

身份认证与管理的安全部署

在实现了边际安全之后，业务和应用的安全问题开始浮出水面。只有身份认证和管理技术能够密切结合企业的业务流程，防止重要资源不被非法访问。数据存在的价值就是被合理访问。建立信息安全体系的目的是保证系统中的数据只能被有权限的“人”访问，未经授权的“人”无法访问数据。如果没有有效的身份认证手段，访问者的身份就很容易被伪造，使得任何安全防范体系都形同虚设。就象人们建造了一座非常结实的保险库，安装了非常坚固的大门，却没有安装门锁。

如果把信息安全体系看作一个木桶，那么防火墙、入侵检测、VPN、安全网关等就是木桶的壁板，身份认证就相当于木桶底。可以说，身份认证用于解决访问者的物理身份和数字身份的一致性问题，给其他安全技术提供权限管理的依据，而防火墙等技术针对数字身份进行权限管理，解决数字身份能干什么的问题。

由此可见，身份认证是整个信息安全体系的基础。
无所不在的身份认证

相信大家都记得这样一幅漫画，一条狗在计算机前一边打字，一边对另一条狗说：“在互联网上，没有人知道你是一个人还是一条狗！”这个漫画说明了在互联网上很难进行身份识别。

身份认证是指计算机及网络系统确认操作者身份的过程。计算机和计算机网络组成了一个虚拟的数字世界。在数字世界中，一切信息包括用户的身份信息都是由一组特定的数据表示，计算机只能识别用户的数字身份，给用户的授权也是针对用户数字身份进行的。而我们生活的现实世界是一个真实的物理世界，每个人都拥有独一无二的物理身份。如何保证以数字身份进行操作的访问者就是这个数字身份的合法拥有者，是一个重要的安全问题。身份认证技术的诞生就是为了解决这个问题。

如何通过技术手段保证物理身份与数字身份相对应呢？在真实世界中，验证一个人的身份主要通过三种方式：一是根据你所知道的信息来证明身份（what you know），假设某些信息只有某人知道，比如暗号等，通过询问这个信息就可以确认此人的身份；二是根据你所拥



有的物品来证明身份（what you have），假设某一物品只有某人才有，比如印章等，通过出示该物品也可以确认个人的身份；三是直接根据你独一无二的身体特征来证明身份（who you are），比如指纹、面貌等。

不过，你所知道的信息有可能被泄露或者还有其他人知道，因此仅凭一个人拥有的物品判断其身份是不可靠的，这个物品有可能丢失，也有可能被人盗取，从而伪造此人的身份。

从是否使用硬件，身份认证技术可以分为软件认证和硬件认证。从认证需要验证的条件来看，身份认证技术还可以分为单因子认证和双因子认证。这里需要对单因子认证和双因子认证说几句。仅通过一个条件来验证一个人的身份的技术称为单因子认证。由于只使用一种条件判断用户的身份，单因子认证很容易被仿冒。双因子认证通过组合两种不同条件（如通过密码和芯片组合）来证明一个人的身份，安全性有了明显提高。RSA SecurID以及飞天诚信epass1000等都是双因子认证技术的代表产品。从认证信息来看，身份认证技术还可以分为静态认证和动态认证。现在计算机及网络系统中常用的身份认证方式主要有以下几种。

用户名 / 密码方式

用户名 / 密码是最简单也是最常用的身份认证方法，是基于“what you know”的验证手段。每个用户的密码是由用户自己设定的，只有用户自己才知道。只要能够正确输入密码，计算机就认为操作者就

是合法用户。实际上，由于许多用户为了防止忘记密码，经常采用诸如生日、电话号码等容易被猜测的字符串作为密码，或者把密码抄在纸上放在一个自认为安全的地方，这样很容易造成密码泄漏。即使能保证用户密码不被泄漏，由于密码是静态的数据，在验证过程中需要在计算机内存中和网络中传输，而每次验证使用的验证信息都是相同的，很容易被驻留在计算机内存中的木马程序或网络中的监听设备截获。因此用户名/密码方式一种是极不安全的身份认证方式。

