计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20140755
52(11):2645-2655,2015

增强的基于生物密钥智能卡远程身份认证方案

徐钦桂[1] 黄培灿[1] 杨桃栏[2]
[1](东莞理工学院计算机学院 广东东莞 523808)
[2](国防科学技术大学计算机学院 长沙 410073)
(dgxuqg@126.com)

An Enhanced Biometrics-Key-Based Remote User Authentication Scheme with Smart Card

Xu Qingui[1], Huang Peican[1], and Yang Taolan[2]
[1](*Computer Institute, Dongguan University of Technology, Dongguan, Guangdong* 523808)
[2](*College of Computer, National University of Defense Technology, Changsha* 410073)

Abstract Biometrics-based remote user authentication scheme with smart card enforces triple protection including smartcard hardware, user password authentication and biometrics recognition, which brings new breakthrough to authentication. Khan-Kumari scheme, which is characterized with high security performance, is reviewed. Four defects that may do harm to authentication are found in this scheme: flawed encapsulation of user identity secrets, improper access way of them, lack of message freshness check, and insufficient interaction between authentication parties. An enhanced biometrics-key-based remote user authentication scheme with smart card is put forward in this paper. Our scheme enforces four enhancing procedures: mutal verifiable dual factors are used to protect user identity secrets, and playback messages are recognized based on message freshness check, and protected parameters are transmitted after encrypted with dynamic Hash key integrating time flag, and authentication process is made be completed gracefully with acknowledgement message. With these measures, user identity protection is enhanced remarkably. Hence, resistance against smart card cracking, message replay, identity impersonation and service refusal is aggrandized. Security analysis shows that the enhanced scheme effectually fixes vulnerabilities found in Khan-Kumari scheme with small computation and communication cost, achieving remarkably enhanced security performance in defending against varying attacking means. Under the circumstances that even dual protection measures are compromised, the probability of impersonation and authentication failure caused by attacks can be made be less than 10^{-38}.

Key words mutual authentication; smart card; biometrics-key; network security; multi-factor authentication

摘 要 基于生物特征的智能卡身份认证提供智能卡硬件、口令验证、生物特征识别三重保护,给身份认证技术带来新的突破点.回顾了具有较高安全性能的 Khan-Kumari 方案工作原理,指出该方案存在身份密值封装不当、密值使用方式不合理、新鲜性检测功能缺失、认证双方交互不够充分等缺陷,可导致身份认证安全性受损.提出一个增强的基于生物密钥智能卡远程身份认证方案,用可相互验证的双要素对用户身份密值实施联合保护,基于新鲜性检测、识别重放消息,以融入时标的动态散列值密钥加密传输受保护参数,增加确认消息完善认证流程,增强了用户身份密值的保护强度,提高了对智能卡破解、消息

收稿日期:2014-08-19;**修回日期**:2015-02-28
基金项目:国家自然科学基金项目(61300198,61402106);广东省科技计划基金项目(2007A060304003);东莞市高等院校科研机构科技计划项目(2012108102035,2012108102007)

重放、身份冒充、拒绝服务等攻击的抗击能力.安全性分析表明,增强方案以较低的计算与通信开销,有效修复了 Khan-Kumari 方案中的缺陷,安全性能获得显著增强,即使在两重保护失效条件下,发生身份冒充、认证失败的概率可控制在至 10^{-38} 以下.

关键词 双向身份认证;智能卡;生物密钥;网络安全;多因素认证

中图法分类号 TP309.1; TP393.08

自 1981 年 Lamport[1] 发表不安全通信环境下基于一次性口令智能卡认证方案以来,基于智能卡身份认证成为研究热点,到目前出现了很多不同改进方案[2-7],并在安全性要求较高的电子商务、电子政务等领域得到广泛应用.但有时存在智能卡硬件保管不善、口令选择不当的问题,一旦它们被攻击者获取,就容易实施身份冒充攻击[8-10].而人类指纹、虹膜、掌纹等生理特征具有唯一性,不随时间、外部环境而变化,能防伪造、防遗失,破解难度大,将生物特征或生物密钥纳入用户身份认证属性范畴,能提高身份认证可靠性[8,10],近年来不少学者开始探索基于生物密钥智能卡认证方案.

Lee 等人[8] 早于 2002 年将生物特征引入基于智能卡认证方案,在智能卡基础上增加 ElGamal 私钥加密与指纹验证方法;但 Lin 与 Lai[9] 于 2004 年发现其中存在身份冒充漏洞,并提出修复方案,Khan 与 Zhang[10] 还发现 Lee 方案存在服务器欺骗缺陷.近年来,基于生物特征智能卡认证方法成为信息安全领域关注的研究热点之一.2009 年,张凡等人[11] 提出一种基于模糊提取的远程双向生物认证,以容错方式从生物特征输入中可靠地提取出均匀分布的随机密钥,通过集成口令和智能卡产生多因素认证方案,能抵抗假冒攻击和多服务器合谋攻击.2010 年,Li 与 Hwang[12] 提出一种基于生物特征智能卡远程认证方案,基于散列运算实现双向认证、防抵赖与口令修改功能.可不久,Li 等人[13] 发现 Li-Hwang 方案存在消息篡改与中间人攻击缺陷.Das[14] 发现 Li-Hwang 方案还存在智能卡正常登录被拒的问题,并提出具有防身份冒充、服务器伪装、并行会话攻击与口令盗窃能力的修复方案.2012 年,An[15] 发现 Das 方案引入了一个严重漏洞,攻击者无需输入口令就可实施用户冒充与服务器冒充攻击,并通过双向认证,作者给出了一个安全增强的漏洞修复方案.2013 年,Khan 与 Kumari[16] 发现 An 方案也存在漏洞,攻击者可利用侦听获得的登录请求消息,实施离线口令猜测攻击,盗取用户口令与用户身份密值,进而实施身份冒充与服务器伪装攻击,作者给出一个支持匿名登录消息的改进方案,是目前能提供较高安全性能的基于生物特征智能卡认证方案.

尽管 Khan-Kumari 方案[16] 修复了 Li-Hwang[12] 及其改进方案[13-15] 中发现的诸多漏洞和缺陷,认证可靠性与抗攻击能力大为增强,但我们发现 Khan-Kumari 方案依然存在一些脆弱环节与有待改进之处.本文首先回顾 Khan-Kumari 方案的协议流程,分析该方案存在的脆弱性与可能造成的损害;然后,讨论安全增强措施,提出一个可修复这些漏洞的增强方案;最后分析增强方案的安全性与效率.

1 Khan-Kumari 方案回顾与脆弱性分析

1.1 Khan-Kumari 方案简要回顾

Khan-Kumari 方案由用户 U_i、服务器 S_j 与注册中心 R 组成,服务器与注册中心共享 2 个秘值 x_s 与 y_s.身份认证包含注册、登录、认证和口令更新 4 个阶段,注册与口令更新阶段通过安全信道传递消息,登录与认证阶段允许通过非安全信道传递消息,以增强认证方案适用性.

1.1.1 注册阶段

用户 U_i 插入智能卡 SC_i,输入用户名 ID_i、口令 PW_i 与随机数 K_i,通过特定设备采集生物特征信息 B_i,将 ID_i,$PW_i \oplus K_i$ 与 $B_i \oplus K_i$ 通过安全信道传到注册中心 R.

R 用单向散列函数 $h(\cdot)$ 计算 4 个参数:$f_i = h(B_i \oplus K_i)$,$r_i = h(PW_i \oplus K_i) \oplus f_i = h(PW_i \oplus K_i) \oplus h(B_i \oplus K_i)$,$c_i = h(x_s \| y_s) \oplus f_i = h(x_s \| y_s) \oplus h(B_i \oplus K_i)$,$e_i = h(ID_i \| x_s) \oplus r_i = h(ID_i \| x_s) \oplus h(PW_i \oplus K_i) \oplus h(B_i \oplus K_i)$,将 $\{c_i, e_i, h(\cdot)\}$ 写入智能卡 SC_i,将 SC_i 与 f_i 通过安全信道提供给 U_i.

