基于时戳的口令鉴别方案的改进

亓文华 张其善 刘建伟

(北京航空航天大学 电子信息工程学院, 北京 100083)

摘 要: 对 Yang和 Shieh提出的一种基于时戳的口令鉴别的方案进行了安全性分析,指出其方案存在初始化阶段需要把用户口令交给 KIC(Key Information Center)和用户不能验证 KIC身份的缺点。在此基础上提出的新方案对注册、登录、验证和口令修改过程都做了改造,用户在注册阶段提交基于口令的单向运算值而不是口令本身,并且用户和 KIC之间共享秘密信息,从而成功克服了原有方案的缺陷。用户提交口令单向运算值在验证效果上和提交口令本身是相同的,而且避免了口令泄露;用户和 KIC之间共享的秘密信息可以使用户验证 KIC的身份。新方案可以有效抵抗伪造攻击,即使服务器被攻破或内部人泄露信息也不会造成用户私人信息的泄露,具有比原方案更高的安全性。

关 键 词: 智能卡; 身份鉴别; 时戳; 伪造攻击

中图分类号: TN 918

文献标识码: A 文 章 编 号: 1001-5965(2007)05-0577-03

Enhancement of a timestamp-based password authentication scheme

Qi Wenhua Zhang Qishan Liu Jianwei

(School of Electronics and Information Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

Abstract: Yang and Shieh have proposed a timestamp-based password authentication scheme using smart card. The weakness of Yang and Shieh's scheme is submitting password in plaintext and not authenticating key information center(KIC) by user. The new scheme improved the process of registration, login, authentication and update password. The user submitted the password's hash value instead of the password's plaintext, and shared the secret information with the KIC. Submitting the password's hash value is the same as password in authentication, and avoiding the password's exposure. With the secret information, the user can authenticate the KIC. The new scheme can overcome all of the above vulnerabilities, can resist the forged login attack and never revel the privacy of user even if the server is attacked.

Key words: smart card; authentication; timestamp-based; forged login attack

1999年, Yang和 Shieh在文献[1]中介绍了一种利用智能卡并基于时戳的口令鉴别方案. 在此方案中用户可以自由地选择和更改口令,并且服务器也不需要存储用户的口令表. 但在 2002年, Chan和 Fan分别在文献[2-3]中指出针对 Yang-Shieh方案的伪造攻击方案. 2004年 Wang和 Li在文献[4]中对 Yang-Shieh方案的安全性做了进一步的改进. 在 Yang-Shieh方案中,用户在注册时需要把口令提交给密钥信息中心(KIC, Key Information Center). 如果用户在许多地方都使用同一口令的话,这会泄露用户的私人信息. Yang-Shieh方案在验证阶段,只有 KIC验证用户的过程,而没有用户验证 KIC的过程,这就容易伪造一个 KIC,造成中间人攻击. 针对 Yang-Shieh验证方案中存在的缺陷,本文提出了一种新的基于智能卡的改进的身份验证方案. 该方案可以有效抵抗伪造攻击,并且即使 KIC被攻破或内部人泄露信息也不会造成用户私人信息的泄露,所以新的方案比原方案具有更高的安全性.

收稿日期: 2006-06-26

作者简介: 亓文华(1977-),男,山东莱芜人,博士生, qiwenhua@263.net

1 Yang-Shieh方案

Yang-Shieh的方案分为三个阶段: 注册、登录和验证. 其详细过程如下.

1.1 注册阶段

当一个新用户 U_i 想要注册到 KIC时, 把自己的 ID号 I_{idi}和个人口令 I_{pwi}通过安全的通道送到 KIC, 然后 KIC执行下列的操作:

1) 产生两个大素数 p和 q并计算 $n=p\times q$.

2) 选择一个素数 e和一个整数 d, 使其满足 $e\cdot d=1\bmod(p-1)(q-1)$.

3) 找到一个整数 g, 使其为 GF(p)和 GF(q)的素元.

4) 计算用户的安全信息 S_i

$$S_i=(I_{idi})^d \bmod n \tag{1}$$

5) 产生用户 U_i的智能卡标识 I_{cidi}

$I_{cidi}=f(I_{idi}, d)$, 其中 $f(x, y)$为单向函数.

6) 计算 H_i

$$H_i=g^{I_{pwi}\times d}\bmod n \tag{2}$$

n, e和 g公开, p, q和 d由 KIC安全保存, KIC把 n, e, g, I_{idi}, I_{cidi}, S_i, H_i存入用户 U_i的智能卡中.

1.2 登录阶段

当用户 U_i想登录到 KIC时, 他把智能卡插入到智能卡读写器中, 并且输入自己的 I_{idi}和个人口令 I_{pwi}. 如果 I_{idi}与存储在智能卡中的相同, 则智能卡执行下列的操作:

1) 产生一个随机数并且计算下列两个整数:

$$X_i=g^{I_{pwi}\times r_i}\bmod n \tag{3}$$

$$Y_i=S_i\times h_i^{f(I_{cidi}, T)\times r_i}\bmod n \tag{4}$$

其中 T是当前的时戳.

