

可穿戴设备拥有者转换协议的设计

胡舜, 翁健, 刘家男

(暨南大学 信息科学技术学院, 广东 广州 510632)

摘要: 近年来, 可穿戴设备作为一类新型的智能设备正在改变着人们的生活方式。当这类设备处在多用户环境下时, 应该考虑拥有者转换这一场景。为了解决可穿戴设备在拥有者转换场景下面临的安全隐私问题, 设计了一个安全的可穿戴设备拥有者转换协议。该协议包括初始化、相互认证和密钥更新 3 个阶段。安全性分析表明本协议能够抵御传统的信道攻击和拥有者转换场景下的特殊攻击。实验分析表明所提方案具有较高的效率, 能够适用于可穿戴设备环境。

关键词: 可穿戴设备; 拥有者转换; 信号干扰; 安全分析

中图分类号: TP368.33

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2015.00010

An ownership transfer protocol for wearable devices

HU Shun, WENG Jian, LIU Jia-nan

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

Abstract: Recently, wearable devices acted as a kind of smart devices are changing people's life style. When these devices are used in multi-user setting, ownership transfer should usually be considered. To resolve the security and privacy problems introduced in the ownership transfer process of wearable devices, a secure ownership transfer protocol including initialization, mutual authentication and key change for wearable devices was introduced. The security analysis indicates that the proposed protocol can resist either normal channel attacks or special attacks appeared in the ownership transfer scenarios. The experiment results indicate that the proposed scheme is fairly efficient and is quite suitable for wearable devices.

Key words: wearable device; ownership transfer; signal interfere; security analysis

1 引言

近年来, 越来越多的智能可穿戴设备进入到人们的生活中。它们以便携性和实用性, 逐步影响人们的生活方式, 提高人们的生活品质。例如, 智能腕表在跑步时追踪路程、速度、时间和消耗热量等数据, 以帮助用户制定运动计划、检测用

户身体状况等。然而, 这些可穿戴设备在使用过程中存在一系列安全问题。例如, 可穿戴设备通常保存有用户的健康信息和通讯信息等隐私数据, 而这些数据的泄露将会给用户带来难以估量的损失。因此, 隐私保护成为可穿戴设备面临的首要问题。针对可穿戴设备的隐私数据攻击主要分为两类。第一类是针对可穿戴设备本身的攻击。

收稿日期: 2015-09-18; **修回日期:** 2015-10-08. **通信作者:** 翁健, cryptjweng@gmail.com

基金项目: 国家自然科学基金资助项目 (61272413, 61472165); 教育部高等学校博士学科点专项科研基金博导类基金资助项目 (20134401110011)

Foundation Items: The National Natural Science Foundation of China (61272413, 61472165); The Research Fund for the Doctoral Program of Higher Education of China (20134401110011)

该类攻击主要为:当用户的可穿戴设备被恶意攻击者获取后,攻击者可以从可穿戴设备中读取用户存储在设备里面的敏感数据等。针对这一类攻击,需要在可穿戴设备上部署相应的身份认证方案,如密码认证、图形认证和指纹认证方法等。第二类攻击是针对可穿戴设备与移动终端之间通信信道的攻击。该类攻击主要包括:攻击者伪造、假冒移动终端与可穿戴设备进行通信;攻击者拦截并修改可穿戴设备与移动终端间的通信数据;攻击者从通信过程中获取可穿戴设备 ID 并对其进行 DOS 攻击。针对这一类攻击最有效的防御方法是让可穿戴设备和移动终端实行双向认证,并采取可信信道来对二者间传输的内容进行保护。

然而,在可穿戴设备的实际应用中,这种可信信道方案存在一定的实现难度。因为可穿戴设备和移动终端需要提前进行协商并得到一个通信密钥,才能在后续进行安全的数据传输。然而,通信双方在密钥协商过程中会面临来自外界的安全挑战,尤其在拥有者转换场景下更加容易面临一系列攻击。