IC 卡认证

IC 卡是一种内置集成电路的芯片，芯片中存有与用户身份相关的数据，IC 卡由专门的厂商通过专门的设备生产，是不可复制的硬件。IC 卡由合法用户随身携带，登录时必须将 IC 卡插入专用的读卡器读取其中的信息，以验证用户的身份。IC 卡认证是基于“what you have”的手段，通过 IC 卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从 IC 卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在安全隐患。

动态口令

动态口令技术是一种让用户密码按照时间或使用次数不断变化、每个密码只能使用一次的技术。它采用一种叫作动态令牌的专用硬件，内置电源、密码生成芯片和显示屏，密码生成芯片运行专门的密码算法，根据当前时间或使用次数生成当前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。用户使用时只需要将动态令牌上显示的当前密码输入客户端计算机，即可实现身份认证。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，所以只要通过密码验证就可以认为该用户的身份是可靠的。而用户每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。

动态口令技术采用一次一密的方法，有效保证了用户身份的安全性。但是如果客户端与服务器端的时间或次数不能保持良好的同步，就可能发生合法用户无法登录的问题。并且用户每次登录时需要通过键盘输入一长串无规律的密码，一旦输错就要重新操作，使用起来非常不方便。

生物特征认证



生物特征认证是指采用每个人独一无二的生物特征来验证用户身份的技术。常见有指纹识别、虹膜识别等。从理论上说，生物特征认证是最可靠的身份认证方式，因为它直接使用人的物理特征来表示每一个人的数字身份，不同的人具有不同的生物特征，因此几乎不可能被仿冒。

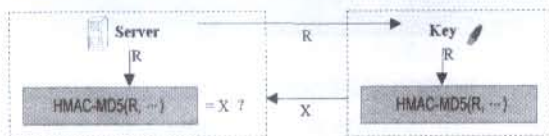
生物特征认证基于生物特征识别技术，受到该技术成熟度的影响，采用生物特征的认证技术具有较大的局限性。首先，生物特征识别的准确性和稳定性还有待提高，特别是如果用户身体受到伤病的影响，往往导致无法正常识别，造成合法用户无法登陆。其次，由于研发投入较大和产量较小等原因，生物特征认证系统的成本非常高，目前只适合于一些安全性要求非常高的场合，如银行、部队等使用，还无法做到大面积推广。

USB Key 认证

基于 USB Key 的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key 是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用 USB Key 内置的密码算法实现对用户身份的认证。基于 USB Key 身份认证系统主要有两种应用模式：一是基于冲击/响应的认证模式，二是基于 PKI 体系的认证模式。

每个 USB Key 硬件都具有用户 PIN 码，以实现双因子认证功能。USB Key 内置单向散列算法 (MD5)，预先在 USB Key 和服务器中存储一个证明用户身份的密钥，当需要在网络上验证用户身份时，先由客户端向服务器发出一个验证请求。服务器接到此请求后生成一个随机

数并通过网络传输给客户端（此为冲击）。客户端将收到的随机数提供给插在客户端上的 USB Key，由 USB Key 使用该随机数与存储在 USB Key 中的密钥进行带密钥的单向散列运算（HMAC-MD5）并得到一个结果作为认证证据传送给服务器（此为响应）。与此同时，服务器使用该随机数与存储在服务器数据库中的该客户密钥进行 HMAC-MD5 运算，如果服务器的运算结果与客户端传回的响应结果相同，则认为客户端是一个合法用户，原理如下图所示。



USB Key 进行身份认证的原理

图中“R”代表服务器提供的随机数，“Key”代表密钥，“X”代表随机数和密钥经过 HMAC-MD5 运算后的结果。通过网络传输的只有随机数“R”和运算结果“X”，用户密钥“Key”既不在网络上传输也不在客户端电脑内存中出现，网络上的黑客和客户端电脑中的木马程序都无法得到用户的密钥。由于每次认证过程使用的随机数“R”和运算结果“X”都不一样，即使在网络传输的过程中认证数据被黑客截获，也无法逆推获得密钥。这就从根本上保证了用户身份无法被仿冒。飞天诚信的 ePass1000 就属于这一类产品。

