文章编号:1009-3087(2016)01-0091-08 DOI:10.15961/j.jsuese.2016.01.014

基于智能卡的多服务器远程匿名认证密钥协商协议

李艳平[1],刘小雪[1],屈 娟[2],鲁来凤[1]
(1.陕西师范大学 数学与信息科学学院,陕西 西安 710119;2.重庆三峡大学 数学与统计学院,重庆 404000)

摘 要:针对Xu等近期提出的一个基于智能卡的动态身份用户远程认证方案(简称XJWM)进行分析,指出其不能抵抗冒充攻击和密钥泄露攻击,且不能实现前向安全和后向安全。利用Diffie-Hellman密钥协商算法及生物认证技术,提出一个新的多服务器环境下多因子远程匿名认证密钥协商协议。新方案不仅有效弥补了XJWM方案存在的安全缺陷,而且增加了智能卡对持卡者的口令与生物信息的认证,避免了智能卡丢失引起的冒充攻击。最后,用改进的BAN逻辑证明了新方案密钥协商的正确性、会话密钥机密性与新鲜性以及双向认证性。安全性和性能分析说明,新方案在少量增加计算量的情况下具有良好的安全性。

关键词:智能卡;密钥协商;匿名认证;Burrows-Abadi-Needham(BAN)逻辑
中图分类号:TN918;TP393 **文献标志码**:A

Multi-server Anonymous Remote Authenticated Key Agreement Protocol Based on Smart Card

LI Yanping[1], *LIU Xiaoxue*[1], *QU Juan*[2], *LU Laifeng*[1]
(1. College of Mathematics and Info. Sci., Shaanxi Normal Univ., Xi'an 710119, China;
2. School of Maths. and Statistics, Chongqing Three Gorges Univ., Chongqing 404000, China)

Abstract: In order to efficiently eliminate the security shortcomings of the dynamic ID based remote user authentication scheme using smart cards (short for XJWM scheme) proposed by Xu et al., a new multi-server and multi-factor anonymous remote authenticated key agreement protocol was presented, based on Diffie-Hellman key agreement algorithm and biometrical authentication technology. The new protocol can not only overcome the security flaws of XJWM scheme, but also add smart card's password and bio information authentication for the cardholder to avoid the smart card stolen attack. The security of the new protocol was proved by the improved BAN logic and the result showed that the new scheme can ensure the correctness of key agreement, key confidentiality, key freshness and mutual authentication. The security and performance analysis demonstrated that the proposed protocol provides better security without increasing too much computation overhead.

Key words: smart card; Diffie-Hellman key agreement; anonymous authentication; BAN logic

随着人们对网络的依赖与日俱增,单服务器已无法满足人们的基本需求。文献[1]研究发现,通常每个用户在1个月内平均登陆25个不同的服务器,需用户反复注册,并记住大量的用户名及口令,给用户带来诸多不便与安全隐患。在多服务器环境中,若一个账户和口令可登录多个服务器并获得不同服务器的网络服务,则可给用户带来极大便利。因此,设计安全有效的多服务器环境下的认证协议是亟待解决的应用需求问题。

2000年,Lee等[2]基于大数分解问题和Hash函数的单向性,首次提出一个多服务器环境下的身份认证协议。不久,该方案被证明无法实现其声称的用户匿名性并存在2种攻击[3]。后来,Liao等[4]提出基于智能卡的多服务器动态ID认证方案,实现了用户的匿名性,但因不能实现双向认证,故易受中间人攻击。Lee等[5]提出一个基于动态身份的远程多

收稿日期:2015-09-22
基金项目:国家自然科学基金资助项目(61402275;61402015;61272436;61373150);陕西师范大学研究生培养创新基金资助项目(2015CXS022)
作者简介:李艳平(1978—),女,副教授,博士.认证议及其可证安全性研究. E-mail:lyp@snnu.edu.cn
网络出版时间:2016-1-11 19:33:27 **网络出版地址**:http://www.cnki.net/kcms/detail/51.1596.T.20160111.1933.002.html

服务器认证方案。2013 年,Xu 等[6]指出 Lee 等方案不能抵抗离线字典攻击,且方案效率低,口令不易更改,并提出一个新的方案(XJWM 方案),经分析发现该方案依旧存在 3 个严重的安全漏洞。Chuang 和 Chen[7]提出一个基于生物信息的多服务器的认证密钥协商协议,但该方案存在服务器仿冒攻击、用户冒充攻击、智能卡丢失攻击[8-11]。由于口令容易泄露、遗忘,智能卡容易丢失、共享,仅基于口令智能卡的认证易存在安全隐患。相比之下,将稳定的、易于提取的生物信息作为可靠的认证因子成为近年认证协议研究的主流技术[7-12]。

基于 XJWM 方案,结合生物认证技术[7-12],设计了一个基于智能卡、口令与生物信息的多因子认证密钥协商协议。先对持卡人通过口令及指纹信息进行双因子认证,认证通过智能卡才能激活,以协助用户完成与服务器的认证与密钥协商。其中,指纹信息比人脸、虹膜更易于提取且不易伪造,一定程度上提高了方案可行性与安全性[8]。整个认证与密钥协商过程仅需 2 条交互消息,且在交互过程中运用动态的身份信息代替用户真实身份,保护了用户隐私。用改进的 BAN 逻辑[11]证明了新方案密钥协商的正确性、会话密钥机密性与新鲜性及双向认证性。

1 XJWM 方案概要

XJWM 方案中参与方有用户 U_i、服务器、注册中心 RC(其中,RC 与每个服务器共享 $h(x)$,x 为系统主密钥)。方案包括 5 个阶段[6]:注册阶段、用户登录阶段、认证阶段、会话密钥更新阶段和口令变更阶段(因口令变更阶段与 XJWM 方案安全性分析无关,故略去)。方案中所使用的部分符号及其含义如表 1 所示。

