关于动态口令及其令牌的研究进展

陈泽凯
（厦门大学信息科学与技术学院计算机科学系，福建 厦门 361005）

摘　要：动态口令广泛应用于网上银行、电子支付等领域，目前朝着多因子认证的方向发展，其令牌种类众多，移动互联网时代下移动设备将成为一种重要的选择。本文介绍了各类动态口令及其令牌并分析了其面临的安全挑战和解决方案，对其应用和发展作了展望。
关键词：动态口令；令牌；移动设备；时间；事件；挑战应答
DOI:10.16640/j.cnki.37-1222/t.2016.04.193

1　引言

动态口令是一种重要的身份认证技术，常用的密码很容易被窃取或猜测，动态口令克服了其长期使用同一口令的缺陷。动态口令在电子商务、互联网金融等领域得到了广泛应用，企业或银行开发了自用方案如 SecurID、U 盾、口令卡等，一些企业也推出相关定制产品。本文重点介绍动态口令的类型及令牌和近年来的研究成果，并其发展方向作了展望。

2　动态口令技术的分类

动态口令主要有基于事件同步、基于时间同步、基于挑战应答三种类型，传递使用的令牌包括短信、手机、专有令牌（智能卡和芯片设备）、网页、硬拷贝等。

2.1　基于事件的动态口令

基于事件的动态口令通过特定的事件次序及相同的种子值作为输入，通信双方维护相同的计数器以得到一致的口令，当前口令的产生依赖先前的口令，如哈希链方案和 S/Key 方案。哈希链方案通过哈希函数 F 对种子 x 进行迭代运算（F(…F(x)…)）生成口令，第 i 次认证要求客户端提供哈希链上的第 N-i 个口令 $F^{N-i}(x)$，服务端验证 $F(F^{N-i}(x))$ 是否等于 $F^{N-i+1}(x)$，一定程度上解决了不安全环境下的认证问题；S/Key 方案选择 MD4 作为哈希函数，在生成的 128 位摘要只取 64 位转换为单词，通信双方需要维护相同的字典库和计数器，S/Key 方案能够有效防止重放攻击，但并不能抵抗小数攻击，攻击者冒充服务端要求客户端提供一个迭代数 M 的口令，得到 $F^{M}(x)$ 后就能计算出所有满足 M<K<N 的 $F^{K}(x)$。

近几年 RFC-4226 提出了更安全的 HMAC-base OTP（简称 HOTP）方案，应用于各类专有令牌。该方案中令牌和认证服务器共享加法计数器 C 和对称密钥 K，通过 HMAC-SHA1/MD5 算法生成消息认证码 HMAC 提供给用户，认证码具有抗碰撞性和消息认证属性。该方案克服了多重哈希运算产生口令的弱点，即运算量过大和小数攻击。HOTP 需要解决对称密钥共享的和计数器同步（如文献 [1] 的基于窗口的重同步方案），并使用智能卡或芯片设备。

2.2　基于时间的动态口令

基于时间的动态口令按时间的使用方式分为两类：第一类只是用时间间隔作有效性约束，如短信验证码要求在一分钟内使用；第二类使用时间作为输入参数，如 RFC-6238 中提出的 time-based OTP（简称 TOTP）方案。TOTP 和 HOTP 的主要区别是用时间代替计数器作为输入参数，使用 HMAC-SHA-256/512 算法生成消息认证码，每个时间间隔产生一个口令，间隔之外口令即失效，同步标准统一且不会有重复的输入，时效性更强。在一些场合可用 TOTP 替换 HOTP，如文献 [2] 实现了一种高效的基于各类芯片的 TOTP 动态口令卡，依靠晶体振荡器提供时间因素。TOTP 目前较多使用手机令牌，如用于两步验证的“ Google Authenticator ”，用于更换设备登录账户的“ Facebook Login Approval ”；文献 [3] 基于手机令牌提出了可应用于网上银行和 ATM 系统的 TOTP 认证方案；时间同步在移动设备上实现也较容易。

2.3　基于挑战应答的动态口令

基于挑战应答的动态口令在每次认证时服务器端都给客户端发送一个不同的挑战，客户端程序收到挑战后做出相应的应答，双方通常会共享密钥、应答产生函数等，挑战应答可以结合时间或事件作为输入的口令生成算法，比如加入时间的有效性约束；反之，对于 HOTP 和 TOTP 也可加入挑战应答机制来提高安全性。为了判断请求证明者的合法性，一般需对挑战加密或签名，并与其他因子结合。文献 [4] 结合 S/Key 与挑战应答机制，通过与密钥异或计算加密的挑战和序列数实现了双向认证，但多次使用相同密钥可能带来风险；文献 [5] 将用户信息和挑战连接后再进行哈希生成挑战码，并使用了公钥算法加密认证过程，但需要可安全携带数字证书或密钥的专有令牌。

3　安全挑战和解决方案

安全挑战无处不在，目前在安全敏感的场合一般都会使用动态口令，若每一项应用都使用独立的令牌，需要管理的令牌数量和种类将越来越多，使用成本过高；动态口令存在着各种潜在漏洞，主要体现在密钥、盐、生物特征模板等秘密信息的保护，公钥、数字签名、挑战等认证因素的防伪等方面；此外还要防范攻击者截取口令在恶意篡改的会话中使用。

目前动态口令的令牌以智能卡和芯片设备为主，随着移动互联网的发展，基于移动设备的应用越来越多，移动设备是一个新的选择，对客户端的数字签名还能携带公钥。秘密信息保护包括存储和传输两个方面。在存储方面，芯片设备的安全性最高，通过用户设置 PIN 码保护令牌的安全即可；若采用移动设备，可通过 PIN 码、图案识别等方式保护令牌，但需防止木马窃取信息。客户端的数字签名可以完成对服务端的认证，在不使用 CA 证书的情况下达到较好的安全性。

4　结语

动态口令技术目前基本采用多因子认证，基于事件、时间和挑战应答三类动态口令方案有着各自的优势，应根据不同场合选择因子设计合适的方案。在可预见的将来，智能卡和芯片设备仍是主流令牌，移动设备则展现了独有的优势，不仅通用性高，而且可以使用时间、数字签名甚至生物特征等因子（指纹 / 虹膜识别设备陆续出现），移动设备还可作为鉴别用户的关键信息，在移动互联网时代拥有良好的应用前景。

参考文献：
[1] 刘潇，刘巍然，李为宇．一种改进的动态口令生成算法及重同步方案 [J]．计算机研究与发展 ,2012,49(12):2611-2618.
[2] 郑强，高能，张令臣．基于 SM3 算法的动态口令卡的设计与实现 [J]．计算机应用与软件 ,2013,30(02):14-17.
[4] 何冰．简单易行的 S_KEY 认证改进方案 [J]．计算机应用 ,2011,31(04):996-998.

作者简介：陈泽凯（1990-），男，福建漳州人，硕士，研究方向：信息安全。