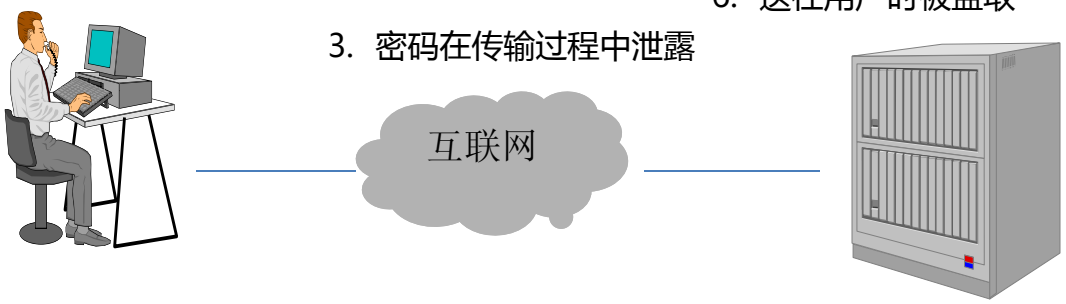
传统用户名和静态密码认证方案的弱点

随着互联网的普及和用户访问大型云计算资源池的需求不断增长，传统的用户名和静态密码系统的安全性显得非常脆弱。

密码在前端使用过程中泄露
1. 被“间谍”软件盗取
2. 被虚假电子邮件或网站截获

密码在后端维护中泄露
4. 生成时被盗取
5. 储存时被盗取
6. 送往用户时被盗取



图一.密码在使用、传输和维护过程中的六个潜在的密码泄露点

众所周知，计算机用户进行身份验证的基础是用户名及其相关的“静态”密码。这种静态的密码可供多次使用，直至被用户明确地修改。静态的密码容易被意外泄露，而近来还有更大的风险来自窃取密码的恶意行为，包括入侵程序和黑客的攻击，例如假电子邮件的形式（“钓鱼”），虚假网站等。其中最常用的黑客方法是使用“间谍软件”来窃取受害者的身份和密码，而击键和鼠标动作也可以在不知情的情况下被捕获。

AT.Pass 解决方案

AT.Pass是一种先进的一次性密码（OTP）双因素认证解决方案。它可简易整合至客户自己的应用系统、VPN网络以及其它访问控制系统和用户认证方案。

AT.Pass依赖于安装在不同客户端设备的软件令牌生成一次性密码。这些客户端设备 包括智能手机(iOS，安卓，Windows)，平板电脑和个人计算机。这些设备作为“容器”存放着软件令牌并按需生成一次性密码。

AT.Pass还提供基于短信的OTP和口令卡作为备选方案供用户选择。口令卡是一张预生成的OTP列表，用户申请口令卡时，系统会通过注册邮箱发送给用户。

AT.Pass 一次性密码
双因素认证解决方案

产品特性

AT.Pass为不同大小规模的部署而设计。它使用工业标准协议和接口模式，支持与用户应用的简易整合。

软件令牌适用于多种设备	软件令牌适用于: • iOS 设备 • 安卓设备 • Windows 设备 • J2ME 设备
令牌分发	• 通过软件下载完成在线分发； • 申请口令卡OTP密码列表时，密码列表通过电邮发送。
令牌安全性	通过强大的加密方式保护令牌秘密。令牌可以被卸载但不能被转移至其它设备。
个性化令牌	每个令牌秘密都在关联时生成。一旦新令牌下载并关联后，旧令牌即自动失效。
强加密算法	AT.Pass使用SHA-1,SHA-2与专用算法的组合生成一次性密码。
支持多应用	可被多个应用系统共享。VPN，SSO和多个应用组合后，可与AT.Pass整合以提供统一的用户认证服务。
简易整合	支持RADIUS, OpenID 和Web Services API 以实现与不同系统的整合。
高性能和可靠性	AT.Pass可设置为负载均衡，Active-Active模式，多服务器部署以及高可用性的群集数据库。

AT.Pass 荣获2005年
香港资讯科技银奖

AT.Pass 服务器的系统要求	
操作系统	任何支持Java JRE 1.6 或以上的操作系统。
数据库	• MySQL 5.0 或以上； • PostgreSQL 8.4 或以上； • MS SQL 2008 或以上； • Oracle 9i 或以上。
令牌“容器”的系统要求	
操作系统	• iOS • 安卓 • Windows phone • 任何支持 J2ME (包括 黑莓)的操作系统 • Windows

地址：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
电话：+852 3125-9000
传真：+852 2668-2166

http://www.iaspec.com