用户 U_i 收到智能卡 SC_i 与 f_i 后,计算 2 个参数:$g_i = (ID_i \| PW_i) \oplus f_i$,$j_i = (ID_i \| PW_i) \oplus K_i$,一并写入智能卡 SC_i,这样 $SC_i = \{c_i, e_i, g_i, j_i, h(\cdot)\}$.

1.1.2 登录阶段

用户 U_i 插入智能卡 SC_i,键入用户名 ID_i 与口令 PW_i,同时用特定设备采集生物特征信息 B_i,SC_i 提取 $f_i = (ID_i \| PW_i) \oplus g_i$,$K_i = (ID_i \| PW_i) \oplus j_i =$

$(ID_i\|PW_i)\oplus(ID_i\|PW_i)\oplus K_i$,比较 f_i 与 $h(B_i\oplus K_i)$,若相等则接受用户输入信息,否则终止登录过程.

接着,SC_i 产生登录随机数 R_c,恢复参数 $r_i=h(PW_i\oplus K_i)\oplus f_i=h(PW_i\oplus K_i)\oplus h(B_i\oplus K_i)$,计算 $M_1=c_i\oplus f_i=h(x_s\|y_s)\oplus h(B_i\oplus K_i)\oplus h(B_i\oplus K_i)=h(x_s\|y_s)$,$M_2=e_i\oplus r_i=h(ID_i\|x_s)\oplus h(PW_i\oplus K_i)\oplus h(B_i\oplus K_i)\oplus h(PW_i\oplus K_i)\oplus h(B_i\oplus K_i)=h(ID_i\|x_s)$,$M_3=M_1\oplus R_c=h(x_s\|y_s)\oplus R_c$,$M_4=(h(M_1)\|R_c)\oplus ID_i=h(h(x_s\|y_s)\|R_c)\oplus ID_i$,$M_5=h(M_2\|R_c)=h(h(ID_i\|x_s)\|R_c)$,向服务器 S_i 发送登录请求消息 $Q_1=\{M_3,M_4,M_5\}$.

1.1.3 认证阶段

S_i 收到 SC_i 的登录请求 Q_1,先计算 $M_6=h(x_s\|y_s)$,$M_7=M_3\oplus M_6=h(x_s\|y_s)\oplus R_c\oplus h(x_s\|y_s)=R_c$,$ID_i=M_4\oplus(M_6\|M_7)=h(h(x_s\|y_s)\|R_c)\oplus ID_i\oplus h(h(x_s\|y_s)\|R_c)=ID_i$;接着检查 ID_i 的有效性,计算 $M_8=h(ID_i\|x_s)$,比较 M_5 与 $h(M_8\|M_7)$,若相等则接受 Q_1,产生认证随机数 R_s,计算 $M_9=M_8\oplus R_s=h(ID_i\|x_s)\oplus R_s$,$M_{10}=h(M_8\|R_s)=h(h(ID_i\|x_s)\|R_s)$;然后向 SC_i 发送响应消息 $Q_2=\{M_9,M_{10}\}$.

SC_i 收到响应消息 Q_2,计算 $M_{11}=M_9\oplus M_2=h(ID_i\|x_s)\oplus R_s\oplus h(ID_i\|x_s)=R_s$,比较 M_{10} 与 $h(M_2\|M_{11})$,若相等,则认为服务器通过认证;然后计算 $M_{12}=h(M_2\|R_c\|M_{11})=h(h(ID_i\|x_s)\|R_c\|R_s)$,并发送响应消息 $Q_3=\{M_{12}\}$ 给 S_i.

S_i 收到 Q_3,比较 M_{12} 与 $h(M_8\|M_7\|R_s)$,若相等,则认为 U_i 通过认证,S_i 与 U_i 之间双向认证成功.

1.1.4 口令更新阶段

口令更新包括 4 个步骤:1)U_i 插入智能卡,输入用户名 ID_i 与口令 PW_i;2)SC_i 采集生物特征信息 B_i,提取参数值 $f_i=(ID_i\|PW_i)\oplus g_i$ 与 $K_i=(ID_i\|PW_i)\oplus j_i$,比较 f_i 与 $h(B_i\oplus K_i)$,若相等则允许更新口令,否则终止口令更新过程;3)SC_i 计算 $(g_i)_{new}=(ID_i\|(PW_i)_{new})\oplus f_i$,$(j_i)_{new}=(ID_i\|(PW_i)_{new})\oplus K_i$,$(e_i)_{new}=e_i\oplus h(PW_i\oplus K_i)\oplus h((PW_i)_{new}\oplus K_i)$;4)$SC_i$ 分别用 $(g_i)_{new}$,$(j_i)_{new}$,$(e_i)_{new}$ 更新涉及用户口令的参数 g_i,j_i,e_i.

1.2 Khan-Kumari 方案脆弱性分析

我们假定攻击者 U_a 有能力控制不安全信道,可以侦听、录制、拦截、篡改、回放消息,插入伪造消息[14-16],或通过暴力攻击手段获取智能卡中所有参数[17-18].通过认证协议分析我们发现,虽然 Khan-Kumari 方案[16]修复了 Li-Hwang[12],Das[14],An[15]等方案的漏洞,能防范 U_a 实施口令猜测、用户身份冒充与服务器伪装等攻击,但仍然存在身份密值封装不当、密值使用不合理、消息新鲜性检测功能缺失、认证双方交互不够充分等缺陷,在遭受攻击情况下可导致身份冒充、服务器伪装、拒绝服务等损害.

1.2.1 用户身份密值封装有漏洞

Khan-Kumari 方案虽然用 2 个参数 $h(PW_i\oplus K_i)$,$h(B_i\oplus K_i)$ 封装保护用户身份密值 $h(ID_i\|x_s)$,但由于 $h(B_i\oplus K_i)$ 可由 $h(PW_i\oplus K_i)$ 与 SC_i 内部参数导出,一旦 SC_i 与 PW_i 为 U_a 获得,生物特征 B_i 的验证保护将自然崩溃,攻击者 U_a 仅凭 PW_i 可从 SC_i 破解 $h(ID_i\|x_s)$ 并实施身份冒充.

具体破解过程为:1)攻击者 U_a 窃得智能卡 SC_i,先修改智能卡代码,删去 f_i 与 $h(B_i\oplus K_i)$ 比较操作,并在登录阶段输入正确的 ID_i 与 PW_i;2)这时,SC_i 就将恢复参数 $f_i=g_i\oplus(ID_i\|PW_i)$,$K_i=(ID_i\|PW_i)\oplus j_i$,$r_i=h(PW_i\oplus K_i)\oplus f_i$,并利用参数 $e_i=h(ID_i\|x_s)\oplus r_i$,$c_i=h(x_s\|y_s)\oplus f_i$,解封用户身份密值 $h(x_s\|y_s)=c_i\oplus f_i$,$h(ID_i\|x_s)=e_i\oplus r_i$,智能卡被成功破解;3)有了 $h(ID_i\|x_s)$ 与 $h(x_s\|y_s)$,U_a 即可构造正确的消息分量 $M_3\sim M_5$,发出登录正常的请求消息 $Q_1=\{M_3,M_4,M_5\}$,绕开生物特征认证,冒充 U_i 完成与 S_i 间的双向身份认证.

1.2.2 用户身份密值使用方式不当

Khan-Kumari 方案直接以 $h(ID_i\|x_s)$ 为密钥、基于异或运算加密传输受保护参数,$h(ID_i\|x_s)$ 失密风险大,一定条件下可导致身份冒充危害.

由于 S_i 直接用 $h(ID_i\|x_s)$ 加密服务器随机数 R_s,计算消息分量 $M_9=h(ID_i\|x_s)\oplus R_s$ 通过消息 Q_2 进行传输.若某次认证过程的服务器随机数 R_s 被泄露,攻击者 U_a 同时获得 Q_2 与 R_s,他就可用消息分量 M_9 破解 U_i 身份密值 $h(ID_i\|x_s)=M_9\oplus R_s$.

