的访问规则就一定是对的呢？经理如何确信自己对员工的访问授权得当，而没有给予员工远大于他们工作需要的访问权限呢？

供应系统只是按照它事先的配置去工作，如果规则有误，供应系统就会错误地设置账户。核实供应系统是否按照政策去运行，唯一正确的方法是对它的功能进行审计："重新认证（Recertification）"就是极佳的审计过程。

何谓重新认证呢？重新认证是指以下过程：收集用户的访问权限信息，做对比性分析，确认该访问权限是否有效，是否有必要。审计功能与企业的供应系统一同使用，从而构成一个反馈回路（feedback loop），以确保供应系统对每项访问权限的授权都是得当的。这个过程定义起来很容易，可是实施起来却很麻烦。因此，企业必须遵循一系列预先确定的步骤，来合理的执行重新认证过程。

重新认证过程的第一步是，获取对所有账户的访问权，收集被供应系统的访问信息。在供应部署的最初阶段，这项工作是由审计者和安全人员进行的。他们要么亲自提取账户的信息，制成类似于电子表格格式的信息来做对比，要么请求授予在业务系统上的管理员权限，对已授权账户的信息进行审查。然后，在供应部署更为成熟的阶段中，大多数企业利用重新认证系统从业务系统上周期性地自动提取文件信息，来进行分析。当企业准备自动地提取访问信息时，会受到以下几个因素影响。

- 有多少系统是被供应的（provisioned）：庞大的系统数目会使个人对账户信息的访问变得困难。
- 参与到系统审计任务中的安全人员数量。
- 属企业独有部分的比重有多大：空间上分散的系统，不同业务类型的管理结构，针对不同管理类型的各种授权过程，这些都会影响到信息提取过程的快慢。企业独有的部分比重越小，信息提取速度越快。

- 由供应系统定期管理的账户数目。

下一步，需要对收集到的访问信息进行标准化处理并做比较。例如，针对主机 ACF2 权限的隐藏名，比如 ASYSRDPRGC1USER11，会导致外部审计者或安全人员无法了解供应系统到底赋予了用户何种权限。每个系统的访问权限都要转化为一套共同的访问规则，要同供应系统保持一致（如，基于角色或业务功能访问），这样就能进行一对一的比较。这一过程可以让人工去完成，使用带有转换公式（translation formulas）的电子表格，并进行高亮显示。但是，如果这一过程涉及较多的系统和账户，那么人工操作所耗的时间和难度就会增大。

这一步骤较为复杂，可以借助商用的企业访问管理工具（如，Aveksa 公司的 Access Certification、Oracle 公司的 Oracle Identity Analytics、Novell 公司的 Access Governance Suite 等）来进行这项工作。这些系统都具有应用程序连接器，能够自动提取账户信息，除此之外还配备了知识引擎（knowledge engines），从而将应用程序的权限转化为和供应系统一样的规则。账户信息被标准化处理之后，这些工具的知识引擎就能进行对比性分析了。这一步骤的最终结果是对以下两种情况做出确认和报告："致命"的访问权限组合、由于供应系统疏忽而导致的不合理授权。

另一种情况，职能经理可能将系统账户和权限授权给某个终端用户。如果是这种情况，在账户的访问权限信息被整理和标准化之后，应该有通知职能经理下述内容：他们需要为职员核实一些应用程序账户。可以通过电子邮件或利用类似于微软 Exchange Messaging 服务的任务通知系统来进行通知。然后，职能经理可以利用某种应用程序来对职员的访问权限进行审核和更新。如果有必要的话，审核和更新工作应该在职员的访问权限被核准之前进行。虽然这种通知界面部署在内部，但企业在这一步骤中所使用的访问管理工具也提供了通讯接口，用来通知经理，或提供经理在审核时所需的网络应用程序。

最后，如果在上述的重新认证过程中发现了无效的访问权限，该信息必须反馈到供应系统，从而对错误账户进行改正或删除。同时，对创建这些无效账户的访问规则要进行识别和修改，确保不再发生类似的不当配置。在最初的供应实施中，该项操作可以由人来完成。不过，企业在最后肯定希望建立这样一种工作流程，即账户信息可以从核实工具中自动输入到供应系统中，而这些核实工具是用来确保反馈回路能达到最优化的。

