AT.Pass

一次性密码
双因素认证解决方案

白皮书

永泰信息技术服务有限公司
香港新界沙田
香港科学园二期
科技大道西 8 号
尚湖楼 5 楼 511 室

目录

1. 介绍

本白皮书目的

本白皮书旨在帮助读者更详细地剖析静态“用户名和密码”系统，理解其局限性，从而评估其它可替代的认证方案。

用户认证方案的评估框架基于以下三个因素：

1. 系统安全的健壮性
2. 易用性
3. 成本效率

本白皮书可供公司管理层和 IT 主管阅读，供他们在技术评估、整合与采购过程中参考；也可供其他感兴趣读者阅读。读者需理解一些信息安全的基本知识，以便掌握本白皮书的精髓。

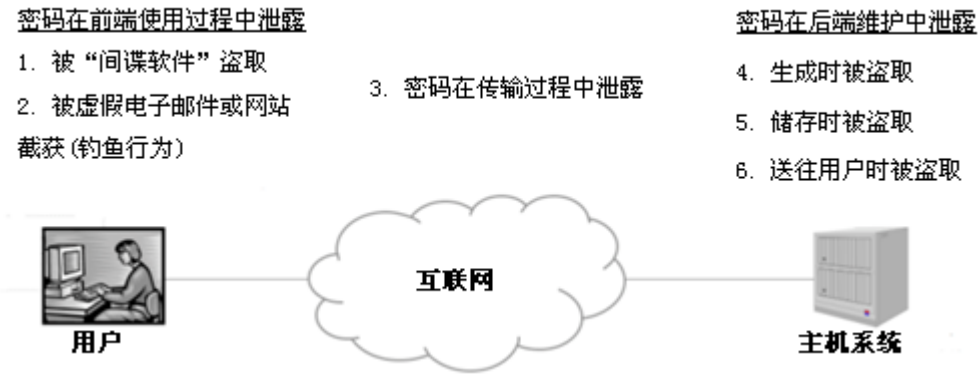
静态“用户名和密码”系统中存在的问题

如何准确分辨一个人，在生活中的许多方面都是至关重要的。在现实世界中 ,我们分辨人的方法是很微妙的。对于认识的人 ,我们可识别他们的脸、声音和个性。对于不认识的人，我们可依靠额外的身份证明，如身份证、驾驶证、出生证明、护照，甚至通过别人介绍等方式。至于一个人要与计算机系统“对话”的时候，最常用的识别方法之一，就是通过一系列的代码或数字，传统上被称为“用户 ID”和“密码”，作为认证的手段。

时至今日，信息和通信技术（ICT）在商业和社会领域中已经扮演着一个不可或缺的角色，并且影响着每个人的生活。因此，传统的“用户名和密码”系统的脆弱性显得更为明显。 传统的“用户名和密码”系统，不论在登陆过程，还是密码生成，储存和分发过程，都有泄漏密码的风险。诸如给密码加密后再传送、要求用户经常更改密码等方式可以提高系统的安全性。然而，这些措施都只能解决部分的脆弱性问题。

随着电子商务、云计算、移动网络及社交网络应用的普及，“用户名和密码”系统的脆弱性就更加明显。当工作站和主机系统暴露在开放的网络，

并且这网络不再由单一机构管理时，伴随着用户数量的日益增长和访问地点的日益分散，信息系统的安全风险便会增加。



密码在使用、传输和维护过程中的六个潜在密码泄露点

小知识:

- 在计算机系统使用“用户名和密码”作为个人身份的认证方式，可以一直追溯到 50 年代。
- 在只有小部分人能使用计算机的早期，“用户名和密码”系统还是足够安全的。
- 在 2005 年之前，双因素认证尚未普及，网上银行的客户很容易被“网络钓鱼”方式骗取用户名和密码。

认证的三个因素

如何使用更健壮的认证措施保障用户，是企业 IT 执行人员正面对的一个重要议题。其中，多因素认证，即，使用两种或多种的认证方式做身份认证，是一种更安全的方法，能将获授权个体与非获授权个体进行区分。