下面考虑这样的场景:用户 Alice 拥有一块智能手表,与其智能手机连接并传递信息。当 Alice 的朋友 Bob 借用 Alice 的智能手表,并归还后,就产生了智能手表的二次拥有者转换过程,一次是从当前用户 Alice 变更到新用户 Bob,另一次是从新用户 Bob 变更回旧用户 Alice。在智能手表第一次拥有者转换过程完成后, Alice 保存在智能手表上的数据有可能会泄露给 Bob。同样,当 Bob 返还智能手表给 Alice 的时候, Bob 的数据也有可能泄露给 Alice。解决这个问题最简单的方法是对智能手表进行数据初始化,即进行拥有者转换之前,删除智能设备上保存的所有数据。然而这种方法的缺陷在于:每转换一次拥有者,当前拥有者都需要对存储在智能手表上的数据进行备份并保存在电脑上,然后初始化智能手表,而转换后的拥有者则需要还原之前备份的数据。毫无疑问,这种繁琐的操作会消耗双方大量的精力和时间。另一种方法是在拥有者转换过程中依然保存 Alice 和 Bob 的数据,但是数据是经过加密后存储在可穿戴设备上的。此时,智能手表分配不同的会话密钥给 Alice 和 Bob。而 Alice 和

Bob 通过各自的会话密钥与智能手表进行通信。这种方法实现的前提有两点:①智能手表上数据加密的高效性;②智能手表支持不同的会话密钥并与其通信。因此,如何构造一种高效的具备密钥更新性能的加密方案,成为解决智能设备上的拥有者转换过程中的数据安全与隐私保护问题的关键。

为了解决上述问题,设计了一个交互式安全的拥有者转换协议。该协议支持智能设备与拥有者之间的双向认证,同时可以保证 Alice 和 Bob 在不知道对方会话密钥的情况下实现智能手表的拥有者转换,并且该方案可以抵御传统的信道攻击和拥有者转换场景下的特殊攻击,同时具有较高的执行效率与实际应用的可行性。

2 相关工作

2.1 可穿戴设备研究现状

当前针对可穿戴设备的研究主要集中在利用可穿戴设备辅助实现一些其他功能^[1,2]。Wahbah 等人^[3]提出了人在不同状态下,所携带的可穿戴设备使用能耗及电池能量采集状态不同,并对此进行了实验。Magalhães 等人^[4]设计了一套生物入侵防护系统,而这套系统将可穿戴设备用作一个辅助设备。另外,可穿戴设备还被大量使用于健康领域。Prabhakar^[5]提出利用设备作为一个健康辅助应用。Wang 和 Huang^[6]提出利用可穿戴设备来监控电力工人的健康情况。Zheng^[7]等人介绍了 4 种可穿戴技术,这些技术对应的设备可监测人体健康信息并发送给医生,便于医生诊断和进行疾病的预防。另外,可穿戴设备还可以作为一种辅助设备帮助残疾人更好地生活。Matsubara 等人^[8]设计了 GaitEcho。这是一个可穿戴听觉信息反馈设备,用来帮助盲人和有视觉障碍的人更好地与人沟通。Gorman^[9]设计了一种声音定位设备以帮助听力障碍的人更好地获取声音信号。Fontana 等人^[10]设计了一个新颖的可穿戴传感系统 AIM,该系统可以检测人们的日常摄食行为。Gruebler 和 Suzuki^[11]设计了一种使用生理信号读取积极面部表情的可穿戴设备。该设备通过记录大量的用户面部表情来帮助医生更好地研究患者。Lyons 和 Profita^[12]从宏观的层次介绍了可穿戴环境,并

深入研究了携带可穿戴设备对人们日常肢体姿势的影响。为了实现在移动应用环境下人们可以不断认证和登陆服务器, Ojala 等人^[13]提出了一种可穿戴认证设备。该设备是一个腕带, 可以认证用户指纹并测量用户的心率和皮肤温度。用户利用该设备认证指纹后可无需使用其他信息而直接登陆到远程计算机上。Periaswamy^[14]提出了利用可穿戴设备作为辅助设备来实现 RFID 标签的拥有者转换。

