对 Liao 等人身份鉴别方案的分析与改进

潘春兰[1],周安民[1],肖丰霞[2],王书歌[1]
PAN Chun-lan[1],ZHOU An-min[1],XIAO Feng-xia[2],WANG Shu-ge[1]

1.四川大学 电子信息学院 信息安全所,成都 610064
2.山东水利职业学院,山东 日照 276826
1.Information Security Institute,School of Electronics and Information Engineering,Sichuan University,Chengdu 610064,China
2.Shandong Vocational College of Water Conservancy,Rizhao,Shandong 276826,China
E-mail:panchunlan00@163.com

PAN Chun-lan,ZHOU An-min,XIAO Feng-xia,et al.Improved remote user authentication scheme.Computer Engineering and Applications,2010,46(4):110-112.

Abstract: Smart card-based authentication is a two-factor authentication mechanism,which is widely used for remote user authentication.In 2006,Liao et al proposed a smart card-based authentication.Based on the modern studies,the safety flaws of Liao et al's program are pointed out.And then an improved authentication scheme based on smart card is proposed.The improved program not only maintains the advantages of the Liao et al's program,but also performs better among efficiency,security and flexibility.
Key words: authentication;two-factor;safety flaws

摘 要:基于智能卡的身份鉴别是一种双因子鉴别,被广泛应用于鉴别远程用户的身份。2006 年,Liao 等人提出了一种基于智能卡的身份鉴别方案。在目前身份鉴别研究的基础上,分析指出了 Liao 等人方案存在的安全漏洞,并对方案作了改进,改进后的方案不仅保持了 Liao 等人方案的优点,而且极大地增强了系统的高效性、安全性和实用性。
关键词:身份鉴别;双因子;安全漏洞
DOI:10.3778/j.issn.1002-8331.2010.04.035 **文章编号**:1002-8331(2010)04-0110-03 **文献标识码**:A **中图分类号**:TP393.08

身份鉴别用于实现网络通信方的身份的互相验证,在网络安全中占据十分重要的位置。因为智能卡在金融、医疗、交通以及教育领域的广泛应用,而且可以身兼数职,满足了大众化信息处理的要求,所以基于智能卡的身份认证技术是具有广泛应用前景的一种强力身份认证技术[1]。

1999 年,Yang 和 Shieh[2]提出了一种利用智能卡实现基于时间戳的远程身份鉴别方案,在方案中,用户可以任意选择和改变口令,而远端服务器不需要存储口令或验证表就可以执行用户鉴别, 验证阶段用到的所有元素都由用户方产生和提供。在后来的研究中[3-4],人们发现该方案存在安全脆弱性,容易受到非法登录攻击。2003 年,Shen、Lin 和 Hwang[4]在其基础上提出了一种可抗非法登录攻击的改进方案。随后,又出现了一系列的改进方案。其中,2005 年,Lee-Chiu[5]指出 Wu-Chieu[6]的方案中存在安全隐患,并做了改进。到 2006 年,Liao 等人在前人研究的基础上, 也提出了一种用户可以自由选择和更改口令,能够抵抗非法登录攻击的身份鉴别方案[7]。

该文对 Liao 等人方案的鉴别原理和安全性做了详细分析,指出 Liao 等人方案易于遭受口令猜测攻击、假冒攻击和拒绝服务器攻击等,并结合现代身份鉴别方案的新发展对其进行了改进,提出了一种高效安全的鉴别方案。

1 Liao 等人方案

1.1 对 Liao 等人方案的回顾

为方便叙述,对文中用到的符号和标识作如下说明:

C,S: 分别表示客户端和远程服务器端;
U: 表示用户;
SC: 表示智能卡;
ID,PW: 分别表示用户身份标识符和登录口令;
x: 服务器固定密钥;
$h(\cdot)$: 表示散列运算,如 SHA-1 算法;
$\oplus,\|$: 分别代表异或运算符和连接操作符;
$\Rightarrow$: 安全通信信道;
$\rightarrow$: 普通通信信道;
P: 是一个大素数;
g: 是有限域 $GF(P)$上的本原元。