有了 $h(ID_i\|x_s)$,U_a 若侦听到来自 SC_i 的正常登录请求消息 $Q_1=\{M_3,M_4,M_5\}$,就可选择认证随机数 R_{sa},计算 $M_{9a}=h(ID_i\|x_s)\oplus R_{sa}$,$M_{10a}=h(h(ID_i\|x_s)\|R_{sa})$,向 SC_i 发送响应消息 $Q_{2a}=\{M_{9a},M_{10a}\}$;$SC_i$ 收到 Q_{2a},从 M_{10a} 提取 $M_{11}=M_{9a}\oplus M_2=h(ID_i\|x_s)\oplus R_{sa}\oplus h(ID_i\|x_s)=R_{sa}$,比较 M_{10a} 与 $h(M_2\|M_{11})=h(h(ID_i\|x_s)\|R_{sa})$,二者相等,双向身份认证通过,$U_a$ 成功冒充了服务器 S_i 完成与 U_i 的双向身份认证.

U_a 还可录制来自 U_i 的登录请求消息 $Q_1=\{M_3,M_4,M_5\}$,其后向 S_i 发送重放消息 $Q_{1a}=Q_1$;

S_i 将接受 Q_{1a}，向 U_a 发送响应消息 $Q_2=\{M_9, M_{10}\}$，其中 $M_9=h(ID_i\|x_s)\oplus R_s$，$M_{10}=h(h(ID_i\|x_s)\|R_s)$；$U_a$ 计算 $R_s=M_9\oplus h(ID_i\|x_s)$，$M_{12a}=h(h(ID_i\|x_s)\|R_c\|R_s)=h(M_5\|R_s)$，向 S_i 发送欺骗响应消息 $Q_{3a}=\{M_{12a}\}$；S_i 比较 M_{12a} 与 $h(M_8\|M_7\|R_s)=h(h(ID_i\|x_s)\|R_c\|R_s)$，二者相等，$U_a$ 被当做 U_i 通过认证，U_a 成功冒充 U_i.

1.2.3 消息新鲜性检测功能缺失

Khan-Kumari 方案未实现消息新鲜性检查功能，SC_i 与 S_i 均不区分新鲜消息、重发消息和回放消息，这就可能导致正常登陆请求因攻击者干扰而被拒.

比如，U_a 侦听并保存 SC_i 发出的登录请求消息 $Q_1=\{M_3, M_4, M_5\}$，并立即重发干扰消息 $Q_{1a}=Q_1$. S_i 首先收到 SC_i 发出的 Q_1 并接受之，产生认证随机数 R_{si} 并计算 $M_7=R_c$，$M_8=h(ID_i\|x_s)$，$M_9=h(ID_i\|x_s)\oplus R_{si}$，$M_{10}=h(h(ID_i\|x_s)\oplus R_{si}\|R_{si})$，向 SC_i 发送响应消息 $Q_2=\{M_9, M_{10}\}$；紧接着，S_i 又收到 U_a 发出的 Q_{1a}，由于不进行消息新鲜性与重复性检查，也接受之，并选择另一认证随机数 $R_{sa}\neq R_{si}$，计算 $M_{9a}=h(ID_i\|x_s)\oplus R_{sa}$，$M_{10a}=h(h(ID_i\|x_s)\|R_{sa})$，向 U_a 发送响应消息 $Q_{2a}=\{M_{9a}, M_{10a}\}$；$SC_i$ 收到响应消息 Q_2，计算 $M_{12}=h(h(ID_i\|x_s)\|R_c\|R_{si})=h(h(ID_i\|x_s)\|R_c\|R_{si})$，向 S_i 发响应消息 $Q_3=\{M_{12}\}$；S_i 收到 Q_3，比较 $M_{12}=h(h(ID_i\|x_s)\|R_c\|R_{si})$ 与 $h(M_8\|M_7\|R_{sa})=h(h(ID_i\|x_s)\|R_c\|R_{sa})$，二者不一致，$S_i$ 拒绝 U_i 正常登录请求.

1.2.4 认证双方交互不充分

在 Khan-Kumari 方案中，SC_i 向 S_i 发送 Q_1，启动身份认证过程，S_i 审查 Q_1 有效，向 SC_i 发送 Q_2；SC_i 审查 Q_2，若有效则认可 S_i 身份，最后向 S_i 发送 Q_3，S_i 审查 Q_3，若有效则认可 SC_i 身份. 这里存在的问题是，自 SC_i 发出 Q_3 后，虽然 S_i 身份是已经被 SC_i 确认，但 U_i 身份是否被 S_i 确认取决于 Q_3 能否准确无误传输给 S_i. 若 Q_3 丢失或被篡改，S_i 尚未认可 U_i 身份，但此时 SC_i 开始发送数据消息，则这些数据消息必然为 S_i 所拒绝，造成拒绝服务的错误. 其根本原因是认证双方交互不充分，S_i 未将对 U_i 身份的认证结果反馈给 SC_i，认证流程并未真正完成.

2 增强的基于生物密钥认证方案

本文在保持 Khan-Kumari 方案[16]优势的基础上，针对其存在的薄弱环节，提出一个增强方案，修复 Khan-Kumari 方案存在的缺陷，提高身份认证安全性与可靠性. 主要增强措施包括：1)用可相互验证的双要素对用户身份密值实施联合保护，防止基于部分输入信息破解智能卡受保护密值；2)增加基于时标的消息新鲜性检查，消除消息重放带来的干扰；3)采用融入时标的动态散列值密钥，抵抗基于消息分析方法破解用户身份密值的攻击；4)增加确认消息完善认证流程，抵抗拒绝服务攻击.

表 1 所示为增强的基于生物密钥认证方案符号定义：

Table 1 Symbol Definition

表 1 符号定义

Symbol	Description
R	Trustable Registration Center
S_i	Server
U_i	User
U_a	Attacker
ID_i	ID of User U_i
PW_i	Password of U_i
X	Biometrics Captured from U_i in Registration Stage
Y	Biometrics Captured from U_i in Logon Stage
ST_i	Biometric Template of U_i
B_i	Biometrics Key of U_i
SC_i	Smart Card of U_i
K_i	Random Number U_i Chooses
x_s, y_s	Shared Secret Key between R and S_i
$h(\cdot)$	One-way Hash Function
$h(ID_i\|x_s)$, $h(x_s\|y_s)$	Idenfication Secret Key of U_i
$\oplus$	Exclusive or
$\|$	Concatenation

2.1 用户注册

在注册阶段，用户 U_i 与注册中心 R 一起完成智能卡 SC_i 的创建.

1) 用户 U_i 键入用户名 ID_i、口令 PW_i 与随机数 K_i，通过特定设备采集生物特征信息 $X=\{x_1, x_2, \cdots, x_m\}$ 并绑定选定的生物密钥 B_i，将参数 ID_i，$PW_i\oplus K_i$，$B_i\oplus K_i$ 通过安全信道传递给注册中心 R；

2) R 用与服务器 S_i 共享的密码键值 x_s 与 y_s，计算 2 个参数：

$$c_i=h(x_s\|y_s)\oplus h(PW_i\oplus K_i),$$

$$b_i=h(ID_i\|x_s)\oplus h(B_i\oplus K_i),$$

并通过安全信道发送给 U_i；

3) U_i 计算 3 个参数:

$e_i=b_i\oplus h(B_i\oplus K_i)\oplus h(PW_i\oplus B_i\oplus K_i)=$
$h(ID_i\|x_s)\oplus h(PW_i\oplus B_i\oplus K_i)$,

$g_i=h(ID_i\|PW_i\|B_i)$,

$j_i=(ID_i\|PW_i)\oplus K_i$,

并将 $K_i,c_i,e_i,g_i,j_i,h(\cdot)$写入智能卡 SC_i,得到 $SC_i=\{ST_i,K_i,c_i,e_i,g_i,j_i,h(\cdot)\}$.

$h(ID_i\|x_s)$用同时依赖于 2 个要素 PW_i,B_i 的散列值进行封装,SC_i 只有获得 2 个正确的要素值,才能正确解封用户身份密值,堵塞了 Khan-Kumari 方案用户身份密值的封装漏洞.

