走进单点登录

走进单点登录

SSO，也就是单点登录（single sign-on），它是是一种认证方法，要求用户只登录一次，使用一个用户 ID 和密码，登录多个应用、系统或 Web 网站。企业的单点登录（SSO）为终端用户提供了改善用户经验，帮助 IT 员工减少管理大量应用上的密码的成本。在本技术专题指南中，将主要通过专家回答用户问题的方式，解密单点登录，带领大家走进单点登录。

单点登录是什么

单点登录（SSO）是一种认证方法，它要求用户只登录一次，使用一个用户 ID 和密码，登录多个应用、系统或 Web 网站。而 Open Group 对单点登录的定义是：“单点登录（SSO）是用户认证和授权的单一行为可以允许一位用户访问他的访问许可中包含的所有电脑和系统，而不要输入多个密码的机制。单点登录减少了人为错误，这是系统失败的重要因素，需求量很大，但是很难实施。”本部分还将介绍单点登录的工作原理。

- 什么是单点登录（SSO）？
- 单点登录的工作原理
- SSO：企业部署的强大认证

单点登录的配置实施

SSO 开发的最重要的部分是策划。实施 SSO 有很多种选择，这取决于你公司的规模和配置 SSO 的范围以及采用 SSO 后不同系统的风险等级。企业需要以特定的需求、架构和基本结构配置它的 SSO 系统。本部分将对 SSO 的部署实施提出建议。

- 企业单点登录的实施须知
- 企业实施单点登录的最佳做法

- 企业单点登录：简化认证过程
- 客户端服务器应用上的 SSO

单点登录的影响和做用

单点登录（SSO）可以简化用户和 IT 管理员登录过程，并减少了管理 IT 员工大量密码的成本。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，它是一把双刃剑。

- 单点登录会改善安全性吗
- 单点登录对遵从法规的影响

什么是单点登录（SSO）？

问：单点登录（SSO）怎么工作呢？

答：单点登录（SSO）是一种认证方法，它要求用户只登录一次，使用一个用户 ID 和密码，登录多个应用、系统或 Web 网站。在使用单点登录之前，用户必须输入用户 ID 和密码，通常每个都不相同，每次他们登录到同一个会话的不同的应用或者系统的时候也不相同。很显然这样很费时间，特别是在业务环境中，时间就是金钱，而时间的浪费是因为员工必须在每次从桌面访问新系统的时候都要登录。

SSO 通常通过单独的软件认证模式实施，而这些软件模式是作为需要登录的所有应用的网关的。这种模式可以认证用户，然后进行繁重的工作——管理对其他应用的访问。它的作用是作为所有需要登录的信任状得主数据存储。

SSO 模式的一个例子是微软的 Passport，它可以允许用户注册一次，然后作为多个网站的网关，通常他们每个都要求登录。还有一些商业的 SSO，例如 Computer Associates 的 eTrust，而 Linux 上的 Java 和 PAM 中还有其他的模式。

虽然 Sso 很方便，但是有人认为它本身就存在安全问题。如果 SSO 被攻击，攻击者就可以无限制地访问需要 SSO 认证中的所有应用。

SSO 通常是需要在实施前慎重规划的大项目。

（作者： Joel Dubin 译者：Tina Guo 来源：TechTarget 中国）

单点登录的工作原理

问：单点登录如何工作呢？我必须要为每个应用都设置权限和任务吗，还是只需要穿件一次就可以了呢？

答：The Open Group 对单点登录的定义是：“单点登录（SSO）是用户认证和授权的单一行为可以允许一位用户访问他的访问许可中包含的所有电脑和系统，而不要输入多个密码的机制。单点登录减少了人为错误，这是系统失败的重要因素，需求量很大，但是很难实施。”

单点登录系统的工作各不相同。例如，在 Windows NT（或者 2000）网络中，英勇可以使用综合的 Windows NT 认证机制。如果是为特别的用户或者用户组设置的，已经被域名鉴定允许访问的任何人当然可以访问，他们不需要重新登录。

Novell 采用了不同的方法。 所有应用仍然有自己的用户名和密码，但是都存储在所谓的 SecretStore 中。据他们的网站称，“一旦杯 NDS 鉴定，SecretStore 就可以在你第一次使用的时候，自动收集兵加密你的应用密码。当你下次使用应用的时候，应用的客户端将验证你已经被 NDS 认证过了。如果 NDS 回应你通过认证了，客户端就会从 SecretStore 请求你的应用密码。NDS 可以从 SecretStore 中找回密码，并用于让你访问你的目标应用。整个过程只需几秒的时间，并且是完全透明的：一旦被 NDS 认证，单点登录管理剩余的登录过程。”