2) 用户发送登录请求信息 $M=\{I_{idi}, I_{cidi}, X_i, Y_i, n, e, g, T\}$到 KIC.

1.3 验证过程

假设 KIC在 T'接收到用户的登录请示信息 M, KIC执行下列操作验证登录信息的正确性.

1) 验证 I_{idi}是否为一个合法的用户, I_{cidi}是否为一个合法的智能卡标识. 如果不是, 则登录请求被拒绝.

2) 如果 $(T'-T\geqslant)\ \Delta T$, (ΔT表示允许的最大传输延时), 则拒绝用户登录请求.

3) 检查下面等式是否成立

$$Y_i^e=I_{idi}\times X_i^{f(I_{cidi}, T)}\ (\bmod n) \tag{5}$$

如果等式成立, 则登录请求被接受, 否则拒绝登录请求.

下面简要介绍 Chan在文献 [2]中指出的 Yang-Shieh方案的缺陷, 主要思想是一个攻击者可以利用截获的用户与 KIC之间的通信信息来进行登录. 其攻击方案如下:

1) 找到一个值 a满足:

$$a\times f(I_{cidi}, T_g')=f(I_{cidi}, T) \tag{6}$$

其中 T_g'为攻击者的时戳.

2) 计算 X_i'

$$X_i'=(X_i)^a=g^{I_{pwi}\times r_i\times a}\bmod n \tag{7}$$

3) 一个伪造攻击登录请求消息为

$$M'=\{I_{idi}, I_{cidi}, X_i', Y_i, n, e, g, T_g'\}$$

在登录信息验证阶段, KIC接收到 M', 验证 I_{idi}, I_{cidi}和 T_g'. 通过后再验证式 (5)是否成立, 即

$$I_{idi}\times X_i^{f(I_{cidi}, T_g')}\ (\bmod n)=$$
$$I_{idi}\times X_i^{af(I_{cidi}, T_g')}\ (\bmod n)=$$
$$I_{idi}\times X_i^{f(I_{cidi}, T)}\ (\bmod n)$$

所以等式 $Y_i^e=I_{idi}\times X_i^{f(I_{cidi}, T_g')}\ (\bmod n)$成立.

所以登录请求信息 M'能通过系统的验证.

针对 Yang-Shieh的方案不能抗伪造攻击、在注册阶段需要把用户口令交给 KIC和用户不能验证 KIC的弱点, 结合文献 [5-6]的思想, 本文提出了一种新的改进方案.

2 改进的方案

本文提出的方案分为四个阶段: 注册、登录、验证、修改口令.

2.1 注册阶段

当一个用户 U_i要注册到系统时, 把自己的 I_{idi}和 $f(I_{pwi}, I_{idi})$通过安全通道送到 KIC, 接着 KIC执行如下操作:

1) 产生两个大素数 p和 q并计算 $n=p\times q$.

2) 选择一个素数 e和一个整数 d, 使其满足 $e\cdot d=1\bmod(p-1)(q-1)$.

3) 计算 $A_i=f(I_{idi}, s)$, $R_i=A_i\oplus f(I_{pwi}, I_{idi})$这里 s为 KIC的秘密信息. 其中 n, e为公开数据, p, q, d, s为 KIC的秘密信息, 由 KIC安全保存. KIC把 n, e, S_i, I_{idi}, R_i, A_i存储到用户的智能卡中.

2.2 登录阶段

当用户想要登录到系统时, 把智能卡插入到智能卡读写器中, 并且输入自己的 I_{idi}和 I_{pwi}^*. 如果 I_{idi}与存储在智能卡中的相同, 则智能卡执行下列操作:

1) 产生一个随机数 r, 并计算

$$X_i=r^e\bmod n \tag{8}$$

2) 计算

$$V_i=f(I_{pwi}^*, I_{idi})\oplus R_i \tag{9}$$

3) 计算

$$Y_i = V_i^{f(s,T)} \pmod n \quad (10)$$

4) 传送登录请示 $M = \{I_{idi}, Y_i, X_i, T\}$ 到系统.

2.3 验证阶段

假设 KIC在 T'时接收到用户的登录请示信息 M, KIC执行下列操作来验证登录信息的正确性.

1) 验证 I_{idi}是否为一个合法的用户, 如果不是, 则登录请求被拒绝.

2) 如果 $(T' - T) \geqslant \Delta T$, (ΔT 表示允许的最大传输延时), 则拒绝用户登录请求.

3) 计算 $V_i' = f(I_{idi}, s)$ 和 $r' = X_i^d \bmod n$.