供应系统是管理终端用户账户生命周期的强大工具。如果供应系统遵循的规则不健全、或者存在漏洞，那么它们创建的访问规则就会违背企业的政策，或者导致法规遵从的问题。实施重新认证过程属于初期供应系统部署的一部分，是为数不多的用户供应最佳实践之一。对终端用户访问负责的审计人员、安全人员和管理人员而言，他们可以利用该过程来确保工作流程和供应系统内部所配置规则的正确性。另外，通过预先对该过程进行定义，新的系统就可以连接

到供应系统上，新的工作流程也可以明确，而重新认证过程也可以被改正，从而确保供应系统在最开始就是正确的，而不是等到有人访问了他没有权限的信息而发生了安全事件之后。

(作者：Randall Gamby 译者：Sean 来源：TechTarget 中国)

安全认证如何选择 软件认证或取代硬件令牌？

3月18日，RSA遭遇了APT攻击，SecureID被偷。在漫长的近三个月后，RSA对此作出确切的回应，表示将更换SecurID令牌，因为其最大的客户们在针对政府承办商的攻击中受害，他们认为这与双因素认证机制有关。

这一事件将我们忽略的令牌安全问题摆了出来，安全认证成为热点话题。如何保证数据安全？如何实现有效的身份认证和访问管理？在各大厂商均提出令牌更换服务的同时，我们该如何选择？安全认证会又如何发展？带着这些疑问，近日，本站记者专访了CA Technologies亚太区高级认证总监Andy Lee先生。

软件认证的优势

CA Technologies公司在四月份的时候曾推出了CA ArcotID安全软件认证更换计划，软件认证与硬件令牌非常不同，什么是软件认证？它有什么优势？它是否会在未来替代硬件令牌？

对此，Andy Lee表示，提到硬件令牌有几个事情大家可以做参考，第一件事情，过去这么多年，我们在跟客户交流的时候，大家都有一个共识，带一个额外的硬件令牌非常的不方便。仅是从使用者的经验上来说，当令牌没带的时候，比如说一个企业用它的令牌来看邮件，你没有这个硬件令牌，真的是束手无策，完全没有办法。而软件认证则可以解决使用者方便性的问题。

第二点，用户数据的隐私性。当一个安全性的产品，你提供的厂商那里还存有一部分你的秘密时，你一定会感到不安，害怕数据泄漏。这方面，软件认证是完全不知道你的秘密是什么的。

第三点，还有一个安全领域里比较重要的事情是公开性，假如你的计算方法不能公开的，这本身就是一个秘密了，而这个秘密是有部分人知道的，这样一来，这个人或者这一群人就变成泄密的关键点。而安全是你应该看到这一切，CA Technologies的算法就是完全公开的来做的。

另外一点，这是更有利的。硬件令牌没办法漫游，所谓的漫游是说，硬件令牌是实体的，我今天摆在家里就在家里。而Arcot ID是安全软件认证，所以可以在Arcot的服务器上也存

有一份用户的资料。比如说你今天出门，没带电脑（手机不带的情况不太大）。假设在机场，你需要连接你公司的网络，Arcot 可以让你漫游一份到浏览器的记忆体里面，假如说你有 Arcot server，你可以用各种形式，比如说你发一个临时性密码的短信，让它能够暂时性地发一份 Arcot ID 到你的记忆系统，让你一次性地使用。当你用完，看完邮件以后，把浏览器给关了，这个 Arcot ID 就没了。

Arcot OTP 也是针对这点，Arcot OTP 是利用你的手机或者 iPad 的处理系统，能够把你的令牌摆在你的随身携带的平台上面。如果是硬件令牌没带放在家里，大部分情况下，今天可能不上网银了，假如手机没有带的话，很多人可能会回家拿，因为手机是生活的一部分。Arcot OTP 的最主要的针对的就是这种移动平台。比起 Arcot OTP，Arcot ID 是基于 PKI 的认证，它可以做更多的事情。比如满足数字签名的需要，文件处理的需要等等。

运用 Flash 解决软件认证发展的阻碍

软件认证尽管有如此多的好处却没有得到大量的普及，这是为什么呢？

Andy Lee 谈到了软件认证发展开始遇到的阻碍。什么样的阻碍呢？你用一个软件不管是笔记本或者台式机，做认证这些事情的时候，需要运行一些软件。那你就必须买存储软件，对很多客户来说，这是一件很麻烦的事情。尽管你的软件再容易安装，或者他们有人用 Java F 的形式，它都会影响到用户体验。用户会思考软件来自哪里？能不能信任？很多人一看到选择框时，第一件事就是看哪个是 NO，然后点下去，根本不看里面的内容，这样一来，软件认证没办法工作。

