一种基于消息认证码的身份认证算法①

王松波 (湛江师范学院 商学院 广东 湛江 524048)

摘 要: 针对电子商务中广泛使用的密码身份认证法存在的易泄漏、重放攻击、负担过重等问题，提出一种基于消息认证码的身份认证算法，来解决上述问题。本算法具有失效次数和失效时间两个特性，不需要任何口令和验证表，因此具有稳定的安全性。此外本算法客户端计算量很小，可以用于手机等计算能力有限的环境。

关键词: 电子商务; 身份认证; 消息认证码

User Authentication Scheme Based on Message Authentication Code

WANG Song-Bo (Zhanjiang Normal University, Zhanjiang Guangdong 524048, China)

Abstract: For easy leak, replay attacks, the burden of overweight and other issues in password-based user authentication schemes for electronic commerce, this paper proposes a user authentication scheme based on message authentication code to solve these problems. This algorithm has countable and time-bound features, does not require any password or verification table, it is under firm security. This algorithm has a lower computational overhead on client, can be used in mobile environment with limited computing capability.

Keywords: electronic commerce; user authentication; message authentication code

1 引言

电子商务中为了保护用户隐私和系统安全，对远程用户进行身份认证是电子商务系统必须重点考虑的问题。目前已存在多种身份认证的方法，如密码，指纹，智能卡等，其中基于密码的身份认证方法使用较为广泛。最简单的密码身份认证是在服务端存储用户名/密码表，每个用户的密码是由用户自己设定的，只有用户自己才知道，只要能够正确输入密码，服务器就认为操作者是合法用户。实际上，密码很容易泄漏，即使能保证用户密码不被泄漏，由于密码是静态的数据，在验证过程中需要在计算机内存中和网络中传输，而每次验证使用的验证信息都是相同的，很容易被驻留在计算机内存中的木马程序或网络中的监听设备截获。因此，从安全性上讲，用户名/密码方式一种是极不安全的身份认证方式。改进的方式可以用验证表代替密码表[1]，通过单向哈希函数或者加密算法对密码进行加密，服务器存储加密后的密码。虽然通过这种方式密码不会泄漏，但是攻击者仍然可以通过替换服务器数据库中某用户加密后密码或附加用户名/加密密码对的方式进入服务器，所以服务器数据库的安全仍然是问题。

基于密码的身份认证另一个重要的安全隐患是重放攻击[2,3]，在用户和服务器之间网络不安全的情况下，攻击者可以通过发送一个先前截获的服务器已接收过的包，来达到欺骗系统的目的。

为了提高安全性，一些方法[4,5]去除了密码表或验证表，但是这些方法存在计算和通信负担过重的问题，更重要的是，不能对用户的使用次数和使用时间进行控制，不能满足电子商务对身份认证的要求。因为一些电子商务的服务，例如在线游戏，付费电视，需要对用户使用次数和使用时间进行限制，当用户超过使用次数或者使用时间时，将中止为此用户提供服务，

① 基金项目:湛江师范学院博士专项研究项目(ZW0707)
收稿时间:2010-04-16;收到修改稿时间:2010-05-24

直到该用户再次付费。

本文提出一种基于消息认证码的身份认证算法来解决上述问题。基于消息认证码的身份认证算法过程如下：首先必须先注册并缴费，成为合法用户，服务提供商(SP)提供给注册用户一个用户 ID，一个密码(PW)，和一组动态口令(TKs)。当用户需要系统服务时，通过用户 ID，PW 和一个 TK 登录系统。系统不需要保存任何密码表或验证表，每个 TK 只能在使用期限内使用一次。根据以上设计思想，本文采用二次剩余理论实现身份认证算法，主要分为三个阶段：(1)注册阶段。(2)登录阶段。(3)验证阶段。在这三个阶段以前，还要初始化一些系统参数，首先要选择两个大质数 p，q，要求 $(p-3)$和$(q-3)$同时可被 4 整除，然后计算 $n=p\times q$，p，q 是保密的，只公开 n。下面本文将详细介绍以上三个阶段。

2　注册阶段

在注册阶段，用户向 SP 注册，获得 t 个 TK，每个 TK 只能在失效时间内使用一次。每个用户在注册阶段要经过以下几个步骤。

(1) U_i 向 SP 发送注册请求，请求内容包括个人信息以及申请的 TK 数量，并且 SP 需要得到付费确认。

(2) SP 为 U_i 生成一个唯一的用户标识 ID_i 和一个整数 r_i，满足 $\gcd(r_i,n)=1$，$r^{\frac{p-1}{2}}\neq 1 \bmod p$，$r^{\frac{q-1}{2}}\neq 1 \bmod q$。根据欧拉准则可以得到 $r_i\in NOR_P \wedge NOR_q$。

