多服务器环境下动态身份认证密钥协商方案

曹 阳
(陕西理工大学 数学与计算机科学学院,陕西 汉中 723000)

摘 要:为了提高远程用户利用网络从不同服务器访问时身份认证的安全性,基于 ECC 密码体制及离散对数问题的难解性,利用 hash 函数的单向性,结合用户身份、口令提出了一种多服务器环境下动态身份认证密钥协商方案。该方案使用 hash 函数隐藏用户口令、身份,信息发送都是在安全信道上发送,由注册阶段、登录阶段、认证密钥协商阶段、口令更改阶段四个部分组成。注册时用户 U_i 向注册中心 RC 传送的是匿名身份;登录时用户 U_i 的身份是动态身份,实现了用户的强匿名性;密钥协商时实现了可信注册中心 RC、服务器 S_j 及用户 U_i 三方相互认证。分析表明,方案具有抗重放攻击、抗伪造攻击、抗恶意合法用户攻击、三方认证、强匿名性等安全性。

关键词:多服务器;ECC;动态身份;密钥协商
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2018)05-0131-04
doi:10.3969/j.issn.1673-629X.2018.05.030

Dynamic Identity Authentication Key Agreement Scheme under a Multi-server Environment

CAO Yang
(School of Mathematics and Computer Science, Shaanxi University of Technology, Hanzhong 723000, China)

Abstract: In order to improve the security of remote users' identity authentication with network to visit from different servers, based on ECC cryptography and the intractability of discrete logarithmic, with the one-way hash function, we propose a dynamic identity authentication key agreement scheme under a multi-server environment combined with the users' identity and password. It takes advantage of hash function to hide the user's password and identity. Message routing is completed through secure channel, consisting of register stage, login stage, authentication key agreement stage and password change stage. User U_i sends an anonymous identity to the registry when registering. In logging, the identity of user U_i is dynamic, which realizes the user's strong anonymity. In key agreement, a three-party mutual authentication is completed among a reliable registry RC, S_j server and user U_i. The analysis shows that the scheme has such security features as resisting replay attacks, resisting forgery attack, anti-malicious legal user attacks, three-party authentication proposed, and strong anonymity.

Key words: multi-server; ECC; dynamic identity; key agreement

0 引 言

在网络时代,远程用户从不同的服务器获得网络服务已不再是难事,用户可使用传统的单服务器架构[1-2]来满足自己的需求。但随着因特网的迅速发展,网络服务的需求也相应增长,单服务器架构也就很难满足这些需求,需要多个服务器在不同的位置提供服务。近年来研究人员针对多服务器认证问题,引入了口令、身份标识、基因等,目的是为了提高用户认证时信息的安全性。例如,文献[3]提出了一种多服务环境下的身份认证协议,但该协议不能抵抗伪造攻击和会话密钥泄露攻击;文献[4]基于智能卡提出一种多服务器多环境下的动态身份认证协议,但该协议通信复杂度太高[5];文献[6]提出了基于口令的高效安全的多服务器认证方案,但该方案存在离线口令猜测攻击;文献[7]基于单向 hash 函数提出了无验证表的高效多服务器认证方案,但该方案不能抵抗内部攻击,无服务周期管理等;文献[8]基于自认证公钥提出了一种多服务器远程用户身份认证方案,但该方案不能

收稿日期:2017-05-05 **修回日期**:2017-09-06 **网络出版时间**:2018-02-08
基金项目:国家自然科学基金(21373132);陕西省教育科研计划项目(17JK0148)
作者简介:曹 阳(1978-),女,硕士,讲师,研究方向为信息安全与计算机应用。

抵抗伪造攻击、无前向安全性;文献[9]提出的基于智能卡的多服务器远程认证方案,不能抗重放攻击,无双向认证。类似的方案[10-15]还有很多,在此不再加以一一论述。