冲击响应模式可以保证用户身份不被仿冒，却无法保护用户数据在网络传输过程中的安全。而基于 PKI (Public Key Infrastructure, 公钥基础设施) 构架的数字证书认证方式可以有效保证用户的身份安全和数据安全。数字证书是由可信任的第三方认证机构颁发的一组包含用户身份信息（密钥）的数据结构，PKI 体系通过采用加密算法构建了一套完善的流程，保证数字证书持有人的身份安全。然而，数字证书本身也是一种数字身份，还是存在被复制的危险。使用 USB Key 可以保障数字证书无法被复制，所有密钥运算由 USB Key 实现，用户密钥不在计算机内存出现也不在网络中传播，只有 USB Key 的持有人才能够对数字证书进行操作，安全性有了保障。

由于 USB Key 具有安全可靠，便于携带、使用方便、成本低廉的优点，加上 PKI 体系完善的数据保护机制，使用 USB Key 存储数字证书的认证方式已经成为

目前主要的认证模式。

未来，身份认证技术将朝着更加安全、易用、多种技术手段相结合的方向发展。USB Key 将会成为身份认证的主要发展方向，USB Key 的运算能力和易用性也将不断提高。随着指纹识别技术的不断成熟和成本降低，USB Key 将会使用指纹识别技术以保证硬件本身的安全性。

化繁为简的集成身份管理

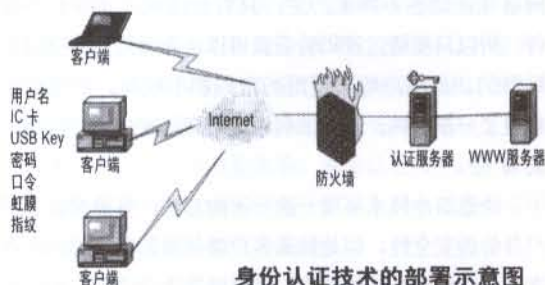
身份认证是身份管理的基础。在完成了身份认证之后，接下来就要进行身份管理。

在许多企业里，某个员工离开原公司后仍然还能通过原来的账户访问企业内部信息和资源，原来的信箱仍然可以使用。为什么会出现这种现象呢？原因在于，当员工离开公司后，尽管人事部门将其除名，但在 IT 系统中相应的多个用户授权却没有被及时删除。

据统计，每个员工在公司里注册的用户账号最多可以达到 17 个之多，如 E-mail 账号、登录内部网络账号、访问企业特定应用的账号等。当员工数量越来越多时，管理员不可能对每一个离职员工的系统账号进行彻底删除。只要存在一个没有被删除的账号，就会给系统留下后门。身份管理系统能够解决以上问题。

集成身份管理的内涵

几乎每个安全的 IT 系统都有自己独特的身份认证与管理技术，但是企业中越来越多的 IT 系统，再加上企业需要与合作伙伴甚至客户的系统进行沟通，带来了日趋复杂的身份管理，简化统一身份管理的需求催生了集成的身份管理，这种技术是否真正得到广泛应用还要取决于标准的不断成熟。



身份认证技术的部署示意图

身份管理分为两个方面：管理企业内部用户和管理企业外部用户，即合作伙伴和供应商等。相对而言，管理内部用户身份要比管理外部用户身份容易一些。

自员工工作加入公司、合作伙伴签约后，身份管

理系统就开始追踪和管理所有的关系。随着身份的改变，身份识别管理可以自动实现所要求的访问变更，并且启动所有的工作流程和批准过程。对于一个内部用户而言，身份识别管理的时间跨度从员工加入公司开始直到这名员工离开公司。进入公司后，新员工最先接触的系统是人力资源系统，然后会获得门卡、办公设备等工具，然后还会获得网络的授权，通过授权访问公司的资源。这些不同的应用系统可能来自于不同的厂商，而身份管理系统可以把这些资源都集中起来。新员工的资料一旦添加到人力资源管理系统之后，系统就会自动生成各种口令和授权，基于Web的授权也可以在这个流程中一次性完成，而且还会把这名员工在公司里所做的任何访问都记录下来。当员工离开时，网管员只需将其从人力资源管理系统中删除，身份识别管理系统就会自动地到所有的后台系统中把与该员工相关的授权全面删除，这是一个非常自动化的过程。