作者简介:潘春兰(1983-),女,在读硕士研究生,研究方向为网络与信息系统安全;周安民(1963-),男,研究员,四川大学电子信息学院信息安全工程系主任和信息安全研究所总工程师,科研方向为信息安全体系、关键技术和产品的研究、开发;肖丰霞(1982-),女,教师;王书歌(1984-),女,在读硕士研究生,研究方向为网络与信息系统安全。
收稿日期:2008-08-12 **修回日期**:2009-12-11

1.1.1 注册阶段

在此阶段,服务器 S 选择一个大素数 P,其中 g 是有限域上的本原元。

(1)$U\Rightarrow S:ID,h(PW)$

用户自由选择登录口令 PW 和随机数 r,计算 $h(r\oplus PW)$,发送 ID 和 $h(r\oplus PW)$给 S 请求注册。

(2)$S\Rightarrow U:SC\{ID,M,P\}$

S 计算 $M=g^{h(x\|ID)+h(PW)}(\mathrm{mod}\ p)$,将包含信息$\{ID,M,P\}$的智能卡 SC 签发给用户。

1.1.2 登录阶段

(1)U 把 SC 插入读卡器,输入 ID 和 PW。

(2)$SC\rightarrow S:\{ID\}$

SC 发送信息$\{ID\}$给 S 请求登录。

(3)$S\rightarrow SC:\{h(M''),R\}$

S 自动生成一随机数 R,计算 $M''=g^{h(x\|ID)R}(\mathrm{mod}\ p)$,$h(M'')$,发送信息$\{h(M''),R\}$给 SC。

(4)$SC\rightarrow S:\{ID,V,T_U\}$

SC 计算 $M'=(Mg^{-h(PW)})^R(\mathrm{mod}\ p)$,比较 $h(M'')?=h(M')$,如果不相等,拒绝登录请求,否则 SC 计算 $V=h(T_U\|M')$,其中 T_U 是客户端当前时间戳,发送信息$\{ID,V,T_U\}$给 S。

1.1.3 鉴别阶段

(1)S 验证 ID 和 T_U:若 ID 的格式非法或者 $T_U=T_S$ 或者 $T_S-T_U>\Delta T$(其中 T_S 为服务器的当前时间戳),S 拒绝用户的登录请求。ΔT 表示由传输延迟产生的可以接受的最大时间间隔。

(2)$S\rightarrow U:\{M_3,T_S\}$

S 计算 $V'=h(T_U\|M'')$,比较 $V'?=V$。若不相等,S 终止本次会话;否则,S 通过对 U 的身份鉴别。

1.1.4 口令更改阶段

U 想要将原来口令 PW 更改成新口令 PW_{new} 时,须进行下列操作。

(1)智能卡计算 $c_1=g^{h(PW_{new})}(\mathrm{mod}\ p)$,$c_2=Mg^{-h(PW)}(\mathrm{mod}\ p)$,$M^*=c_1*c_2$。

(2)智能卡将 M^* 存入智能卡,完成口令更改。

1.2 对 Liao 等人方案的脆弱性分析

(1)口令猜测攻击和假冒攻击

Liao 等人的方案在注册阶段以后,智能卡中包含$\{ID,M,P\}$的信息。假设用户的智能卡丢失,攻击者会通过能量分析攻击(Differential Power Analysis)[8]可以获取任何数据值,进而实施口令猜测攻击。攻击者将尝试所有可能的口令 PW',直到找到正确的口令使得 $M'=g^{h(x\|ID)+h(PW')}(\mathrm{mod}\ p)$成立。一旦得到正确的口令,攻击者就可以通过伪造验证信息 $h(M'')$来假冒用户。因此,Lee-Chiu 的方案易于遭受口令猜测攻击和假冒用户攻击。