针对多服务器环境下用户认证的安全性问题,基于 ECC 密码体制,结合动态身份,文中提出了一种多服务器环境下的动态身份认证密钥协商方案。

1 认证密钥协商方案

设 $U=\{U_1,U_2,\cdots,U_n\}$ 为远程用户,$S=\{S_1,S_2,\cdots,S_n\}$ 为服务器组,RC 为可信注册中心。RC 选取有限域 F_p 上的安全椭圆曲线 $E(F_p)$,G 为 $E(F_p)$ 的基点,其阶为 q(q 为大素数),且该曲线满足椭圆曲线离散对数问题的难解性,公开 $E(F_p)$,G,q。方案中信息都是在安全信道上发送,由注册阶段、登录阶段、认证密钥协商阶段、口令更改阶段四个部分组成,方案中用到的主要参数描述见表 1。

表 1 参数描述

参数	含义	参数	含义
U_i	第 i 个用户	x	RC 的私钥
S_j	第 j 个服务器	y_j	RC 和 S_j 共享的秘密信息
$H()$	单向安全 hash 函数	$E_x()$	用密钥对消息进行对称加密
UID_i	用户 U_i 的身份标识	$D_x()$	用密钥对消息进行对称解密
CUID_i	用户 U_i 的动态身份标识	T_{ij}	RC 为用户 U_i 设定的可以访问服务器 S_j 的服务周期
UPW_i	用户 U_i 的口令	$\oplus$	异或运算
SID_j	服务器 S_j 的身份标识	$\|$	级联运算

1.1 注册阶段

(1) S_j 选取随机数 SID_j 作为自己的身份标识,并将其发送给 RC。RC 收到 S_j 发送的身份标识 SID_j 后计算 $R_j=H(H(\mathrm{SID}_j)\oplus y_j)$,发送 R_j 给 S_j,S_j 收到 R_j 后将其存储,结束注册。

(2)用户选取随机数 UID_i 和 UPW_i,其中 UID_i 作为用户的身份标识,UPW_i 作为用户的口令。将 $(H(\mathrm{UID}_i),H(H(\mathrm{UID}_i)\oplus \mathrm{UPW}_i G))$ 发送给 RC。

(3)RC 收到 $(H(\mathrm{UID}_i),H(H(\mathrm{UID}_i)\oplus \mathrm{UPW}_i G))$ 后计算:$A_i=H(x\oplus H(\mathrm{UID}_i))$,$B_i=A_i\oplus H(H(\mathrm{UID}_i)\oplus \mathrm{UPW}_i G)$,$C_i=H(A_i)$,$A_{ij}=H(B_i\|\mathrm{SID}_j)$,$D_{ij}=E_{y_j\oplus T_{ij}}(A_{ij})$,并将 $(B_i,C_i,A_{ij},T_{ij},H())$ 发送给 UID_i,D_{ij} 发送给 S_j 结束注册。

1.2 登录阶段

(1)用户 U_i 输入自己的身份标识 UID_i 和口令 UPW_i,系统计算:$A_i^*=B_i\oplus H(H(\mathrm{UID}_i)\oplus \mathrm{UPW}_i G)$,$C_i^*=H(A_i^*)$,若 $C_i^*=C_i$,说明输入的信息正确,否则系统拒绝登录请求。

(2)用户选取随机数 $\alpha,\alpha\in F_p$,计算:$N_1=H(A_i\|\alpha G)$ $\mathrm{CUID}_i=E_{A_{ij}}(r_k\|H(H(\mathrm{UID}_i)\oplus A_{ij})\|H(\mathrm{UID}_i))$,其中 r_k 表示用户的登录次数,发送登录请求信息 $(\mathrm{CUID}_i,\alpha G,N_1,H())$ 给 S_j。

1.3 认证密钥协商阶段

(1) S_j 收到用户登录请求信息 $(\mathrm{CUID}_i,\alpha G,N_1,H())$ 后,选取随机数 $\beta,\beta\in F_p$,计算 $N_2=H(R_j\|\beta G)$,同时将 $(\mathrm{CUID}_i,\alpha G,N_1,D_{ij},N_2,\beta G,H())$ 发送给 RC。

