第 38 卷 第 3 期
Vol.38 No.3

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 安全技术 •

文章编号：1000—3428(2012)03—0137—02 文献标识码：A 中图分类号：TP309

基于生物特征的鲁棒远程用户认证方案

张韶远，卢建朱

(暨南大学信息科学技术学院，广州 510632)

摘 要：将生物特征信息、单向哈希函数和智能卡等技术相结合，提出一种基于生物特征识别的身份认证方案。利用时戳生成一次性共享信息，以提高系统的鲁棒性。分析结果证明，该方案可防止伪装攻击、重放攻击和拒绝服务攻击。用户与服务器仅需 2 次握手即可实现相互认证，由此节约系统的通信成本，提高认证效率。

关键词：基于生物特征的认证；单向哈希函数；时间戳；远程用户；智能卡；可信第三方；一次性共享密钥

Biometrics-based Robust Remote User Authentication Scheme

ZHANG Shao-yuan, LU Jian-zhu

(College of Information Science and Technology, Jinan University, Guangzhou 510632, China)

【Abstract】An efficient biometrics-based mutual authentication scheme is proposed, which is based on personal biometrics, one-way Hash function and smart card. For enhancing the system security, a one-time key is generated by using the timestamp. In the scheme, the authentication process can resist all known attacks including replay attacks and the DoS attacks, and needs only twice online message transmissions. Analysis shows that the scheme is secure and effective.

【Key words】biometrics-based authentication; one-way Hash function; timestamp; remote user; smart card; trusted third party; one-time shared key

DOI: 10.3969/j.issn.1000-3428.2012.03.046

1 概述

传统的远程身份认证系统大多是基于用户名和口令的。基于用户名和口令的认证系统简单方便。为便于记忆，用户常把口令设置成特殊的(如生日或姓名)或比较简短的字符串，攻击者采用口令猜测或字典攻击的方法就可得到它们。

人的生物特征具有不容易被复制、不容易被伪造和不容易丢失等特点。随着局部特征技术[1]等识别技术的发展，将传统的远程身份认证与生物特征识别技术有机结合，可构造鲁棒的远程认证系统[2]。许多密码学家及相关技术人员已进行了广泛的研究[3]。文献[4]基于用户的指纹特征和有限域上离散对数难问题，提出了一个远程用户认证方案。然而，该方案可能遭受伪装攻击[5]。文献[6]将生物特征识别技术和安全的单向哈希函数相结合，提出了基于智能卡的远程用户认证方案。该方案直接使用共享秘密 $h(UID_i \| X_S)$ 进行用户与服务器的认证，这样容易造成该密钥的泄漏，危及整个系统的安全。本文将身份信息、口令和生物特征三方因素相结合设计了一个认证方案。

2 鲁棒的身份认证方案

本文的远程用户认证方案由系统初始化、用户注册、用户登录、双方认证和交换密钥的生成 5 个阶段组成，其安全性基于安全的单向哈希函数。

2.1 系统初始化

假设系统存在一个可信的第三方 TA。TA 选取一个安全的单向哈希函数 $h(\cdot)$，且每个服务提供者 S_j 与 TA 建立了一个共享的密钥 X_{S_j}。然后，TA 公开 $h(\cdot)$，并秘密保存 X_{S_j}。

2.2 用户注册

U_i 通过安全渠道将自己的身份标识 UID_i、用户口令 PW_i 及生物特征 B_i 发送给 TA，申请注册。TA 收到 U_i 的请求信息后，执行如下操作实现对 U_i 的授权：

(1)计算身份特征 B_i 和口令 PW_i 的哈希值，得 $f_i = h(B_i)$ 和 $r_i = h(PW_i \| f_i)$。

(2)利用共享的密钥 X_{S_j} 计算 $e_i = h(UID_i \| X_{S_j}) \oplus h(PW_i \| f_i)$。

(3)将 $(UID_i, h(\cdot), f_i, e_i)$ 存储到智能卡中，并通过安全渠道将智能卡送到用户手中。

2.3 用户登录

用户登录如下：

(1)用户将智能卡插入读卡器，输入自己的生物特征 B_i^*。智能卡先计算哈希值 $f'_i = h(B_i^*)$，再与存储数据 f_i 验证，成功后用户 U_i 生成随机数 R_U，并输入口令 PW_i。