2.2 RFID 拥有者转换研究现状

RFID 标签拥有者转换场景最早是由 Saito 等人^[15]提出来的。他们考虑到了有 TTP 和没有 TTP 两种情况并提出了相应的简单解决方案。此后, Kulseng 等人^[16]提出了一个相互认证协议来保障标签在拥有者转换过程中的安全。Osaka^[17]在总结当时关于 RFID 标签拥有者转换安全需求后, 提出了一个能满足当时所有安全需求的拥有者转换方案。Song^[18]将拥有者转换过程分为两个部分: 传输会话密钥给新用户和更新密钥。这是一个重要变革, 因为他们首次考虑到了拥有者转换过程中更新密钥的情况, 并强调了其重要性。Kapoor 和 Piramuthu^[19]发现当时大部分 RFID 标签拥有者转换协议都有漏洞, 因此, 针对该漏洞提出了一个全新的拥有者转换方案。该方案是一个没有 TTP 参与的轻量级方案。他们在方案中假设 R1 和 R2 之间存在一个安全信道并可以明文传输敏感数据。经过改进后, Jorge^[20]提出了一个新的拥有者转换方案。该方案满足部署了噪声信道的拓展通信模型。Chen^[21]从实际出发, 在 2013 年提出了一种全新的移动支付应用场景, 并将之前的方案改进后应用到该场景中。

3 方案描述

整个拥有者转换过程由 3 个阶段组成: 初始化阶段、相互认证阶段和密钥更新阶段。

3.1 参数介绍

- 1) CO: 新拥有者的智能手机, 也代表新拥有者角色。
- 2) OO: 旧拥有者的智能手机, 也代表旧拥有者角色。
- 3) WD: 需要进行拥有者转换的可穿戴设备;

4) S_1 : 旧拥有者和可穿戴设备间共享的会话密钥, 该密钥用于加密旧拥有者和可穿戴设备间的通信信息。

5) S_2 : 新拥有者和可穿戴设备间共享的会话密钥, 该密钥由新拥有者产生, 并用于加密未来新拥有者和可穿戴设备间的通信信息。

6) B_{CO} : 新拥有者智能手机的蓝牙地址。

7) B_{WD} : 可穿戴设备的蓝牙地址。

8) N_1 : 同一用户手动在旧拥有者智能手机和新拥有者智能手机上输入的数字, 该数字经过拓展后将暂时作为这两台智能手机间通信信息加密的会话密钥。

9) N_2 : 同一用户手动在新拥有者智能手机和可穿戴设备上输入的数字, 该数字经过拓展后将暂时作为这两个设备间通信信息加密的会话密钥。

10) TID_{WD} : 可穿戴设备产生的暂时性 ID, 该 ID 用于在本次拥有者转换过程中标记可穿戴设备的身份, 在拥有者转换过程结束后立刻失效。

11) R_1 : 旧拥有者智能手机产生的一个随机数。

12) R_2 : 新拥有者智能手机产生的一个随机数。

13) $H(a)$: 参数 a 的散列值。

3.2 初始化阶段

初始化阶段是一个准备阶段, 为后续 CO 和 WD 进行相互认证奠定基础。该阶段中, OO 将 CO 相关信息发送给 WD, 将 WD 相关信息发送给 CO。

如图 1 所示, 初始化阶段具体流程如下。

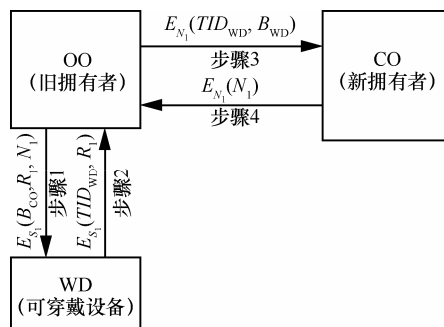


图 1 初始化阶段过程

1) OO 产生一个随机数 R_1 , 然后使用之前与 WD 进行通信的会话密钥 S_1 对 CO 的蓝牙地址、随机数 R_1 和用户手动输入的数字 N_1 进行加密, OO 将加密后的信息 $E_{S_1}(B_{CO}, R_1, N_1)$ 发送给 WD。

2) WD 使用与 OO 进行通信的会话密钥 S_1 对

收到的密文进行解密后，将得到的3个参数存储在本地内存中。

3) WD产生一个用于本次拥有者转换的暂时ID TID_{WD} ，然后使用会话密钥 S_1 对 TID_{WD} 和 R_1 进行加密后将密文信息 $E_{S_1}(TID_{WD}, R_1)$ 发送给 OO。

4) OO 使用会话密钥 S_1 解密收到的密文信息。此时 OO 将本地产生的和收到密文解密后得到的 R'_1 进行比较。若两个数字相同，则保存解密得到的 TID_{WD} ，若不相同，则丢弃该条信息并中断与 WD 的连接。

5) OO 使用用户在 OO 和 CO 上手动输入的不同数字 N_1 对 TID_{WD} 和 WD 的蓝牙地址 B_{WD} 进行加密后，将密文 $E_{N_1}(TID_{WD}, B_{WD})$ 发送给 CO。

