

对一种基于口令和时间限制的用户身份认证协议的改进

叶俊, 付宇

(四川理工学院理学院, 四川 自贡 643000)

摘要:电子商务的应用越来越广泛, 高效且安全的电子商务协议研究是近期研究的热点。对 Luon - Chang Lin 等提出的基于口令和时间限制的用户身份认证的电子商务应用协议进行了分析。此协议的口令计算是基于模平方根难解问题的, 但是此阶段的方案存在漏洞并且运算效率低。对此提出了基于 Hash 链的改进方案, 并且对新方案进行了安全性分析, 此方案解决了原方案方案的漏洞并且比原方案中的方案更加高效和安全。

关键词:协议; hash 函数; 安全

中图分类号: TP309

文献标识码: A

引言

电子商务的应用越来越广泛, 如何保证电子商务的安全性和提高其效率是近年来研究的热点。在电子商务中, 身份认证^[14]是一个很重要的环节, 在此方面已经有许多文献进行了研究, 许多基于口令的用户身份认证协议已经提出^[5-9]。文献[7]给出了一种基于口令和时间限制的可计数的用户身份认证协议, 此协议基于模平方根的难解问题, 但是在协议的运算效率很低。因此, 本文提出了一种基于 Hash 链的改进方法, 从而提高了其效率。

1 Hash 链^[10-12]简介

密码学中的 Hash 函数是一个压缩函数, 它将任意长度的消息压缩成固定长度的比特串。Hash 函数需要满足以下 3 个性质:

(1) 给定一个 hash 值 h , 要找到一个 x 使得 $H(x) = h$ 在计算上是不可行的。

(2) 给定一个 x , 要找到一个 $y, y \neq x$ 使得 $H(x) = H(y)$ 在计算上是不可行的。

(3) 找到 2 个不同的消息 x 和 y 使得 $H(x) = H(y)$ 在计算上是不可行的。

Hash 链是由一个公开的密码学 Hash 函数 h 进行递

归运算得到的。随机选取一个种子值 s , 令 $x_0 = s$, 在此基础上创建一条长为 $n + 1$ 的 Hash 链: $x_i = h(x_{i-1}), i = 1, 2, \dots, n$ 。

2 文献[7]用户口令方案重述

设 j 表示用户在允许的 t 次登陆机会中尚未登录次数, TK_j 为表示第 $(t - j + 1)$ 次登陆所需要的信息, $TK_j: \{TID_j, ED_j, \alpha_j\}$, t 为预先给定的允许用户 U_i 登录系统的次数, 系统计算

$$PW_i^{(j)} \equiv r_i^{2^j} \equiv (r_i^{2^{j-1}})^2 \pmod{n}$$

$$\alpha_j = MAC_p(ID_i \| TID_j \| ED_j \| PW_i^{(j-1)})$$

$$j = 1, 2, \dots, t$$

这里 $\|$ 表示将两块数据连接到一起, TID_j 表示 TK_j 的序列号, ED_j 表示 TK_j 的过期时间, $PW_i^{(j)}$ 为用户第 $(t - j + 1)$ 次登陆系统的口令, $MAC_p(\cdot)$ 表示生成消息认证码并且用 p 作为密钥用 DES 或者 FEAL 对消息认证码进行加密。

系统将 $ID_i, TK_1, TK_2, \dots, TK_t$ 和 $PW_i^{(t)}$ 发送给用户 U_i 。

若用户 U_i 登录成功, 将使得第(7)步成立的 $R_a^{(j)}$ 作为下一次用户登录的口令 $PW_i^{(a-1)}$ 发送给用户。

3 对文献[7]中协议的分析

文献[7]中协议是建立在模平方根难解的基础之上的,并且是运用到电子商务中。但是由上述协议可知,在身份认证阶段的第(5)步,需要计算模平方根 $x^2 = PW_i^{(a)} \bmod n$,但是在实际运算中,计算模平方根的效率很低。并且模平方根可能出现循环的现象。例如,

$$7^2 = 18 \bmod 31, 18^2 = 14 \bmod 31$$

$$14^2 = 10 \bmod 31, 10^2 = 7 \bmod 31$$

而用户的下一次登陆口令为上一次口令的模平方根,这样口令可能出现循环,一旦出现循环用户就可以提前知道下一次的口令。系统存在一定的漏洞。

为了填补此漏洞并且提高运作的效率,本文提出了以下的基于 Hash 链的改进方案。

4 对文献[7]中协议的改进

4.1 注册阶段

(1)对于用户 U_i ,系统随机选择 m 组数据 $r_j = (x_j, y_j) (j = 1, 2, \dots, m)$,经过这 m 个点 $(x_1, y_1), (x_2, y_2), \dots, (x_m, y_m)$ 构造 $m-1$ 次插值多项式 $A(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1}$,使之满足 $y_j = A(x_j) (1 \leq j \leq m)$,则 $A(x)$ 的系数为 $(a_0, a_1, \dots, a_{m-1})$; 然后令 $r_i = a_0 \| a_1 \| \dots \| a_{m-1}$, ($\|$ 表示连接符),这就是系统生成的随机数 r_i ;

(2)计算用户口令

$$PW_i^{(j)} = h^j(r_i)$$

并且保存(其中 $h(\cdot)$ 为一 Hash 函数, h^j 表示连续用 Hash 函数作用 j 次);

(3)系统计算

$$\alpha_j = MAC_{r_i}(ID_i \| TID_j \| ED_j \| PW_i^{(j-1)})$$

$$j = 1, 2, \dots, t$$

(4)系统将 $ID_i, TK_1, TK_2, \dots, TK_t$ 和 $PW_i^{(1)}$ 发送给用户 U_i , 其中 TK_j 包含信息 $\{TID_j, ED_j, \alpha_j\}$ 。