表 1 部分符号及其含义

Tab. 1 Part of notations

符号	定义
$\|$	字符串链接符号
$\oplus$	异或操作运算
$h(\cdot)$	单向 Hash 函数
$E_k(\cdot)/D_k(\cdot)$	密钥 k 下对称加、解密算法,$\|k\|=l$
$A\Rightarrow B:M$	A 将消息 M 通过安全信道发给 B
$A\rightarrow B:M$	A 将消息 M 通过公开信道发给 B

1.1 注册阶段

R1:U_i 选取身份 ID_i 及口令 PW_i,生成随机数 b,计算 $CID=h(ID_i\|b)$。然后,$U_i\rightarrow RC:CID$。

R2:RC 计算 $B_i=h(CID\|h(x))$,将$(CID,B_i,h(\cdot))$ 写入智能卡。然后,$RC\Rightarrow U_i$:智能卡。

R3:U_i 计算 $R_i=h(PW_i\|ID_i)$,$BPW=h(PW_i\oplus ID_i)\oplus B_i$,将 R_i、BPW 代替 B_i 写入智能卡中。最终,智能卡中包含信息$(CID,R_i,BPW,h(\cdot))$。

1.2 用户登录

L1:U_i 插入智能卡,输入 ID_i' 和 PW_i'。

L2:智能卡验证 $R_i'=h(PW_i'\|ID_i')\stackrel{?}{=}R_i$。如果不相等,则拒绝请求。否则,执行 L3。

L3:智能卡产生 2 个随机数 b_{new} 和 N_i,计算 $CID_{new}=h(CID\|b_{new})$,$V_i=CID_{new}\oplus h(B_i\|N_i)$,$Q_i=h(CID_{new}\|B_i\|N_i)$,$U_i\rightarrow S_j:CID,V_i,Q_i,N_i$。

1.3 认证阶段

V1:S_j 计算 $B_i=h(CID\|h(x))$,$CID_{new}=h(B_i\|N_i)\oplus V_i$,验证 $Q_i\stackrel{?}{=}h(CID_{new}\|B_i\|N_i)$。若不等,则放弃对此登录请求继续认证。若相等,则执行 V2。

V2:S_j 产生一个随机数 N_j,计算 $B_{new}=h(CID_{new}\|h(x))$,$V_j=B_{new}\oplus h(B_i\|N_j)$,$Q_j=h(CID\|B_{new}\|N_j)$。然后 $S_j\rightarrow U_i:V_j,Q_j,N_j$。

V3:U_i 计算 $B_{new}=V_j\oplus h(B_i\|N_j)$,验证 $Q_j\stackrel{?}{=}h(CID\|B_{new}\|N_j)$。若不等,则终止会话。否则,$U_i$ 成功认证 S_j。然后,U_i 计算 $BPW_{new}=B_{new}\oplus h(PW_i\oplus ID_i)$,将$(CID_{new},BPW_{new})$ 写入数据库。最后,U_i 计算会话密钥 $SK=h(N_i\|N_j\|B_i)$ 和 $Q_{ij}=h(N_i\|B_i\|N_j\|B_{new})$。$U_i\rightarrow S_j:Q_{ij}$。

V4:S_j 验证 $Q_{ij}\stackrel{?}{=}h(N_i\|B_i\|N_j\|B_{new})$。若不等,则终止会话。否则,$S_j$ 计算会话密钥 $SK=h(N_i\|N_j\|B_i)$。

1.4 会话密钥更新阶段

C1:U_i 产生随机数 N_i^*,计算 $V_i^*=N_i^*\oplus h(B_i\oplus h(N_i\|N_j))$,$Q_i^*=h(N_i^*\oplus B_i)$。$U_i\rightarrow S_j:V_i^*,Q_i^*$。

C2:S_j 计算 $N_i^*=V_i^*\oplus h(B_i\oplus h(N_i\|N_j))$,检验 $Q_i^*\stackrel{?}{=}h(N_i^*\oplus B_i)$。若不等,拒绝申请。否则,产生随机数 N_j^*,计算 $V_j^*=N_j^*\oplus h(B_i\oplus h(N_i\|N_j))$,$Q_j^*=h(N_j^*\oplus B_i)$,$S_j\rightarrow U_i:V_j^*,Q_j^*$。

C3:U_i 计算 $N_j^*=V_j^*\oplus h(B_i\oplus h(N_i\|N_j))$,$Q_j^*\stackrel{?}{=}h(N_j^*\oplus B_i)$,若不等,终止会话。否则,计算新的会话密钥 $SK=h(N_i^*\|N_j^*\|B_i)$,并计算 $Q_{ij}^*=h(N_i^*\oplus N_j^*\oplus B_i)$,$U_i\rightarrow S_j:Q_{ij}$。

C4:S_j 验证 $Q_{ij}^*\stackrel{?}{=}h(N_i^*\oplus N_j^*\oplus B_i)$。若不等,终止会话。否则,计算新会话密钥 $SK^*=h(N_i^*\|N_j^*\|B_i)$。

2　XJWM 方案的安全性分析

2.1　冒充攻击

在多服务器环境中,每个服务器拥有相同的 $h(x)$,恶意服务器 S_k 可成功冒充用户 U_i 和诚实服务器 S_j。

1) 冒充合法用户 U_i

S_k 截获消息 CID,计算出 $B_i = h(CID \| h(x))$,选择随机数 b_{new}^* 和 N_i^*,计算 $CID_{new}^* = h(CID \| b_{new}^*)$,$V_i^* = CID_{new}^* \oplus h(B_i \| N_i^*)$,$Q_i^* = h(CID_{new}^* \| B_i \| N_i^*)$,$S_k \rightarrow S_j$:$CID, V_i^*, Q_i^*, N_i^*$,收到消息后,$S_j$ 计算 $B_i = h(CID \| h(x))$,$CID_{new}^* = V_i^* \oplus h(B_i \| N_i^*)$,验证 $Q_i^* \stackrel{?}{=} h(CID_{new}^* \| B_i \| N_i^*)$,等式显然成立。至此,$S_k$ 冒充 U_i 成功通过 S_j 验证。

