身份认证管理

身份认证管理

当身份窃取猖獗的时候，有力地用户认证、客户认证和合作伙伴认证是至关重要的措施。有了用户名和密码就足够了吗？双因素认证是有效的方法吗？还是无力应对新出现的威胁呢？本专题将提供全面的信息，帮助理解目前的认证方式和面临的挑战，并且介绍如何采用安全的认证系统。

什么是身份认证

什么是认证呢？认证包括决定是否是用户，实际是，他或者她想要成为谁。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。那么使用认证要考虑哪些因素呢？

- ❖ 什么是身份认证？

ID 和密码认证

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……

- ❖ ID 和密码认证：利用管理和策略保证数据安全

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其他的认证方法可以更强大……

- ❖ 生物认证的设备、系统和实施

企业单点登录

单点登录（SSO）是一种可以简化用户和 IT 管理员登录过程的技术形式。通过 SSO，用户可以一次输入她或他的用户名和密码访问多个应用。用户被授予了访问特别应用的权限，当他们输入了他们的认证后就可以访问所有的这些应用，这就减少了连续的提示。SSO 还减少了管理 IT 员工的无数密码的成本……

- ❖ 企业单点登录：简化认证过程

PKI 和数字证书

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 和数字证书：安全、认证和采用

安全令牌和智能卡

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……

- **安全令牌和智能卡认证**

什么是身份认证？

身份认证包括决定是否是用户，实际是，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)

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)

企业单点登录：简化认证过程

单点登录（SSO）是一种可以简化用户和 IT 管理员登录过程的技术形式。通过 SSO，用户可以一次输入她或他的用户名和密码访问多个应用。用户被授予了访问特别应用的权限，当他们输入了他们的认证后就可以访问所有的这些应用，这就减少了连续的提示。SSO 还减少了管理 IT 员工的无数密码的成本。

SSO 系统通过在特定服务器上的集中认证改善安全状况。所有的认证信任状必须首先通过特定的 SSO 服务器，然后它就会通过它存储的某个用户的认证信任状。这种集中认证更可能减少单因素认证系统的恶意认证。另外，SSO 系统通常提供了对敏感数据的更强大的存储，因为他们通常是受企业防火墙保护的。

SSO 还可以帮助用户帐户日志和监控的存储——例如，不活跃员工帐户的排除，跟踪用户行为——这不仅改善了企业的安全状况，还是萨班斯法案（SOX）的要求。

虽然单点登录对于用户和 IT 管理员来说都很方便，但是它对企业安全也产生了一些风险。如果恶意黑客获得了用户的 SSO 信任状的控制，黑客就可以访问多个应用而不是一个，这就增加了潜在的破坏程度。为了阻止对恶意访问，必须要有彻底的详细地执行和配置过程，以及安全的数据传输和存储。

SSO：执行和配置

当准备好单点登录的执行时，需要考虑企业的规模和企业等级的风险等级。企业需要以特定的需求、架构和基本结构配置它的 SSO 系统。

为了避免恶意访问，执行 SSO 的每个方面都必须深入查看企业的认证的访问控制策略。保证目前的策略可以保护敏感信息非常重要。受到攻击的 SSO 信任状和不太好的认证模式可能导致对一些敏感数据的非授权访问。

管理员必须知道企业系统需要哪种类型的认证，以及在开始配置之前，系统正在使用什么样的目录服务。必须要充分了解使用 SSO 的位置以及原因。是为了网络访问还是 Web 访问？是在硬件上使用，还是在软件上使用，或者两者都要用？

基于软件的 SSO 系统在大型企业中更受欢迎。这些系统由各种功能模块组成，在这些系统上配置的难度更高，并且要求有专门的硬件。此外，基于硬件的 SSO 的使用需要网络架构的兼容性，但是配置会更容易，这使得这种类型的系统更受小型企业的欢迎。

一旦决定了企业使用 SSO 的位置和原因，必须要决定哪一个系统需要 SSO 访问。作出这个决定的最好方法是查看员工最常用的系统。通过检查员工的行为，管理员可以决定哪些系统需要访问控制，以及需要采用什么技术，这都取决于用户访问应用还是网络系统。

最后，SSO 的配置必须要有规划并一步步地实现，这一点很重要。如果这个过程的处理不谨慎，出现了一些错误，企业的整个访问管理架构可能存在同时崩溃的风险。

(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）

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。

智能卡可以帮助减少黑客从电脑中窃取储存或者传输的信息的危险。信息是在智能卡上处理的，这样信息就可以不离开智能卡或者传送到另外的计算机上。

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)