CA Arcot 一开始也在挣扎这个事情怎么样来解决，直到后来 Adobe 变成 Arcot 的投资人，Adobe 又收购了 Micro media，大家用的 Flash 是由他们来提供的。然后 Arcot 就想到了用 Flash 来做分发渠道，因为 Flash 在全球的台式机和手提电脑的占有率超过了 99%。

这样一来，对使用者而言，什么东西都不需要安装，可以直接使用。我觉得这种方式更合适，也许在一个企业里，企业的 IT 可以强制性的或帮助性的让员工在他的机器上面安装一套软件。但是针对消费大众，比如银行的客户，没有办法做这件事情，完全要依赖消费大众他们有没有办法做这个安装的工作。现在，我们把这套手续移除掉，这个就形成了及时使用，不需要任何损耗。我觉得这个从实用性来讲，应该是一个很大的长处。

软件漏洞对对软件认证的影响

问：您刚才说把它嵌入到 Adobe 的 Flash 中，前一阵 Adobe 的 Flash 漏洞有很多，黑客攻击也特别多，Flash 软件的安全问题对安全认证是否有影响？

Andy Lee：我们只是运算的软件利用它这个来做分销渠道。所以它的安全性跟我们的认证是不影响的。我稍微解释一下不影响的原因，如果你使用一个软件的方式来保护一个东西，比如说私钥，通常你会让使用者选一个他想用的保护方式。举个例子，假如说现在有一句话是"我们今天早上 10 点开会"，这句话用一个密码'123'来保护。所谓的保护，就是安全区域某种形式的密码。如果你用'456'来试的话，它出来的结果是没有意义的乱码。直到你拿'123'试的时候，出现了这句话。那么你就知道保护这句话的密码是'123'。在安全领域，我可以尝试任何组合的密码做这样的攻击，直到我攻击成功为止。

在密钥保护方面也是这样，直到有一个结果出来，符合它的数学特征，那就是试功了。Arcot ID 的关键保护原理在于，不管你怎么试，试出来的结果都是有意义的。用刚刚的例子，"我们今早上 10 点开会"，你拿'123'可以显示出来，你拿'456'的时候，它将显示"我们中午 12 点吃饭"，你用'789'，显示"我们下午六点下班"。每一个都是有意义的，所以你攻击时无从晓得到底窃取成功没有。它使用的方式是从服务器上做一个数字签名。签完以后送回服务器，服务器拿你的公钥来，公钥试这个数字签名对不对，我在服务器端就知道你用的是错的私钥。只有在服务器端这个可以被检测。这点非常重要，我之前说，机场的那种情况下把你的文件保存在浏览器记忆系统里面去，就算有人把你的浏览器记忆系统给偷了，他拿了你的 Arcot ID 的复制品，他来做这个离线的东西也没办法试。你在别人的机器上面放置一个复制品，人家也没办法试。你无法知道你试的结果是对是错。我们在 1999 年 IT 会议上面发表了关于这方面的文章。没有秘密，所有东西都是公开的，我们怎么做的，什么样的形式完全是公开存在的。

软件认证对硬件令牌的挑战

问：现在硬件令牌市场普及率很高，贵公司的这种形式，我觉得还是挺有挑战的，对市场也是一种震撼吧。

Andy Lee：我想我们的出发点最主要是针对客户，因为很多客户他们有这样的疑虑，我们至少能够让他们有一个安心的解决方案。昨天听说国内有一家很大的银行，已经买了 14000 万令牌，你说把这 14000 万个令牌，全部替换掉需要多少钱。对于硬件令牌的更换不是那么容易做的。

图为坐在采访会议室的 Andy Lee

云计算趋势下的云认证

Andy Lee 表示，CA ArcotID 安全软件认证主要为云计算服务。Arcot 很早就在做云认证了，现在全球以我们的产品来保护的认证已经超过一亿五千万。

目前我想说，大部分人在考虑云计算时，第一件考虑的事情就是安全。怎么样有足够的安全？我们一开始就做这方面的事情。我想云计算已经是不可避免的趋势，就跟当初有人说不需要，传统的客户服务器运转好好的。现在有谁敢这样说。

软件认证或取代硬件令牌？

在问到安全认证的趋势时，Andy Lee 说道，"我想中国有一句俗话，一种米养百样人。比如说在某些情况下，你公司只有 50 个人，那你觉得每个人发个令牌没什么了不起的，很容易。在这个规模很小的情况下，选择性非常多。公司只有 5 个人，你可以用指纹，读视网膜。假如说到了比较大一点的层面，你就得考虑大部分人的方便性，怎么样照顾到给他们硬件令牌的安全性。硬件令牌是有它的历史原因的，没有人质疑它安全性怎么样，人们觉得手上握一个东西，感觉很安全。所以我觉得这个事情应该是见仁见智的，有的企业需要考虑安全性，假如有比硬件更安全，更方便的使用的话，他当然会做这样的考虑。"

