OTP技术的一种改进方案与应用

Realization of a New Scheme of Improvement on OTP Authentication Technology

李凤银　刘培玉　(济南山东师范大学信息管理学院　250014)　　鞠宏伟　(　　250023)

摘要：本文详细讨论了"一次性口令"认证技术的原理和实现过程，分析了常用OTP认证不能抵御主动攻击和内部攻击的局限性，以及OTP认证存在小数攻击等安全漏洞，提出了一种改进方案，这种改进的OTP方案能够在不增加用户负担的情况下抵御小数攻击和重放攻击，并用Java实现了其在网上会员制电子书店中的应用。

关键词：一次性口令　小数攻击　重放攻击

1 引言

随着Internet的迅猛发展，Web服务已经得到越来越广泛的应用。为了安全、保密及计费的需要，一些Web应用服务器在为用户提供服务时必须验证用户的身份，以确保只有经过授权的合法用户才能得到服务。

常用的认证方法类似于Unix操作系统登录过程中输入用户名和口令的形式，但这种认证方式具有不安全性，最大的问题是用户名和口令均以明文方式在网络中传输，难以支持敏感的、重要的数据交换。而基于证书的数字签名认证技术，必须以完善的CA(Certification Authorit，证书授权中心)体系为基础，这在我国才刚刚起步。而且，这种认证方案技术复杂、成本高，适合于跨地区跨行业的大型网络应用系统。

在网络中，窃取系统口令文件和偷听网络连接获取用户名和口令进行重放攻击是最常见的攻击方式，如果网上传送的口令只使用一次，攻击者就无法用窃取的口令来访问系统，一次性口令系统就是为了抵制这种重放攻击而设计的。"一次性口令（One-Time Password，OTP）"认证技术无需第三方公证、实现方案简单、成本低，而且由于在一次性口令认证系统中，只有一个一次性的口令通过网络的传输到达认证方，用户的秘密通行短语在任何时间都不在网上传输，所以可以有效地抵御重放攻击，为企业Intranet提供足够的安全性，所以，对于企业Intranet采用无需第三方公证的"一次性口令（One-Time Password，OTP）"认证技术是一种切实可行、安全有效的解决方案。

本文介绍了常用的一次性口令认证技术及其实现方案，分析其存在易受小数攻击的安全漏洞，提出了一种改进方案和并用Java实现了其在网上电子书店中的应用。

2 OTP技术原理与实现方案

2.1 OTP技术的原理

OTP认证是一种摘要认证，单向散列函数（即信息摘录函数，也叫安全Hash函数）在其中起着非常重要的作用，它以变长的信息为输入，把其压缩成一个定长的值输出，即使输入的信息只有微小的改变，输出的定长值（信息摘录）也会发生很大的变化。由于输入的长度大于输出的长度，因此会有不同的输入产生相同输出的可能。然而对于单向散列函数而言，给定输入计算对应的输出在计算上容易实现，而给定输出去寻找对应的输入则是计算上不可行的，所以将单向散列函数值（信息摘录）在网上传输是安全的，目前，著名的Hash函数有MD4、MD5、SHA，MD5是MD4的扩展，被认为是具有足够的安全强度，但计算速度比MD4慢，MD5的设计是面向32比特的，它计算出的信息摘录长度为128比特。

OTP认证的基本思想是：在登录过程中基于用户的秘密通行短语（Secure Pass Phrase，SPP）加入不确定因素，使每次登录过程中摘录所得的密码（即一次性口令OTP）都不相同，用户真正的秘密通行短语SPP根本不在网络上传输，从而可以提高登录过程的安全性。例如，信息摘录函数我们采用MD5，不确定因素我们取为机器的随机数或时间戳，则一次性口令OTP=MD5（用户名+秘密通行短语+随机数/时间戳），这里的'+'代表联接运算。这样，由于随机数/时间戳的动态变化，OTP每次都是不同的，而系统接收到一次性登录口令后以同样的算法做一个验算即可验证用户的合法性。

2.2 OTP认证技术的实现方案

我们以S/Key机制为例介绍OTP认证系统的实现方案。

OTP系统包括两个方面：客户机（用户端）和系统主机（服务器端）。服务器端产生挑战（Challenge）信息，并在随后校验客户端送来的一次性口令应答（Response）的正确性。在客户机上有一个OTP计算器，用于摘录产生一个对应于挑战的一次性口令应答。OTP系统允许用户安全地改变他的通行密语。当运行OTP系统时，只有一个仅用一次的口令穿过网络，在Bellcore公司的OTP产品S/Key系统中它以6个简单英语单词的形式出现(基于易读性和易操作性，S/Key系统将生成的64位一次性口令基于一专用词典转换成6个简单英语单词)。

服务器端产生的挑战信息由两部分组成，即种子Seed和迭代次数Seq。迭代次数Seq为一个整数，其初值初始化为口令序列的元素个数N减1（即N-1），每成功使用一次递减1，种子Seed可以是一个任意长的字符串，但RFC2289建议由10-63个字母/数字组成，不能有空格。