2) 冒充合法服务器 S_j

S_k 截获消息 V_j、Q_j、N_j,选择随机数 N_j^*,计算 $B_{new} = h(h(CID \| b_{new}^*) \| h(x))$,$V_j^* = B_{new} \oplus h(B_i \| N_j^*)$,$Q_j^* = h(CID \| B_{new} \| N_j^*)$,$S_k \rightarrow U_i$:$V_j^*, Q_j^*, N_j^*$。收到消息后,$U_i$ 计算 $B_{new} = V_j^* \oplus h(B_i \| N_j^*)$,验证 $Q_j^* \stackrel{?}{=} h(CID \| B_{new} \| N_j^*)$,等式显然成立。至此,$S_k$ 冒充 S_j 成功通过 U_i 验证。

2.2　密钥泄露攻击

任意攻击者,通过边信道攻击技术[13-15],获取智能卡中的秘密信息 R_i、BPW 并截获公共信道中的 N_i、N_j,攻击者计算 $B_i = BPW \oplus R_i$,利用 N_i、N_j 求出会话密钥 $SK = h(N_i \| N_j \| B_i)$。故在智能卡非抗窜扰假设下,XJWM 方案不能抵抗密钥泄露攻击。

2.3　不满足前向安全和后向安全性

从第 1.4 节会话密钥更新阶段可看出,新的会话密钥 $SK^* = h(N_i^* \| N_j^* \| B_i)$ 中 B_i 一直不变。由第 2.1 节可知,若 $h(x)$ 泄漏或智能卡内信息被非法读取,攻击者易计算得 B_i,也易从公共信道上截获之前的 N_i、N_j 或从之后交互信息计算出 N_i^*、N_j^*。从而攻击者可轻松计算得之前的会话密钥 SK 和新的会话密钥 SK^*,进一步可解密用 SK 加密或者 SK^* 加密的一切消息,即 XJWM 方案不满足前向安全和后向安全性。

3　多服务器环境下远程匿名认证与密钥协商协议

提出的方案保留了 XJWM 方案优点,弥补了原方案的不足。考虑到会话时间较短且更新会话密钥计算成本类似于会话密钥协商成本,故提出的方案中舍去会话密钥更新阶段,新增了系统初始化阶段用于产生注册中心 RC 与多服务器共享参数,以及智能卡丢失后重新颁发阶段,故提出的方案共包括以下 6 个阶段。

3.1　系统初始化阶段

RC 建立系统参数:选素数 p 满足 $2^{L-1} < p < 2^L$,$L = 1\,024$,素数 q 满足 $q \mid p-1$ 且 $\mid q \mid \geq 512$,任意 $h(1 < h < p-1)$ 满足 $g = h^{(p-1)/q} \bmod p > 1$。选择 Hash 函数 $h_1(\cdot):\{0,1\}^* \rightarrow \{0,1\}^l$、$h_2(\cdot):\{0,1\}^* \rightarrow Z_q^*$、$h_3(\cdot):\{0,1\}^* \rightarrow G$,并公开 $(p, q, g, h_1(\cdot), h_2(\cdot), h_3(\cdot))$。设 RC 拥有 t 个服务器 $\{S_1, S_2, \cdots, S_t\}$,每个服务器 S_j 选择随机数 $SK_{S_j} = x_{S_j} \in Z_q^*$ 作为私钥,计算相应公钥 $PK_{S_j} = g^{x_{S_j}} \bmod p$ 并公开。RC 随机选取系统主密钥 x 并与所有服务器共享,随机选取 y_j 为 S_j 在 RC 处身份标志。$RC \Rightarrow S_j$:x, y_j,秘密保留 x 和 (y_j, S_j) 列表。

3.2　注册阶段

R1:U_i 选取用户名 ID_i,利用指纹采集仪采集指纹数字信息 b_i,然后,$U_i \Rightarrow RC$:ID_i, b_i。

R2:RC 检查 ID_i、b_i 是否已在数据库。若为首次注册,令注册次数 $I = 1$,否则,令 $I = I + 1$。RC 产生随机数 r_i,计算 $CID_i = h_1(ID_i \| b_i \| r_i \| I)$(随机化用户匿名),$B_i = h_1(CID_i \| x)$。令 $Set = \{h_1(y_1), h_1(y_2), \cdots, h_1(y_t)\}$,将 $(CID_i, B_i, Set, h_1(\cdot), h_2(\cdot), h_3(\cdot))$ 写入智能卡。并将列表 (ID_i, b_i, r_i, I) 写入数据库。$RC \Rightarrow U_i$:智能卡。

R3:U_i 先选口令 PW_i,接着计算 $R_i = h_3(ID_i \| PW_i)^{h_2(b_i)} \bmod p$,$BPW = B_i \oplus h_1(PW_i \| R_i)$,然后,将 R_i、BPW 替换 B_i 写入智能卡。最终,智能卡上存储信息为 $(CID_i, R_i, BPW, Set, h_1(\cdot), h_2(\cdot), h_3(\cdot))$。

3.3　用户登录

L1:U_i 将智能卡插入服务器 S_j 远程终端读卡器,采集指纹信息提取数字特征 b_i,输入 ID_i、PW_i、b_i。

L2:智能卡验证 $h_3(ID_i \| PW_i)^{h_2(b_i)} \bmod p \stackrel{?}{=} R_i$。若不相等,智能卡显示失败,终止登录(智能卡对合法用户的认证)。否则,执行 L3。

L3:智能卡通过远程终端读卡器读取服务器的 y_j,验证 $h_2(y_j) \in Set$。若不通过,则终止登录。否则,取随机数 $a \in Z_q^*$ 和当前时戳 T_i,计算 $A = g^a \bmod p$,$B_i = BPW \oplus h_1(PW_i \| R_i)$,$Q_i = h_1(CID_i \| B_i \| h_1(y_j) \| T_i)$,$DH = PK_{S_j}^a \bmod p$,$C = E_{DH}[CID_i, Q_i, T_i]$。最后 $U_i \rightarrow S_j$:A, C。

