

[文章编号] 1003—4684(2020)02-0067-03

适用于电子健康系统的高效密钥协商协议

杨博文, 翟之博, 徐 湘, 徐 丹, 谢昆明

(湖北工业大学计算机学院, 湖北 武汉 430068)

[摘 要] 智能设备的计算能力和内存有限,难以保护用户的大量私有数据。虽然有些研究已经在用户和医疗服务器之间建立了一个安全的会话密钥,但在保持匿名性和低能耗方面仍然存在不足。针对此问题设计了一种隐私保护机制,在身份验证和密钥协商过程中,由于传输的消息不可追踪,所以有很高的用户匿名性。性能分析表明,该方案在安全性和资源占用方面均符合标准。

[关键词] 身份验证; 电子医疗保健; 隐私保护

[中图分类号] TP391 [文献标识码] A

在过去的十年中,互联网设备已经取代了老式的台式机和医疗设备。随着物联网技术的进步,各种手持和可穿戴的设备(例如,平板电脑、智能手表和智能手环)可以充当传感器和监视器。通常,这些设备安放在患者的身体上或患者居住的地方,收集实时数据,将它们发送到远程服务器,然后发送到客户端。诊断和应急决策可以根据接收到的信息和个人电子健康记录进行。然而,无线通信的自然缺陷引起了人们对电子健康服务中隐私保护的极大关注。由于医疗数据在不安全的公共网络传输,患者的隐私容易受到多种攻击。

1 方案提出

本文提出了一种实用的认证密钥协商方案,能够满足电子健康安全需求和计算需求。主要功能如下:

服务器上的安全认证:在提出的方案中,医疗服务器负责检查用户的有效性。为了防止服务器知道密码,使用异或操作将随机字符串与其组合,然后在服务器端匹配两个屏蔽字符串,而不是将真实密码与之匹配。因此,医疗服务器可以验证密码,而不存储和获得具体值。

强大的隐私保护:在存储设备中,智能卡、数据库受到随机数的保护,以确保只有用户拥有真正的密码。针对匿名性和不可追踪性,提出了一种打破传输消息联动的动态机制。数据库和智能卡的相关值将在每次成功登录后更新。可以证明方案在真实或随机模型下是语义安全的。

效率:所提出的方案是轻量级的,因为只用到了哈希函数。所以该系统拥有较高的安全性和高效性。

2 方案介绍

2.1 注册阶段

首先,用户选择用户名 ID_u ,并输入口令 PW 。生成一个随机数 r_0 ,分别与 ID_u 和 PW 连接并获得对应哈希值,用户端可以将两个值 hID 和 hPW 发送给服务器 S 。服务器在收到用户发送过来的消息后,产生一个随机数 r_1 ,并且计算 $P = h(hID || x)$ 和 $R = P \oplus h(hID || r_1)$,其中 x 是服务器 S 的密钥。然后服务器将 hID 、 hPW 储存在数据库中,并将 $R, r_1, h(\cdot)$ 储存在用户的智能卡中。最后,服务器通过安全手段,将智能卡交予用户。当用户拿到智能卡时,计算 $verify = h(ID_u || r_0 || PW || r_1)$, $Z = h(ID_u || PW || r_1) \oplus r_0$,并将 $verify, Z$ 储存到智能卡中,从而完成注册阶段,具体过程见图 1。

