



技术与解决方案

Technologies and Solutions

飞天OTP动态令牌身份认证系统

当今社会已经进入信息化、数字化时代，数字数据和数字通信已经成为人们日常生活中不可分割的一部分，这些资源不但对组织机构具有巨大的价值，而且也涉及到最终用户的利益。随着技术环境和应用环境的改变，特别是熟悉计算机技术的人越来越多，各种攻击技术、破解技术以及攻击工具和破解工具通过网络广泛传播的情况下，静态密码的安全性缺点显露无疑。

飞天动态口令身份认证系统通过使用动态口令身份认证技术来提高身份认证的准确性，有效避免静态口令身份认证的安全性缺点和PKI身份认证技术操作环境和操作方式的不方便、不灵活缺点，达到安全性和方便性同时提高的效果。

飞天动态口令身份认证系统对各种应用环境具有广泛的灵活性和适应性，能够适应各种使用环境，只需要在服务器端安装和配置相应的身份认证模块，无需增加任何硬件设备、接口等。无需对客户端软件做任何的改动，也无需在客户端安装任何软件。

飞天动态口令身份认证系统组成

飞天动态口令身份认证系统包括认证服务器、认证备份服务器、管理工作站、动态口令令牌、认证代理以及认证客户端，基本结构如图所示。

1. 认证服务器

飞天动态口令身份认证服务器完全独立于应用服务器的业务系统，只需要在业务系统中安装认证代理模块即可，不用更改应用系统原有网络结构设计。

认证服务器是完成用户身份认证功能的核心，根据具体的需求情况，可以为业务系统的登录、关键业务处理等操作提供用户身份认证功能。当业务处理需要进行动态口令身份认证时，用户通过其所持有的动态口令令牌获得动态口令，然后输入业务系统提示窗口中，由业务系统发送到认证服务器进行认证，如果认证成功，用户可以继续进行操作，如果认证失败，用户的操作将被终止或要求重新进行认证。

2. 认证备份服务器

认证备份服务器是对认证服务器的完全备份，它能够在认证服务器发生故障或检修时，及时接管认证服务器的认证工作。

3. 管理工作站

管理工作站提供动态口令身份认证系统的管理界面，它在网络管理员与认证服务器之间提供一个友好的操作界面，便于网络管理员对系统进行管理和维护。通过管理工作站，网络管理员可以进行系统配置、动态令牌管理（比如添加、删除、和用户绑定、锁定、解锁等）、用户管理（比如添加、删除、分配令牌等）以及认证日志管理等操作。

4. 动态口令令牌

动态口令令牌是一个单独的硬件设备，使用时无需连接任何外部设备，所以具有很大的灵活性，登录应用系统时，只需要激活动态口令令牌，将生成的动态口令输入登录窗口中的对应位置即可。



技术与解决方案

Technologies and Solutions

5. 认证代理

认证代理提供应用服务器与认证服务器之间的连接通道，认证代理从应用服务器接收认证请求并传递给认证服务器，然后从认证服务器接收认证响应并传递给应用服务器。

6. 认证客户端

认证客户端是指用户进行操作以前需要进行动态口令身份认证的应用系统终端。用户在进行操作以前，需要使用自己的动态口令令牌生成动态口令并提交给系统进行认证，如果认证成功，用户才能进行操作，如果认证失败，用户的操作将被终止或要求重新认证。



飞天动态口令认证解决方案系统组成图

飞天动态口令身份认证系统的认证过程

飞天动态口令身份认证系统作为一个安全的身份认证系统平台，提供系统化的、完整的动态口令身份认证服务。用户将帐号、静态密码和动态口令信息等封装在认证请求中传递给认证服务器，认证服务器根据接收到的认证请求从数据库系统中读取相关信息并执行认证，认证完成后将认证结果封装在认证响应中并返回给用户。在认证过程中，认证服务器还会记录日志信息。

飞天动态口令身份认证系统采用先进、实用、成熟的技术和开放体系结构，具有高可靠性、高可用性和高可维护性，性能优良、配置灵活、具备良好的性能价格比和系统扩充能力，通过提供广泛的数据库支持，为满足用户环境的差异性提供了良好的灵活性和适应性。