2.2 时间同步与用户登录

在登录阶段,U_i 插入智能卡 SC_i,输入用户名 ID_i、口令 PW_i;通过特定设备采集生物特征信息,提取生物密钥 B_i 交由 SC_i 进行正确性验证;SC_i 解封 U_i 用户身份密值,从服务器 S_i 获取系统时间进行时间同步,产生与发送具有时鲜性的登录请求.

2.2.1 口令与生物特征验证

用户 U_i 键入用户名 ID_i、口令 PW_i,通过特定设备采集用户生物特征信息 $Y=\{y_1,y_2,\cdots,y_m\}$并提取生物密钥 B_i 交由 SC_i,SC_i 比较 g_i 与 $h(ID_i\|PW_i\|B_i)$,若一致则认为 ID_i,PW_i,B_i 通过验证. 由于散列值 $h(ID_i\|PW_i\|B_i)$同时融入了 PW_i,B_i 的正确值,只有这 2 个要素同时正确才能通过验证,这就实现了用户口令与生物特征相互验证,一方要通过验证取决于另一份也通过验证,解决了 Khan-Kumari 方案可绕开生物特征验证的缺陷.

2.2.2 同步智能卡当前时间

智能卡 SC_i 从服务器 S_i 获取正确的系统时间,校准本地时间,执行时间同步.

1) 智能卡 SC_i 选择随机数 RC_0,计算:

$K_i=j_i\oplus(ID_i\|PW_i)$,

$MC_1=c_i\oplus h(PW_i\oplus K_i)$,

$MC_2=e_i\oplus h(PW_i\oplus B_i\oplus K_i)$,

$MC_3=h(MC_1\|RC_0)\oplus ID_i$,

$MC_4=h(MC_2\|RC_0\|ID_i)$,

向 S_i 发送时间同步请求消息 $Q_{01}=\{$"requestTime", $RC_0,MC_3,MC_4\}$.

在这里,由于 MC_2 是用 $h(PW_i\oplus B_i\oplus K_i)$从参数 e_i 解封而来,只有 PW_i,B_i 均正确无误才能恢复正确的用户身份密值 $h(ID_i\|x_s)$,从而执行正常的用户登录和身份认证过程,即使攻击者 U_a 通过篡改 SC_i 代码屏蔽了口令与生物特征验证功能,SC_i 也难以得到正确的 $h(ID_i\|x_s)$,从而实施身份冒充攻击.

2) S_i 收到 Q_{01}后计算:

$MS_1=h(x_s\|y_s)$,

$ID_i=MC_3\oplus h(MS_1\|RC_0)$,

$MS_2=h(ID_i\|x_s)$,

再计算 $h(MS_2\|RC_0\|ID_i)$,并与 MC_4 比较,若不一致则忽略 Q_{01},否则取当前系统时间为时标 T_0,计算:

$MS_3=h(MS_2\|T_0\|RC_0)$,

向 SC_i 发送时间同步消息 $Q_{02}=\{$"syncTime", T_0, $MS_3\}$.

3) SC_i 收到 Q_{02},计算 $h(MC_2\|T_0\|RC_0)$,并与 MS_3 比较,若不一致则忽略 Q_{02},否则用 T_0 校准智能卡中当前系统时间.

2.2.3 发送登录请求消息

SC_i 读取当前系统时间为时标 T_1,选择随机数 RC_1,计算:

$MC_5=h(MC_1\|T_1)\oplus ID_i$,

$MC_6=h(MC_2\|T_1)\oplus RC_1$,

$MC_7=h(MC_2\|RC_1\|T_1)$,

向 S_i 发送登录请求消息 $Q_1=\{$"login", T_1,MC_5, $MC_6,MC_7\}$.

在这里,用 $MC_2=h(ID_i\|x_s)$与时间标记 T_1 串接后计算的散列值 $h(MC_2\|T_1)$作为动态密钥来加密传输随机数 RC_1,即使 RC_1 被破解或外泄,U_a 也仅能破解本次传输的动态密码 $h(MS_2\|T_2)$,用户身份密值 $h(ID_i\|x_s)$仍然保持安全. SC_i 与 S_i 创建的其他随机数都采用这种方式进行加密传输,克服了 Khan-Kumari 方案中用户身份密值使用方式不当的问题.

2.3 双向身份认证

在双向认证阶段,在 SC_i 与 S_i 之间交换 4 个用动态密钥加密的消息,双方检查消息新鲜性与完整性,解密消息内容,根据对方是否知晓用户身份密值 $h(ID_i\|x_s)$与 $h(x_s\|y_s)$的推断来判定对方身份的真实性.

2.3.1 登录请求与响应

S_i 收到登录请求消息 Q_1,先取得当前系统 T_2,检查新鲜性条件 $0<T_2-T_1<\delta$,若成立则 Q_1 通过新鲜性检查,否则忽略 Q_1;接着计算 $ID_i=MC_5\oplus h(MS_1\|T_1)$,$RC_1=MC_6\oplus h(MS_2\|T_1)$,比较验证码 MC_7 与 $h(MS_2\|RC_1\|T_1)$,若一致则 Q_1 通过完整性检查,否则忽略 Q_1;再检查 Q_1 是否为重复消息,若为重复消息则向 SC_i 重发消息 Q_2,否则选择随机数 RS_1,计算:

$MS_4=h(MS_2\|T_2)\oplus RS_1$,

$MS_5=h(MS_2\|RC_1\|RS_1\|T_2)$,

向 SC_i 发送响应消息 $Q_2=\{$"serverReply", T_2, MS_4, $MS_5\}$.

2.3.2 服务器身份认证

SC_i 收到响应消息 Q_2, 取当前系统时间 T_3, 检查条件 $0<T_3-T_2<\delta$ 是否成立, 若成立则 Q_2 通过新鲜性检查, 否则忽略 Q_2; 接着, 计算 $RS_1=MS_4\oplus h(MC_2\|T_2)$, 比较验证码 MS_5 与 $h(MC_2\|RC_1\|RS_1\|T_2)$, 若不相等则忽略 Q_2, 若相等则服务器 S_i 身份通过认证. SC_i 也检查 Q_2 是否为重复消息, 若是则向 S_i 重发消息 Q_3, 否则选择随机数 RC_2, 计算:

$$MC_8=h(MC_1\|T_3)\oplus ID_i,$$

$$MC_9=h(MC_2\|T_3)\oplus RC_2,$$

$$MC_{10}=h(MC_2\|RC_2\|RS_1\|T_3),$$

向 S_i 发送响应消息 $Q_3=\{$"userReply", T_3, MC_8, MC_9, $MC_{10}\}$, 并计算会话密钥:

$$S_{key}=h(MC_2\|(T_1\oplus T_2\oplus T_3)\|(RC_1\oplus RS_1\oplus RC_2)).$$

2.3.3 用户身份认证

S_i 收到响应消息 Q_3, 取系统时间 T_4, 检查条件 $0<T_4-T_3<\delta$, 若成立则 Q_3 通过新鲜性检查, 否则忽略 Q_3; 接着, 计算 $ID_i=MC_8\oplus h(MS_1\|T_3)$, $RC_2=MC_8\oplus h(MS_2\|T_3)$, 比较验证码 MC_{10} 与 $h(MS_2\|RC_2\|RS_1\|T_3)$, 若不一致则忽略 Q_2, 若一致则用户 U_i 身份通过认证; 最后 S_i 还对 Q_3 进行重复性检查, 若为重复消息则仅重发消息 Q_4, 否则计算:

$$MS_6=h(MS_2\|T_4\|RC_1\|RS_1\|RC_2),$$

向 SC_i 发送认证确认消息 $Q_4=\{$"Confirm", T_4, $MS_6\}$, 计算会话密钥:

$$S_{key}=h(MS_2\|(T_1\oplus T_2\oplus T_3)\|(RC_1\oplus RS_1\oplus RC_2)).$$

2.3.4 用户登录完成

SC_i 接收认证确认消息 Q_4, 取当前时间 T_5, 检查条件 $0<T_5-T_4<\delta$, 若成立则 Q_4 通过新鲜性检查, 否则忽略 Q_4; 然后比较验证码 MS_6 与 $h(MC_2\|T_4\|RC_1\|RS_1\|RC_2)$, 若二者相等则用户登录过程完成, 准备发送消息, 否则忽略 Q_4. 认证确认消息 Q_4 解决了 Khan-Kumari 方案中双向验证不充分的问题, 可避免正常登陆被拒措施.