6) CO 使用 N_1 解密收到的信息，并获得 WD 的暂时 ID TID_{WD} 和 WD 的蓝牙地址 B_{WD} 。

7) CO 发送一个应答信息 $E_{N_1}(N_1)$ 给 OO，该信息用于表明 CO 收到了 OO 发送过来的信息 $E_{N_1}(TID_{WD}, B_{WD})$ 。

3.3 相互认证阶段

相互认证是一个重要阶段。在该阶段中，CO 和 WD 将通过蓝牙地址和散列值对双方的身份进行验证，从而抵御假冒和伪造攻击。

如图2所示，该阶段具体流程如下。

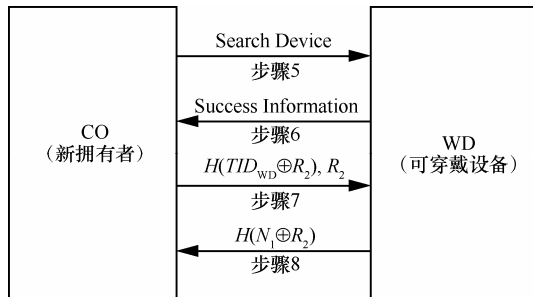


图2 相互认证阶段过程

1) 通过之前从 OO 处接收的 WD 的蓝牙地址 B_{WD} ，CO 搜索附近的蓝牙设备并找到指定蓝牙地址的设备，然后发送连接请求给该设备。

2) 在收到连接请求后，WD 获得请求设备的蓝牙地址并与之前从 OO 处接收的 CO 的蓝牙地址进行比较。若两个蓝牙地址相同，则接受请求并发送连接成功信息给对方设备，若不相同，则丢弃该请求并发送拒绝连接信息给对方设备。

3) 在接收到连接成功信息后，CO 产生一个随机数 R_2 ，并计算 TID_{WD} 和 R_2 组合后的散列值

$H(TID_{WD} \oplus R_2)$ 。然后 CO 将该散列值和 R_2 一起发给 WD。

4) 在收到 CO 发来的信息后，WD 利用接收的 R_2 和本地存储的 TID_{WD} 计算其异或后的散列值 $H'(TID_{WD} \oplus R_2)$ ，并比较 H' 和接收到的 H 。若相同，则 WD 确认当前与其通信的设备是新拥有者 CO，若不同，则 WD 会中断与当前设备的连接。

5) WD 确认 CO 身份后先计算 N_1 和 R_2 的异或值，然后计算其散列值 $H(N_1 \oplus R_2)$ ，并发送给 CO。

6) CO 收到 WD 发来的信息后，先在本地计算 $H'(N_1 \oplus R_2)$ ，然后与收到的散列值进行比较，若 $H'(N_1 \oplus R_2) = H(N_1 \oplus R_2)$ ，则 CO 确认当前与其通信的设备是 WD，若不相同，则 CO 中断与当前设备的连接。

3.4 密钥更新阶段

在该阶段中，WD 通过与 CO 协商获得一个全新的会话密钥 S_2 ，该密钥用于未来 CO 和 WD 之间通信的数据加密。

如图3所示，密钥更新阶段具体流程如下。



图3 密钥更新阶段流程

1) 用户在 CO 和 WD 上手动输入相同的数字 N_2 。

2) CO 生成会话密钥 S_2 ，然后将 S_2 和 R_2 进行组合，利用 N_2 对组合后的值进行加密，进而将密文 $E_{N_2}(S_2, R_2)$ 发送给 WD。

3) WD 使用密钥 N_2 对收到的密文进行解密，然后对解密后的 R'_2 与本地存储的 R_2 进行比较，若相同，则存储 S_2 ，否则丢弃该条信息。

4) WD 将 S_2 和 R_2 进行组合后进行散列加密，然后将散列值 $H(S_2, R_2)$ 发送给 CO。

5) 在收到来自 WD 的信息后，CO 利用本地存储的 S_2 和 R_2 组合后计算出一个散列值 $H(S_2, R_2)$ ，然后与收到的 H' 进行比较。若 $H' = H$ ，则 CO 确信 WD 已经将会话密钥更新为 S_2 ，其也将会话密钥改为 S_2 ，然后发送一条确认信息 $E_{S_2}(R_2)$ 给 WD。

