基于事件同步及异步的动态口令身份认证技术研究*

刘知贵[1,2]，臧爱军[3]，陆荣杰[1]，郑晓红[1]

(1. 西南科技大学 计算机科学与技术学院，四川 绵阳 621010；2. 西南交通大学 计算机与通信工程学院，四川 成都 610031；3. 石家庄学院 计算机系，河北 石家庄 050035)

摘　要：动态口令身份认证中有两种不常应用的技术——事件同步技术和异步口令技术,它们避免了时间同步令牌中存在的缺点,事件同步技术通过次数进行同步,异步口令技术避免了口令失步的问题。给出了两种技术混合使用的一种认证模型,并比较了三种技术的优缺点。

关键词：事件同步；异步；动态口令；挑战/应答

中图法分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1001-3695(2006)06-0133-02

Dynamic Password Authentication Based on Event-synchronous and Challenge/Response Technology

LIU Zhi-gui[1,2], ZANG Ai-jun[3], LU Rong-jie[1], ZHENG Xiao-hong[1]

(1. *School of Computer Science & Technology, Southwest University of Science & Technology, Mianyang Sichuan* 621010, *China*; 2. *School of Computer & Communication Engineering, Southwest Jiaotong University, Chengdu Sichuan* 610031, *China*; 3. *Dept. of Computer Science, College of Shijiazhuang, Shijiazhuang Hebei* 050035, *China*)

Abstract: Nowadays there are two unusual technologies of dynamic password authentication: Event-synchronous and Challenge/Response. They can avoid the shortcomings of time-dependent tokens. Event-synchronous rely on the input event but an internal clock. The usage of asynchronous tokens is always consistent. It also gives an authentication model with the two technologies and compares three dynamic password styles.

Key words: Event-synchronous; Asynchronous; Dynamic Password; Challenge/Response

为解决静态口令安全性的问题,在 20 世纪 90 年代出现了动态口令技术，近 10 年以来在国内外的金融、电信、电子商务等领域得到了广泛的应用。而国内也有一些公司开发了自己的动态口令产品,可以说动态口令对于我们来说已经不是一个新鲜的话题了。但是在众多的应用中,大部分的动态口令产品是基于同一种技术——时间同步机制,多数的使用者也自然而然地认为动态口令的产品都是基于时间同步的。实际上这种时间同步机制的动态口令技术存在着自身不可避免的缺陷——时间漂移,越来越多的用户在使用过程中已经发现了这种弊病。

动态口令技术主要分两种[1],即同步口令技术和异步口令技术(挑战—应答方式)。其中的同步口令技术又分为:①时间同步口令;②事件同步口令。

由于近年事件同步动态口令产品在国外的广泛应用,在本文着重介绍事件同步动态口令技术。

1　动态口令技术简介

动态口令技术是一种让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的技术[4]。它采用一种称之为动态令牌的专用硬件、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。用户使用时只需要将动态令牌上显示的当前密码输入客户端计算机即可实现身份的确认。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仿冒合法用户的身份。动态口令技术采用一次一密的方法,有效地保证了用户身份的安全性。

收稿日期：2005-06-22；修返日期：2005-09-28

2　事件同步技术原理

基于事件同步的令牌原理是通过某一特定的事件次序及相同的种子值作为输入,在算法中运算出一致的密码。不同于时间同步技术,事件动态口令技术是让用户的密码按照使用次数不断动态变化。它是在用户每次按一下令牌时产生一个密码,同步原理如图 1 所示。

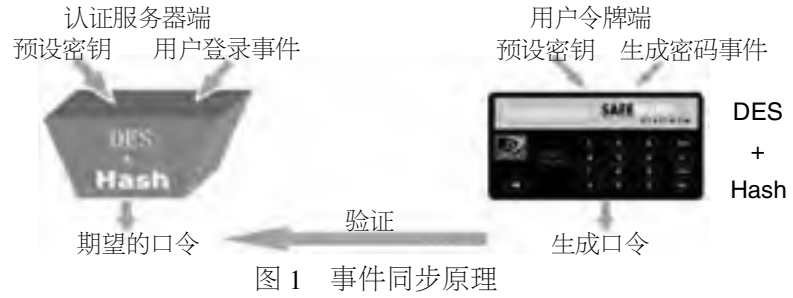

图 1　事件同步原理

用户令牌用预设的密钥与用户按键的次数通过密码算法(DES + Hash 等)生成本次所需的口令,认证服务器端同时是根据每次用户登录事件计算出相同密码,与传过来的口令进行

比较,以确认登录人的身份。如果用户连续按了多次令牌,认证服务器端可以在一个规定的次数范围内自动计算出所有口令并比较,用此方法解决事件同步的失步问题。

基于事件同步的令牌也同样存在失去同步的风险,如用户多次无目的地生成口令等。对于令牌的失步,事件同步的服务器使用增大偏移量的方式进行再同步,其服务器端会自动向后推算一定次数的密码来同步令牌和服务器。当失步情况非常严重,大范围超出正常范围时,有的公司产品会设计通过连续输入两次令牌计算出的密码,服务器将在较大的范围内进行令牌同步。一般情况下,令牌同步所需的次数不会超过三次,但在极端情况下,不排出失去同步的可能性,如电力耗尽、在更换电池时操作失误等。此时,令牌仍可通过手工输入由管理员生成的一组序列值来实现远程同步,而无须返回服务器端重新同步,这一点是优于时间同步令牌的。目前时间同步令牌一般通过增大偏移量的技术(前后 10mins)来进行远程同步,确保其能够继续使用,降低对应用的影响;但对于超出默认的时间同步令牌(共 20mins),将无法继续使用或进行远程同步,必须送回服务器端另行处理。