采用单点登录还有其他方法。

在任何情况下，它的意思也就是你需要定义谁可以访问每个应用，到那些层面。但是，如果你定义了标准用户组或者任务，应用和应用之间使用相同的定义应该相当简单。

采用单点登录是一种安全而不繁琐的方法，在采用前需要经过慎重的考虑。

(作者： Stephen Mencik 译者：Tina Guo 来源：TechTarget 中国)

SSO：企业部署的强大认证

企业的单点登录（SSO）为终端用户提供了改善用户经验，帮助 IT 员工减少管理大量应用上的密码的成本。如果单个认证受到攻击，攻击者就可以访问所有可解除到的资源。很容易被破解的到处可见的简单密码可以在 SSO 中提供恰当的认证吗？

在回答这个问题之前，需要清楚 SSO 是广泛的认证管理架构的一部分。每一个 SSO 都应该和企业的授权/访问控制模式的分析相连，确保敏感资源实际被保护了。如果 Sso 信任状被攻击了，就会很糟糕，但是如果因为脆软的访问空间，被攻击的信任状提供了对非授权（或者）敏感资源的访问，对安全管理团队来说都会很糟糕。

在很多年里，密码是认证机制的首选。密码简单、方便而且配置成本基本是零。当然，每一中方便都会被攻击。首先，密码很容易被窃取，而且会受到强力的字典攻击。如果需要更强大的密码，用户就会不可避免地经常忘记——导致咨询者成本的提高。为了弥补这些高成本，价格合适的自助式密码设置产品可以使用流水线的方式完成这个过程。

密码是否提供了足够的安全性和被保护的对象有很大的关系。安全是巨大的风险/回报分析，而安全的从业者需要每天的潜在风险是否值得更严格的安全设置成本。当然，法规要求对它造成了一点影响，因为攻击的成本比过去高了一些。所以安全性需要经常确认，而分析仍然需要做。

很多企业选择替换和/或使用其他认证方法对密码进行补充，确保 SSO 证书受到了恰当的保护。在双因素认证中出现的一次性密码很受欢迎，因为 RSA 的 SecurID 等技术的支持在每个应用网络访问产品中都采用了，使综合产品最小化。智能卡中包含数字证书证明身份，它在欧洲和很多政府环境中都很受欢迎。

从负面来说，发布、管理和更新令牌和智能卡都不便宜。还有用户体验和培训等并发问题，因为丢失的智能卡会令关键员工在重要时刻进不了重要系统。这样会使安全员工在管理层中很不受欢迎。

尽管存在这些问题，智能卡在以后的两三年中将会成为更加普遍的方式。Bill Gates 在 2006 年的 RSA 大会上讲明微软把智能卡最为了 Vista 操作系统认证策略的基石（通过收购 Alacris）。不管我们喜不喜欢，在大部分微软推广的情况中——它都会成为考虑因素。

认证的下一种选择是生物认证。生物认证技术曾经被大力推广过（主要是厂商），来代替现有的认证方法（智能卡或者令牌），同时使用独特的认证方法，例如指纹或者视网膜的方式。当然，生物认证的限制是准确性。有一小部分的人没有可识别的指纹，所以指纹扫描器不是 100% 的有效。

还有一些新技术，例如 BioPassword 非常有趣。这些人使用一种算法，通过用户输入密码的方式来决定登录企图的合法性。我知道这好像还有些路要走，但是它却是有效。当然，为了获得必须的令牌和密码的基础知识，新技术必须要定价，并和流行的应用和设备整合在一起。

最好的认证机制就是上面这些了。新的风险管理技术，我称作“承接认证（contextual authentication）”，它有希望更具用户想做的事情要求合适的认证水平。考虑一下它衍生物。在你自己的策略基础上，可以决定哪些请求之需要简单的密码，哪些需要电话认证，一些生活问题或者一次性密码。或者所有这些都需要。

承接认证确实在一定程度上改变了用户的经历。你可以要求一级认证（简单密码）来访问电脑或者网络，而二级认证（一次性密码或者智能卡）可以访问人力资源或者财政数据。而对于敏感应用就可以把生物认证添加到整合的认证的方法中。在严格意义上来说，这已经不是真正的 SSO 了，因为它意味着用一个信任状交换两个或者三个，但是交换的结果大大提高了安全性。

它从本质上就很有意义。如果想要进行百万美元的转账，你可能需要在银行中要求更强大的认证级别，而不是检查平衡，不吗？为什么不在内部也使用这种方法呢？它可以允许“正好合适”的级别的认证，这取决于想要操作的用户类型。