6) WD 在收到来自 CO 的确认信息 $E_{S_2}(R_2)$ 后利用本地存储的 S_2 进行解密得到 R_2' , 然后比较 R_2' 和本地保存的 R_2 。若相等, 则 WD 确认以后和 CO 间通信使用 S_2 进行信息加密, 若不相等, 则 WD 立刻发送一条同步失败的信息给 CO 并中断与 CO 的连接。

7) 若 CO 收到来自 WD 的同步失败的信息则丢弃本地存储的 S_2 , 并重新开始当前阶段第 2) 步。

4 安全分析

4.1 针对传统攻击

1) 中间人攻击

中间人攻击主要指第三方恶意用户通过拦截或篡改正在通信的数据从而达到欺骗通信双方并获得通信内容的目的。中间人攻击包括两种主要方式: 信息篡改和信息窃取。

本文设计的拥有者转换方案能有效防止这两种方式的攻击。在初始化阶段, OO 与 WD 之间通信的信息采用共享密钥 S_1 进行加密。即使攻击者拦截了该部分的通信信息, 也无法获知其中的内容, 因为攻击者并不知道 S_1 。若攻击者篡改了该部分信息, 则通信的一方收到信息后利用 S_1 无法进行有效解密, 此时很容易知道信息已经被篡改, 然后进行信息重发。在初始化阶段, OO 与 CO 之间通信采用用户手动输入的数字 N_1 进行信息加密。由于 N_1 属于同一个用户手动输入, 且类似于实际生活中用户在 POS 机输入密码, 用户会采取一些姿势尽量确保该密码不会被其他人看到, 因此可以理解为第三方攻击者有极低概率获得 N_1 , 因此该攻击者很难窃取和篡改 OO 和 CO 之间传输的信息。在相互认证阶段, CO 和 WD 之间采用散列值比较的方法进行相互身份认证。即便第三方攻击者拦截步骤 10 的信息, 也无法直接解密, 因为散列函数具有单向性。同时, 信息中附带传输的 R_2 也无法进行篡改, 因为攻击者无法同时修改 $H(TID_{WD} \oplus R_2)$ 和 R_2 以达到 WD 能验证通过的目的。在密钥更新的过程中, 步骤 9 传输的数据使用同一用户手动输入的数字 N_2 进行加密, 跟前面提到的 N_1 一样, 攻击者很难获得 N_2 的值, 因此几乎不可能进行该部分信息的解密和篡改。步骤 11 仅仅是一条确认信息, 本身价值很低, 且攻击者并不

知道 CO 最新生成的 S_2 , 因此, 也无法进行解密和篡改。

2) 反同步攻击

反同步攻击主要指攻击者通过拦截关键的几条通信信息从而达到通信双方存储信息不同步, 影响后续通信的目的。

本文设计的拥有者转换方案充分考虑到了这种攻击的可能性并能有效抵御这种攻击。在整个拥有者转换方案实现过程中, 最有可能遭受攻击的步骤有步骤 4、步骤 10 和步骤 11。若步骤 4 被拦截后, OO 无法收到来自于 CO 的确认信息, 即 OO 并不知道自己所发送的 $E_{N_1}(TID_{WD}, B_{WD})$ 是否被 CO 收到。若 CO 未收到该信息, 则后续的 CO 和 WD 就无法进行有效的相互认证。在本方案设计中, 采用在 OO 端设置一个定时器, 若在指定时间内未收到来自于 CO 的信息, 则重新发送 $E_{N_1}(TID_{WD}, B_{WD})$ 。若步骤 10 被拦截后, 可能出现 WD 认为 S_2 是将来与 CO 进行通信的会话密钥, 而 CO 由于未收到 WD 返回的信息, 因此其直接丢弃了 S_2 , 这就造成以后 CO 和 WD 之间无法通信的情况, 本方案可有效避免这种情况。因为当 CO 在一定周期内没有收到 WD 的回复时, 会重新发送步骤 9 的信息, 而 WD 在未收到来自于 CO 的确认信息时, 不会将存储的 S_2 看作以后与 CO 通信的会话密钥。若步骤 11 被拦截后, 可能出现 WD 认为 CO 并未受到自己发送的步骤 10 的信息, 从而丢弃 S_2 , 而此时 CO 已经将会话密钥改为了 S_2 , 从而使 CO 和 WD 之间不同步。为了解决这个问题, 在 WD 上设置了一套重传机制, 在规定时间内若 WD 未收到来自于 CO 的步骤 11 的信息, 则会重新发送步骤 10 的信息给 CO。