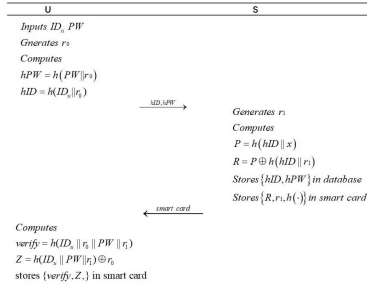


图 1 注册阶段

[收稿日期] 2019—09—23

[第一作者] 杨博文(1998—),男,湖北南漳人,湖北工业大学学生,研究方向为软件工程与信息安全

2.2 登录和认证阶段

阶段一:登录时,用户首先需要插入智能卡,并输入自己的用户名 ID_u 和口令 PW 。智能卡会自动计算 $r_0' = Z \oplus h(ID_u || PW || r_1)$, $verify' = h(ID_u || r_0' || PW || r_1)$ 。由于用户智能卡中储存有 $verify$,那么只需比较 $verify'$ 和 $verify$ 是否相等即可验证用户输入的用户名和口令的正确性。若不等,则提示用户用户名或口令输入错误,若相等则继续执行后续步骤。智能卡产生一个随机数 r_2 ,并计算 $hID' = h(ID_u || r_0')$, $P' = R \oplus h(hID' || r_1)$, $Q = P' \oplus r_2 \oplus h(PW || r_0')$, $S = Q \oplus hID'$, $T = h(hID' || r_2 || p')$ 。最后,用户将消息 $\{Q, S, T\}$ 通过公共信道发送给服务器。

阶段二:服务器在收到用户发送过来的消息后,计算得到 $hID'' = Q \oplus S$,并通过 hID'' 搜索数据库,得到对应的 hPW 。然后计算 $P'' = h(hID'' || x)$, $r_2' = Q \oplus P'' \oplus hPW$,并验证之前接收的 T 是否等于 $h(hID'' || r_2' || P'')$ 。若不相等,则服务器拒绝此次登录请求;若相等,则服务器产生两个随机数 r_3, r_4 ,并计算 $v_1 = P'' \oplus r_3$, $v_2 = h(P'' || r_2' || r_3 || r_4)$, $v_3 = h(v_1 || r_2') \oplus r_4$, $SK = h(P'' || r_2' || r_3 || r_4)$ 。最后,服务器将消息 $\{v_1, v_2, v_3\}$ 发送给用户。

阶段三:用户接收到服务器的返回消息后,可以使用自己的已知数据计算出 r_3', r_4' 的值,并检查 v_2 是否与 $h(P' || r_2 || r_3' || r_4')$ 相等。若不等,则用户立即结束此次登录过程,并重新执行阶段一中的流程;若相等,用户计算得到 $\{Z_{new}, verify_{new}\}$,并使用 $\{Z_{new}, verify_{new}\}$ 代替智能卡中的值 $\{Z, verify\}$ 。最后用户计算得到与服务器端的 SK 相同的会话密钥,具体过程见图 2。



图 2 登录和认证阶段

3 相关攻击的预防

这一部分,将通过分析一些可能的攻击来讨论和证明笔者提出的协议的安全性。

重放攻击:方案中,如果黑客监听到用户合法的登录请求消息 $\{Q, S, T\}$ 并记录下来,并在某一时刻向医疗服务器 S 发送这一消息。黑客会通过服务器的验证且获得消息 $\{v_1, v_2, v_3\}$ 进行下一步的智能卡端的验证,但此时黑客并没有上一次用户卡中随机数 r_2' 的值。他将会在用户端验证 v_2 的过程中失败,因此黑客不能构建与医疗服务器 S 或用户 U 的独立连接。

离线秘钥猜测攻击:假设黑客拦截用户 U 和医疗服务器 S 之间传输的所有消息,并发起离线秘钥攻击。因为发送的信息并不直接包含用户的 ID 和密码,黑客不能通过截获的消息确定他猜到的每个密码是否正确。因此,如果没有对应用户的智能卡,就不能成功执行离线秘钥攻击。

离线密码猜测攻击:因为用户 U 和医疗服务器 S 之间在公共信道上传输消息,黑客可以获取消息 $\{Q, S, T, v_1, v_2, v_3\}$,但是随机数 r_2' 的值黑客未知,由于公式和哈希函数的存在,黑客不能在有限的时间内计算出用户的密码 PW 的值,甚至用户名 ID 的值。因此黑客不能猜测出用户 U 密码的值。

去同步攻击:在所提出的方案中,医疗服务器 S 计算 SK 后,向用户发送确认消息 $\{v_1, v_2, v_3\}$ 。如果用户接收到确认消息,则它将计算的 SK 存储为共享会话密钥。如果这个过程被阻塞,用户将不会在给定时间内接收确认消息。在这种情况下,用户将删除 SK 并重新启动登录和身份验证过程。因此,在重启身份验证过程中,用户和服务器就会使用新的共享会话密钥。因此,所提出的方案能够抵抗去同步攻击。