2.4 口令修改

首先, U_i 插入智能卡 SC_i, 键入用户名 ID_i 与口令 PW_i, 从特定设备采集 U_i 生物特征信息 Y, 用 Y 提取生物密钥 B_i, SC_i 比较 g_i 与 $h(ID_i\|PW_i\|B_i)$, 若二者匹配则 U_i 用户名、口令与生物特征通过验证, 否则终止口令更新过程; 然后, U_i 输入新口令 $(PW_i)_{new}$, SC_i 提取 $K_i=(ID_i\|PW_i)\oplus j_i$, 计算:

$$(c_i)_{new}=c_i\oplus h(PW_i\oplus K_i)\oplus h((PW_i)_{new}\oplus K_i),$$

$$(j_i)_{new}=(ID_i\|(PW_i)_{new})\oplus K_i,$$

$$(g_i)_{new}=h(ID_i\|(PW_i)_{new}\|B_i),$$

$$(e_i)_{new}=e_i\oplus h(PW_i\oplus B_i\oplus K_i)\oplus h((PW_i)_{new}\oplus B_i\oplus K_i);$$

最后, SC_i 分别用 $(c_i)_{new}$, $(g_i)_{new}$, $(j_i)_{new}$, $(e_i)_{new}$, 更新涉及用户口令的参数 c_i, g_i, j_i, e_i.

3 增强方案安全性能与效率分析

3.1 增强方案安全性能完备性分析

支持生物特征验证智能卡身份认证是一种三因素身份方案, 它通过智能卡硬件保护、口令验证、生物特征验证三重措施保护用户身份密值. 在这 3 种要素中, 由于生物特征对人体的不可分离特性, 假设增强方案生物特征验证环节总是可靠的, 这样就可将用户 U_i 身份所处安全状态分为三重保护、两重保护、单重保护 3 种: 1) 三重保护是 SC_i 硬件保护、PW_i 验证、B_i 验证都对 $h(ID_i\|x_s)$ 起保护作用的状态; 2) 两重保护是智能卡 SC_i 被 U_a 盗取, 仅 PW_i 验证与 B_i 验证起保护作用的状态; 3) 单重保护是指 SC_i 与 PW_i 验都被 U_a 获取, 仅 B_i 验证起保护作用的状态.

对应 U_i 所处安全状态, 我们将攻击行为归为 3 类: 1) 在三重保护状态下, U_a 主要通过消息侦听、拦截、分析、篡改、伪造手段, 试图推断密值 $h(ID_i\|x_s)$, 再实施身份认证攻击; 2) 在两重保护状态下, U_a 可用物理方法对 SC_i 实施暴力攻击, 读出 SC_i 参数, 更改 SC_i 代码, 试图破解 $h(ID_i\|x_s)$, PW_i, B_i 等敏感信息, 再实施身份认证攻击; 3) 在单重保护状态时, U_a 同时获取 SC_i 硬件与 PW_i, 借此实施 $h(ID_i\|x_s)$ 破解与身份认证攻击. 我们也将 U_a 攻击可能带来的危害分为 3 种: 1) 身份冒充, 包括用户身份冒充与服务器身份冒充; 2) 正常身份认证失败, 包括正常登陆失败与拒绝服务; 3) 用户身份密值、用户口令、生物密钥等敏感信息泄露. 增强方案安全性能及完备性可用 3 种保护状态下的安全性能 (即攻击手段造成损害概率) 来反映. 为便于定量分析, 用 L_{Key}, L_{ID}, L_{PW}, L_B, L_{Hash}, L_{Time}, L_{Random} 分别表示服务器共享密值 x_s 与 y_s、用户 ID、口令 PW、生物密钥 B、$h(\cdot)$ 散列值、时间标志、随机数长度, 假设 $L_B\geqslant L_{Hash}$.

3.1.1 三重保护状态下安全性能

该状态下, U_a 不持有任何与 U_i, S_i 有关的敏感信息, 甚至可能不知 U_i 用户名 ID_i. U_a 主要攻击手段可为消息篡改与伪造、消息回放、消息分析.

1) 抗消息回放攻击性能

由于增强方案对登录和身份认证过程传输的4个消息 Q_1,Q_2,Q_3,Q_4 均作新鲜性检查,U_a 虽能侦听、保存消息,但 SC_i 与 S_i 均能识别和处理回放消息:超过 δ 时间的回放消息会被接收方丢弃;δ 时间内回放消息被当作重复消息处理,都不改变认证双方的内部状态,不会导致正常认证失败.

2) 抗消息伪造与篡改攻击性能

U_a 若欲冒充用户 U_i,需伪造有效的 Q_{01},Q_1,Q_3,正确解码 Q_{02},Q_2,Q_4,但因增强方案采用融入 $h(ID_i\|x_s)$ 的散列值验证消息完整性,U_a 必先猜测 U_i 用户名 ID_i、身份密值 $h(ID_i\|x_s)$、用户共享密值 $h(x_s\|y_s)$,全部猜中的概率低至 $2^{-(L_{ID}+2L_{Hash})}$;U_a 若欲冒充服务器 S_i,则需猜测 x_s,y_s,全部猜中的概率仅为 $2^{-2L_{Key}}$.

U_a 若要扰乱 SC_i 与 S_i 之间的认证过程,造成正常登录失败或拒绝服务,需伪造有效消息或篡改正常消息,扰乱接收方记录的随机数或时间标志值.伪造有效消息需获得密值 $h(ID_i\|x_s)$ 与 $h(x_s\|y_s)$,若伪造来自 SC_i 的有效消息,需猜测2个密值,一次全部猜中概率为 $2^{-2L_{Hash}}$;若伪造来自 S_i 的有效消息,仅需猜测 $h(ID_i\|x_s)$,一次猜中概率为 $2^{-L_{Hash}}$.被篡改的正常消息容易通过消息中的校验分量检测出来,逃过检测的难度与猜测用户身份密值相当.

3) 抗消息分析攻击性能

增强方案中,PW_i 与 B_i 同时参与登录与认证过程的消息构造,消息分析手段对破解 PW_i 与 B_i 无效.$h(ID_i\|x_s)$ 要么与时标串接后计算用于随机数加密的动态密钥散列值,或与时标、随机数运算后用于消息完整性验证的散列值.如在消息 Q_2 中,先用 $h(ID_i\|x_s)$ 创建动态密钥 $h(h(ID_i\|x_s)\|T_1)$,加密 RC_1 构造消息分量 $MC_6=h(h(ID_i\|x_s)\|T_1)\oplus RC_1$,再用 $h(ID_i\|x_s)$ 与 RC_1,T_1 连接后,计算消息验证码 $MC_7=h(h(ID_i\|x_s)\|RC_1\|T_1)$.$U_a$ 即使得到 MC_6,MC_7,RC_1,T_1,要实施消息分析攻击也只能猜测用户身份密值 $h(ID_i\|x_s)$,用 MC_6,MC_7 验证猜测结果正确性,一次猜中概率仅为 $2^{-L_{Hash}}$.

4) 抗已知随机数消息分析攻击性能

很多基于智能卡身份认证方案需加密传输随机数,历史随机数泄露可导致 $h(ID_i\|x_s)$ 失密[12-16].增强方案修复了这个缺陷,以 Q_1 为例,SC_i 用动态密钥将随机数 RC_1 加密成 $MC_6=h(h(ID_i\|x_s)\|T_1)\oplus RC_1$.若 U_a 仅知 Q_1 而不知 RC_1,则无法算得 $h(h(ID_i\|x_s)\|T_1)$,更难以破解 $h(ID_i\|x_s)$;若 U_a 同时获知 Q_1 与 RC_1,可算得 $h(h(ID_i\|x_s)\|T_1)=MC_6\oplus RC_1$.但 U_a 若要实施正常登录失败或拒绝服务攻击,仍需获知 $h(ID_i\|x_s)$.由于 $h(\cdot)$ 具有单向散列性,从 $h(h(ID_i\|x_s)\|T_1)$ 破解 $h(ID_i\|x_s)$ 的难度等同于随机猜测,一次猜中概率仅为 $2^{-L_{Hash}}$.若需冒充 U_i 身份或冒充服务器 S_i 与 U_i 交互,还需猜测 $h(x_s\|y_s)$,二者都猜中概率为 $2^{-2L_{Hash}}$.