(2)根据用户的输入口令 PW_i、随机数 R_U 和当前时间戳 T_U，智能卡利用存储数据 e_i 计算 $M_1 = h((e_i \oplus h(PW_i \| f'_i)) \| T_U)$，$M_2 = M_1 \oplus R_U$，$r_U = h(R_U)$。

(3)智能卡将认证信息发送给服务器，即 $U_i \to S_j$：(UID_i, M_2, T_U, r_U)。

2.4 双方认证

双方认证过程如下：

(1)服务器 S_j 认证用户 U_i 的合法性

1)假设 S_j 在时刻 T'_U 接收到该请求。S_j 首先检查用户的身份 UID_i 的格式是否正确，然后计算 $T'_U - T_U$。若 $T'_U - T_U > \Delta T_U$，S_j 拒绝用户 U_i 的请求。这里，ΔT_U 为用户请求的

基金项目：广东省产学研基金资助项目(2008B090500201, 2009B010800023)

作者简介：张韶远(1986－)，男，硕士研究生，主研方向：无线网络安全；卢建朱，副教授、博士

收稿日期：2011-07-07 **E-mail：**zhangshaoyuan@foxmail.com

最大时延。

2)当 $T'_U - T_U < \Delta T_U$，S_j 随机选取整数 R_S，利用当前时间戳 T_S 和共享密钥 X_{S_j} 计算：$M_3 = h(UID_i \| X_{S_j})$，$M_4 = M_2 \oplus$ $M_4 = M_2 \oplus h(M_3 \| T_U)$，其中，$\oplus$ 表示按位异或操作。

3)根据用户发来的 r_U，验证等式 $r_U = h(M_4)$ 是否成立。若等式不成立，则双方认证失败。只有当等式成立时，服务器才会继续执行以下的操作：$M_5 = h(M_3 \| T_S) \oplus R_S$，$M_6 = h(M_3 \| T_U \| T_S \| M_4)$。

4)服务器 S_j 将认证信息发送给用户 U_i，即 $S_j \to U_i$：(M_5, M_6, T_S)。

(2)用户 U_i 认证服务器 S_j 的合法性

1) U_i 在时刻 T'_U 接收到该请求。S_j 首先检查用户的身份 UID_i 的格式是否正确，然后计算 $T'_U - T_U$。若 $T'_U - T_U > \Delta T_U$，S_j 拒绝用户 U_i 的请求。这里，ΔT_U 为用户请求的最大时延。

2) U_i 收到服务器 S_j 发来的认证信息后，利用在用户登录阶段计算出来的 r_i'，再根据智能卡中存储的 e_i，得到 $M'_6 = h((e_i \oplus r_i) \| T_U \| T_S \| R_U)$。然后，$U_i$ 验证 T_S 的有效性和等式 $M'_6 = M_6$。若上述 2 个条件同时成立，则服务器 S_j 是合法的授权服务器。

基于生物特征的远程用户认证方案如图 1 所示。

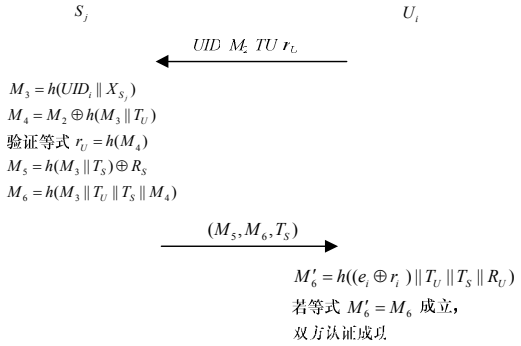

图 1 基于生物特征的远程用户认证方案

2.5 交换密钥的生成

在服务器 S_j 和用户 U_i 都通过身份验证后，通信双方可从对方提供的消息中直接计算交换密钥，其具体操作如下：

(1)根据 U_i 发送的消息 (UID_i, M_2, T_U, r_U)，S_j 计算共享密钥 $sk^{(k)} = h(h(UID_i \| X_{S_j}) \| R_S \| R_U)$。

(2)根据登录阶段计算所得的 e_i 和 r_i，U_i 利用接收的消息 (M_5, M_6, T_S) 计算 $sk^{(k)} = h((e_i \oplus r_i) \| R_S \| R_U)$。