此外,Liao 等人的方案只提供了服务器对用户的单向身份鉴别,并没有提供用户对服务器的身份鉴别。所以对于 Liao 等人的方案,攻击者可以假冒服务器来获取用户的数据信息。因此,方案易于遭受假冒服务器攻击。

(2)口令更改的拒绝服务器攻击

在口令更改阶段,假设攻击者偷走了某合法用户 U 的智能卡,将智能卡插入读卡器,并输入任意两个登录口令 PW_m 和 PW_m^* 充当原口令和新口令,请求更改口令。智能卡计算 $c_1=g^{h(PW_m^*)}(\mathrm{mod}\ p)$,$c_2=Mg^{-h(PW_m)}(\mathrm{mod}\ p)$,$M^*=c_1*c_2=g^{h(PW_m^*)}Mg^{-h(PW_m)}(\mathrm{mod}\ p)=g^{h(x\|ID)+h(PW)-h(PW_m)+h(PW_m^*)}$。当智能卡提示输入新口令时,攻击者再提交另一个任意口令,此时智能卡计算 $k_m=k_i\oplus h(PW_m)\oplus h(PW_m^*)=h(K_S)\oplus h(PW_i)\oplus h(PW_m)\oplus h(PW_m^*)$,将 M^* 代替 M。这样,在登录阶段,合法用户 U 不能验证合法的服务器。此外,在鉴别阶段,服务器不会通过对合法用户 U 的身份认证。因此,该方案易于遭受拒绝服务器攻击。

2 改进方案

利用哈希运算代替计算复杂的幂运算,运算开销小;注册登录阶段引入随机数对口令进行了哈希摘要处理,登录信息未包含任何口令信息,口令猜测难度加大;验证阶段,采用了质询响应机制实现了双向鉴别,并引入随机数代替时间戳,避免复杂时间同步问题和重放攻击;用户可以自由选择和更改口令,口令更改不需要服务器的参与,代价较低。

2.1 注册阶段

(1)$U\Rightarrow S:ID\|hpw$

用户 U 自由选择登录口令 PW 和一随机数 r,计算 $hpw=h(PW\oplus r)$通过安全信道向服务器发送 hpw 和 ID 进行注册。

(2)$S\Rightarrow U:SC\{C_1,C_2,h(\cdot)\}$

S 收到注册请求后,自动生成随机数 R,取密钥 x,计算 $C_1=h(ID\|x\|R)\oplus hpw$,$C_2=h(h(ID\oplus x\oplus R)\oplus hpw)$,$S$ 将包含信息$\{C_1,C_2,h(\cdot)\}$的智能卡通过安全信道签发给用户。

(3)S 将 R、ID 写入注册用户数据库。

(4)U 将 r 写入智能卡,无需记住 r。

2.2 登录阶段

(1)$U\rightarrow SC:ID\|PW$

用户 U 要登录到服务器 S,把智能卡插入终端,提交身份 ID 和口令 PW。

(2)$SC\rightarrow S:\{ID\}$

智能卡 SC 首先判断用户 U 的合法性。SC 取出 r,计算 $hpw^*=h(PW\oplus r)$,$k=C_1\oplus hpw^*$,$C_2^*=h(k\oplus hpw^*)$,判断 $C_2^*=?C_2$,若不相等,拒绝发送登录请求;否则,发送$\{ID\}$给 S,请求登录。

2.3 身份鉴别阶段

服务器 S 收到登录请求$\{ID\}$后,服务器 S 和智能卡 SC 会执行下列操作:

(1)$S\rightarrow SC:m_1$

S 根据注册用户数据库验证 ID 的合法性。若不合法,拒绝登录;否则,生成随机数 R_{S1},取出密钥 x 和 R,计算 $k^*=h(ID\|x\|R_i)$,$m_1=k^*\oplus R_{S1}$,发送 m_1 给 SC。