3.4 认证阶段

R1:S_j 取当前时戳 T_i^*,计算 $DH = A^{SK_j} \bmod p$,$D_{DH}[C] = \{CID_i, Q_i, T_i\}$,验证 $T_i^* - T_i \overset{?}{\leq} \Delta T$($\Delta T$ 为平均网路时延)。若不成立,则终止认证;否则,计算 $B_i = h_1(CID_i \| x)$,并验证 $h_1(CID_i \| B_i \| h_1(y_j) \| T_i) \overset{?}{=} Q_i$,若不相等,则终止认证,否则,执行 R2。

R2:S_j 取随机数 $d \in Z_q^*$ 和当前时戳 T_j,计算 $Q_j = h_1(CID_i \| B_i \| h_1(y_j) \| T_j)$,$D = g^d \bmod p$,$DH' = A^d \bmod p$,$C' = E_{DH'}[Q_j, T_i, T_j]$ 和会话密钥 $SK = h_1(DH' \| T_i \| T_j)$。$S_j \rightarrow U_i: D, C'$。

R3:U_i 计算 $DH' = D^a \bmod p$,解密 $D_{DH'}[C'] = \{Q_j, T_i, T_j\}$,取当前时戳 T_j^* 验证 $T_j^* - T_j \overset{?}{\leq} \Delta T$。若不成立,则终止认证;否则,验证 $Q_j \overset{?}{=} h_1(CID_i \| B_i \| h_1(y_j) \| T_j)$,若不等则终止认证,否则,$U_i$ 成功认证 S_j 并计算得会话密钥 $SK = h_1(DH' \| T_i \| T_j)$。

3.5 口令变更阶段

因敌手易进行口令猜测攻击,用户需定期更新智能卡口令,用户执行以下操作:

C1:U_i 插入智能卡,提取指纹数字信息 b_i,输入 ID_i、PW_i、b_i,请求修改旧口令 PW_i。

C2:智能卡验证 $h_3(ID_i \| PW_i)^{h_2(b_i)} \bmod p \overset{?}{=} R_i$。若不等,则拒绝修改;否则,智能卡提示 U_i 输入新口令 PW_{new}。

C3:智能卡计算 $R_{new} = h_1(ID_i \| PW_{new})^{h_2(b_i)} \bmod p$,$BPW_{new} = B_i \oplus h_1(PW_{new} \| R_{new})$,用 R_{new} 和 BPW_{new} 替换原来的 R_i、BPW 并保存到智能卡中。

3.6 智能卡重新颁发与升级

吊销:智能卡被盗或丢失,任何其他用户要激活智能卡进行远程认证登录,必须输入 ID_i、PW_i、b_i 并验证 $h_3(ID_i \| PW_i)^{h_2(b_i)} \bmod p \overset{?}{=} R_i$,$R_i$ 存储于智能卡内。因生物信息 b_i 是唯一的,任何其他用户无法激活智能卡,故丢失的智能卡只能报废,提出的方案无需考虑智能卡吊销问题。

补发:丢失智能卡的 U_i 可向 RC 提交指纹信息 b_i,申请颁发新智能卡。RC 通过 b_i 从数据库中找出列表 (ID_i, b_i, r_i, I),令 $I = I + 1$,重复注册阶段 R2 和 R3,生成新智能卡给用户。

升级:用户 U_i 可定期向 RC 请求升级智能卡,用户向 RC 提供 ID_i、b_i 和智能卡,RC 查找已存列表 (ID_i, b_i, r_i, I),计算 $h_1(ID_i \| b_i \| r_i \| I)$ 与智能卡内存储的 CID_i 进行匹配。若匹配失败,RC 拒绝请求;否则 RC 动态更新智能卡中 Set 集服务器列表,完成智能卡的升级。

4 提出的方案安全性分析与证明

假设:① 求解群 $G = \langle g \rangle$ 中离散对数问题(DLP)是困难的;②RC 是诚实可信的,即 RC 不会冒充诚实服务器和用户;③ 智能卡是非抗窜扰的,即敌手 $\mathcal{A}$ 可通过边信道攻击技术[13-15],获取智能卡中存储的秘密信息。因认证协议的理想属性和安全目标尚无明确文献规定,选择用户匿名性、双向认证性、前向安全性 3 个主要的理想属性以及抗离线口令猜测攻击、抗内部人攻击、抗智能卡丢失攻击等 5 个主要安全目标展开分析。

4.1 安全性分析

4.1.1 匿名性

提出的方案中,公开信道上交互的所有信息均无用户 ID_i 的明文形式,而是被系统随机化后的匿名 $CID_i = h_1(ID_i \| b_i \| r_i \| I)$。由 Hash 函数的单向性知敌手 $\mathcal{A}$ 无法求出 ID_i。即使通过边信道攻击获得智能卡上存储的信息,敌手 $\mathcal{A}$ 也无法从 CID_i、R_i 推导出用户 ID_i 信息。在 U_i 与服务器 S_j 认证过程中,S_j 只知道通过匿名 CID_i 获得服务器的相关信息,不知道其真实身份,有效地保护了用户的匿名性和隐私性。

4.1.2 双向认证性

利用 Diffie-Hellman 密钥交换,用户 U_i 利用 S_j 的公钥加密信息得密文 C,只有当使用 S_j 的私钥才能解密 C 且返回消息中有 T_i 时,说明对方拥有服务器 S_j 的私钥。同理当 U_i 收到 (D, C') 时,只有 U_i 的随机值 a 才能生成正确密钥 DH' 并解密 C',说明 S_j 的匿名通信对象前后一致,即 U_i 与服务器 S_j 实现了双向认证。

4.1.3 会话密钥的前向安全性和后向安全性

会话密钥 $SK = h_1(DH' \| T_i \| T_j)$ 由双方选择随机数 a、d、T_i、T_j 所决定。因每次认证时所选取的随机数和登录时间不同,且这些信息只有认证双方才知道,故每次产生的会话密钥也不同且只有协商双方知晓,即会话密钥满足新鲜性与机密性。敌手 $\mathcal{A}$ 无法从当前的会话密钥计算出前一轮或后一轮会话密钥,因此,提出的方案具有会话密钥的前后向安全性。