3 安全性分析

本文方案的安全性基于安全的单向哈希函数，并利用延时限制提高系统的安全性和效率。

(1)认证双方的私有信息是安全。服务提供者的私钥 X_{S_j} 是安全的。用户 U_i 根据智能卡存储的数据 e_i、PW_i 和 B_i 计算 X_{S_j} 需要求解单向哈希函数。如果要通过用户和服务器传输的信息 M_2、M_5 和 M_6 求 X_{S_j}，则将 2 次面临求解安全的单向哈希函数问题。

用户的口令 PW_i 与生物特征信息 B_i 是安全的。PW_i 和 B_i 的相关信息都不在网上进行传输，攻击者不可能从交换信息中获得它们。即使攻击者窃取了智能卡，也不能得到用户的生物特征信息 B_i 和 PW_i。因为由 f_i 和 e_i 求 PW_i 和 B_i 面临安全的单向哈希函数问题。

(2)用一次共享信息建立用户和服务器的认证，提高了系统的鲁棒性。当用户向服务器发出第 k 次请求信息 (UID_i, M_2, T_U, r_U) 后，服务器计算出本次请求的共享信息 $M_{U-S}^{(k)}$。由于每次请求的共享信息 $M_{U-S}^{(k)}$ 不同，因此用于认证的共享信息是一次性的。

(3)可防止伪装攻击。攻击者 $\tilde{S}_j$ 不可能伪装为服务器 S_j 欺骗合法用户 U_i。为了欺骗 U_i，没有密钥 X_{S_j} 的 $\tilde{S}_j$ 需要根据窃听的请求信息 (UID_i, M_2, T_U, r_U)，向 U_i 发送一个形式为 $(\tilde{M}_5, \tilde{M}_6, T_{\tilde{S}})$ 的合法响应。$\tilde{S}_j$ 必须计算出正确的值 M_3，这对于没有密钥 X_{S_j} 的 $\tilde{S}_j$ 是不可能的。反之，攻击者 $\tilde{U}_i$ 由于没有口令 PW_i 和生物特征 B_i，因此不可能伪装成 U_i 欺骗合法服务器 S_j。

(4)可抵抗重放攻击和抑制拒绝服务攻击。服务器能立即验证用户的请求信息是否合法，并且只要 2 次哈希操作和一次异或操作，因此对攻击者的非法请求信息能够马上拒绝，避免服务器会话表的溢出。此外，请求的延时限制 ΔT_U 可进一步降低拒绝服务攻击的成功率。用户给服务器的请求信息和服务器的响应信息都带有时间戳，重放攻击不能成功。

总之，在通信成本方面，本文方案的远程用户终端发送和接收消息各 1 次，而文献[6]的远程用户终端需要发送消息 2 次、接收消息 1 次，因此，本文性能有所提高。

4 结束语

本文在保证服务器成本开销合理的前提下，降低了客户端的成本开销，提高了认证系统的鲁棒性。下一步将对服务器端的算法做进一步的优化，以减少服务器端的运算开销。

参考文献

[1] 曹 健, 王武军, 韩 飞, 等. 基于局部特征的目标识别技术研究[J]. 计算机工程, 2010, 36(10): 203-205.

[2] Maty V, Riha Z. Security of Biometric Authentication Systems[C]//Proc. of 2010 International Conference on Computer Information Systems and Industrial Management Applications. Krackow, Germany: [s. n.], 2010.

[3] Lin Chu-Hsing, Lai Yi-Yi. A Flexible Biometrics Remote User Authentication Scheme[J]. Computer Standards and Interfaces, 2004, 27(1): 19-23.

[4] Lee J K, Ryu S R, Yoo K Y. Fingerprint-based Remote User Authentication Scheme Using Smart Cards[J]. Electronic Letters, 2002, 38(12): 554-555.

[5] Hsieh B T, Yeh H Y, Sun H M, et al. Cryptanalysis of a Fingerprint-based Remote User Authentication Scheme Using Smart Cards[C]//Proc. of the 37th Annual International Carnahan Conference on Security Technology. Washington D. C., USA: IEEE Press, 2003.

[6] Li Chun-Ta, Hwang Min-Shiang. An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards[J]. Journal of Network and Computer Applications, 2010, 33(1): 1-5.

编辑 张正兴