

Topsense OTP 产品为身份鉴别用户提供增强的身份认证，同时为基于各种网络的应用服务提供安全访问基础

通用算法

Topsense OTP 产品采用了国际通用的散列加密算法（HOTP），具备强大的抗攻击能力

简单易用

用户只需轻松触发产品上的按键，即可获得一个安全的用以确认他们数字身份的动态密码

无空间、时间限制

Topsense OTP 产品采用了各种便携式设计，可以被方便的带到任何地方，从而实现本地或远程的登陆

在进行安全方案设计时，一个层面必须依赖于另一个层面。"安全金字塔"必须建立在管理策略和过程的基础上，而用户认证是整个金字塔的关键组成模块。若不首先采用强力用户认证，其余的授权层面、加密层面和审计层面就会变得毫无意义。因此无论是在 VPN、RAS、Web 电子商务，还是在企业网络应用中，都必须采用强力用户身份认证，确保网络资源访问的合法。

* 目前身份认证的现状

在计算机网络中，最常见而简单的访问控制方法是通过对静态口令的匹配来确认用户的真实性。而调查表明，有 60% 的系统首先被攻击和突破的地方是口令。许多最具危害性的犯罪都拥有共同的特点：即绕过密码保护以获取对信息或资金的访问权限。信息安全的关键在于确切地了解谁正在访问您的最机密的网络信息资产。不幸的是，事实证明，建立在静态口令之上的安全机制非常容易被黑客攻破。

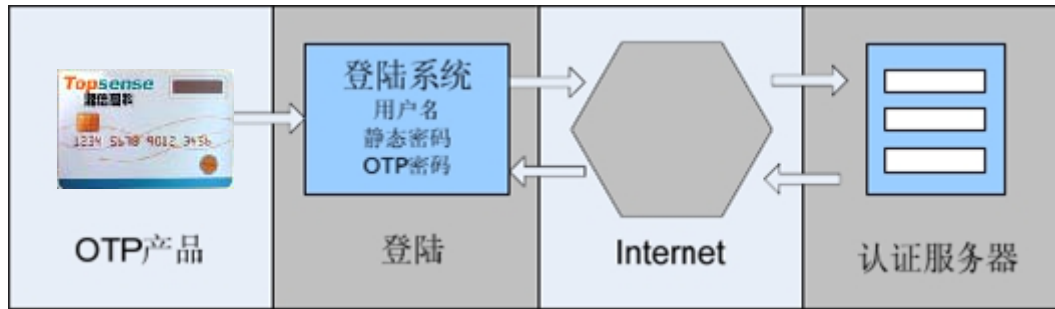
* 传统身份认证方式存在的问题

密码本身只能对真实性进行低级的认证。静态密码存在很多缺陷，如：密码容易被他人猜测或通过交际工程学、社会工程师等途径获取，输入密码时容易被人窥视，密码容易被很多工具破解，存在着没有被检测到的缺陷和漏洞，密码可以在网络离线时被窥测，密码和文件容易从 PC 和服务器上被转移等等。虽然一次性密码比可重用的静态密码强壮，但它们仍存在能被利用的弱点（需要更多的技巧），其中包括中间人攻击和竞争攻击。而且一次性密码依然是单因素认证，而不是我们所说的强力用户认证。因此静态密码是最不安全、最弱的一种识别与身份认证手段。

* 解决办法

将密码设置为“静态+动态”的形式。其中静态的密码是用于在设立账户时设置的只有用户自己知道的密码。而动态密码也称一次性密码（One-time Password—OTP），它指用户的密码按照时间或使用次数不断动态变化，每个密码只使用一次，动态密码采用一种称之为动态令牌的专用硬件，大小相当于一张 U 盘，显示方式类似于电子手表，它内置电源、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。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，所以只要密码验证通过，系统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。

Topsense OTP 产品应用架构



用户将 OTP 令牌所产生的动态密码，输入到身份验证平台设备中，身份验证平台会将用户 ID 信息及动态密码通过网络发送往系统认证服务器，而认证服务器会将认证结果通过网络传回验证平台。获得资格认证的客户可以获得系统应用层所提供的相应服务。

Topsense OTP 产品应用领域

- * 网络银行/电子银行
- * 网络游戏
- * 网上证券交易
- * 电子邮件
- * 即时通信
- * 电子购物
- * 企业内部信息管理

www.topsensetech.com

北京鼎信高科信息技术有限公司

北京市海淀区上地信息路11号彩虹大厦北楼306

TEL: 010-62963695

FAX: 010-62960847