3 异步动态口令技术原理

异步口令技术也可称为挑战—应答技术,它是一种交互方式。其基本思想是通信双方掌握相同的口令产生方法和用户的秘密身份信息,当用户申请登录系统时,由系统方(认证方)随机产生一个动态性数据并提供给用户,用户使用该数据和自己的身份信息构造一个口令,并提交给系统进行认证。其过程如图 2 所示。认证服务器提出挑战(Challenge),用户将此 Challenge 输入令牌中,计算出应答值(Response)回复给认证服务器。

图 2 异步口令技术原理

4 事件同步/异步动态口令认证流程

访问者输入用户名和动态口令,提出对目的访问请求,被身份认证代理截获。一旦认证被拦截,用户的身份证书就会被传递到认证服务器(AAA Server)。AAA Server 将用户的 ID 和口令与 AAA 中或 LDAP 中储存的资料进行比较,判断它们是否匹配。如果用户 ID 相匹配,就用用户的数据库记录来核对其任务和可以访问的资源,如果用户成功地通过了所有这些认证步骤,他们就被获准访问网络了。一般来说管理员会根据用户的身份、所属组织或访问动作的属性来制定访问策略。其流程如图 3 所示。

5 三种技术的比较

(1)时间同步。基于令牌和服务器的时间同步一般每 60s 产生一个新口令。由于时间上总是有些偏移,要求其服务器能够十分精确地保持正确的时钟,同时对其令牌的晶振频率有严格的要求,从而降低系统失去同步的几率。但由于令牌的工作环境不同,在磁场、高温、高压、震荡、浸水等情况下易发生时钟脉冲的不确定偏移和损坏,故对于时间同步的令牌要求必须进行较好的保护。同样,对于基于时间同步的服务器应较好地保护其系统时钟,不要随意更改,以免发生同步问题,从而影响全部基于此服务器进行认证的令牌。

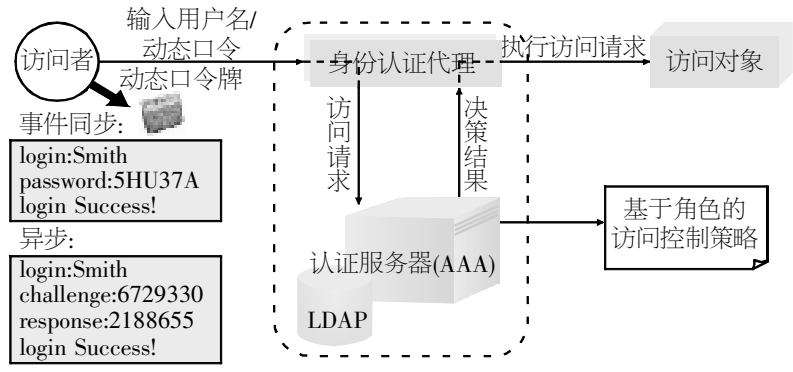

图 3 动态口令身份认证访问流程

(2)事件同步。基于事件同步的令牌其运算机理决定了其整个工作流程与时钟无关,不受时钟的影响,令牌中不存在时间脉冲晶振。因此基于事件的令牌可以适用于非常恶劣的环境而不受使用的影响,即使令牌不小心掉进水里浸泡也不会受太大的影响。

(3)异步口令技术。对于异步令牌,由于在令牌和服务器之间除相同的算法外没有需要进行同步的条件,故能够有效地解决令牌失步的问题,降低对应用的影响,同时极大地增加了系统的可靠性。异步口令使用的缺点主要是在使用时用户需多一个输入挑战值的步骤,对操作人员增加了复杂度,故在应用时,将根据用户应用的敏感程度和对安全的要求程度来选择密码的生成方式。

6 结束语

身份认证被认为是信息安全市场未来几年的发展动态。动态口令已被越来越多的单位所接受,多了解一些动态口令的相关技术会对我们按需求实施身份认证项目有很大的帮助。目前能将事件同步和异步口令技术整合在一起的产品不多,在我们接触的国内外产品中,SecureComputing 公司的 SafeWord PremierAccess 是一套值得推荐的产品。它最早由 ARPANET 的安全技术小组进行研究,目前的应用已经遍及全世界,其中著名的花旗银行是它最大的用户。当然,在信息安全越来越重要的今天,希望会有更先进的技术出现以满足我们不断的需求。

参考文献:

[1] vent-synchronous Tokens Versus Time-dependent Tokens[EB/OL]. http://www.securecomputing.com/index.cfm?skey=969, 2002-02.

[2] A Comparison of Two Different Approaches to Using Dynamic Passwords[EB/OL]. http://www.quizid.com/media/dynamic_passwords.pdf, 2002-10.

[3] 张利华. 一种增强的智能卡口令认证方案[J]. 计算机工程与应用, 2004, 38(31).

[4] 连一峰, 王航. 网络攻击原理与技术[M]. 北京: 科学出版社, 2004.

作者简介:

刘知贵(1966-),男,四川绵阳人,教授,主要研究方向为自动控制理论、计算机网络技术及安全策略;臧爱军(1975-),男,河北保定人,助教,主要研究方向为计算机网络安全防护与网络教学;陆荣杰(1971-),男,河北人,硕士研究生,主要研究方向为网络技术、网络安全;郑晓红(1979-),四川人,硕士研究生,研究方向为网络技术等。