OTP系统的安全性基于安全Hash函数，在S/Key实现方案中可以选择MD4、MD5或SHA作为安全Hash函数，它们的输出都是128位。S/Key口令产生程序把Seed和用户输入的通行密语（可任意长）连接起来，再用安全Hash函数进行多次摘录，摘录次数为挑战中给出的迭代次数Seq，运算结果为64位二进制数，作为用户的一次性口令。

S/Key系统的实现可分以下三个阶段：

(1) 注册阶段。用户A随机选择一个固定秘密口令SPP和一个种子Seed，并计算出一个具有N个元素的动态口令序列：H（SPP ‖ Seed），H2（SPP ‖ Seed），…，HN-1（SPP ‖ Seed），HN（SPP ‖ Seed），这里，SPP ‖ Seed表示用户的秘密通行短语和种子的联接结果，HN（SPP ‖ Seed）表示对SPP ‖ Seed进行N次Hash运算得到的信息摘录。该序列的特点是后一个元素正好是前一个元素经过一次Hash运算得到的；并把下列数据通过安全信道提交给服务器端主机：用户名User，种子Seed，口令序列的元素个数N，以及主机验证用户第一个口令的验证因子HN（SPP ‖ Seed）。用户保留SPP，以后依次使用的口令分别是HN-1（SPP ‖ Seed），HN-2（SPP ‖ Seed），…，H2（SPP ‖ Seed），H1（SPP ‖ /Seed）共N-1个口令，在实际应用中，考虑到安全性，当Hash函数迭代的次数小于等于5时，必须重新进行初始化。

(2) 口令产生阶段。S/Key口令产生程序把种子Seed和用户输入的秘密通行短语（SPP，可任意长）连接起来，再用单向安全Hash函数进行一次摘录，将得到的128位输出经半加折叠成64位，再将此64位的折叠结果作为安全Hash函数的输入再次摘录，…，如此循环，重复摘录Seq次，得到64位的OTP，再将该OTP基于一专用转换词典DC（Dictionary for Converting Between S/Key 6-Word and Binary Formats，共2048个单词），转换为一个由6个短英文单词组成的短语，每个单词长1～4个字母，每个单词都取自该词典。口令产生过程如图1所示。

(3) 校验阶段。经过Seq次迭代的OTP的校验过程可描述如下：

① 客户端用户A向主要提出登录请求；

② 服务器端主机向用户A发出挑战信息，其中包括口令的迭代次数Seq和种子Seed；

③ 用户A根据挑战信息中的迭代次数Seq和种子Seed，基于选定的安全Hash函数计算一次性口令OTP= HSeq（SPP//Seed），并将OTP发送到主机；

④ 主机对收到的OTP再用相同的Hash函数摘录一次，若运算结果与先前存储的OTP相同，则认证成功，并将此OTP存储以作下次使用；否则，认证失败，拒绝响应用户请求。

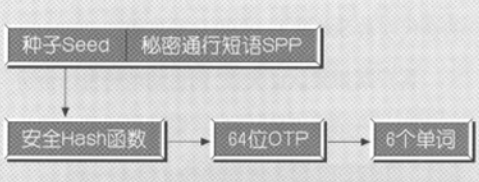

图1 OTP口令产生模型

由上述可知，S/Key方案克服了引言中所提到的传统口令识别系统所具有的缺陷，尤其是传统口令识别系统无法解决的重传攻击问题。例如，非法的窃听者即使在线截获了用户的经Seq次迭代的口令HSeq（SPP//Seed），由于H是安全的单向Hash函数，他无法求得用户的下一次使用的口令Hseq-1（SPP//Seed），从而有效抵御了重传攻击问题。

3 OTP认证系统的安全漏洞及其改进

S/Key OTP是一次性口令认证系统的典型实现，由于用户的秘密通行短语既不存储在服务器和客户机中，也不在网络上传输，在认证过程中只有一次性的口令OTP在网络上传输一次，故其认证系统具有一定的安全强度，但由于其种子和迭代值均采用明文传输，不能保护系统免受组织"内部工作"攻击和主动攻击，还给黑客攻击留有重放攻击的安全漏洞。如黑客在用户向服务器请求认证时，假冒用户截取服务器传来的种子和迭代值，并修改迭代值为较小值，然后假冒服务器，将得到的种子和较小的迭代值发给用户。用户利用黑客发过来的种子和较小的迭代值计算一次性口令发给服务器，黑客再次截取用户传来的一次性口令，并利用已知的单向散列函数依次计算较大迭代值的一次性口令，就可获得该用户后继的一系列口令，进而在一段时间内冒充合法用户而不被察觉。这就是所谓的小数攻击。所以，标准的S/Key实现方案不能抵御小数攻击。

为防止小数攻击，我们对标准S/Key方案可做如下改进：

在服务器端保存迭代次数Seq的同时，在客户端保留迭代次数的备份Seq′，并且和服务器端的Seq同步变化。这样每次客户端收到服务器端发来的挑战值，取出其中的迭代次数Seq和自己保存的迭代次数Seq′相比较，只有在一致的情况下才计算一次性口令OTP并发送到服务器，否则拒绝响应。这样，花费极小的存储代价就可以有效防止攻击者通过修改迭代次数Seq进行小数攻击。