4) 下面的等式是否成立:

$$Y_i = V_i^{f(r', T)} \pmod n \quad (11)$$

如果成立, 则系统验证了用户; 如果不成立, 则拒绝登录请求.

5) KIC取当前时间 T''计算 $A = f(V_i', T'')$, 并把 $M_1 = \{A, T''\}$ 回送给用户.

6) 用户接收到 KIC送回的信息 M_1后, 如果 $(T'' - T') \geqslant \Delta T$, 则退出登录请求.

7) 验证 $A = f(V_i, T'')$是否成立, 如果成立, 则用户验证了 KIC, 否则退出登录请求.

2.4 修改口令阶段

当用户想要修改个人口令时, 插入智能卡到智能卡读写器, 输入个人的 I_{idi}和旧的个人口令 I_{pwi}^*, 如果 I_{idi}与存储在智能卡中的相同, 则智能卡执行下列操作:

1) 计算 $R_i \oplus A_i = f(I_{idi}, I_{pwi}^*)$是否正确, 如果不正确, 则认为输入的个人口令错误, 退出修改密钥过程.

2) 用户输入新口令 I_{pwnew}, 计算 $R_i = A_i \oplus f(I_{pwi}, I_{idi}) \oplus f(I_{pwi}, I_{idi}) \oplus f(I_{pwnew}, I_{idi})$, 修改口令过程结束.

3 安全性分析

1) 此方案的安全性建立在大数模幂乘算法的基础上, 而大数模幂乘算法被认为是安全的.

2) 伪造登录信息来欺骗 KIC时, 攻击者发送登录信息 $M = \{I_{idi}, Y_i, X_i, T\}$, 其中 T为攻击者的时间, I_{idi}为一个合法的用户 ID号. 攻击者可以通过 2.3节所描述的登录验证阶段中步骤 1)、2)的验证. 在步骤 4)时, 由于 KIC计算的 $Y_i^* = V_i^{f(r', T)} \pmod n$, 而 $V_i' = f(I_{idi}, s)$, $r' = X_i^d \bmod n$, 由于攻击者不知道 s, 所以 $Y_i^* \neq Y_i$, KIC因此拒绝攻击者的登录请求, 攻击失败.

3) 当攻击者通过向用户发送伪造的 $M_1 = \{A, T''\}$来欺骗用户时, 由于 $V_i = f(I_{idi}, s)$, $A = f(V_i, T'')$, 攻击者不知道 KIC的 s, 在验证过程的第 7)步用户检查 $A \neq f(V_i, T'')$, 退出登录请求, 攻击失败.

4) 在注册阶段, 当一个用户 U_i要注册到系统时, 把自己的 I_{idi}和 $f(I_{pwi}, I_{idi})$ ($f(x, y)$为一个单向函数, I_{pwi}为个人口令) 通过安全的通道送到 KIC, 由于用户 U_i提交给 KIC的是 $f(I_{pwi}, I_{idi})$, 而不是 I_{pwi}, 所以即使 KIC被攻破或内部人泄露信息, 也不会造成用户私人信息的泄露.

4 结束语

本文通过分析 Yang-Shieh口令鉴别方案得到此方案的安全性缺陷. 其安全缺陷包括无法抗伪造攻击的缺陷和在注册阶段需要把个人用户信息提供给 KIC的缺陷. 在此基础上, 本文提出改进方案, 新的方案在注册、登录、验证和修改口令四个阶段都做了改进. 分析表明, 新方案可以有效抵抗伪造攻击, 攻击者所截获的信息对认证来说都是不完备的, 并且即使 KIC被攻破或内部人泄露信息也不会造成用户私人信息的泄露. 新的方案具有比原方案更高的安全性.

参考文献 (References)

[1] Yang W H, Shieh S P. Password authentication schemes with smart cards[J]. Computers& Security, 1999, 18(8): 727-733

[2] Chan C K, Cheng L M. Cryptanalysis of a timestamp-based password authentication scheme[J]. Computer & Security, 2002, 21(1): 74-76

[3] Fan L, Li J H, Zhu H W. An enhancement of timestamp-based password authentication scheme[J]. Computer & Security, 2002, 21(7): 655-667

[4] Wang Y J, Li J H. Security improvement on a timestamp-based password authentication scheme[J]. IEEE Transaction on Consumer Electronics, 2004, 50(2): 580-582

[5] Ku W C, Chen S M. Weaknesses and improvements of an efficient password based user authentication scheme using smart cards[J]. IEEE Transaction on Consumer Electronics, 2004, 50(1): 204-207

[6] Yoon E J, Ryu E K, Yoo K Y. Further improvement of an efficient password based remote user authentication scheme using smart cards[J]. IEEE Transaction on Consumer Electronics, 2004, 50(2): 612-614

[7] Shieh W G, Wang J M. Efficient remote mutual authentication and key agreement[J]. Computers& Security, 2006, 25(1): 72-77

(责任编辑: 娄　嘉)