3.1.2 两重保护状态下安全性能

此状态假定 U_a 获得智能卡 SC_i,掌握读出智能卡参数、修改智能卡代码的技术,实施智能卡破解攻击.

1) 抗智能卡密值破解攻击性能

从增强方案用户注册过程可知,$h(ID_i\|x_s)$,PW_i 与 B_i 等敏感信息存储保护是通过 SC_i 中 $e_i=h(ID_i\|x_s)\oplus h(PW_i\oplus B_i\oplus K_i)$,$g_i=h(ID_i\|PW_i\|B_i)$,$j_i=(ID_i\|PW_i)\oplus K_i$ 等参数来实现的.在正常登录流程中,U_i 输入 PW_i 与 B_i,SC_i 从 j_i 还原 $K_i=j_i\oplus(ID_i\|PW_i)$,从 e_i 还原 $h(ID_i\|x_s)=e_i\oplus h(PW_i\oplus B_i\oplus K_i)$,并用 g_i 验证 PW_i,B_i 的正确性.U_a 若要利用 SC_i 破解 $h(ID_i\|x_s)$,一种方法是猜测 PW_i,B_i,计算 $h(ID_i\|x_s)=e_i\oplus h(PW_i\oplus B_i\oplus K_i)$;另一种方法是直接猜测 $h(ID_i\|x_s)$,2种方法成功概率分别为 $2^{-(L_{PW}+L_B)}$ 与 $2^{-L_{Hash}}$.U_a 若要利用 SC_i 破解 PW_i 或 B_i,需同时猜中 PW_i 与 B_i,用参数 g_i 验证猜测结果正确性,一次全部猜中概率仅为 $2^{-(L_{PW}+L_B)}$.

2) 抗身份认证过程攻击性能

尽管 U_a 持有 SC_i,但 SC_i 对其实施身份认证过程攻击并无帮助.U_a 若要冒充 U_i,需猜测 PW_i 与 B_i,全部猜中的概率低至 $2^{-(L_{PW}+L_B)}$;若要冒充 S_i,需猜测 $h(ID_i\|x_s)$ 与 $h(x_s\|y_s)$,成功概率仅为 $2^{-2L_{Key}}$.U_a 若要扰乱 U_i 与 S_i 之间认证过程,至少需要获得 $h(ID_i\|x_s)$,一次猜中的概率仅为 $2^{-L_{Hash}}$.

3.1.3 单重保护状态下安全性能

该状态下,U_a 不但拥有智能卡 SC_i,还知晓用户口令 PW_i.只要获取正确的 B_i,就可解封密值 $h(x_s\|y_s)$ 与 $h(ID_i\|x_s)$,实施身份认证攻击.U_a 虽可利用 PW_i 恢复参数 $K_i=j_i\oplus(ID_i\|PW_i)$,$h(x_s\|y_s)=c_i\oplus h(PW_i\oplus K_i)$;但因 $h(ID_i\|x_s)$ 用 $h(PW_i\oplus B_i\oplus K_i)$ 封装在参数 $e_i=h(ID_i\|x_s)\oplus h(PW_i\oplus B_i\oplus K_i)$ 中,SC_i 并未存储 B_i 与 $h(PW_i\oplus B_i\oplus K_i)$ 的值,U_a 只能通过 B_i 猜测值来计算 $h(PW_i\oplus B_i\oplus K_i)$,用 $g_i=h(ID_i\|PW_i\|B_i)$ 验证 B_i 正确性,进而计算 $h(ID_i\|x_s)=e_i\oplus h(PW_i\oplus B_i\oplus K_i)$,一次猜中概率

仅为 2^{-L_B}. 因此通过获取 $h(ID_i\|x_s)$ 与 $h(x_s\|y_s)$, 实施用户身份冒充、服务器身份冒充、正常登陆失败、服务拒绝等攻击, 攻击成功概率低至 2^{-L_B}.

表 2 给出了本文增强方案安全性能完备性, 系统不但在三重保护完好时获得很高的安全性能, 而且在智能卡硬件 SC_i 与用户口令 PW_i 两重保护被突破条件下, U_a 攻击给带来各种危害的概率都在 $2^{-L_{Hash}}$ 或 2^{-L_B} 以内, 若设 $L_B=L_{Hash}=128$, 则用户 U_i 被冒充、认证被扰乱或身份密值被泄露的概率可降低至 10^{-38}, 表明增强方案安全性能高、完备性好.

Table 2 Security Completeness of Proposed Improved Scheme

表 2 本文增强方案安全性能完备性

Protection State	Attack Means	User Impersonation	Server Impersonation	Logon Failure	Service Refual	Leakage of User Secret Key	Leakage of User Password	Leakage of Biometric Key
Triple Protection State	Message Forgery and Tampering	$2^{-(L_{ID}+2L_{Hash})}$	$2^{-2L_{Key}}$	$2^{-L_{Hash}}$	$2^{-L_{Hash}}$			
	Message Replay	0	0	0	0			
	Message Analysis					$2^{-L_{Hash}}$	0	0
	Message Analysis with Known Random Number	$2^{-2L_{Hash}}$	$2^{-2L_{Hash}}$	$2^{-L_{Hash}}$	$2^{-L_{Hash}}$	$2^{-L_{Hash}}$		
Duel Protection State	Smartcard Cracking	$2^{-(L_{PW}+L_B)}$	$2^{-2L_{Key}}$	$2^{-L_{Hash}}$	$2^{-L_{Hash}}$	$2^{-L_{Hash}}$	$2^{-(L_{PW}+L_B)}$	$2^{-(L_{PW}+L_B)}$
Single Protection State	Attacking with Known User Password	2^{-L_B}	2^{-L_B}	2^{-L_B}	2^{-L_B}	2^{-L_B}		2^{-L_B}

3.2 增强方案安全性对比分析

我们以支持生物特征验证的 Li-Huang 方案、Li-Niu 方案[13]、Das 方案、An 方案、Khan-Kumari 方案为参照, 从功能特性、智能卡防丢失与防网络攻击 3 个方面, 对本文增强方案的安全性能进行对比分析.

3.2.1 功能特性对比

身份认证的可靠性、抗攻击能力与认证方案实现的功能特性密切相关.

6 种方案都提供双向身份认证功能, 但仅 Khan-Kumari 与本文增强方案对用户 ID_i 进行加密传输, 实现匿名认证特性, 提高了网络攻击的难度.

6 种方案都接受生物特征输入, 智能卡 SC_i 仅允许用户 U_i 在输入正确的口令 PW_i 提供生物特征信息 B_i 后, 发出有效的登录请求. 除本文增强方案外, 其他方案都要求采集设备提供 U_i 精确的生物特征信息, 这与指纹、虹膜等生物特征值本质上具有模糊特性[19-21]相矛盾; 本文增强方案将生物特征绑定精确的生物密钥 B_i, 允许用户生物特征信息包含一些噪声干扰[19], 适用性更好.

3.2.2 智能卡防丢失性能对比

基于智能卡身份认证方案需要考虑智能卡丢失、盗窃、克隆等问题. 非法获得智能卡 SC_i 的攻击者 U_a 可能借此实施生物特征验证功能屏蔽、口令猜测、敏感信息破解等攻击, 一种安全的认证方案应具备智能卡防丢失保护功能, 有效防范这 3 种攻击手段.

