文章编号:1001 - 9081(2005)10 - 2289 - 02

基于智能卡的远程口令认证方案

王 猛, 卢建朱, 李晓峰
(暨南大学 计算机科学系, 广东 广州 510632)
(iamrich@sina.com)

摘 要:提出了一个基于 RSA 系统和智能卡的远程口令认证系统方案。相对于其他方案,本方案的客户端用户可以自由选择口令,并根据需要自己及时更新口令,服务器端不用保存用户的任何认证信息。方案基于成熟的 RSA 密码系统和单向安全的 hash 函数,操作简单,切实可行。

关键词:口令认证;hash 函数;RSA;智能卡
中图分类号: TP393.08 **文献标识码**:A

Remote password authentication scheme based on smart card

WANG Meng, LU Jian-zhu, LI Xiao-feng
(*Department of Computer Science, Jinan University, Guangzhou Guangdong* 510630, *China*)

Abstract: A remote password authentication scheme based on the RSA cryptography and smart card was presented. Compared with other schemes, our scheme has the following advantage: Each user can freely choose his own password and can renew the password himself in time according to the user's need. Any authentication messages for clients are never saved in the servers. It is based on the RSA cryptography and one-way secure hash function, so its realization is simple and reliable.

Key words: password authentication; hash function; RSA; smart card

0 引言

基于口令的认证方式是远程用户认证中最常用的一种技术,但它存在安全问题。基于智能卡的认证方式是一种个人身份识别码(PIN)与智能卡相结合的双因素认证方式,即使 PIN 或智能卡被窃取,用户仍不会被冒充。

在远程口令认证方案的设计中,目前主要有两种方式:1)口令是经服务器端计算后指定给客户端用户的,客户端用户不能够自由选择口令,服务器不需保存用户的任何认证信息;口令的安全性依赖于密钥中心。2)用户口令由自己选择,口令对系统也是保密的,服务器根据用户提交的信息计算保存相应的认证信息;用户认证信息表随着用户的不断加入而增大,耗时的认证信息检索降低了系统的认证效率。

智能卡也称 CPU 卡。基于智能卡的口令认证方案利用智能卡的特性,将一些认证信息保存在智能卡上,根据智能卡和用户的个人身份识别码能鉴别持卡人是否为该卡的合法使用者,增强了系统的安全性,提高了认证的效率。

基于 RSA 密码系统和安全单向的 hash 函数,借助智能卡功能,本文设计了一个安全高效的远程口令认证方案。该方案中,用户口令由用户自己选取,用户能根据需要及时更新口令,且服务器不用保存用户的任何认证信息,提高了系统的安全性和有效性。

1 基于智能卡的远程口令认证方案

基于智能卡的远程口令认证方案中,系统不需存储任何与用户相关的数据,用户验证简单、高效;系统存在一个密钥中心(KC),负责生成系统的公共参数和发放新用户的智能卡;用户口令可由用户自行选择,KC 根据用户的身份标识 ID 和提供的口令 P 计算嵌入智能卡的信息。方案由系统初始化、用户注册、用户登录、系统验证和用户密钥更新五个过程组成。

1.1 系统初始化

根据给定的系统安全参数 l,系统随机选取两个长度为 l 比特的大素数 p 和 q,计算 $n = pq$ 和 $\varphi(n) = (p-1)(q-1)$。H 是一个安全的 hash 函数,g 是有限域 $GF(p)$ 和 $GF(q)$ 的本原元。系统再随机选取一素数 e,计算密钥 d:d 满足 $ed \equiv 1(\mathrm{mod}\varphi(n))$。最后,系统公开系统参数 (n,g,H) 和 KC 的公钥 e,将密钥 d 以专门的安全机制保存在 KC 中,同时销毁 p 和 q。

1.2 用户注册

用户 U_i 选择口令 P_i,然后将 P_i 及其身份标识 ID_i 传送给 KC。在确认 U_i 的有效身份后,KC 计算嵌入 U_i 智能卡的信息:

$$S_i = P_i \oplus H(d \| ID_{KC} \| ID_i) \quad (1)$$

$$h_i = (g^{ID_i})^d \mathrm{mod} n \quad (2)$$

最后,KC 将系统公开参数 (n,g,H)、KC 的公钥 e 和信息 (S_i,h_i) 写入用户 U_i 的智能卡中,然后将智能卡交给用户 U_i。

1.3 用户登录

假设用户 U_i 当前登陆时间为 T。当 U_i 将智能卡插入读卡器、键入其 P_i 时,智能卡随机生成一个整数 r_i,然后按如下方式计算:

$$C_1 = S_i \oplus P_i \quad (3)$$

$$C_2 = C_1 \oplus H(r_i) \quad (4)$$

$$C_3 = h_i^T \oplus H(H(r_i)) \quad (5)$$

然后,向服务器发送 (ID_i,C_2,C_3,T)。

收稿日期:2005 - 04 - 01;**修订日期**:2005 - 06 - 28
基金项目:国家自然科学基金资助项目(60173038);广东省自然科学基金资助项目(010421)
作者简介:王猛(1979 -),男,河南人,硕士研究生,主要研究方向:网络通信与网络安全; 卢建朱(1965 -),男,湖南郴州人,副教授,博士,主要研究方向:多媒体中的数据处理和通信技术、计算机网络安全; 李晓峰(1978 -),男,黑龙江人,硕士研究生,主要研究方向:网络通信与网络安全.

1.4 系统验证

当服务器接收到用户 U_i 发来的消息(ID_i, C_2, C_3, T) 时，记下相应的接收时刻 $\tilde{T}$。服务器按如下方式进行验证：

1）根据给定一个有效时间 ΔT，检查 $\tilde{T}$ 是否满足 $\tilde{T} - T \leqslant \Delta T$。若条件不成立，则登陆失败；

2）计算：

$$\tilde{C}_2 = C_2 \oplus H(d \| ID_{KC} \| ID_i) \quad (6)$$

$$\tilde{C}_3 = C_3 \oplus H(\tilde{C}_2) \quad (7)$$

3）验证下述等式是否成立：

$$\tilde{C}_3^e \equiv g^{ID_i T} (\mathrm{mod} n) \quad (8)$$

若等式成立，则接受用户 U_i 登录请求；否则，登陆失败。

下面定理说明了上述口令认证过程是正确的。

定理　设 ID_i 和 P_i 分别是用户 U_i 登陆阶段提交的身份标识和口令，则(ID_i, C_2, C_3, T) 是合法用户 U_i 提交的当且仅当根据提交消息计算的 $\tilde{C}_3$ 和 T 满足 $\tilde{C}_3^e \equiv g^{ID_i T} (\mathrm{mod} n)$。

证明　从(1)，(3) 和(4) 式，我们有：

$$\begin{aligned} C_2 &= S_i \oplus P_i \oplus H(r_i) \\ &= P_i \oplus H(d \| ID_{KC} \| ID_i) \oplus P_i \oplus H(r_i) \\ &= H(d \| ID_{KC} \| ID_i) \oplus H(r_i) \end{aligned}$$

结合(6)，可得：

$$\begin{aligned} \tilde{C}_2 &= H(d \| ID_{KC} \| ID_i) \oplus H(d \| ID_{KC} \| ID_i) \oplus \\ &\quad H(r_i) = H(r_i) \end{aligned}$$

根据(2)、(5) 和(7)，有：

$$\begin{aligned} \tilde{C}_3 &= h_i^T \oplus H(H(r_i)) \oplus H(\tilde{C}_2) \\ &= h_i^T \oplus H(H(r_i)) \oplus H(H(r_i)) = h_i^T = (g^{ID_i T})^d \mathrm{mod} n \end{aligned}$$

所以 $\tilde{C}_3^e \equiv g^{ID_i T} \mathrm{mod} n$。

1.5 用户口令的更新

当用户 U_i 想将口令 P_i 更新为 P_i^* 时，只需要在智能卡中计算：$D = P_i^* \oplus P_i$，$\tilde{S}_i = D \oplus S_i$，然后用 $\tilde{S}_i$ 替换智能卡中嵌入的信息 S_i 即可。

2 安全性分析

本文案的安全性是基于安全单向的 hash 函数和大整数分解难问题的。具体分析如下：

1）秘密密钥 d，只为服务器端所知，是保证实现本认证系统安全的关键，因而需要用专门的安全机制进行密码保存。

2）攻击者利用自己的 ID_i 和智能卡上的信息(S_i, h_i)，安全单向的 hash 函数使攻击者从(1) 得到的 $H(d \| ID_{KC} \| ID_i) = P_i \oplus S_i$ 得到 d 不可能实现，而试图利用(2) 式中 $h_i = (g^{ID_i})^d \mathrm{mod} n$ 来求出 d，面临求离散对数难问题。

3）如果客户端使用者 U_i 不小心遗失智能卡，因为拾得者无法得知口令 P_i，因而无法正确计算(3) 中的 $C_1 = S_i \oplus P_i$，从而无法假冒认证信息(C_2, C_3)。

4）使用者不小心泄漏了身份 ID_i 和口令 P_i，入侵者如果没有此智能卡，则因为无从知道(S_i, h_i)，从而很难仿制出(3) 中的 $C_1 = S_i \oplus P_i$ 和 (5) 中的 $C_3 = h_i^T \oplus H(H(r_i))$，从而无法假冒认证信息$(C_2, C_3)$。