(2)$SC\rightarrow S:\{m_2,m_3\}$

SC 生成随机数 R_U,计算 $m_2=h(h(m_1\oplus k)\oplus R_U)$,$m_3=k\oplus R_U$,发送验证信息$\{m_2,m_3\}$给 S。

(3)$S\rightarrow SC:m_4$

S 计算 $R_U^*=k^*\oplus m_3$,$m_2^*=h(h(R_{S1})\oplus R_U^*)$,比较 $m_2^*?=m_2$,若不相等,S 中止本次会话;否则,S 认为 U 为合法用户,生成随机数 R_{S2},计算 $m_4=h(h(R_U^*)\oplus R_{S2})$,$m_5=k_i^*\oplus R_{S2}$,发送信息$\{m_4,m_5\}$给 SC。

(4)SC 验证 S 的合法性

SC 计算 $R_{S2}^*=k\oplus m_5$,$m_4^*=h(h(R_U)\oplus R_{S2}^*)$,比较 $m_4^*?=m_4$,若 $m_4^*\neq m_4$,放弃本次登录;否则,通过对 S 的身份认证。

2.4 口令更改阶段

如果用户 U 想要更改口令,不需要服务器参与,只需要智能卡完成下列操作:

(1)用户 U 将智能卡插入读卡器,提交其身份 ID 和口令 PW,请求更改口令。

(2)智能卡 SC 首先判断用户身份 ID 的合法性。若 ID 非法,拒绝口令更改请求;否则,SC 取出 r,计算 $hpw^*=h(PW\oplus r)$,$k=C_1\oplus hpw^*$,$C_2^*=h(k\oplus r)$,比较 $C_2^*=?C_2$,如果不相等,拒绝口令更改请求;否则提示用户选择新登录口令 PW_{new}。

(3)智能卡 SC 提交新登录口令 PW_{new},计算 $C_1^*=k\oplus PW_{inew}$,将 C_1^* 写入智能卡代替 C_1 完成口令更改。

3 方案安全性分析

该方案依赖于哈希算法的强度以及安全强度很高的双因子智能卡。

(1)抗口令猜测攻击

在注册阶段,用户自主选择登录口令 PW 和随机数 r,采用 $h(\cdot)$算法对口令和随机数进行消息摘要处理,把处理后的注册信息 hpw 通过安全信道传送给服务器,随后服务器对注册信息同样进行哈希处理后写入智能卡,并通过安全信道签发智能卡给用户,无法实施口令猜测攻击;在登录阶段,智能卡通过对用户的身份验证后,发送{ID}给 S,因不包含任何口令登录信息,不能实施口令猜测攻击;在身份鉴别阶段,假设攻击者截获了身份鉴别信息,基于 HMAC 算法的安全强度,以及引入质询随机数 R_{S1}、R_U、R_{S2} 来保证每次身份鉴别信息的随机性,攻击者也无法获取秘密信息 $k=h(ID\oplus K_s\oplus R)$;此外,用户可以自由更改口令 PW,增加了口令猜测的难度。因此,该方案可以有效抵抗口令猜测攻击。

(2)抗假冒攻击

该方案实现 C-S 之间的双向身份鉴别。在客户端,基于智能卡的身份鉴别是一种双因子鉴别,假设攻击者取得合法用户的智能卡,没有正确的用户标志符 ID 和登录口令 PW_i 也无法假冒合法用户;在服务器端,即使攻击者成功获得注册用户数据库中的信息 ID 和 R,没有服务器密钥 x 也无法计算密钥信息 $k=h(ID\oplus x\oplus R)$来假冒服务器;在身份鉴别过程中,即使攻击者截获身份鉴别信息 m_1 和{m_2,m_3},因为不知道密钥信息 k,无法得到质询随机数 R_U,同时引入 R_{S2},不能伪造鉴别信息 m_4 和 m_5。因此,该方案可以有效抵抗假冒攻击。