(作者：Mike Rothman 译者：Tina Guo 来源：TechTarget 中国)

企业单点登录的实施须知

问：在企业中采用单点登录的必要/必须技术组件是什么？

答：还没有的整套的 cookie cutter 要求或者组件可以在企业中采用单点登录时使用。它主要取决于两个因素：企业的规模和采用 SSO 后不同系统的风险等级。

除此之外，SSO 也有不同的类型，例如软件模式或者硬件应用。还有，这都取决于企业规模和业务需求。

但是，通常每一个 SSO 的实施都应该有：系统详细目录、需求分析和开发时间表。

在设置 SSO 系统前，需要了解有哪些系统、他们需要什么类型的认证以及正在使用的目录服务。SSO 的目的之一是把不同的系统合起来。所以，良好的 Sso 系统应该可以和 Active Directory 以及 LDAP 一起工作，也可以处理环境中不同类型的认证系统。要考虑的另一件事是企业是否需要在网络访问或者 Web 访问上也需要执行严格的 SSO。

下一步，进行需求分析，决定哪些系统应该可以使用 SSO 访问。用户访问最多的系统是哪些？他们是 Web 应用和网络系统混合的系统吗？这些可以决定实施 SSO 的时候必须那些技术组件。

最后，必须要有开发模式。用户必须要习惯使用 SSO 系统。必须要有循环，这样如果出错了，或者员工遇到了困难，不会立刻影响到整个访问管理架构。

SSO 的关键因素之一是它是软件安装还是硬件安装。如果是软件安装。例如使用 IBM 的 Tivoli，就需要专门的服务器来运行系统。还有一点很重要就是要根据企业的特殊需求定制 SSO 开发资源。

如果是硬件安装，例如 Imprivata Inc.的 all-in-one 工具，产品就必须可以和网络架构兼容。

(作者：Joel Dubin 译者：Tina Guo 来源：TechTarget 中国)

企业实施单点登录的最佳做法

问：我希望在我们银行中配置单点登录（SSO）。这样的配置存在哪些常见的障碍？在企业中、Web 上或者处理系统中配置 SSO 的最好的做法是什么？

答：SSO 开发的最重要的部分是策划。实施 SSO 有很多种选择，这取决于你公司的规模和配置 SSO 的范围。银行还需要考虑法规，例如萨班斯法案（SOX）和 FFIEC。

由于 SSO 开发可能横跨多个不同的系统和平台，你先应该决定哪些系统需要注册。这样的选择应该基于你的员工使用最多的系统，例如邮件或者企业内网，看它是否需要登录。其次，决定适合企业的 IT 结构和基础架构的产品类型。

最大的障碍是计划那些系统因该包括到安装中，以及如何同时把它们和 SSO 技术同步。SSO 只是可以快速完成的简单开发。应该慎重策划，并在企业用户的不同小组中分布实施。

另外重要的一点是确保 SSO 系统和企业现有的 IT 架构向吻合。SSO 可以以硬件或者软件的方式实施。在这种情况下，都是对成员应用的网关认证。换句话说，用户认证到 SSO 网关，然后它就转向，并代表用户进行认证。SSO 系统是应用登录信任状的主数据存储。

软件 SSO 系统由模块组成，通常位于专门的服务器上。这些模块要求一些配置和调整，而在把它们和自己的应用相连接的时候还需要额外的开发努力。这类的产品包括 IBM 的 Tivoli Access Manager、Citrix Password Manager 和 Entrust GetAccess。由于对专门硬件和配置的要求，这些系统通常是用于大型企业。

对于硬件 SSO，要求较少配置的一个产品是 Imprivata 的 OneSign Single Sign On。这种工具在员工应用的简单注册中存在基于 Web 的 front end。Imprivata 是服务于中型

企业以及没有员工或者广泛的软件配置专业技术的企业的。还有，因为它自己的服务器设备齐全，小型公司就不需要在专门的 SSO 上投资了，就像软件 SSO 模块所要求的。

对于 Web Sso 产品，Microsoft Passport Network 允许用户在多个网站访问上只注册一次。在这种情况下，Passport 的作用就相当于在线 SSO 网关。

因为 SSO 可能成为认证失败的单独的一点，SSO 系统的所有的部分都需要在企业内部保护。如果恶意用户获得了 SSO 登录信任状，系统上所有注册的应用都会有风险。