3) 重放攻击

重放攻击主要指攻击者拦截通信双方以前通信的内容, 并将相同的内容发送给通信其中一方以达到冒充另一方角色的目的。该攻击通常出现在通信双方相互认证身份的过程中。

本文设计的拥有者转换方案能有效抵御这种攻击。实际上, 在本方案中攻击者更加愿意仿造 CO 从而获得可穿戴设备的使用权, 而不是仿造可穿戴设备。而其目的无法实现, 主要存在以下几个原因: 首先, 在初始化阶段用户在 CO 和 OO 上手动输入一个临时密钥 N_1 , 该密钥只在本次拥

有者转换过程中有效,而在下一次拥有者转换过程中失效。在这种情况下攻击者重放拦截的信息将变得没有意义,因为此时 N_1 已经发生改变。在相互认证阶段重放攻击也没有作用。因为本方案采用蓝牙地址和散列值的双重认证方式,而攻击者在初始化阶段中并不能解密出 CO 的蓝牙地址,因此也无法冒充 CO 进行相互认证。当然,即使攻击者通过其他渠道获知 CO 的蓝牙地址并冒充 CO 发送信息给 WD 也没用。因为其并不知道 WD 在本次拥有者转换过程中生成的临时 $IDTID_{WD}$,也就无法发送能通过 WD 验证的有效信息。在密钥更新阶段中,攻击者没有机会进行重放攻击,因为其没有机会与其中的设备建立连接。因此本方案可有效抵御重放攻击。

4.2 针对特殊攻击

1) 前向攻击

前向攻击主要指 CO 有机会破解 OO 和 WD 通信的信息。例如,在 OO 和 WD 进行通信时,CO 可以拦截部分通信信息先保存起来,等其拿到 WD 的所有权后再通过一些方法将这些信息进行解密并获得之前 OO 和 WD 之间的通信内容。

本方案能有效抵御这种攻击。因为在可穿戴设备的拥有者转换过程开始前,WD 和 OO 之间使用会话密钥 S_1 进行通信,而 CO 并不知道这个密钥。在本方案实现的过程中,CO 没有机会知道 S_1 。因此,即便 CO 拦截并记录了 OO 和 WD 之间通信的信息,也无法解密。

2) 后向攻击

后向攻击主要指在可穿戴设备进行拥有者转换后,OO 想要破解 CO 和 WD 之间的通信信息并获得通信内容。

本方案能有效抵御这种攻击。在密钥更新阶段,CO 和 WD 之间通过用户临时输入的共享密钥 N_2 进行通信加密。而 OO 并不知晓该密钥。密钥更新阶段完成后,WD 将丢弃之前与 OO 进行通信的会话密钥 S_1 ,而使用 S_2 作为唯一的会话密钥。此时,OO 无法破解信息并得到 S_2 ,也就无法威胁 CO 和 WD 之间的通信安全。

3) 抵赖攻击

抵赖攻击主要指在可穿戴设备拥有者转换过程完成后,新用户 CO 进行抵赖,拒不承认其获得了可穿戴设备的所有权。

这种攻击将无法生效,因为当前大多数可穿

戴设备采用 Android 操作系统。该操作系统类似于智能手机上的 Android,目前只支持单用户登录,即可穿戴设备同时只能与一台智能手机进行通信。在拥有者转换方案执行完成后,WD 已经将存储的会话密钥由 S_1 改变为 S_2 。此时,只有 CO 能够与其通信,OO 无法再与其进行通信。因此,CO 将无法抵赖其已经获得了 WD 的所有权。