(3) U_i 申请 t 个 TK，SP 计算

$$PW_i^{(j)}\equiv r_i^{2^j}\equiv\left(r_i^{2^{j-1}}\right)^2 \bmod n$$

$$a_j=MAC_P\left(ID_i\|TID_j\|ED_j\|PW_i^{(j-1)}\right)$$

这里 $j=1,2,\mathbf{K},t$，符号$\|$表示两个整数的连接，TID_j 是 TK_j 中一个唯一的数字序列，ED_j 是 TK_j 的失效时间。每个 TK_j 包含信息$\{TID_j,ED_j,a_j\}$。

(4) 最后，SP 发送 $ID_i,TK_1,TK_2,\mathbf{K},TK_t$ 和 $PW_i^{(t)}$ 给 U_i，U_i 可以将这些信息存储到计算机，智能卡或者手机里，$PW_i^{(t)}$ 只对 TK_t 有效。

3　登录阶段

U_i 在失效时间内都可以使用 TKs，每个都有一个与其对应的 $PW_i^{(t)}$，以验证 TK_t 的有效性，以及用户的合法性。

在这个阶段，假设 U_i 已经拥有一个 TK_a 以及与其对应的 $PW_i^{(a)}$，其中 $a\in[1,t]$，U_i 通过以下步骤获得服务：

(1) U_i 从客户端时钟获得一个时间序列 TS。

(2) U_i 计算 $b_a=MAC_{a_a}(ID_i\|TS)$。

(3) U_i 向 SP 发送 $ID_i,PW_i^{(a)},TID_a,ED_a,TS$ 和 b_a。

4　验证阶段

在这个阶段，假设 SP 在 TS' 时间收到了 U_i 发送的 $ID_i,PW_i^{(a)},TID_a,ED_a,TS$ 和 b_a，SP 通过以下步骤验证登录的合法性：

(1) SP 首先检查收到的时间戳，ΔTS 为合法时间间隔，如果 $(TS'-TS)>\Delta TS$，说明登录请求可能被拦截，则驳回请求。

(2) 检查 ID_i 和 TID_a 的格式，如果格式不合法，则驳回请求。

(3) 检查 TID_a 是否使用过，如果使用过，则驳回请求。

(4) 检查是否过期，如果 $TS>ED_a$，则驳回请求。

(5) 如果登录请求经过了上面的检验，接下来，SP 通过已知的 p 和 q 计算 $PW_i^{(a)} \bmod n$ 的 4 个可能的平方根。计算公式如下：

$$R_a^{(1)}\equiv u\times q\times q^*+v\times p\times p^* \bmod n$$

$$R_a^{(2)}\equiv u\times q\times q^*-v\times p\times p^* \bmod n$$

$$R_a^{(3)}\equiv -u\times q\times q^*+v\times p\times p^* \bmod n$$

$$R_a^{(4)}\equiv -u\times q\times q^*-v\times p\times p^* \bmod n$$

其中 $u\equiv PW_i^{(a)\frac{p+1}{4}} \bmod p$，$v\equiv PW_i^{(a)\frac{q+1}{4}} \bmod q$，$p^*=p^{-1} \bmod q$，$q^*=q^{-1} \bmod p$。

(6) SP 计算 4 个候选的 $a_a^{(1)}$，$a_a^{(2)}$，$a_a^{(3)}$，$a_a^{(4)}$，计算公式如下：$a_a^{(j)}=MAC_p(ID_i\|TID_a\|ED_a\|R_a^{(j)})$ 这里 $j=1,2,3,4$。

(7) SP 判断 $MAC_{a_a^{(j)}}(ID_i \| TS) = b_a$，这里 $j = 1,2,3,4$。如果存在某个 $a_a^{(j)}$ 满足等式，则接受登录请求，否则驳回请求。

(8) 如果登录请求经过了上面的检验，接下来，匹配的平方根 R_a 将作为下一个 TK_{a-1} 的密码 $PW_i^{(a-1)}$，即 $PW_i^{(a-1)} = R_a$，SP 发送 $PW_i^{(a-1)}$ 给 U_i，$PW_i^{(a-1)}$ 通过对称加密算法加密，加密密钥为 a_a。

4 性能分析

通过实验检验本文方法的安全性，并对其性能做出分析。

(1) 安全性分析

本文方法安全性基于计算模平方根，其计算复杂度等价于对大数进行因式分解。下面详细分析其安全性:

保持 SP 的密钥 p 和 q 的安全对于整个系统的安全是十分重要的，如果密钥被泄漏，入侵者就可以为任意用户伪造 TKs，下面说明密钥 p 和 q 的不可计算性。

首先，通过公共参数 n 很难得到 p 和 q，其困难在于大数因式分解，无法在多项式时间内通过公共参数 n 得到 p 和 q。

本算法中，$PW_i^{(a-1)}$ 是 $PW_i^{(a)} \bmod n$ 的 4 个可能的平方根中的一个，根据模平方根理论，如果 $PW_i^{(a-1)}$ 已知，可以容易得到另一个模平方根 $PW_i^{(a-1)}$。下面证明，即使知道两个模平方根 $PW_i^{(a-1)}$ 和 $PW_i^{(a-1)}$，仍然很难对 n 因式分解。