(2) RC 收到 S_j 发送的 $(\mathrm{CUID}_i,\alpha G,N_1,D_{ij},N_2,\beta G,H())$ 后,计算 $A_{ij}=D_{y_j\oplus T_{ij}}(D_{ij})$,并用 A_{ij} 解密动态身份 CUID_i,得到 $H(H(\mathrm{UID}_i)\oplus A_{ij})'$,$H(\mathrm{UID}_i)'$,然后比较 $H(H(\mathrm{UID}_i)\oplus A_{ij})'$ 与 $H(H(\mathrm{UID}_i)\oplus A_{ij})$ 是否相等,若不等则拒绝认证,否则继续比较 $H(\mathrm{UID}_i)'$ 与 $H(\mathrm{UID}_i)$ 是否相等,若不等则拒绝认证,否则验证 T_{ij} 是否过期,若过期则终止,否则 RC 计算 $N_1^*=H(H(H(\mathrm{UID}_i)\oplus x)\|\alpha G)$,$N_2^*=H(H(H(\mathrm{SID}_j)\oplus y_j\|\beta G))$。验证等式 $N_1^*\stackrel{?}{=}N_1$,$N_2^*\stackrel{?}{=}N_2$ 是否成立,若不成立则终止,否则 RC 继续计算 $X=H(H(H(\mathrm{SID}_j)\oplus y_j\|\alpha G\|\beta G))$,$Y=H(H(H(\mathrm{UID}_i)\oplus x)\|H(\mathrm{SID}_j)\|\alpha G\|\beta G)$,$N_3=X\oplus Y$,$N_4=H(X\oplus Y)$,并将 (N_3,N_4) 发送给 S_j。

(3) S_j 收到 (N_3,N_4),计算 $X^*=H(H(H(\mathrm{SID}_j)\oplus y_j\|\alpha G\|\beta G))$,$N_3\oplus X^*=X\oplus Y\oplus X^*=Y$,$N_4^*=H(X^*\oplus Y)$,验证 $N_4^*\stackrel{?}{=}N_4$ 是否成立,若不成立则终止,否则 S_j 认证 RC 是可信的,解密 D_{ij} 得到 A_{ij},并用 A_{ij} 解密动态身份 CUID_i,可以得到 r_k',$H(\mathrm{UID}_i)$,$H(H(\mathrm{UID}_i)\oplus A_{ij})$。$S_j$ 比较 $r_k'\stackrel{?}{=}r_k$ 是否相等,若不相等则终止,若相等则计算 $\mathrm{SK}=\beta(\alpha G)$,$N_5=H(H(\mathrm{UID}_i)\|H(\mathrm{SID}_j)\|Y\|\mathrm{SK})$,并将 $(\beta G,N_5)$ 发送给 U_i。

(4) U_i 收到 $(\beta G,N_5)$ 后,计算 $A_i=B_i'\oplus H(H(\mathrm{UID}_i)\oplus \mathrm{UPW}_i G)$,$\mathrm{SK}=\alpha(\beta G)$,$Y^*=H(A_i\|H(\mathrm{SID}_j)\|\alpha G\|\beta G)$,$N_5^*=H(H(\mathrm{UID}_i)\|$

$H(\mathrm{SID}_j) \| Y^* \| \mathrm{SK})$,验证等式 $N_5^* \stackrel{?}{=} N_5$ 是否成立,若不成立则终止会话,否则 U_i 认为 RC、S_j 是可信的,并计算发送 $N_6 = H(Y^* \| \mathrm{SK})$ 给 S_j。