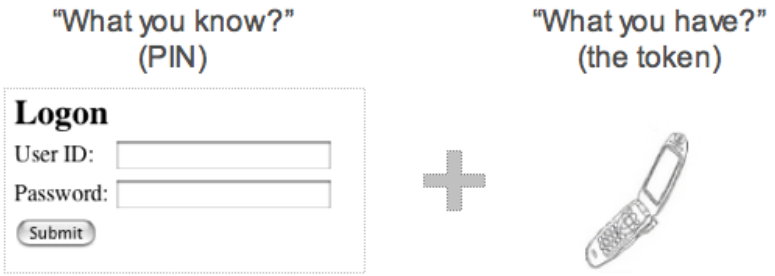
身份认证方式的三种因素的例子

一般来说 ,个人访问信息系统的认证方式主要有以下三种不同类型(或者说“因素”):

1. 第一种类型是专用知识– 也就是问“你知道什么”。 如果某人知道一个仅验证方和呼叫方知道的私密，验证方可认为此呼叫方是意向用户。这是传统静态“用户名和密码”系统的基本前提。
2. 第二种类型是个人物品—也就是问“你拥有什么”。 如果某人能展示一个仅为意向呼叫方所有的个人物品，验证方可认为此呼叫方是意向用户。就像现实世界中检查身份证明一样。问题是如何通过网络检测个人物品，诸如物理令牌、智能卡和手机等。
3. 第三种是生物特征—也就是问“你是谁”。 例如指纹、视网膜、声音模式、面形、手形和手写笔迹等。

在认证中使用双因素

为使被授权用户访问更高安全性的信息系统，人们通常使用“双因素”认证方案加强这种情况下的认证。此类“双因素”认证系统通常验证“你拥有什么”和“你知道什么”两个因素。偶尔地，当系统安装了特定的生物信息阅读机，且对安全的需求可以保证这么昂贵的安装费用时，生物认证也可在系统中部署。



使用 PIN 码和令牌方式的双因素认证

尽管技术上可行 ,但现实中几乎找不到三因素认证系统 ,即是需要验证“你知道什么”、“你拥有什么”与“你是谁”三个问题的。

安全需求与便于使用通常是对立的。我们必须合理的平衡处理、谨慎的权衡，才能设计出一个优秀的系统。

评估认证系统的标准

我们相信对一个认证解决方案作出公正而准确的评估，是对所涉及方案的多个特征的折中权衡过程。通常情况下，我们使用以下三个标准评估一个认证方案：

1. 安全性
2. 易用性或用户便利性
3. 涉及成本

首要标准：安全性

这是首要也是最重要的标准。众所周知，没有“十全十美”、绝对牢不可破的安全方案。因此，这里应该问的问题是：

“此方案对于系统所需目的而言，是否足够安全？”

以下的一些认证方案被认为是安全性较高的:

公钥基础设施（PKI）是一个公认的安全框架，许多国家和城市都通过了数字签名相关法规，使数字签名的文件和合同行为具有与手写签名相同的法律地位。数字签名是使用公钥加密技术验证电子文档中经过加密处理的“摘要”。为确保 PKI 系统的安全，对于呼叫方或个人的秘密钥匙（技术上称之为“私钥”），必须在其整个产生、储存以及分发周期中小心地加以保护。特别是，使用“软”密钥存储的 PKI 系统比那些使用硬件密钥存储的面临更高的风险。

高安全性的生物系统使用高安全性的硬件设备捕获生物的“模板”，诸如指纹，视网膜，脸型，然后与储存中的模板作出比较，完成身份认证过程。

第二标准：易用性

安全性和易用性往往都不共存，甚至是对立的。即使 PKI 被公认为当今最高安全认证方案之一，其受广泛采纳的步伐还是很缓慢。原因之一是 PKI 系统不仅实施、维护费用昂贵，而且难以使用。