4.1.4 抗离线口令猜测攻击

由第 4.1.1 节可知提出的方案满足匿名性,$\mathcal{A}$ 无法获得用户 ID_i。由 Hash 函数的单向性知,$\mathcal{A}$ 要伪造出 PW_i^*、ID_i^* 与 b_i^* 使得 $R_i = h_3(ID_i \| PW_i)^{h_2(b_i)} \bmod p =$

$h_3(ID_i^* \| PW_i^*)^{h_2(b_i^*)} \bmod p$ 成立是困难的。即$\mathcal{A}$获得智能卡中存储的 R_i,利用离线口令猜测 PW_i 并通过验证也是困难的,因此提出的方案抗离线口令猜测攻击。

4.1.5　抗智能卡丢失攻击

设$\mathcal{A}$通过边信道攻击获得智能卡中的秘密信息 $(CID_i, R_i, BPW, Set, h_1(\cdot), h_2(\cdot), h_3(\cdot))$,由第 4.1.1 节知,$\mathcal{A}$无法获取用户的 ID_i 及 PW_i,再次登陆时需指纹数字信息,由指纹信息的不可伪造性,敌手$\mathcal{A}$无法冒充用户激活智能卡协助其登录服务器,故提出的方案可抵抗智能卡丢失攻击。

4.1.6　抗内部攻击

多服务器环境中,RC 管辖的所有服务器拥有相同的 $h(x)$ 和不同的电子身份标志 y_j。S_k 在未知 y_j 的情况下冒充 S_j,需通过验证 $h_1(CID_i \| B_i \| h_1(y_j) \| T_i) \stackrel{?}{=} Q_i$。此外,每个服务器都有不同的公私钥对,$S_k$ 无法解密 U_i 发给 S_j 的消息 (A, C),从而无法冒充 S_j,故提出的方案能抵抗恶意服务器内部攻击[15]。由第 4.1.5 节可知恶意用户 U_k 因为不能提供正确的 ID_i、PW_i、b_i 来激活用户 U_i 的智能卡,故提出的方案能抵抗恶意用户内部攻击。

4.1.7　抗中间人攻击

若中间敌手$\mathcal{A}$想冒充合法用户 U_i 取信 S_j,首先须伪造出认证挑战(A^*, C^*)。假设$\mathcal{A}$通过边信道攻击获得智能卡中秘密信息 $(CID_i, R_i, BPW, Set, h_1(\cdot), h_2(\cdot), h_3(\cdot))$,选择当前时间戳 T^* 和随机值 $a^* \in Z_q^*$,易构造 $A^* = g^{a^*} \bmod p$,$DH^* = PW_{S_j}{}^{a^*} \bmod p$,难构造 $C^* = E_{DH^*}(CID_i, Q_i^*, T^*)$,因敌手不知道主密钥 x 和 $h_1(y_j)$,故难以构造合法的 $B_i^* = h_1(CID_i \| x^*)$ 和 $Q^* = h_1(CID_i \| B_i^* \| h_1(y_j^*) \| T^*)$ 让服务器 S_j(拥有身份标志 y_j)并通过验证 $h_1(CID_i \| B_i \| h_1(y_j) \| T^*) \stackrel{?}{=} Q_i$。因此,提出的方案能抵抗中间人冒充用户攻击。

若$\mathcal{A}$想冒充合法服务器 S_j 取信 U_i,首先要伪造出认证响应(D^*, C'^*)。设$\mathcal{A}$获得智能卡中秘密信息 $(CID_i, R_i, BPW, Set, h_1(\cdot), h_2(\cdot), h_3(\cdot))$,选择当前时戳 T^* 和随机数 $d^* \in Z_q^*$,易计算 $D^* = g^{d^*} \bmod p$,$DH'^* = A^{d^*} \bmod p$,$C'^* = E_{DH'^*}(Q_j^*, T_i^*, T^*)$,其中,$Q_j^* = h_1(CID_i \| B_i^* \| h_1(y_j^*) \| T^*)$。敌手$\mathcal{A}$不知道主密钥 x 和 $h_1(y_j)$,伪造 $B_i^* = h_1(CID_i \| x^*)$ 和 $h_1(y_j^*)$。U_i 收到(D^*, C'^*),选择当前时间戳 T_j^*,计算 $DH'^* = D^{*a} \bmod p$,$D_{DH'^*}(C'^*) = (Q_j^*, T_i^*, T^*)$,验证 $h_1(CID_i \| B_i \| h_1(y_j) \| T^*) \stackrel{?}{=} Q_j^*$。因此,提出的方案能抵抗中间人冒充服务器攻击。

综上所述,提出的新方案能抵抗中间人攻击。

4.1.8　抗重放攻击

提出的方案中采用了随机数 a、d 和自验证的时间戳 T_i、T_j[16],参与生成会话密钥,由于每次登陆时 4 个值不同,既保证了会话密钥新鲜性,又有效防止了重放攻击。时间戳作为认证方案的随机数参与协议,节省了产生随机数的计算开销。灵活的平均网络时延 ΔT 释放了时间同步性要求。

因用户 U_i 对服务器 S_j 是匿名的,故 S_j 只需认证会话对象前后一致即可。用户 U_i 只有输入正确的 ID_i、PW_i、b_i 才能激活智能卡,故只要智能卡开始认证计算,服务器 S_j 就认为 U_i 为智能卡的合法拥有者。因注册阶段的交互信息均在安全信道上传输,可认为注册阶段是安全的。

4.2　安全性证明

2001 年,李益发首次克服了 BAN 类逻辑分析协议时需要理想化过程的缺陷,提出 BAN 逻辑分析认证密钥协议的改进方法。改进的 BAN 逻辑继承原逻辑简单实用优点,且将认证逻辑建立在谓词逻辑坚实理论之上,使公理系统更加可靠[11]。下面介绍后继证明中用到的符号、公理及定理。