(5) S_j 收到 U_i 发送来的 N_6 后,计算 $N_6^* = H(Y \| \mathrm{SK})$,判断等式 $N_6^* \stackrel{?}{=} N_6$ 是否成立,若不成立则终止会话,否则 S_j 确定 U_i 为合法用户。S_j,U_i,RC 三方相互认证后,共享会话密钥为: $\mathrm{SK} = \alpha\beta G$。

2　方案分析

2.1　安全性分析

(1)强匿名性。

方案是基于动态身份设计的,用户 U_i 的真实身份从未在公共网络上传输。注册时用户 U_i 向控制中心 RC 传送的是匿名身份 $H(\mathrm{UID}_i)$,若攻击者要知道 U_i 的真实身份,他必须解决哈希函数 $H()$ 的单向性问题。登录时,U_i 使用的是动态身份 CUID_i,由 $\mathrm{CUID}_i = E_{A_{ij}}(r_k \| H(H(\mathrm{UID}_i) \oplus A_{ij}) \| H(\mathrm{UID}_i))$ 知,攻击者要知道用户的真实身份,他就必须知道 A_{ij},由 $A_{ij} = H(B_i \| \mathrm{SID}_j)$,$B_i = A_i \oplus H(H(\mathrm{UID}_i) \oplus \mathrm{UPW}_i G)$,$A_i = H(x \oplus H(\mathrm{UID}_i))$,$H(\mathrm{UID}_i)$ 可知是不行的。一方面,x 是 RC 的私钥;另一方面仍然是哈希函数 $H()$ 的单向性问题,所以攻击者无法确定用户的身份。因此方案具有强匿名性。

(2)抗离线口令猜测攻击。

由 $H(H(\mathrm{UID}_i) \oplus \mathrm{UPW}_i G)$ 知,用户的口令是由哈希函数 $H()$ 保护的,即使攻击者通过一些方法得到了用户的身份,他也无法知道用户的口令 UPW_i,由 $\mathrm{UPW}_i G$ 知, UPW_i 的安全性基于离散对数问题的难解性。

(3)抗重放攻击。

如果攻击者窃听到用户 U_i 和服务器 S_j 之间的通信,并伪装成 U_i 将登录请求信息发送给 S_j,由 $(\mathrm{CUID}_i, \alpha G, N_1, H())$ 知, α 是用户在每一次登录请求时选取的随机数,显然, α 使得每一次会话中的信息都是不同的,即使攻击者知道了某一次会话消息,也无法在下次会话中使用。同样攻击者也无法伪装成 S_j 与 U_i 通信,因为 β 也是随机数。所以方案抗重放攻击。

(4)抗内部攻击。

方案中的内部攻击是指系统管理者有目的地泄露用户的秘密信息。方案中用户提交的注册信息 $(H(\mathrm{UID}_i), H(H(\mathrm{UID}_i) \oplus \mathrm{UPW}_i G))$ 是受哈希函数 $H()$ 保护的,且口令 UPW_i 通过用户身份隐藏,加之离散对数的难解性,攻击者不可能得到用户的口令,即方案可以抵抗内部攻击。

(5)抗恶意合法用户攻击。

一个恶意合法用户 U' 可能收集到的信息有:一是 U' 自己的身份 UID' 和口令 PW';二是从信道上窃听或截获目标用户登录时的请求信息。由方案可知,用户登录时使用的是动态身份,由 $\mathrm{CUID}_i = E_{A_{ij}}(r_k \| H(H(\mathrm{UID}_i) \oplus A_{ij}) \| H(\mathrm{UID}_i))$ 知, U' 必须知道 A_{ij}。若由 $A_i = H(x \oplus H(\mathrm{UID}_i))$,$B_i = A_i \oplus H(H(\mathrm{UID}_i) \oplus \mathrm{UPW}_i G)$,$A_{ij} = H(B_i \| \mathrm{SID}_j)$ 计算出正确 A_{ij},U' 必须知道 RC 的私钥 x 及其身份 SID_j;若从 D_{ij} 进行解密得到 A_{ij},由 $D_{ij} = E_{y_j \oplus T_{ij}}(A_{ij})$ 知, y_j 是 RC 和 S_j 之间的私钥。因此 U' 无法伪造用户登录请求信息。