例如，正规的证书颁发机构的实务准则要求在发出数字证书之前，进行面对面的验证用户身份证明；这是很重要的一步，因为数字证书代表了个人

在网上的身份；任何证书在签发过程中的纰漏，都有可能造成灾难性的后果。然而，也有一些特殊的 PKI 系统，试图简化证书申请过程：有些 PKI 系统为了获得更高易用性，牺牲了一定的安全性；而另外有一些 PKI 系统使用专用加密方式以保护证书生成和发放过程。另一个基于 PKI 认证系统的使用障碍是：认证证书本是用户和主机系统的责任，证书颁发机构通常只发放证书，并不会自动认证证书。一方面，对用户而言，认证证书是一个需要相当技术的工作；另一方面，对主机系统而言，以证书撤销列表（CRL）或在线证书状态协议（OCSP）的方法进行证书认证，又耗费大量资源。

生物识别系统也存在使用问题。对于整体人群而言，没有任何单一的生物识别技术是 100%可靠的。举例来说，约 5%的人可能无法使用到某种类型的生物识别技术，如指纹；而生物特征识别系统中的错误接受与错误拒绝之比（FAR/FRR）变化幅度很大，介乎 60% - 90%。

第三标准：成本

总体拥有成本（TCO），包括实施的初始成本、运行中的维护、支持成本，是一个重要的评估标准。安全、易用的身份验证系统可能价格不菲。例如，使用短信（SMS）的一次性密码系统可能造成巨额的运营成本，因此，使用短信的一次性密码系统通常限制在较小范围内且是关键的交易上使用，而不是普通登录或其它一般用途。基于硬件令牌的一次性密码系统也很昂贵，每个令牌费用可能高达 20-30 美元，使大规模实施的系统望而却步。因此，硬件令牌的一次性密码系统通常仅限于特别的市场，如在虚拟专用网（VPN）和企业银行应用等。同样，要实现使用智能卡或硬件令牌的 PKI 认证系统通常也是昂贵的。

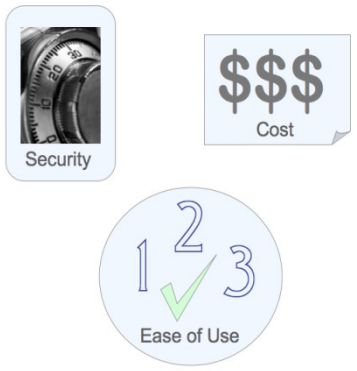
硬件令牌一次性密码系统和 PKI 系统的巨大成本还来自于令牌分发过程产生的巨大行政成本。令牌可能被丢失、损坏或仅仅是由于电池耗光而到达其使用寿命，我们绝不可低估更换令牌所需的成本。

强大的生物特征识别系统可能也相当昂贵。他们采用安全且往往是专用的硬件设备，以读取生物特征进行模板比对。昂贵的实施和维护成本，使一般用途望而却步。

小结

评估认证系统的适当性和有效性，通常公认的有以下三个最重要的标准：

1. 安全
2. 易用
3. 成本



评估标准

在给定环境下评估一个认证方案，“适合用途”是衡量其适用性的最终标准。平衡上述三大标准是您在选择方案时最关键的考虑。

2. AT.PASS 介绍

一次性密码

个人电脑、工作站和各种各样的客户端设备包括平板电脑、智能手机等与主机系统之间的连接容易受到攻击，这是设计信息系统过程中常考虑的问题之一。

这些客户端设备往往在品牌和型号方面各不相同，分散在不同的地方，且其所有权和管理权责也非常多样化。由于欠缺足够的防御机制以对抗不同类型的入侵，这些设备极容易受到攻击，而这种欠缺都是真实存在的，而且是急切需要解决的。

我们可以不断地提醒用户维护客户端设备的完整性。但是，仅仅依靠用户他们使用正确的技术操作以堵截安全缺口、预防欺骗是不现实的。我们还必须注意到，用户往往需要使用向公众开放的客户端设备访问在线系统，这些公共客户端设备的安全性倍受质疑。