1)基本的命题符号

Σ为所有消息集,$\Im$ 为时间戳集,$\aleph$ 为随机数集,$\Re$ 为协议中新建会话密钥集,$\neg A$ 表示 A 的否定,$P \ni X$ 表示 P 生成了 X,$P \mid\equiv X$ 表示 P 相信 X 是真的,$P \lhd X$ 表示 P 看见了 X,$X > P$ 表示 X 是给 P 的,$\&(P)$ 表示 P 正在参与执行协议的通信,$\#(X)$ 表示 X 是新鲜的,$Y = \rho(X)$ 表示 Y 包含 X 或由 X 和其他比特串级联生成,$P \Rightarrow Q$ 表示 P 的意定的协议对象是 Q,$P \overset{K}{\leftrightarrow} Q$ 表示 K 是 P 和 Q 的共享密钥,$\{X\}_K$ 为用密钥 K 加密消息 X 所得的密文,$\Gamma \mid\lhd X$ 表示 X 仅且由集合 Γ 的成员共享,$\Gamma \lhd X$ 表示最多只有 Γ 的成员看见了 X,$\{\varphi, \psi\} \mid\!- \xi$ 表示由 φ 和 ψ 可推导出 ξ。

2)公理及定理

①基本集合公理

$$\mathrm{ABS}: X \in \Sigma \rightarrow (P \mid\equiv X \in \Sigma \leftrightarrow P \lhd X)。$$

②函数集合判别公理

$$\mathrm{AGF}: (P \lhd \{X_1, \cdots, X_n\}) \rightarrow (P \lhd F(X_1, \cdots, X_n));$$

$$\mathrm{ATM4}: (P \mid\equiv X \in \Sigma) \leftrightarrow (X = H(Y) \wedge P \mid\equiv Y \in \Sigma)。$$

③消息生成公理

$$\mathrm{AMG2}: X \in \aleph \cup \Pi \rightarrow (P \ni X \rightarrow P \mid\equiv \#(X))。$$

④身份认证公理

$$\mathrm{AIP3}: P \mid\equiv (Q \mid\approx X \in \Sigma) \rightarrow P \mid\equiv \&(Q),$$

AIP6:$(X \in \Sigma \wedge P \mid\sim X \succ Q) \rightarrow (P \Rightarrow Q)$。

⑤新鲜性公理

AFM1:$(X \in \Im) \rightarrow (P \mid\equiv Q \mid\sim \rho(X) \rightarrow P \mid\equiv \#(\rho(X))$,

AFM3:$(X \in \Sigma \wedge \#(X)) \rightarrow (\rho(X) \in \Sigma \rightarrow \#(\rho(X)))$。

⑥由符号给出的定理

TDD10:$(P \overset{K}{\leftrightarrow} Q) \leftrightarrow (K \in \Re \wedge \{P,Q\} \mid\equiv \{P,Q\} \mid\trianglelefteq K)$;

TDD15:$P \mid\approx X \leftrightarrow (P \mid\sim X \wedge \#(X))$。

⑦关于对称密钥定理

TSK14:$(P \overset{K}{\leftrightarrow} Q) \rightarrow (P \lhd \{X\}_K \rightarrow (P \lhd X))$。

⑧非对称密钥公理

AAK2:$P \mid\equiv K \in \Re \rightarrow ((P \lhd K) \wedge P \mid\equiv (Q \lhd K^{-1} \rightarrow Q \mid\trianglelefteq K^{-1}))$。

⑨关于“说过”谓词的定理

TSD1:$\{P \lhd \{X\}_K, P \overset{K}{\leftrightarrow} Q, P \mid\equiv \neg (P \ni \{X\}_K), P \mid\equiv X \in \Sigma\} \mid- P \mid\equiv Q \mid\sim \{X\}_K$。

⑩关于信宿定理

TDM1:$\{P \lhd \{X\}_K, P \overset{K}{\leftrightarrow} Q, P \mid\equiv \neg (P \ni \{X\}_K), P \mid\equiv X \in \Sigma\} \mid- P \mid\equiv X \succ P$。

用改进的BAN逻辑[12]证明提出方案的登陆与认证密钥协商阶段是安全的。

1)协议描述

msg1:$U_i \rightarrow S_j : g^a, \{M, T_i, h_1(M \parallel N \parallel T_i)\}_{DH}$;

msg2:$S_j \rightarrow U_i : g^d, \{T_i, T_j, h(M \parallel N \parallel T_j)\}_{DH'}$。

其中,$M = h_1(U_i \parallel r \parallel I)$,$N = h_1(M \parallel x) \parallel h_1(y_j)$。

认证完成的同时获得会话密钥

$$SK = h_1(DH' \parallel T_i \parallel T_j)。$$

2)协议理想化描述

T1:$S_j \lhd g^a, S_j \lhd \{M, T_i, h_1(M \parallel N \parallel T_i)\}_{DH}$;

T2:$U_i \lhd g^d, U_i \lhd \{T_i, T_j, h(M \parallel N \parallel T_j)\}_{DH'}$。

3)协议初始化假设

H1:$U_i \mid\trianglelefteq a, U_i \mid\equiv \#(a), U_i \mid\equiv \#(T_i)$。

H2:$S_j \mid\trianglelefteq d, S_j \mid\equiv \#(d), S_j \mid\trianglelefteq SK_{SK_j}, S_j \mid\equiv \#(T_j)$。

H3:$U_i \mid\equiv \neg (U_i \ni \{T_i, T_j, h_1(M \parallel N \parallel T_j)\}_{DH'})$;

$U_i \mid\equiv \neg (U_i \ni g^d)$。

H4:$S_j \mid\equiv \neg (S_j \ni \{M, T_i, h_1(M \parallel N \parallel T_i)\}_{DH}$;

$S_j \mid\equiv \neg (S_j \ni g^a)$。

H5:$U_i \overset{M,N}{\leftrightarrow} S_j$。

H6:$\{DH, DH', SK\} \in \Re \subset \Sigma$。

H7:$\{T_i, T_j\} \in \Im \subset \Sigma, \{a, d\} \in \aleph \subset \Sigma$。

4)安全目标

G1:密钥协商的正确性

$U_i \lhd SK, U_i \mid\equiv SK \in \Sigma, S_j \lhd SK, S_j \mid\equiv SK \in \Sigma$。