因为 SSO 一个访问的集中点，它可以被用于严密地监控用户访问。萨班斯法案（SOX）等法规要求这样严密的观察。另外，因为 SSO 安装很复杂，他们需要存储大量的认证。这也是审计员和法规执行人员需要查看的资料。

（作者：Joel Dubin 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)

客户端服务器应用上的 SSO

问：SSO 可以在客户端应用上采用吗？

答：可以。Kerberos 就是客户端 Sso 系统的案例。

在 Web 服务中，Passport 和 Liberty（编者注）都是 SSO 解决方案，是为有效的 SSO 设计的。现在，当然，在 Passpot 中也发现了漏洞，Kerberos 用了很长时间才消除漏洞，这很不容易。但是当然是可以实现的。

编者注：Liberty 是 Liberty Alliance 的简称，自由联盟，它是一个可相容的身份认证服务规范；Passport 则是一个由微软控制的中央式身份认证服务。

（作者：Jonathan Callas　译者：Tina Guo 来源：TechTarget 中国）

单点登录会改善安全性吗

问：我的公司正在决定企业是否应该优先考虑使用单点登录。在这种情况下，它可以大幅改善安全性吗？

答：单点登录（SSO）是一把双刃剑。SSO 自己不会真正的改善安全性，而且事实上，如果配置不合理就会降低安全性。SSO 是用于为用户提供便利的。

随着公司系统的增加，每一个都要求有自己的密码，SSO 可以减轻登录到每个系统上所花费的时间的负担。但是同时，如果 SSO 受到攻击，它就会把城堡钥匙交给恶意用户。另一方面，信任状也减少了，也就是说可能丢失或者受到攻击的量减少了。

所以即使 SSO 不是安全万能药，它也可以对企业的信息安全项目作出积极贡献。下面是如何做。

SSO 系统通常是基于复杂的系统管理应用上的，例如 IBM Tivoli，或者硬件应用，例如 Imprivata Inc.的产品。结果，SSO 系统把认证集中在特别的服务器上。他们通过使用存有 SSO 模块的专门服务器实现。这些服务器 是作为 SSO 的看门人，确保所有的认证都首先经过 SSO 服务器，然后传送存储的信任状，用以认证使用 SSO 系统特殊应用。这种集中化要求更多的策划、调整和审计，防御除单点认证系统之外的恶意访问。

此外，SSO 系统通常在存储认证信任状和加密密钥上有更安全的方式，这样黑客破解就会更困难。他们还可以存在于公司的 IT 架构深处，通常是在多重防火墙之后的安全位置。

所有这些都要求大量的额外存储，这是审计员和法律人员所喜欢的。所以，虽然法规不是必然等同于安全，但是法规也需要些额外的步骤可以提高安全性。萨班斯法案的 404 部分要求对控件的存档，并且大部分的 SSO 系统都可以满足这个要求。

这些文档要求包括对用户帐户的日志和监控。跟踪用户，剪除长期离职员工的不活跃的帐户，监控可疑活动都是 SSO 的一部分，并且这些还可疑增加企业的 IT 安全性。

(作者：Joel Dubin 译者：Tina Guo 来源：TechTarget 中国)

单点登录对遵从法规的影响

问：单点登录对遵从法规是有帮助还是有阻碍?

答:单点登录(SSO)本身对于遵从法规的努力既没有帮助也没有阻碍。遵从法规的范畴很广，根据你的行业，它意味着许多事情。然而，虽然每一项法规都有不同的要求，但是，每一项法规都有共同性:每一项法规都必须证明保密的客户信息必须得到充分的保护。

因此，单点登录适用于什么地方呢?Sarbanes-Oxley 法案第 404 条款要求企业证明他们有充分的 IT 控制能力保护法律规定的更广泛的金融控制。虽然第 404 条款在具体建议方面的含义比较模糊，但是，它强调了审计的要求。IT 控制应该存档并且证明有充分的政策和程序来保护数据，包括接入控制、加密、防火墙和杀毒保护措施等。

记住这些事情之后，实施单点登录的一个秘密是对专用的单点登录服务器和架构集中进行身份识别。与标准的身份识别系统不同，单点登录通常是比较复杂的。它需要许多计划(这意味着要存档)，并且必须要集成到现有的身份识别系统。除了存档之外，这些系统还需要更多的调整、审计和记录以便使这个系统比用于单个应用程序或者网络的更简单的身份识别系统更健康和不容易受到黑客攻击。

大概正是这种集中化以及实施单点登录所需要的对这个系统的审计和记录文件给那些设法提高你的遵从法规的努力的审计人员留下了深刻的印象。

(作者：Joel Dubin 来源：TechTarget 中国)