安全补丁、防病毒软件更新、防火墙政策和以管理员手段强制用户定期更改密码等，对增加这些客户端设备的安全性是有帮助的。然而，黑客技术日趋复杂，甚至连计算机专家亦不能时刻意识到他们的个人电脑正受黑客威胁。这是一场正在进行的战争，战争双方是黑客群体和诚信守法的用户群体。一些黑客行为可能只是为了好玩和名声，而另一些黑客则企图恶意地窃取机密，给被黑的用户带来实质的损害。其中最臭名昭著的是即使电脑专家亦难以发现的间谍软件。当用户发现它们时往往为时已晚，因为用户不知道间谍软件已经造成了什么程度的危害。一些间谍软件只收集用户行为给其广告客户，而另一些则盗取系统甚至银行帐号等用户的秘密资料。传统的认证系统 ,包括最先进的数字证书应用系统(特别是那些在硬盘上存储私钥的应用系统)，都不能解决这类问题。

通常一次性密码（OTP）系统使用“离线”令牌，即令牌没有与客户端设备有物理连接、或者是电子形式连接，其对间谍软件具有很高的防御度。OTP 令牌使用某种加密算法 ,在固定的时间间隔内或按需随机地生成一次性密码。有些 OTP 令牌需要一个 PIN 码来解锁。OTP 令牌可以是同步或异步的，而同步的 OTP 令牌，令牌同步是与主机的认证服务器同步，同步的方式可以是基于时间或事件，或两者兼而有之。

一次性密码(OTP)系统的典型配置

传统的“离线”OTP 令牌是以嵌入式硬件设备形式分发的。这些硬件设备有可能价格高昂，往往只应用在用户数量小、或需要极高安全性而成本并不是其首要考虑因素的应用上。

还有另一个广泛报道的关于传统硬件令牌一次性密码系统的使用障碍。对依赖时间同步的令牌来说，其方案必须能容纳认证服务器与装载令牌的硬件设备之间的一定程度的时间漂移。为解决这个问题，某些令牌系统将其中一部分时间信息加密，附加到生成的随机数中去。这减小了可用的数字空间，而且降低了认证方案的安全性。

基于硬件令牌的一次性密码系统的维护成本一般都比较高。令牌可能会被丢失或损坏。据统计，硬件令牌的年平均丢失/更换率约为百分之八。分发和重新分发硬件令牌的行政负担实在不容低估。

THE AT.PASS 解决方案

永泰的 AT.Pass 一次性密码双因素认证系统是一个软件方案，克服了上述的传统产品中的许多缺点。

AT.Pass 是与客户令牌和认证服务器同时同步的一次性密码系统。通过已认可的加密算法，服务器得以识别用户身份。传统基于时间参数的令牌的解决方案中，即使使用昂贵的硬件令牌，时间误差也不可避免；而 AT.Pass 系统能避免这种误差。

AT.Pass 使用手机和各类客户端设备作为“容器”储存一次性密码令牌。它支持 Android 手机，iPhone，iPad，Java（MIDP 1.0 和 2.0）手机，并与市面上绝大多数手机和平板电脑兼容。

AT.Pass 系统也提供了其它令牌分发的方法，例如：

- 通过 SMS 发送 OTP，
- 若需要，可向用户的登记邮箱发送预生成的一次性密码列表，即口令卡。

小知识:

- AT.Pass 系统使用特殊的同步算法使一次性密码保持同步，同时保留非常大的有效数字空间以保证最佳安全性，也就是说，即使用户意外的跳过一些由手机令牌生成的密码，只要在一个合理的数量内，认证服务器也能立刻通过验证令牌与令牌保持同步。
- AT.Pass 荣获香港 2005 年 IT 优胜银奖(产品组)。

AT.PASS 的创新设计

AT.Pass 通过创新的设计解决了传统一次性密码系统的一些关键限制，具体方法如下：

1. 令牌分发–根据令牌类型，令牌通过网上下载（如通过 App Store，Android 市场）、电子邮件或短信等方法分发。令牌分发所需的行政和物流的相关成本几乎可以减少为零。