推论 1.设 $x_1 x_1' x_2 x_2'$ 为 $y \bmod n$ 的 4 个可能的平方根，其中 $n = p \times q$，p，q 是两个大质数，如果 $x_1 x_1'$ 为 $y \bmod n$ 的 2 个已知的平方根，即 $x_1 \equiv (n - x_1') \bmod n$，无法在多项式时间内通过 n 因式分解得到 p 和 q。

根据 4.5 中公式，得到

$$
\begin{aligned}
x_1 &\equiv u \times q \times q^* + v \times p \times p^* \bmod n \\
x_1' &\equiv -u \times q \times q^* - v \times p \times p^* \bmod n \\
x_2 &\equiv -u \times q \times q^* + v \times p \times p^* \bmod n \\
x_2' &\equiv u \times q \times q^* - v \times p \times p^* \bmod n
\end{aligned}
$$

其中 $u \equiv PW_i^{(a)^{\frac{p+1}{4}}} \bmod p$，$v \equiv PW_i^{(a)^{\frac{q+1}{4}}} \bmod q$，$p^* \equiv p^{-1} \bmod q$，$q^* \equiv q^{-1} \bmod p$。然后有

$$
\begin{cases} x_1 \bmod p \equiv u \bmod p \\ x_1 \bmod q \equiv v \bmod p \end{cases}
$$

$$
\begin{cases} x_1' \bmod p \equiv -u \bmod p \\ x_1' \bmod q \equiv -v \bmod p \end{cases}
$$

$$
\begin{cases} x_2 \bmod p \equiv -u \bmod p \\ x_2 \bmod q \equiv v \bmod p \end{cases}
$$

$$
\begin{cases} x_2' \bmod p \equiv u \bmod p \\ x_2' \bmod q \equiv -v \bmod p \end{cases}
$$

因此，如果已知 x_1 和 x_1'，有

$$x_1 + x_1' \equiv 0 \bmod p$$

$$x_1 + x_1' \equiv 0 \bmod q$$

这意味着 $p \mid x_1 + x_1'$ 和 $q \mid x_1 + x_1'$。但是，已知 $x_1' \equiv (n - x_1) \bmod n$，因此，$\gcd(x_1 + x_1', n) = n$。无法在多项式时间内通过寻找最大公约数对 n 因式分解。

(2) 性能评价

在本节，将对本算法的计算负担做出分析，对于每个 TK，计算量分为三个阶段，注册阶段，登录阶段，验证阶段，见表一。根据文献[6]中的分析，计算哈希函数和对称密钥加密所需时间只是公开签名密钥加密的 $\frac{1}{1000}$ 和 $\frac{1}{10000}$。并且本算法对客户端的计算能力要求很小，即使在手机上也可以实现。

表 1 每个 TK 的计算时间

阶段	注册阶段		登录阶段		验证阶段	
	用户	SP	用户	SP	用户	SP
模指数	0	0	0	0	0	2
模乘法	0	1	0	0	0	0
哈希函数	0	1	1	0	0	8
对称密钥	0	1	1	0	0	8

(下转第63页)

(上接第125页)

5 结论

本文所提出的一种基于密码的身份认证方法，与其他基于密码的身份认证不同，具有失效次数和失效时间两个特性，应用本方法验证用户合法身份不需要存储任何密码表和验证表，服务端只需要存储密钥对(p,q)，每个客户存储用户/密码对(ID,PW)和购买的TKs。通过实验检验，本方法具有稳定的安全性，计算哈希函数和对称密钥加密所需时间只是公开签名密钥加密的和。因此可广泛用于电子商务中以服务次数计费的场合。另外，本方法应用二次剩余理论建立的身份认证算法对客户端的计算能力要求很小，可以应用在手机等移动设备上。

参考文献

1 Ku WC, Chen SM. Weaknesses and improvements of an efficient passwordbased user authentication scheme using smart cards. IEEE Trans. Consumer Electronic, 2004,50(1):204 –207.

2 Nam J, Lee Y, Kim S, Merkle DWC. Security weakness in a three-party pairing-based protocol for password authenticated key exchange. Information Sciences, 2007,177 (6):1364 – 1375.

3 Furkan Tari, Ant Ozok A, Stephen H. Holden, A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. Proceedings of the second symposium on Usable Privacy and Security, 2006. 56 – 66 .

4 Lu EJL, Huang CJ. A time-stamping proxy signature scheme using time-stamping service. International Journal of Network Security, 2006, 2 (1):43 – 51.

5 Hwang MS, Li LH. A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 2000,46 (1):28 – 30.

6 Yasinsac A, Childs J, Formal analysis of modern security protocols. Information Sciences, 2005,171 (1–3):189 – 211.