伪装攻击:一方面,黑客可以伪装成合法用户 U 向服务器端 S 发送伪造的消息 $\{Q, S, T\}$,但是他不能通过服务器的验证,因为他没有正确的 ID, PW 和 R 的值。另一方面,黑客可以伪装成服务器端来接受正常用户合法的消息 $\{Q, S, T\}$,并向用户端发送伪装的消息 $\{v_1, v_2, v_3\}$ 。但是,黑客缺乏此用户在真正的服务器上对应的 hID, R 和 P 的值,他不能通过在用户端对 V_2 的验证。因此,本方案能抵御黑客的伪装攻击。

内部攻击:假设黑客可以在服务器的数据库端获取大量用户的 hID, R 和 P 的值,因为随机数 r_0 的存在,黑客不能计算得出用户正确 ID 和 PW 的值,也不能得出重要的数据信息 Z 的值。因此,本

方案能阻挡黑客的内部攻击。

4 性能分析

先假设使用一个哈希函数运行的时间为 T_h ,其他类型的操作如生成随机数、拼接、异或的所需时间相较于运行一个哈希函数的时间而言太小,可以忽略不计,所以在性能分析中忽略了此轻量级操作类型的耗时。在经过分析之后,列出表 1 描述方案的性能分析。

表 1 方案的性能分析		T_h
阶段	性能耗时	
	用户端	
注册阶段	4	2
登陆阶段	11	5

从表 1 中可以看出:方案在注册阶段,用户端耗时 4 T_h ,服务器端耗时 2 T_h ,总共用时 6 T_h ;在登陆阶段,用户端耗时 11 T_h ,服务器端耗时 5 T_h ,总共用时 16 T_h 。运行一次哈希函数所需要的时间大概是 0.1 ms。在大多数情况下,注册和登陆阶段,方案耗时都在 2 ms 之内。

通过性能分析,可以得出结论:本方案在实际的应用中具有高效性。

5 结论

本文提出了一种基于动态认证机制的密钥协商

方案,用于保障电子健康系统的用户隐私。传统的身份口令表被动态验证表代替,以提供不可追踪性,从而可以完全保留用户的匿名性。此外,方案只采用了轻量级的哈希和异或操作,与其他相关方案相比,降低了计算成本和通信成本。因此,所提出的方案可以成功地满足电子健康系统的能量消耗和安全需求。

[参 考 文 献]

[1] 余幸杰,高能,江伟玉. 云计算中身份认证技术研究[J]. 信息安全, 2012, (8):71-74.

[2] 周克元. 对两个离散对数数字签名算法的攻击与改进[J]. 科学技术与工程, 2013, 13(32):9725-9729.

[3] 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究[J].软件学报,2003,14(8):1401-1408.

[4] 张绍武,林鸿飞,刘晓霞. 基于概率的信任传播模型[J].计算机科学,2014,41(8):90-93.

[5] 袁峰,程朝辉.SM9 标识密码算法综述[J].信息安全研究,2016,2(11):1008-1027.

[6] 周艺华,蒿金志,赵航. 混合云服务中的跨云际认证机制[J]. 计算机系统应用,2015,24(4):118-122.

[7] 杨晓辉.基于动态 ID 远程用户身份认证方案的改进[J].电子技术,2014(6):40-42.

An Efficient Key Agreement Protocol for Electronic Health System

YANG Bowen,ZHAI Zhibo,XU Xiang,XU Dan,XIE Kunming

(School of Computer Science, Hubei Univ. of Tech., Wuhan 430068,China)

Abstract: With the development of various intelligent wireless devices in the past decade,e-health system has developed into a more patient-centered service.However,the computing power and memory size of these smart devices are limited,so it becomes more difficult for electronic health systems to protect a large number of users' private data.Although some studies have established a secure session key between users and medical servers,there are still shortcomings in maintaining anonymity and low energy consumption.In this study,a dynamic privacy protection mechanism is designed.In the process of authentication and key agreement,all users have high anonymity due to the untraceability of the transmitted messages.In addition,the semantic security of the scheme has been proved under the entity model and the stochastic model.Performance analysis shows that the scheme meets the standards in terms of security and resource occupation.

Keywords: authentication, electronic health care, privacy protection

[责任编辑: 张岩芳]