G2:会话密钥的机密性

$\{U_i, S_j\} \trianglelefteq SK$。

G3:会话密钥的新鲜性

$U_i \mid\equiv \#(SK), S_j \mid\equiv \#(SK)$。

G4:方案的双向认证性

$U_i \mid\equiv \&(S_j), U_i \mid\equiv S_j \Rightarrow U_i, S_j \mid\equiv \&(U_i), S_j \mid\equiv U_i \Rightarrow S_j$。

证明:由H_1、H_2和DHP的困难性得:

S1:$\{U_i, S_j\} \mid\equiv \{U_i, S_j\} \mid\trianglelefteq \{DH, DH'\}$。

由S1、H6和TDD10得S2:$U_i \overset{DH,DH'}{\leftrightarrow} S_j$。

由S2、T1和TSK14得:

S3:$S_j \lhd (M, T_i, h_1(M \parallel N \parallel T_i))$。

由msg1和S3得S4:$S_j \mid\equiv (M, T_i) \in \Sigma$。

由H5、S4、ABS和ATM4得:

S5:$S_j \mid\equiv h_1(M \parallel N \parallel T_i) \in \Sigma$。

由S4和S5得:

S6:$S_j \mid\equiv (M, T_i, h_1(M \parallel N \parallel T_i)) \in \Sigma$。

由T1、H4、S2、S6、TSD1和TDM1得:

S7:$S_j \mid\equiv U_i \mid\sim (M, T_i, h_1(M \parallel N \parallel T_i))$;

$S_j \mid\equiv U_i \mid\sim (M, T_i, h_1(M \parallel N \parallel T_i)) \succ S_j$。

由H7、S7、AFM1和TDD15得:

S8:$S_j \mid\equiv \#(M, T_i, h_1(M \parallel N \parallel T_i))$;

$S_j \mid\equiv U_i \mid\approx (M, T_i, h_1(M \parallel N \parallel T_i))$。

由S6、S8和AIP3得:

S9:$S_j \mid\equiv \&(U_i)$。($*S_j$认证了U_i)

由S6、S9和AIP6得:

S10:$S_j \mid\equiv U_i \Rightarrow S_j$。($*S_j$相信$U_i$是协议对象)

由S6和msg2得S11:$S_j \lhd (T_i \parallel T_j)$。

由H7、S11和ABS得S12:$S_j \mid\equiv (T_i \parallel T_j) \in \Sigma$。

由H2、S2和S12得S13:$S_j \lhd SK$,其中,$SK = h_1(DH' \parallel T_i \parallel T_j)$。

由H2、H6、H7和AFM3得:

S14:$S_j \mid\equiv \#(SK)$。($*S_j$相信SK是新鲜的)

由H5、H6和ABS得:

S15:$S_j \mid\equiv SK \in \Sigma$。($*S_j$相信$SK$是正确的)

由T2、S2和TSK14得:

S16:$U_i \lhd (T_i, T_j, h_1(M \parallel N \parallel T_j))$。

由H1、H7、S16、ABS和ATM4得:

S17:$U_i \mid\equiv (T_i, T_j, h_1(M \parallel N \parallel T_j)) \in \Sigma$。

由T2、S2、S16、S17、TSD1和TDM1,得:

S18:$U_i \mid\equiv S_j \mid\sim (T_j, h_1(M \parallel N \parallel T_j))$;

$U_i \mid\equiv S_j \mid\sim (T_i, T_j, h_1(M \parallel N \parallel T_j)) \succ U_i$。

由H7、S18、AFM1和TDD15得:

S19:$U_i \mid\equiv \#(T_i, T_j, h_1(M \parallel N \parallel T_j))$;

$U_i \mid\equiv S_j \mid\approx (T_i, T_j, h_1(M \| N \| T_j))$。

由 S17、S19、和 AIP3 得:

S20:$U_i \mid\equiv \&(S_j)$。($*U_i$ 认证了 S_j)

由 S17、S20 和 AIP6 得:

S21:$U_i \mid\equiv S_j \Rightarrow U_i$。($*U_i$ 相信 S_j 是协议对象)

由 S17 和 msg1 得 S22:$U_i \lhd (T_i \| T_j)$。

由 H7、S22 和 ABS 得:

S23:$U_i \mid\equiv (T_i \| T_j) \in \Sigma$。

由 H1、S2 和 S23 得:

S24:$U_i \lhd SK$。($*U_i$ 计算出会话密钥 SK)

由 H1、H6、H7 和 AFM3 得:

S25:$U_i \mid\equiv \#(SK)$。($*U_i$ 相信 SK 是新鲜的)

由 H8、S25 和 ABS 得:

S26:$U_i \mid\equiv SK \in \Sigma$。($*U_i$ 相信 SK 是正确的)

由 S2、S15、S23 和 DLP 难题得:

S27:$\{U_i, S_j\} \lhd SK$。($*U_i$ 与 S_j 秘密共享 SK)

综上所述,提出的方案密钥协商的正确性、密钥机密性与新鲜性以及双向认证性均成立。

5　性能分析

在多服务器远程认证方案中,计算量集中在登陆与认证密钥协商阶段,故表 2、3 主要针对该阶段中提出的方案与文献[6 - 7,17 - 18]方案的通信复杂度(交互次数)、存储复杂度(交互消息长度)、计算复杂度以及安全性进行了比较。

表 2 中,t_h、t_e、t_s 分别为 Hash 函数运算时间(0.5 ms)、模指数运算时间(522 ms)、对称的加/解密时间(8.7 ms)[19],忽略不计轻量级⊕、‖ 运算。

表 2　性能比较分析

Tab. 2　Performance comparison

方案	交互次数	交互消息长度/bit	计算复杂度
Li 等方案[17]	2	2 096	$5t_h + 8t_e$
刘莎等方案[18]	2	3 328	$6t_h + 8t_e + 3t_s$
Chuang 等方案[7]	3	1 024	$17t_h$
XJWM 方案[6]	3	1 024	$17t_h$
提出的方案	2	2 304	$7t_h + 7t_e + 5t_s$