4.2 登录阶段

(1)用户 U_i 从授时中心获取当前时间 TS ;

(2)用户 U_i 计算 $\beta_a = MAC_{\alpha_a}(ID_i \| TS)$;

(3) U_i 将 $ID_i, PW_i^{(a)}, TID_a, ED_a, TS$ 和 β_a 以及登录请求发送给系统。

4.3 身份认证阶段

(1)设系统收到用户的登录请求时间为 TS' , 此时系统计算是否有 $TS' - TS > \Delta TS$, 其中 ΔTS 为系统预先设定的所允许的用户发送登录请求和系统接收到用户登录请求的时间差。若 $TS' - TS > \Delta TS$ 成立,则系统拒绝用户请求;

(2)系统验证 ID_i 与 TID_a 是否匹配,若不匹配的拒绝请求;

(3)系统验证 TID_a 是否过期,若过期则拒绝请求;

(4)系统验证是否 $TS < ED_a$, 若不成立,则拒绝服务;

(5)系统验证 $\beta_a = MAC_{\alpha_a}(ID_i \| TS)$ 是否成立,若不成立,则拒绝服务;

(6)若(1)~(5)均验证通过则用户 U_i 登录成功,这时将 $h^{i-1}(r_i)$ 作为下一次的口令 $PW_i^{(a-1)}$ 发送给用户。

5 改进方案的安全性和效率分析

(1)新方案的对抗重复登录的攻击和防止修改 TK_j 的有效时间攻击强度与原方案的安全性一样。

(2) r_i 是由系统产生 m 组随机数,然后将这 m 组随机数联合起来生成的一个新的随机数,攻击者想去猜测 r_i 是不可能的;

(3) $PW_i^{(j)} = h^j(r_i)$, 实际形成一 Hash 链,则每次的口令是不同的,且不知道 r_i 是得不到每次登录的口令的,由于 Hash 函数是一个单向函数,知道前一次的口令想得到下一次的口令,在计算上是不可行的;

(4)文献[7]中基于模平方根的难解问题,其运算速度慢,而改进的方案中使用的是 Hash 函数,计算速度明显比计算模平方根更快。方案的比较见表 1。

表 1 运算效率的比较

	文献[7]	本方案
模指数运算(次)	n	0
模平方根运算(次)	n	0
Hash 函数运算(次)	0	n

6 结论

在电子商务中安全和效率都是很重要的,要在安全的前提下提高效率。本文对文献[7]的协议进行分析,该协议是基于模平方根难解问题的。根据原协议的算法,虽然攻击者几乎不可能计算得到模平方根,但是其运算效率低。本文提出了基于 hash 函数的改进方案,并且对安全性进行了分析,可以看出新的方案比原文献中的方案更加高效和安全。

参考文献:

- [1] Kyungah Shim. Efficient identity-based authenticated key agreement protocol based on Weil pairing[J]. IEEE Electronics Letters, 2003, 39(8): 653-654.
- [2] 肖文, 王移芝, 沈旭昆. 基于 ECC 的 PostgreSQL 口令认证的研究与改进[J]. 计算机工程与设计, 2009, 30

- (7):1603-1604.
- [3] 张利华,章丽萍,张有光,等.基于口令的远程身份认证及密钥协商协议[J].计算机应用,2009,29(4):924-927.
- [4] 朱月珍.基于身份认证的网上证券交易系统的安全性研究[J].计算机应用与软件,2009,6(4):269-270.
- [5] Lee W B,Wu C C,Tsaur W J.A novel deniable authentication protocol using generalized Elgamal signature scheme[J].Information Sciences2007,177(6):1376-1381.
- [6] 雷文,赵攀,张弘.一种动态口令认证方案的研究与改进[J].四川理工学院学报:自然科学版,2009,22(5):47-50.
- [7] Lin Iuon-Chang,Chang Chin-Chen.A countable and time-bound password-based user authentication scheme for the applications of electronic commerce[J].Information Sciences,2009,179(9):1269-1277.
- [8] Nam J,Lee Y,Kim S,et al.Security weakness in a three-party pairing-based protocol for password authenticated key exchange[J]. Information Sciences, 2007, 177 (6): 1364-1375.
- [9] 郑丽萍,易虹.一种PKI体系下的私钥安全存取方案[J].四川理工学院学报:自然科学版,2011,24(1):62-65.
- [10] 贺蕾,甘勇,李娜娜,等.一种基于逆hash链的RFID安全协议[J].计算机应用与软件,2009,26(2):87-88.
- [11] 李章林,卢桂章,辛运伟.基于Hash链的可扩展RFID验证协议[J].计算机工程,2008,34(2):173-175.
- [12] 孟健,杨阳.基于PayWord的自更新Hash链微支付协议[J].计算机工程,2009,35(3):63-65.

Improvement of Time-bound and Password-based User Authentication Protocol

YE Jun, FU Yu

(School of Science, Sichuan University of Science & Engineering, Zigong 643000, China)

Abstract: Electronic commerce is widely used now, and the resent research focus on the efficiency and security of electronic commerce protocols. A countable and time-bound password-based user authentication scheme for the electronic commerce promoted by Iuon-Chang Lin and Chin-Chen Chang is discussed. User's password of the protocols is based on the hard problem modular square root. However, there's a bug in this scheme, and the efficiency of the scheme is low. A new scheme based upon Hash chain is advanced, and its security is discussed. The new scheme has solved the bug in the original scheme, and it is more efficient and safer.

Key words: protocols; hash chain; security