(6)三方双向认证。

在认证密钥协商阶段 2 中,RC 收到 S_j 发送的认证信息 $(\mathrm{CUID}_i, \alpha G, N_1, D_{ij}, N_2, \beta G, H())$ 后,计算 A_{ij},解密 CUID_i,比较了相关信息,并通过 N_1,N_2 认证 S_j。同样在阶段 3 中, S_j 通过 N_3,N_4 认证了 RC 的合法性,在阶段 4 中, U_i 通过 N_5 认证了 S_j 的合法性,在阶段 5 中, S_j 通过 N_6 认证了 U_i 的合法性。因此方案能提供三方认证。

(7)前向安全性。

方案中,如果攻击者知道了传输中所有认证信息和注册中心的主密钥 x,他仍然不能推导出 U_i 和 S_j 之间的会话密钥 $\mathrm{SK} = \alpha\beta G$,因为 α,β 是 U_i 和 S_j 各自选取的随机数,且每次会话时 α,β 都不同,即方案满足前向安全性。

2.2　方案比较

方案从抗重放攻击、强匿名性、抗离线口令猜测攻击、抗内部攻击、抗恶意合法用户攻击、三方认证、前向安全性、服务周期管理八个方面与文献[6-9]进行比较,如表 2 所示。其中“√”表示具有该方面的安全性;“×”表示不具有该方面的安全性;“T_1”表示抗重放攻击;“T_2”代表强匿名性;“T_3”代表抗离线口令猜测攻击;“T_4”代表抗内部攻击;“T_5”代表抗恶意合法用户攻击;“T_6”代表三方认证,“T_7”代表前向安全性,“T_8”代表服务周期管理。

表 2　安全性比较

安全性	文献[6]	文献[7]	文献[8]	文献[9]	文中方案
T_1	√	√	√	×	√
T_2	√	√	√	√	√
T_3	×	√	√	√	√
T_4	√	×	×	×	√
T_5	√	√	×	×	√
T_6	×	×	×	√	√
T_7	√	√	×	×	√
T_8	√	×	×	×	√

3 结束语

文中提出了一种多服务器环境下动态身份认证密钥协商方案,其安全性主要依赖于 hash 函数的单向性、ECC 密码体制的安全性及离散对数问题的难解性。分析表明,方案能抵抗重放攻击、内部攻击、恶意用户攻击,具有三方认证、前向安全性。因此,方案具有一定的实际应用价值。

参考文献:

[1] LI Chunta, LEE Cheng-Chi. A robust remote user authentication scheme using smart card[J]. Information Technology and Control, 2011, 40(3): 236-245.

[2] JIANG Qi, MA Jianfeng, LU Xiang, et al. Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems [J]. Journal of Medical Systems, 2014, 38(2): 1-8.

[3] LI Xiong, XIONG Yongping, MA Jian, et al. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards[J]. Journal of Network and Computer Applications, 2012, 35(2): 763-769.

[4] SOOD S K, SARJE A K. A secure dynamic identity based authentication protocol for multi-server architecture[J]. Journal of Network and Computer Applications, 2011, 34(2): 609-618.

[5] KALRA S, SOOD S. Advanced remote user authentication protocol for multi-server architecture based on ECC[J]. Journal of Information Security an Applications, 2013, 18(2-3): 98-107.

[6] TSAUR W J, LI Jiahong, LEE Wei-Bin. An efficient and secure multi-server authentication scheme with key agreement [J]. Journal of Systems and Software, 2012, 85(4): 876-882.

[7] TSAI J L. Efficient mufti-server authentication scheme based on one-way hash function without verification table[J]. Computers & Security, 2008, 27(3-4): 115-121.