集成身份管理的四个层次

CA eTrust 身份识别解决方案、IBM Tivoli 管理套件都是很具代表性的身份管理解决方案。此外，微软、Novell 也提供类似解决方案。这些解决方案都是由身份认证基础、身份控制、身份生命管理、身份联盟四个层次组成，对内部用户、外部客户以及合作伙伴的身份进行管理。

身份基础层定义了构建身份管理基础架构所需的技术组件。其中，目录模块可以整合不同目录的数据；元目录模块用于进行不同端点数据库之间数据的转换和分发； workflow 模块能够自动执行请求处理过程，并与业务系统进行集成；报告模块用于汇总数据报表。基于标准协议的 Web 技术可以促进不同组件之间通过防火墙进行信息交互。

身份控制层负责管理和审核保护策略在整个企业中执行，支持任何类型的用户身份认证方法，控制已验证用户对任何资源的访问。访问控制与单点登录模块支持 Web 单点登录，进行基于 Web 的分布式管理，集中授权，保护应用程序和操作系统资源。个人信息的访问控制模块保护个人身份信息和执行隐私管理。监控和审核用户活动模块实时监控事件，以检测可能出现的资源滥用或攻击。

身份生命周期管理层负责跨应用平台简化用户应用体验以及进行身份管理和访问策略管理。其中，用户

注册模块用于处理用户信息，根据业务策略进行自动验证、批准和生成用户数据。用户自我管理模块能够降低管理用户请求的成本，帮助改善用户的体验。用户个人偏好管理模块用于管理用户的个人身份信息以及保密合同。用户配置文件管理模块用于处理定义用户所需的属性。凭证管理模块用于管理用户登录信息。策略管理模块用于管理用户访问权限和资源访问策略。

联邦身份层是公司之间身份信息的交互层，允许在 Web 应用程序之间共享用户身份和属性信息。其中跨企业供应模块自动识别不同的用户注册，并为他们提供默认服务。跨企业身份映象模块在企业之间进行凭证与身份的转换，进行“匿名”和“角色”管理。委托代理处理模块用于企业之间建立安全、可信的信息交流。

循序渐进进行身份管理

曾有一位用户向专家提出这样的问题，“应该购买哪种类型的身份管理系统”，“系统是否能在一周之内就能安装好”等。这些问题反映出用户急于求成的心理。专家的意见是，身份认证管理系统并不是即插即用、经过简单安装就能使用的方案，而是需要与业务流程进行紧密磨合，用户必须在进行方案选型之前制订战略规划，找出目前无法妥善解决的问题，并对方案能够实现哪些功能做到心里有数，而这是一个长期摸索的调整过程。

对企业来说，重要的是找到适合自身需求的身份认证管理系统，而不是盲目改动现有的业务管理机制去套用某个解决方案。没有哪种身份认证管理解决方案能够普遍适用于任何企业，成功的身份认证应用通常是在小范围内展开。用户应该从削减成本、理顺 workflow 等问题中挑出自己希望最先解决的问题，然后从那里入手开始。对于企业规模较大的用户来说，还需要了解该项目部署可能涉及的范围。

这里需要提醒用户的是，不要期望立刻从身份管理方案中获得回报。与实施任何大型 IT 项目一样，部署身份管理系统需要时间。用户通常需要几个月时间来搭建身份管理的基础架构，然后再用几个月时间使最早部署的几个功能模块运转起来。在系统部署两三个月之后，用户才开始看到它的价值，其价值完全呈现出来可能需要 6 个月或更长时间。这期间需要用户耐心、细心地发现问题和解决问题。