表 3　安全性比较

Tab. 3　Security comparison

方案	匿名性	双向认证与密钥协商	会话密钥的前后向安全	抗口令离线攻击	抗智能卡丢失攻击	抗内部攻击	抗重放攻击	智能卡撤销	可证明安全
Li 等方案[17]	否	是	是	是	否	否	否	否	否
刘莎等方案[18]	是	是	是	是	是	否	否	是	否
Chuang 等方案[7]	是	是	是	是	否	否	否	否	否
XJWM 方案[6]	否	是	否	是	是	否	是	否	否
提出的方案	是	是	是	是	是	是	否	是	是

表 3 中,交互消息长度是在假设随机数与 Hash 函数输出长度均为 128 bit,系统生成时间戳长度均为 128 bit,模为 1 024 bit,身份及口令的长度均为 128 bit[13]下计算的。

6　结　论

先分析了最近一个基于智能卡的动态身份用户远程认证方案的安全缺陷,分析存在漏洞的主要原因是在多服务器环境中每个服务器拥有相同的 $h(x)$,导致服务器之间易于冒充,且易导致密钥泄露。提出的方案中每个服务器拥有相同的 x 和不同标志的 y_j 来遏制服务器之间的恶意冒充。提出的方案增加了智能卡对持卡人的口令和生物信息的认证,能有效抵抗冒充攻击、会话密钥泄露攻击等。最后,利用改进的 BAN 逻辑证明提出的方案实现了认证密钥协商协议的安全目标,适用于移动网络和普适计算下的多服务器环境中。下一步拟研究不同自治域用户之间的认证与密钥协商协议[20]。

参考文献:

[1] Florencio D, Herley C. A large-scale study of web password habits [C]//Proceedings of the 16th International Conference on World Wide Web. New York: ACM, 2007: 657 - 666.

[2] Lee W B, Chang C C. User identification key distribution maintaining anonymity for distributed computer networks [J]. Computer System Science & Engineering, 2000, 15 (4): 211 - 214.

[3] Wu T S, Hsu C L. Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks [J]. Computers & Security, 2004, 32 (2): 120 - 125.

[4] Liao Y, Wang S. A secure dynamic ID based remote user

authentication scheme for multi-server environm-ent[J]. Computer Standards & Interfaces,2009,31(1):24 - 29.

[5]Lee C C,Lai Y M,Li C T. An improved secure dynamic ID based remote user authentication scheme for multi-server environment[J]. International Journal of Security and Its Application,2012,6(2):203 - 209.

[6]Xu C,Jia Z,Wen F,et. al. Cryptanalysis and improvement of a dynamic ID based remote user authentication scheme using smart cards[J]. Journal of Computational Information Systems,2013,9(14):5531 - 5520.

[7]Chuang C,Chen M. An anonymous multi-server authentication key agreement scheme based on trust computing using smart cards and biometrics[J]. Expert Systems with Applications,2014,41(4):1411 - 1418.

[8]Lin Hao,Wen Fengtong,Du Chunxia. An improved lightweight pseudonym identity based authentication scheme on multi-server environment[M]//Wireless Communications,Networking and Applications,Proceedings of WCNA 2014. New Delhi:Springer India,2016:1115 - 1126.

[9]Choi Y S,Nam J H,Lee D H,et al. Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics[J/OL]. The Scientific World Journal,2014,2014:281305. http://dx. doi. org/10.1155/2014/281305.

[10]Li C T,Lee C C,Chen H H,et al. Cryptanalysis of an anonymous multi-server authenticated key agreement scheme using smart cards and biometrics[C]//Proceedings of 2015 International Conference on Information Networking (ICOIN). Cambodia:IEEE,2015:498 - 502.

[11]Zan Yazhou,Liu Wenfen,Wei Jianghong. Negotiation scheme of multi-server authenticating key based on dynamic ID[J]. Journal of Information Engineering University,2014,15(6):654 - 663.[昝亚洲,刘文芬,魏江宏. 基于动态ID的多服务器认证密钥协商方案[J]. 信息工程大学学报,2014,15(6):654 - 663.]

[12]He D,Zhang Y,Chen J. Robust biometric-based user authentication scheme for wireless sensor networks[J]. Ad Hoc & Sensor Wireless Networks,2015,25(4):309 - 321.

[13]Pippal R S,Jaidhar C D,Tapaswi S. Robust smart card authentication scheme for multi-server architecture[J]. Wireless Personal Communications,2013,72(1):729 - 745.

[14]Cunningham P,Anderson R,Mullins R,et al. Improving smart card security using self-timed circuits[C]//Proceedings of the 8th International Symposium on Asynchronous Circuits and Systems. Washington DC:IEEE Computer Society,2012:211.

[15]Odelu V,Das A K,Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards[J]. IEEE Transactions on Information Forensics and Security,2015:1953 - 1966.

[16]Woei J T,Jia H L,Wei B L. An effiicient and secure multi-server authentication scheme with key agreement[J]. The Journal of Systems and Software,2012,85(4):876 - 882.

[17]Li X,Niu J W,Khan M K,et al. An enhanced smart card based remote user password authentication scheme[J]. Journal of Network and Computer Applications,2013,36(5):1365 - 1371.

[18]Liu Sha,Zhu Shuhua. Anonymity-preserving remote user password authentication with key agreement scheme based on smart cards[J]. Journal of Computer Application,2014,34(7):1867 - 1870.[刘莎,朱淑华. 基于智能卡的远程用户匿名身份认证和密钥协商方案[J]. 计算机应用,2014,34(7):1867 - 1870.]

[19]Wang D,Ma C G,Weng C,et al. Cryptanalysis and improvement of a remote user authentication scheme for resource-limited environment[J]. Journal of Electronics and Information Technology,2012,34(10):2520 - 2526.

[20]Zhang Xue,Li Guangsong,Han Wenbao,et al. Identity-based authenticated key agreement protocol cross autonomous domains[J]. Journal of Sichuan University:Engineering Science Edition,2015,47(4):125 - 131.[张雪,李光松,韩文报,等. 基于身份的跨自治域认证密钥协商协议[J]. 四川大学学报:工程科学版,2015,47(4):125 - 131.]

(编辑 赵 婧)