4) 信号干扰

可穿戴设备的拥有者转换场景通常发生在公共环境中,因此容易遭受来自外界的干扰,主要包括蓝牙信号干扰和可视攻击。

蓝牙信号干扰指设备在开启蓝牙搜索时容易搜索到附近所有的蓝牙设备。由于各个设备的名称随意性很强,很难找到想要进行通信的设备。本方案能有效抵抗蓝牙信号干扰。在初始化阶段,OO 和 WD 开启蓝牙功能后,设备自动进行匹配连接。而 OO 和 CO 通过输入相同的 PIN 码进行连接;在相互认证阶段,CO 存储了 WD 的蓝牙地址,因此可以在开启蓝牙功能后根据对方蓝牙地址直接发送连接请求,而无需搜索附近所有设备再进行筛选。WD 本地存储了 CO 的蓝牙地址,当其收到连接请求后直接判断对方地址,进而拒绝来自于公共环境下其他设备的蓝牙请求,只接受对应蓝牙地址设备的请求。因此,本方案通过使用蓝牙地址,既实现了认证的目的,又帮助设备抵抗公共环境下的蓝牙信号干扰,从而有效提高整套拥有者转换方案的执行效率。

可视攻击主要指在公共环境下恶意第三方用户可能通过视频监控等方式偷窥到用户在设备上输入的密码信息。本方案能有效抵抗这种攻击。因为在整个拥有者转换方案实现过程中,用户主要输入两个参数 N_1 和 N_2 。其中, N_1 主要用来在初始化阶段辅助 OO 将 WD 的设备信息发送给 CO,此后该参数变得毫无意义。 N_2 主要用来在辅助 CO 和 WD 进行密钥协商并确定新的会话密钥 S_2 。在该阶段结束后, N_2 也变得毫无意义。因此,即使恶意攻击者监控到了 N_1 和 N_2 ,在拥有者转换过程完成后也将变得毫无意义。

5 实验分析

5.1 实验目标

可穿戴设备是一个实际存在的设备,拥有者

转换场景是实际存在的场景，在这两个前提下，提出的所有者转换方案需要进行实现。在实验过程中将达到以下几个目标。

- 1) 通过代码将本方案进行实现，表明本文提出的所有者转换方案具备可行性。
- 2) 通过采用不同的对称加密算法实现本方案，统计方案执行时间并评估各种对称加密算法的执行效率及对方案执行时间的影响。
- 3) 通过采用不同的散列算法实现本方案，统计方案执行时间并评估各种散列算法的执行效率及对方案执行时间的影响。
- 4) 通过测量整个所有者转换方案的执行时间表明本方案执行效率较高。

5.2 实验环境

本方案的实验环境包括两个部分：应用开发环境和实验设备。

1) 应用开发环境

目前来说，市面上主流的可穿戴设备均采用 Android 操作系统，如 Samsung Galaxy Gear、Google glass 等。为了满足主流设备的使用，需要将提出的所有者转换方案在 Android 环境下进行实现。因此，采用 Java 编程语言在 Eclipse 开发环境中对本方案进行了实现，并生成了适用于 Android 设备安装的 APK。

2) 实验设备

由于条件限制，采用 3 台智能手机进行本方案的实现，而没有使用真实的可穿戴设备。其中，性能较弱的智能手机模拟可穿戴设备的角色。

实现本方案使用的智能手机及性能如表 1 所示。

在多次试验中，各设备扮演的角色是相同的，如 Samsung I9000 总是扮演旧拥有者的角色，Google Nexus 总是扮演新拥有者的角色，而 Samsung S6852 总是扮演可穿戴设备的角色。

5.3 实验过程

为了达到本实验的 4 个目标，总共做了 9 组实验，各组实验所用的对称算法和散列算法

如表 2 所示。

表 2 各组实验使用算法对照

实验组数	对称加密算法	散列算法
1	DES	MD4
2	DES	MD5
3	DES	SHA1
4	3DES	MD4
5	3DES	MD5
6	3DES	SHA1
7	AES	MD4
8	AES	MD5
9	AES	SHA1

在这 9 组实验中，将 3 种对称算法和 3 种散列算法进行随机搭配，并统计出各种组合情况下的方案的执行时间。这样便于后续分析加密算法和散列算法的选择对于方案执行时间的影响。