(3)抗重放攻击和口令更改的增强

该方案采用质询-响应机制,引入质询随机数 R_{S1}、R_U、R_{S2} 来保证每次身份鉴别信息的随机性。每次进行身份鉴别,服务器端和客户端都要生成随机数作为"质询",要求对方产生对应的"响应",以保证身份鉴别信息的随机性,攻击者无法重放上次进行成功鉴别时的信息,实施重放攻击。

当用户需要更改口令时,插入智能卡并提交 ID 和口令 PW,智能卡需要验证 ID 的合法性及比较 $C_2^*=?C_2$,这就避免了 Liao 等人方案的口令更改缺陷。同时,由于口令更改仅需要智能卡参与即可完成,不需要服务器参与,没有增加计算代价。

4 结语

该方案实现了 C-S 之间的双向身份鉴别,用户可以自由选择和更改口令,可以有效抵抗口令猜测攻击、假冒攻击;在身份鉴别过程中引入质询随机数代替时间戳,即可以保证每次身份鉴别信息的随机性,有效防止重放攻击,又避免了复杂的时间同步问题;此外,方案利用散列运算代替计算难度大且开销很大的幂运算,且口令更改不需要服务器参与,因此,运算代价较低,效率较高。

参考文献:

[1] 斯伦贝谢公司智能卡事业部 Ouvler Piou. 面向电子化未来的智能卡[EB/OL].http://www.cnw.com.cn/issues/2000/47/4720.asp.

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

[3] Fan L,Li J H,Zhu H W.An enhancement of timestamp based password authentication scheme[J].Computers & Security,2002,21(7):665-667.

[4] Shen J J,Lin C W,Hwang M S.Security enhancement for the time-stamp based password authentication scheme using smart cards[J].Computers & Security,2003,22(7).

[5] Lee N Y,Chiu Y C.Improved remote authentication scheme with smart card[J].Computer Standards & Interfaces,2005,27(2):177-180.

[6] Wu S T,Chieu B C.A note on a user friendly remote user authentication scheme with smart cards[J].IEICE Transactions Fundamentals,2004,87-A(8):2180-2181.

[7] Liao I E,Lee C C,Hwang M S.A password authentication scheme over insecure networks[J].J Comput System Sci,2006,72:727-740.

[8] Kocher P,Jaffe J,Jun B.Differential power analysis [C]//Lecture Notes in Computer Science 1666:Proc Advances in Cryptology-CRYPTO'99.Berlin:Springer,1999:388-397.

(上接 42 页)

参考文献:

[1] Kennedy J,Eberhart R.Particle swarm optimization[C]//Proc of IEEE Int Conf on Neural Network,1995.

[2] Clerc M.The swarm and queen:Towards a deterministic and adaptive particle swarm optimization[C]//Proc Congress on Evolutionary,1999:1951-1957.

[3] Sun J.Particle swarm optimization with particles having quantum behavior[C]//Proc 2004 Congress on Evolutionary Computation,2004:325-331.

[4] Sun J.A global search strategy of quantum-behaved particle swarm optimization[C]//Proc 2004 IEEE Conference on Cybernetics and Intelligent Systems,2004.

[5] Ong Y,Keane A,Nair P.Surrogate-assisted coevolutionary search[C]//Proc 9th Int Conf Neural Information Processing,Nov 2002:1140-1145.

[6] Shi Y,Eberhart R.Empirical study of particle swarm optimization[C]//Proc of Congress on Evolutionary Computation,1999:1945-1950.

[7] DeJong K A.An analysis of the behavior of a class of genetic adaptive systems[D].Univ Michigan,AnnArbor,MI,1975.

[8] Cobb H G.Is the genetic algorithm a cooperative learner?[M]//Foundations of Genetic Algorithms.San Mateo,CA:Morgan Kaufmann.

[9] Clearwater S H,Hogg T,Huberman B A.Cooperative problem solving[M]//Computation:The Micro and Macro View.Singapore:World Scientific,1992:33-70.

[10] Southwell R V.Relaxation methods in theoretical physics[M].Oxford,U K:Clarendon Press,1946.