5）如果另一合法客户端用户 U_j 想假冒用户 U_i 身份进入系统，既没有用户 U_i 的智能卡，也没有用户 U_i 的口令，从 3) 和 4) 分析可知，U_j 很难攻击成功。

6）假设入侵者截获从客户端发往服务器端的认证信息(ID_i, C_2, C_3, T)，同上述 2) 一样，入侵者很难从(C_2, C_3) 中分析出 d 和 r_i，从而无法仿制另一个有效信息(ID_i, C'_2, C'_3, T') 进行登录。另一方面，发送的信息中包含时间戳，从而能有效地抵抗重放攻击。

7）如果一个入侵者冒充服务器端，因为他无从知道 d，因此无法利用(6) 得到 $\tilde{C}_2$，因而不能根据(7) 计算出满足(8) 的 $\tilde{C}_3$。此外，直接根据(8) 的 $\tilde{C}_3^e \equiv g^{ID_i T} (\mathrm{mod} n)$ 求 $\tilde{C}_3$，面临分解大整数难问题。

根据上述分析，本文设计的方案是安全、可靠的。

3 结语

本文提出了一种可靠的远程口令认证系统方案，安全性是基于安全单向的 hash 函数和大整数分解难问题的。本文方案具有如下的特点：

1）本方案中，客户端用户的口令是由自己任意选取的。在拿到智能卡后，用户还可自由选择口令，修改原来的口令，增强了口令认证系统的安全性。

2）口令是在客户端计算验证信息，不需要通过公众网络传输给服务器端，从而进一步增强了客户端的用户口令的安全性。另一方面，服务器端每次在验证客户端请求时，不需要查询、匹配庞大的用户 ID-P 表，而在文献[5,7]等方案中，这是必不可少的。

3）本方案采用了成熟的 RSA 系统和单向安全的 hash 函数，RSA 是目前应用最为广泛的公开密钥密码系统及签名系统，几乎所有的智能卡都支持，这给本方案的实现带来了方便，且其安全性具有充分的保障。

4）利用智能卡技术，提高了系统的安全性和认证效率。

参考文献：

[1] SHAMIR A. dentity-based Cryptosystems and Signature Scheme[A]. Proceedings CRYPTO84[C], Springer, Berlin, 1985.47 -53.

[2] CHANG CC, WU TC. Remote Password Authenticated With Smart Card[J]. IEE Proceedings-e, 1991,138(3):165 -168.

[3] HWANG MS, LI LH. A new remote user authenticated scheme using smart card[J]. IEEE Trans. Consumer Electron,2000,46(1):189 -294.

[4] 张聪娥，曹守见，李立新. 一种基于智能卡的口令认证方案[J]. 计算机工程，2004，30(7)：104 -105.

[5] CHANG CC, LIAO WY. Remote Password Authentication Scheme [J]. Computer & Securioy, 1994, 13(2): 137 - 144.

[6] YANG C-C, WANG R-C. An improvement of security enhancement for the timestamp-based password authentication scheme using smart cards [J]. ACM SIGOPS Operating Systems Review, 2004,38(3): 91 -96.

[7] CHANG Y-F, CHANG C-C. A secure and efficient strong - password authentication protocol[J]. ACM SIGOPS Operating Systems Review, 2004,38(3): 79 -90.

[8] CHANG C-C, LIN I-C. Remarks on fingerprint - based remote user authentication scheme using smart cards[J]. ACM SIGOPS Operating Systems Review, 2004,38(4): 91 - 96.

[9] KIM Y-S, LEE S-W, YOO K-Y. ID-based password authentication scheme using smart cards and fingerprints[J]. ACM SIGOPS Operating Systems Review, 2003,37(4): 32 - 41.

[10] KU W-C, CHEN C-M, LEE H-L. Weaknesses of Lee-Li-Hwang's hash-based password authentication scheme[J]. ACM SIGOPS Operating Systems Review, 2003,37(4):19 -25.

[11] TSAUR WJ, WU CC, LEE WB. A smart card-based remote scheme for password authentication in multi-server Internet services[J]. Computer Standards and Interfaces. 2004,27:39 -51.

[12] DAS ML, SAXENA A, GULATI VP. A dynamic ID-based remote user authentication scheme[J]. IEEE Trans. Consumer Electron. 2004,50(2):629 -631.

[13] AWASTHI AK, LAL S. Security analysis of a dynamic ID-based remote user authentication scheme[EB/OL]. http://eprint.iacr.org/2004/238,2005.

[14] AWASTHI AK , LAL S . An enhanced remote user authentication scheme[J]. IEEE Trans Consumer Electron. 2004,50(2):583 -586.