[8] LIAO Yipin, HSIAO C M. A novel multi-server remote user authentication scheme using self- certified public keys for mobile clients[J]. Future Generation Computer Systems, 2013, 29(3): 886-900.

[9] 国佃利. 基于智能卡的多服务器远程认证方案的研究[D]. 济南:济南大学, 2014.

[10] 舒 剑. 高效的基于口令多服务器认证方案[J]. 计算机应用研究, 2015, 32(8): 2444-2446.

[11] 牛 雨. 基于多服务器互相验证的用户身份认证协议[J]. 计算机仿真, 2016, 33(2): 350-354.

[12] 舒 剑. 多服务器环境下基于扩展混沌映射的认证密钥协商协议[J]. 计算机应用研究, 2016, 33(1): 232-235.

[13] 王崇霞, 高美真, 刘 倩, 等. 多服务器环境移动通信网身份认证方案设计[J]. 微电子学与计算机, 2016, 33(6): 152-156.

[14] 李艳平, 刘小雪, 屈 娟, 等. 基于智能卡的多服务器远程匿名认证密钥协商协议[J]. 四川大学学报:工程科学版, 2016, 48(1): 91-98.

[15] 夏鹏真, 陈建华. 基于椭圆曲线密码的多服务器环境下三因子认证协议[J]. 计算机应用研究, 2017, 34(10): 3061-3067.

(上接第 130 页)

[3] 张 雷, 陈 康, 张在飞. 20 路多种类串口卡的设计与实现[J]. 计算机与现代化, 2013(8): 187-191.

[4] 刘桂芝, 都明宇. 监狱安全防范综合管理系统效能评估指标体系分析[J]. 物联网技术, 2016(12): 42-44.

[5] 付 萍. 安全防范系统效能评估研究综述[J]. 科技资讯, 2008(22): 13-14.

[6] 韦瑞林, 董培媛. 对"平安城市"建设及信息化实施方略的研究[J]. 信息安全与技术, 2013(4): 3-5.

[7] 魏娟丽, 翟社平, 王万诚. 视频序列中人体运动目标的检测与跟踪研究[J]. 计算机应用与软件, 2006, 23(4): 139-141.

[8] 李 华, 吴福朝, 胡占义. 一种新的线性摄像机自标定方法[J]. 计算机学报, 2000, 23(11): 1121-1129.

[9] 陈晓明. C⁴ISR 系统效能评估研究[J]. 电光与控制, 2010, 17(1): 48-50.

[10] 石 际. "平安城市"中各种组网方式与 PON 在"平安城市"中的优势[J]. 数字技术与应用, 2012(7): 236.

[11] 徐贵宝, 刘 多. 视频通信的现状与发展趋势[J]. 通信管理与技术, 2007(1): 11-15.

[12] 张 君. 加固计算机肋片散热器的优化设计[J]. 计算机与现代化, 2014(6): 120-123.

[13] 侯志强, 韩崇昭. 基于像素灰度归类的背景重构算法[J]. 软件学报, 2005, 16(9): 1568-1576. PHam

[14] HICKS M J, SNELL M S, SANDOVAL J S, et al. Physical protection systems-cost and performance analysis: a case study[J]. IEEE Aerospace and Electronic Systems Magazine, 1999, 14(4): 9-13.

[15] LI W, XIE L, DENG Z, et al. False sequential logic attack on SCADA system and its physical impact analysis[J]. Computers & Security, 2016, 58: 149-159.

[16] DENG Z, XIE L, RONG Y, et al. Data security transmission mechanism in industrial networked control systems against deception attack[J]. International Journal of Security and Its Applications, 2016, 10(4): 391-404.

[17] LI W, XIE L, LIU D, et al. False logic attacks on SCADA control system[C]//Services computing conference. [s. l.]: IEEE, 2014: 136-140.

[18] LEONE A, DISTANTE C. Shadow detection for moving objects based on texture analysis[J]. Pattern Recognition, 2007, 40(4): 1222-1233.