1) 生物特征验证功能防屏蔽

Khan-Kumari 方案用存储在 SC_i 中的参数 $f_i=h(B_i\oplus K_i)$ 来验证生物信息特征的正确性, 用 $h(PW_i\|K_i)\oplus f_i$ 对 $h(ID_i\|x_s)$ 解封装[16], U_a 可通过修改 SC_i 代码绕开 B_i 验证直接取得 f_i 解封 $h(ID_i\|x_s)$, 生物特征验证防屏蔽性能弱; Li-Huang, Das, An, Li-Niu 等方案[12-15]也采取类似处理方法, 难防 U_a 屏蔽 B_i 验证功能. 本文增强方案用 $h(PW_i\oplus B_i\oplus K_i)$ 封装 $h(ID_i\|x_s)$, 用 $h(ID_i\|PW_i\|B_i)$ 验证 ID_i, PW_i, B_i 的正确性, 仅当 ID_i, PW_i, B_i 输入全部正确无误, SC_i 才能正确解封 $h(ID_i\|x_s)$, 构造有效的认证消息, 使生物特征验证功能屏蔽手段失效.

2) 防敏感信息破解

在 Das 方案中, U_a 从 SC_i 读出参数 $r_i=h(PW_i)\oplus h(B_i)$, $e_i=h(ID_i\|x_s)\oplus r_i$, U_a 可修改 SC_i 代码不用 PW_i 与 B, 直接解封 $h(ID_i\|x_s)=e_i\oplus c_i$[14], 并借此实施身份冒充攻击, 该方案防智能卡破解能力很弱; An 方案与 Khan-Kumari 方案用参数 $f_i=h(B\oplus K_i)$, $r_i=h(PW_i\oplus K_i)\oplus f_i$ 将 $h(ID_i\|x_s)$

封装到参数 $e_i=h(ID_i\|x_s)\oplus r_i$ 中,U_a 必须输入正确的 PW_i 才能解封 $h(ID_i\|x_s)$[15-16],提高了智能卡防破解能力;Li-Huang 与 Li-Niu 方案也采取了类似的防破解措施;本文增强方案同时用 $h(PW_i\oplus B_i\oplus K_i)$ 将 $h(ID_i\|x_s)$ 封装到参数 $e_i=h(ID_i\|x_s)\oplus h(PW_i\oplus B_i\oplus K_i)$ 中,U_a 必先给出得到正确的 PW_i 与 B_i 才能解封 $h(ID_i\|x_s)$,智能卡防破解性能大大提高.

3) 防口令猜测攻击

在 Li-Huang, An, Khan-Kumari, Li-Niu 方案中,U_a 可以屏蔽 SC_i 的 B_i 验证,输入 PW_i 猜测值产生登录请求消息,根据 S_i 响应消息验证 PW_i 正确性,若 PW_i 设置不当就容易被猜中[13-16],因此这些方案容易遭受抗在线口令猜测攻击;采用本文增强方案,需同时猜中 PW_i 与 B_i 才能构造有效的登录请求消息,抗在线口令猜测能力显著增强.

Li-Huang, An, Khan-Kumari, Li-Niu 方案中,SC_i 不验证 PW_i 输入值正确性,直接用于解封 $h(ID_i\|x_s)$[12-13,15-16],离线口令猜测攻击手段无效;在 Das 方案中,SC_i 用预设参数 $r_i=h(PW_i)\oplus f_i$ 验证 PW_i 正确性,允许 U_a 实施离线口令猜测攻击;增强方案用参数 $g_i=h(ID_i\|PW_i\|B_i)$ 验证 PW_i,U_a 必须同时提供正确的 PW_i 与 B_i 才能断定 PW_i 是正确的,SC_i 具有很强的防离线口令攻击能力.

3.2.3 防网络攻击性能对比

1) 防消息分析、篡改与伪造

6 个方案的认证协议都能防止 U_a 通过消息分析推断 $h(ID_i\|x_s)$,每个消息都用与 $h(ID_i\|x_s)$ 有关的散列值进行完整性验证,消息篡改与伪造都将导致完整性验证失败,因此这些方案都能有效抵御消息分析、篡改、伪造攻击,这是对基于智能卡认证方案的基本要求.

2) 防消息回放攻击

Li-Huang, Li-Niu, Das, An, Khan-Kumaris 方案都没有消息新鲜性检查功能,若 U_a 看到 U_i 登录请求消息后,立即回放过时的 S_i 响应消息,SC_i 将记录错误的 S_i 随机数、产生错误的确认消息,最终导致正常登录请求被拒[11-15].本文增强方案检查每个认证消息的新鲜性,会丢弃 U_a 回放的历史消息,有效抵抗消息回放攻击.

3) 防已知随机数消息分析攻击

Li-Huang, Li-Niu, Das, An, Khan-Kumaris 方案直接以 $h(ID_i\|x_s)$ 为密钥加密随机数进行传输.若 U_a 通过某种途径获得某消息分量 $M=R_c\oplus h(ID_i\|x_s)$ 中的随机数 R_c,就可算出 $h(ID_i\|x_s)=M\oplus R_c$,然后借此实施身份冒充攻击.本文增强方案用动态密钥加密随机数,若 U_a 获得某消息分量 $M=R_c\oplus h(h(ID_i\|x_s)\|T)$ 中随机数 R_c,他仅能导出 $h(h(ID_i\|x_s)\|T)=M\oplus R_c$,无从获得 $h(ID_i\|x_s)$,因此已知随机数消息分析攻击是无效的.

具体结果如表 3 所示,可知本文增强方案不但比其他方案提供更多的功能特性、适用性得以增强,而且在智能卡防丢失、防网络攻击等方面的安全性能获得显著提高.

Table 3 Security Perfomance Comparison

表 3 安全性能对比

Categary	Security Item	Li-Huang Scheme[12]	Das Scheme[14]	An Scheme[15]	Khan-Kumari Scheme[16]	Li-Niu Scheme[13]	Proposed Scheme
Function Support	Bidirectional Identity Authentication	Yes	Yes	Yes	Yes	Yes	Yes
	Message Transmission Anonymity	No	No	No	Yes	No	Yes
	Support Biometric Authentication	Yes	Yes	Yes	Yes	Yes	Yes
	Accept Fuzzy Biometric Input	No	No	No	No	No	Yes
Security with Smart Card Lost	Bypass Proof of Biometric Check	Weak	Weak	Weak	Weak	Weak	Excellent
	Anti-crack of Smart Card	Moderate	Very Weak	Moderate	Moderate	Moderate	Excellent
	Anti-online Password Guessing Attack	Moderate	Moderate	Moderate	Moderate	Moderate	Excellent
	Anti-offline Password Guessing Attack	Excellent	Weak	Excellent	Excellent	Excellent	Excellent
Resistance against Network Attack	Registance against Message Tampering and Forgery Attack	Excellent	Excellent	Excellent	Excellent	Excellent	Excellent
	Registance against Message Analysis	Excellent	Excellent	Excellent	Excellent	Excellent	Excellent
	Registance against Message Replay	Moderate	Moderate	Moderate	Moderate	Moderate	Excellent
	Registancea against Message Analysis with Known Randoms	Weak	Weak	Weak	Weak	Weak	Excellent

3.3 认证开销对比

考虑到登录操作频度通常远高于注册与口令修改频度,认证开销分析忽略用户注册与口令修改环节,仅统计用户登录与身份认证过程产生的开销.

认证开销由计算开销与通信开销2个方面,计算开销主要由登录与认证过程散列运算构成,通信开销可用登录期间在智能卡与服务器之间传输的消息长度之和表示.用 T_{Hash} 分别表示1次单向散列运算 $h(\cdot)$ 所需时间,仍然用 L_{ID}, L_{Hash}, L_{Time} 分别表示用户 ID、$h(\cdot)$ 散列值、时间标志长度,6种方案认证开销如表4所示.由于采取了更多的安全性增强措施,本文方案计算开销增加到其他方案的大约3倍,但避开了耗时的大数模幂运算,15次散列运算开销给智能卡带来的负担并不重.