此外，他还补充道，“从另外一个角度来看，也许你保护的东西没有这么严格，你的安全性要求没这么高。大部分人一直不停在关注目前的安全性够不够。我想说，以后的趋势，当然我们是很希望大家能够替换，使用我们的方案，但完全替换可能还要一段时间。就像用钥匙，现在很多人也在用房卡，目前都是并存的。

成本比较：软件方案和硬件方案

任何技术的实施，成本都是其中一个重要的因素，那么相比于硬件方案，软件方案的成本是否有优势呢？

Andy Lee 说道，“我想从硬件的成本上面来看，大家在比的时候，一个令牌多少钱，然后再跟软件比。事实上，这样比是不太对的。你想想，一个硬件的令牌我当初在设定之后怎么发给使用者。假如是企业的员工进办公室领一个，没有代价。可是你想想要是谁买谁领的话，谁来发这个令牌？令牌要存在哪里？需不需要一个库存系统？。很少有人对这些一开始分发的成本进行计算。”

“针对消费者大众的话，我今天用快递，用邮包寄给你，国内的邮寄成本不太高。假如到英国去，你寄一个令牌，大概五六英镑。你寄这个令牌的时候，不可能拿平信，要挂号，收的人要签名，这个成本又很高。而软件在开销上面，是能够帮助一个企业,或者消费大众降低成本的。”

“其次，我们说令牌损失的比率，大家以为不太高，事实上还挺高的。你掉了一个令牌以后还得再发一个，这又是一个成本。你用的令牌假如出了问题，可能是电池没了，现在不能用，那你打电话到客服中心，客服中心的人为了支援这个问题，又是一个成本。这些成本没有计算在里面，，其实隐形的成本相当高。而一个软件认证形式的存在，这些都是不需要开销的。全部是你自己可以完成的事情。所以我觉得从成本效益（性价比）来讲，软件认证远远高于令牌。”

如何平衡安全性与便捷性

目前，就 CA ArcotID 安全软件认证产品来说，在金融，银行以及生物医疗等传统领域都有得到应用。还有一些新的领域，比如说社交网络，网络游戏。Andy Lee 还谈到了各个地区，国家在这方面的使用差别，每个国家在法律执行力和成熟度方面都有很多不同。

“在国内，很早以前在网银这部分有所谓的银监会颁布的命令。可是它当初颁布命令，一开始说拿金额来限制，你单笔交易不能超过一千元，当日交易总额不能超过五千人民币。假如超过的话，你需要来做双重身份认证，这是一个很好很好的初衷。”Andy Lee 说，“我想有很

多大众版的用户，绝对是想用专业版的功能。可是他又有点无奈，万一在三家银行都有账户，每一家买一个令牌，好几百块钱的事情，而且身上带着三个令牌，口袋里一大包。我想政府一开始有这样的法律，是从银行的角度要考虑对消费者要有足够的保护。但是否考虑到他们使用上面的方便性呢。”

“我想这个情形会慢慢好转。我记得一开始的时候，几年以前跟银行交谈的时候，他们的关注方向，比如说五年前，一致在安全上，其他事情都不考虑。什么东西最安全，我就用什么。最近开始有人考虑，要足够安全，可是同样使用者的经验也是很重要的”他补充道。

最后，Andy Lee 表示，“在安全领域，安全性和便捷性通常也需要平衡。这个平衡点在哪里，我想对我们安全技术组来说，我们会做到一个完美的平衡。”

关于 Andy Lee 先生

Andy 先生现任 CA Technologies 亚太区高级认证总监。他曾在 Arcot，PeopleSoft，Vantive，Lucent/Avaya 和 Mosaics 等公司担任高级技术和管理职位，并拥有超过 18 年的企业软件系统开发经验。在他负责监管公司亚太地区以前，他曾任 Arcot 公司研究与开发总监，负责安全商业系统研发。CA Technologies 收购 Arcot 之后，他现在领导 CA Technologies 亚太区高级认证解决方案部。