4 一个改进的OTP系统

基于第一种改进方案，本文作者用Java实现了一个一次性口令认证系统，并将其应用于网上会员制电子书店中。在该系统中，书店会员只要按月或按年交纳一定的会费，就可以在网上享受会员的服务和优惠，其中包括可以访问一些只对会员开放的免费资源，可以以会员的优惠价购书等。而且在该系统中，书店会员只要在每次登录时输入用户名的口令，通过强身份认证后，就可以在电子书店的网站上任意访问为会员开放的资源，而不需再次输入口令。避免了用户每访问一种资源都要输入口令，方便用户的使用。

在该系统中客户端是电子书店的会员，服务器端则是书店的Web服务器。会员通过服务器证书实现对书店Web服务器的身份认证，服务器通过改进的OTP技术认证方案实现对会员的身份认证。客户端（会员）在注册时将秘密信息（用户名User，种子Seed，口令序列的元素个数N，以及主机验证用户第一个口令的验证因子HN(SPP//Seed)等）经服务器的公钥加密后发送给服务器。同时客户端将本地的口令迭代次数Seq初始化为N-1。从安全性和效率两方面综合考虑，我们选用MD5作为S/Key系统的安全Hash函数。

客户端根据迭代次数Seq对秘密通行短语和种子的联接结果SPP//Seed，利用MD5算法计算出OTP并发送给服务器端，服务器端将收到的OTP用相同的摘录函数再摘录一次得到OTP′=MD5(OTP)，若计算出的OTP′与服务器端先前保存的OTP相同则认证通过，否则认证失败。

为减轻用户的负担、方便用户的使用，在本系统中，客户端的OTP计算器由Java Applet实现。而且用户不必拥有证书，也不需要事先安装任何客户程序，用户认证模块和访问控制模块均集成在服务器端的"安全代理服务器"（Secure Proxy，SP）中。改进后的OTP认证方案中用户的认证过程如下：

(1) 用户（书店会员）访问安全站点，下载Applet(OTP计算器)，下载后的Applet将用户的请求次数自动初始化为1。每次Applet向服务器发出认证请求前都检查用户本次登录后的请求次数，若不是第一次请求，则自动产生一条自定义的"免用户认证（AUTH）"HTTP消息头，将"免认证"的消息发送到服务器，由服务器直接提供服务；否则，Applet要求用户输入用户名User和秘密通行短语SPP，Applet产生自定义的"用户认证(AUTH)"HTTP消息头，将用户名发送至SP。

(2) SP响应AUTH消息，若是"免认证"消息头，则直接提供服务；若是"认证消息头"则去查询用户数据库，若为注册用户，读取该用户的种子Seed，迭代次数Seq，构成Challenge并发送给客户端的Applet；否则将"认证失败"信息发送到客户端，认证过程结束。

(3) 客户端Applet从接收到的Challenge中取出迭代次数Seq，并和自己备份的迭代次数Seq′相比较，只有在两者一致的情况下才会Challenge中的相关信息和用户输入的秘密通行密语一起产生OTP，并仍以"AUTH"消息格式传回SP；同时将本地备份的迭代次数Seq′减`1。

(4) SP用与客户端相同的Hash函数对收到的OTP计算OTP′，并与先前保存的OTP比较，相同则认证通过，并将OTP′保存，同时将OTP的迭代次数Seq减1；否则认证失败。

客户端如果认证失败，则自动地将自己备份的OTP迭代次数Seq′加1，恢复到认证之前的状态，以保证和服务器端的Seq保持一致。

会员认证过程如图2所示。

图2 会员认证过程

5 结束语

一次性口令认证技术和基于证书的数字签名技术都是比较好的身份认证技术，数字签名技术既可以提供身份认证服务，也可以进行信息认证，但需要第三方的介入和完善的CA体系，用户在使用时需要安装相应的客户程序，实现成本比较高；标准的一次性口令认证主要用于抵御外部被动攻击，是迄今为止唯一一个理论上不可破译的密码体制，但这种密码体制不能防范组织"内部工作"和主动攻击。改进后的一次性口令认证系统在客户端备份OTP的迭代次数，并让其和服务器端的迭代次数同步变化，每次计算OTP前都进行验证，若出现不一致则拒绝响应，从而可以有效地抵御小数攻击，具有较高的安全性。另外，该系统的实现不需加密，只要通信4次，具有较高的通信效率；客户端无需作任何设置，也不必安装任何软件从而，具有用户使用的方便性。所以本系统是一种比较好的Web用户身份认证服务。

参考文献

1 Haller N，Metz C，Nesser P，etc. A One-Time Password System，RFC 2289.1998-02。
2 Haller N. The S/KEY One-Time Password System(OTP)，RFC 1760.1995-02。
3 Franks J，Hallam-Baker P，Hostetler J，etc. HTTP Authentication:Basic and Digest Access Authentication，RFC 2617. 1999-06。
4 叶锡君、吴国新、许勇等，一次性口令认证技术的分析与改进，计算机工程,2000,26(9):27-29。