Table 4 Authentication Overhead Comparison

表4 认证开销对比

Overhead Type	Li-Huang Scheme[12]	Das Scheme[14]	An Scheme[15]	Khan-Kumari Scheme[16]	Li-Niu Scheme[13]	Proposed Scheme
Smart Card Computation Overhead during User Logon	$4T_{\text{Hash}}$	$5T_{\text{Hash}}$	$5T_{\text{Hash}}$	$5T_{\text{Hash}}$	$7T_{\text{Hash}}$	$15T_{\text{Hash}}$
Server Computation Overhead during User Logon	$3T_{\text{Hash}}$	$5T_{\text{Hash}}$	$4T_{\text{Hash}}$	$5T_{\text{Hash}}$	$6T_{\text{Hash}}$	$15T_{\text{Hash}}$
Communication Overhead during Logon	$4L_{\text{Hash}}+L_{ID}$	$6L_{\text{Hash}}+L_{ID}$	$5L_{\text{Hash}}+L_{ID}$	$6L_{\text{Hash}}$	$5L_{\text{Hash}}+L_{ID}$	$13L_{\text{Hash}}+5L_{\text{Time}}$

由于 SC_i 与 S_i 间交互的增加,本文增强方案通信开销也增加到接近其他方案的3倍,若设 $L_{\text{Hash}}=512$ b, $L_{\text{Time}}\ll L_{\text{Hash}}$,本文增强方案完成一次用户登录所需通信开销在1 KB以内,给通信网络带来的负荷也不算大.

4 结论与展望

基于生物特征的智能卡身份认证同时对"你所知"、"你所有"、"你独有"3个因素进行验证,给用户身份提供智能卡硬件、口令验证、生物特征验证三重保护,大幅增加冒充难度,有效提高身份认证可靠性,增强系统和信息安全,给远程身份认证技术带来了新的突破点.

本文首先回顾了目前具有较高安全性能的Khan-Kumari方案工作原理,分析了该方案仍然存在用户身份密值封装不当、密值使用方式不合理、消息新鲜性检测功能缺失、认证双方交互不够充分等缺陷,可能导致生物特征验证功能被屏蔽、正常登陆失败、拒绝服务等问题,特定情况下还可能造成用户身份密值泄露与身份冒充攻击.本文在保持Khan-Kumari方案的消息传输匿名、双向认证等特性基础上,提出一个增强的基于生物密钥智能卡远程身份认证方案,将具有一定模糊性的用户生物特征信息映射成生物密钥作为用户"你独有"因素,提高了方案适用性;用可相互验证的双要素对用户身份密值实施联合保护,防止基于部分输入信息破解智能卡受保护密值;增加基于时标的消息新鲜性检查,消除消息重放的干扰;采用融入时标的动态散列值密钥,抵抗基于消息分析破解用户身份密值;增加确认消息完善认证流程,抵抗拒绝服务攻击.安全性分析表明,本文增强方案修复了Khan-Kumari方案的缺陷,能可靠抵抗消息篡改、伪造、回放、分析攻击,系统不但在三重保护完好时具有很高的安全性能,而且两重保护失效条件下发生身份冒充、认证被扰乱的概率可降低至 10^{-38} 以下.与其他方案相比,本文方案在智能卡防丢失、防网络攻击等方面的安全性能获得较大增强.虽然计算与通信开销明显高出其他方案,但登录过程仅涉及低开销单向散列运算,给智能卡带来的负担并不重,不足1 KB的通信开销给通信网络带来的负荷也不算大.

基于生物密钥智能卡身份认证的适用性与生物密钥提取的准确性、计算开销、存储开销有着密切的关系.由于生物特征信息的模糊性,用于密钥绑定与密钥提取的生物信息存在不同程度的差异,可能导致生物密钥提取错误[20].为保护生物密钥机密性,生物密钥适合在智能卡内部处理,但生物密钥绑定与提取涉及大量大数模幂运算[20],其计算开销与存储开销可能超出智能卡限制.下一步将探讨适合智能卡的轻量级生物密钥绑定与提取方法研究.

参 考 文 献

[1] Lamport L. Password authentication with insecure communication [J]. Communications of the ACM, 1981, 24 (11): 770-772

[2] Chang C C, Wu T C. Remote password authentication with smart cards [J]. IEE Proceedings E: Computers and Digital Techniques, 1991, 138(3): 165-168

[3] Haller N M. The S/Key™ one-time password system [C] // Proc of the ISOC Symp on Network and Distributed System Security. San Diego, CA: Internet Society, 1994: 151-157

[4] Wang Shiuh-Jeng, Chang Jin-Fu. Smart card based secure password authentication scheme [J]. Computers & Security, 1996, 15(3): 231-237

[5] Hwang M S, Li L H. A new remote user authentication scheme using smart cards [J]. IEEE Trans on Consumer Electronics, 2000, 46(1): 28-30

[6] Chan C K, Cheng L M. Cryptanalysis of a remote user authentication scheme using smart cards [J]. IEEE Trans on Consumer Electronics, 2000, 46(4): 992-993

[7] Wang Ding, Ma Chunguang, Weng Chen, et al. Cryptanalysis and improvement of a remote user authentication scheme for resource-limited environment [J]. Journal of Electronics & Information Technology, 2012, 34(10): 2520-2526 (in Chinese)
(汪定, 马春光, 翁臣, 等. 一种适于受限资源环境的远程用户认证方案的分析与改进[J]. 电子与信息学报, 2012, 34(10): 2520-2526)

[8] Lee J K, Ryu S R, Yoo K Y. Fingerprint-based remote user authentication scheme using smart cards [J]. Electronics Letters, 2002, 38(12): 554-555

[9] Lin C H, Lai Y Y. A flexible biometrics remote user authentication scheme [J]. Computer Standards & Interfaces, 2004, 27(1): 19-23

[10] Khan M K, Zhang J. Improving the security of "a flexible biometrics remote user authentication scheme"[J]. Computer Standards & Interfaces, 2007, 29(1): 82-85

[11] Zhang Fan, Feng Dengguo. Fuzzy extractor based remote mutual biometric authentication [J]. Journal of Computer Research and Development, 2009, 46(5): 850-856 (in Chinese)
(张凡, 冯登国. 基于模糊提取的远程双向生物认证[J]. 计算机研究与发展, 2009, 46(5): 850-856)

[12] Li C T, Hwang M S. An efficient biometrics-based remote user authentication scheme using smart cards [J]. Journal of Network and Computer Applications, 2010, 33(1): 1-5

[13] Li X, Niu J W, Ma J, et al. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards [J]. Journal of Network and Computer Applications, 2011, 34(1): 73-79

[14] Das A K. Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards [J]. IET Information Security, 2011, 5(3): 541-552

[15] An Y. Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards [J]. Journal of Biomedicine and Biotechnology, 2012, 2012: Article ID 519723

[16] Khan M K, Kumari S. An improved biometrics-based remote user authentication scheme with user anonymity [J]. BioMed Research International, 2013, 2013: Article ID 491289

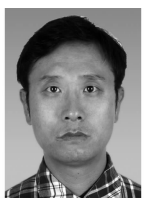
[17] Kocher P, Jaffe J, Jun B. Differential power analysis [G] // Advances in Cryptology—CRYPTO'99. Berlin: Springer, 1999: 388-397

[18] Messerges T S, Dabbish E A, Sloan R H. Examining smart-card security under the threat of power analysis attacks [J]. IEEE Trans on Computers, 2002, 51(5): 541-552

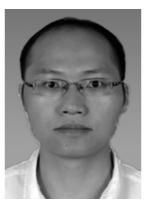
[19] Jain A K, Ross A, Prabhakar S. An introduction to biometric recognition [J]. IEEE Trans on Circuits and Systems for Video Technology, 2004, 14(1): 4-20

[20] Shi Jinyang. Research on key technology of biological ECG and based on fingerprint [D]. Beijing: Tsinghua University, 2010 (in Chinese)
(施金洋. 基于心电和指纹特征的生物密钥技术研究[D]. 北京:清华大学, 2010)

[21] Juels A, Sudan M. A fuzzy vault scheme [J]. Designs, Codes and Cryptography, 2006, 38(2): 237-257



Xu Qingui, born in 1967. Professor and PhD. Member of China Computer Federation. His main research interests include computer architecture, information security, and intelligent detetion and instrument.



Huang Peican, born in 1984. MS. Lecturer. His main research interests include embedded system design and computer architecture (huangpc@dgut.edu.cn).

Yang Taolan, born in 1945. Professor and PhD supervisor. His main research interests include computer architecture and compiler (yangtl@dgut.edu.cn).