（作者：刘平　来源：TechTarget 中国）

更强的双因素认证方案

RSA SecureID 被窃事件已经过去有一段时间了，但是它在认证领域的影响却远没有结束。各大安全厂商纷纷审视自己的认证方案，并推出很多新的认证方式，认证产品的新浪潮正在袭来。或许没有最强的认证解决方案，在不同环境下选择最合适的才是最安全的，那么现在都有哪些认证方案？各方案的优缺点是什么?未来几年还有怎样的发展趋势？针对以上疑问，近日，本站记者采访了 SafeNet 亚太区副总裁陈泓先生。

两种不同的种子生成方案

陈泓先生首先介绍了一些 SafeNet 的整体情况，并对比了其他供应商提供的认证方案。可以从下面这两张图中看到。

在每一个 OTP 里都有一个种子文件，这个种子文件一定要在每一次认证的时候跟这个背后的 OTP 服务器进行签名，它是一个对称算法。通常供应商的做法是这样的，他们在给所有的客户发 token（令牌）的时候，会在自己这里做编程然后把种子文件放进去，这个工作是在供应商自己这边来做的。然后他们会把这个种子文件保留在 OTP 认证的服务器上。

而如果这个种子文件被偷了，它的整个安全系统就崩溃了，因为任何拿到这个种子文件的骇客都可以去仿冒这些客户的身份。然后就可以非法的进入到这些客户的网络里去提取资料。“这就像把所有的鸡蛋都放在一个篮子里”，陈泓说道。

这方面，SafeNet 的方案如上图所示，种子的生成不是在 SafeNet 这边完成的，而是在客户端做的。所以客户有能力去保证他的种子文件能够安全，当然他要设立很多的安全机制。而且如果说一个客户的安全有问题的话，是不会影响到别的客户的。

这两种方案的风险承担不同，用户需要认真考虑作出选择。

云计算与认证市场的趋势

陈泓认为市场的趋势主要有两个方面，第一，OTP 令牌的厂商将有更好的控制力和管理力。针对市场一些新的变化，最明显的就是虚拟化的发展（云计算的普及现在还在初期阶段，与广泛的大众应用还有一些距离），虚拟化在私有企业和银行方面都得到了较好的发展。包括数据中心的整合，很多大企业现在为了节省资源会把很多的数据中心整合到一起，让它的分支机构远程登陆，也就是用 web portals（网站入口）的形式去做远程的访问。这种情况越来越多，如何解决身份认证的问题跟传统的解决方式有很大的不同。

其次，SaaS 的身份认证以前都是用浏览器去进入企业的网路，有一个演变就是从 AD 的网路慢慢转入远程的控制或者以云的方式进行身份认证。在这方面是会有很大的挑战。现在很多员工都有移动设备，如何控制这些设备对企业资源的访问是一个重要的问题。以前很简单的身份认证双因素的这种方式，可能需要有完整的可信的身份认证的环境。

陈泓表示，云计算趋势是必然的，那么安全认证在云计算趋势下的发展是什么呢？陈泓表示有以下四个方面：

- 虚拟化与云安全
- 下一代 PKI 的应用
- 身份认证解决方案
- 合规

而这四个方面也是 SafeNet 这两年发展的主要方向。整个安全市场的趋势主要是两点，陈泓说道，"更好的可控性和可管理性。"

图为 SafeNet 亚太区副总裁陈泓先生

问：有业内人士认为在云环境下的终端是最难管理的，反倒是云环境中的集中式服务器管理会容易一些。我不知道您怎么看这个观点？跟他们的商业模式有关吗？

陈泓：当然是终端最难管理。现在大家用手机、笔记本电脑各种不同的移动设备，你现在要上到云的环境，要如何控制跟管理呢？很难的。另一个方面，如何在供应商那边区分存储的身份。

光学认证方案和软件认证方案

现场，陈泓演示了一个光学交易签名。传统的令牌在确认交易时，要手动输入一些信息，用户可能会觉得很麻烦，光学令牌就省去了手动输入的操作。确认的时候，只要将令牌对着电脑或手机屏幕中闪烁的光源，令牌会自动识别所交易的信息，然后你再确认就可以了。这种方式也可以很好的避免中间人攻击。目前，这种新方案还没有在国内推行。

针对目前有厂商推出的软件认证方案，陈泓表示 SafeNet 也有软件认证的方案，不过软件认证会不会成为趋势现在讨论可能还为时过早。

不同的认证方案，满足不同的需求。在这个信息泛滥，公开隐私的互联网大时代，如何保护自己唯一的身份是一个越来越值得深思的问题。

（作者：刘平　来源：TechTarget 中国）