2. 令牌的安全性–令牌自动装载进手机或目标设备内 ,同时以强大的加密方式保护令牌秘密。令牌一旦被下载至设备中，就不能再转移到其它设备上。

3. 个性化的令牌–每个令牌的独有秘密都在与认证系统关联时生成。这个关联动作在令牌成功下载至设备后即完成。如果用户怀疑他手中的令牌受到安全性威胁，可以以其个人身份下载、激活一个新的令牌。一旦新令牌被关联，旧的自动被注销。

4. 手机作为令牌“容器” –用户可以将令牌作为一个应用，装载到自己的手机、平板电脑甚或电脑上。与传统的硬件令牌不同，用户无需携带另一个硬件以生成一次性密码。

5. 加强的加密算法和已认可的安全设计–基于嵌入令牌的三个层次的秘密（组织、系统及用户），AT.Pass 使用 SHA-1, SHA-2 和专用算法的组合生成一次性密码。主机中加密的用户秘密被储存于一个独立的认证服务器中。因此 ,即使组织内部黑客也难以破解。此外，AT.Pass 系统可以考虑使用硬件安全模块（HSM）保护这些密钥，防止其泄露到认证服务器外。

6. 同时支持多令牌类型–每个用户均可拥有多个令牌，可装载进他/她的手机和电脑中。他/她也可以使用生成的 OTP 列表，此列表是以口令卡的形式分发的。多个令牌之间可以交替使用。

7. 高性能和高可靠性–AT.Pass 系统可配置成负载平衡的服务器设置。当遇到高弹性和高载荷需求时，多个 AT.Pass 认证服务器可以并行的方式运行，从而提高可用性和整体的系统性能。

AT.PASS 与应用系统整合

AT.Pass 支持 RADIUS 标准 ,它可与其它支持此标准的产品整合。此外，亦提供 Web Services 的 API，使资深用户能直接控制和调用由 AT.Pass 提供的各种内置功能。

RADIUS 认证标准

几乎所有现有的 VPN 网络设备(IP-SEC VPN 和 SSL-VPN)、访问控制系统（ACS）、代理和逆向代理服务器，域名服务器和单点登录系统（SSO）等，都使用工业标准的 RADIUS 认证协议。通过简易的“即插即用”，AT.Pass 即可与用户已安装设备进行整合。

Web Services 接口

一组Web Services API与AT.Pass 系统一并提供。通过这些 Web Services API，客户可以定制和构建自己的应用接口，以支持独特的系统管理功能或提供其他不同的用户体验。此接口是为较资深用户、满足用户认证需求而设计，这些资深用户需要控制令牌管理的整个生命周期。

OpenID 接口

AT.Pass 支持 OpenID 基金会的认证标准和其相关的协议。AT.Pass 可配置成为一个 OpenID 提供者，为作为 OpenID 依赖方的任何应用提供认证服务。

使用三大标准评估 AT.PASS

我们可以用之前讨论过的三大标准来评估 AT.Pass:

安全性

与其它离线一次性密码令牌相比，AT.Pass 代表的是最高级别的安全性。

AT.Pass 令牌在手机内存中，受到强大的加密保护，因此是完全安全的。

易用性

系统减轻了物理令牌在初期分发和由于令牌损坏或丢失而重分发过程中的行政负担。AT.Pass 令牌是通过电子方式分发至目标“容器”中。

一次性密码亦可通过短信、口令卡形式分发，用户可以灵活选择。

成本

AT.Pass 系统不论是对少量用户的内部应用 ,还是提供数以千万计用户的大型系统，都可以配置使用。

AT.Pass 系统具有高度的可扩展性。灵活的授权许可方案以令牌数量为基础，配合客户不同和不断变化的需求。

AT.Pass 令牌软件支持 Java 手机，Android 手机，iPhone，iPad 和个人电脑。根据用户选择，可以在所有主流操作系统和不同品牌的硬件设备中操作。这大大减少了基础设施的多样性考虑，从而将平台支持的相关成本控制到最低限度。