5.4 实验结论

在这 9 组实验中，统计了各步骤的执行时间，并对比了 9 组实验执行的总时间。

如图 4 所示，这是第 6 组实验各步骤的执行时间，其中 x 轴代表具体步骤编号，与方案 3 个阶段的各步骤相对应， y 轴代表具体执行时间，单位是毫秒。

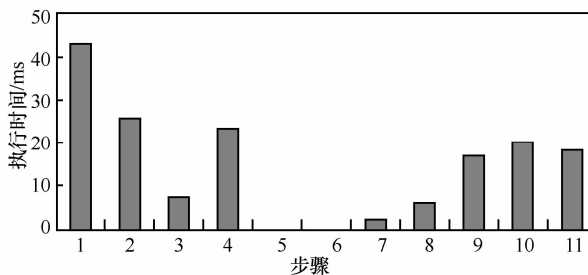


图 4 第 6 组实验各步骤执行时间

通过比较 9 组实验结果可以得到以下结论。

结论 1 对称加密算法的选择对方案执行时间影响较大。

表 1 实验使用智能手机介绍

角色	品牌及型号	主要性能	Android 版本
旧拥有者 (OO)	Samsung I9000	单核 1 GHz, 512 MB 内存	2.3.7
新拥有者 (CO)	Samsung N7102	四核 1.638 MHz, 2 GB 内存	4.1.1
可穿戴设备 (WD)	HTC T328w	单核 1 GHz, 512 MB 内存	4.0.4

从图5中不难发现包含对称加解密算法步骤的执行时间明显大于不包含对称加解密算法的步骤。例如,在初始化阶段中,各步骤均包含对称加密或解密,而这些步骤的执行时间明显较长。步骤7和步骤8仅包含散列运算,因此执行时间较短。

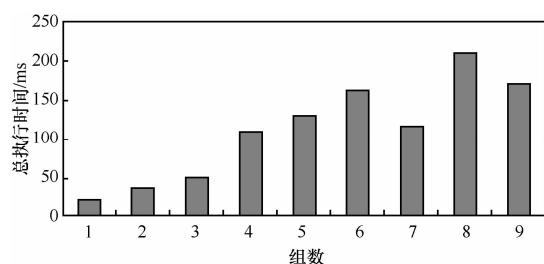


图5 9组实验总时间对比

通过9组实验图的比较,可以发现:总体上来说DES效率>3DES效率>AES效率。

结论2 散列算法的选择对方案执行时间影响较小。

在整套方案中,只有步骤7、步骤8和步骤10涉及到了散列计算。而这3个步骤在方案执行总时间中所占比例不大。另外,通过对以上9组实验的数据分析,发现在选择同样对称算法的前提下,这3个步骤的执行时间差距并不大,因此可以认为,散列算法的选择对本方案的执行总时间影响较小。

结论3 蓝牙通信时间消耗可忽略。

在整套方案中,步骤5是CO搜索并与WD建立蓝牙连接的过程,步骤6是WD通过蓝牙信道发送成功信息的过程,而通过以上9组实验数据发现这两个过程实现时间基本为0ms。注意,为了减少蓝牙搜索时间对方案的影响,在步骤5中通过代码关闭了蓝牙搜索附近设备的过程。因为,当前蓝牙默认搜索附近设备时间是12s,这对方案执行时间有巨大影响。因此,可以确认蓝牙信道传输数据的时间是可以忽略的。

结论4 方案执行总时间范围是2.023s到2.209s。

实际上,整个拥有者转换方案执行时间由3个部分构成:系统运行算法所需的时间、用户手动输入密钥所需的时间以及蓝牙通信所需的时间。其中,用户手动输入密钥所需的时间是不固定的,只能根据用户习惯默认为2s。而根据结论3分析,蓝牙通信时间可以忽略。系统运行算法所需的时间如图5所示,范围是23ms到209ms。

因此,实际上整套方案执行时间应该是实验测量的总执行时间加上用户习惯的2s,即实际执行时间范围是2.023s到2.209s。

5.5 实验影响因素

以上实验结果表明即使在使用同样设备进行多次测试的情况下,实验误差也比较大。这主要来源于Android后台进程的影响。

众所周知,Android系统中后台进程占用大量的CPU资源。在这种情况下,若用户开启一个已有后台进程的程序则会相当快捷。若开启一个新程序则会出现系统反应速度较慢的情况。本方案进行9组实验的方法是修改源代码生成9个不同的APK,并逐一进行测试。这种实验方法导致每次智能手机打开应用都需要较长的时间。另外,在不同时间点手机上运行的后台进程数量和CPU占有量不一样,因此,对实验结果的总执行时间产生了较大影响。

6 结束语

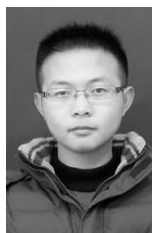
可穿戴设备正在迅速融入人们的生活中,在带来便利的同时也带来了一系列安全问题。然而,此前并未有学者考虑过可穿戴设备拥有者转换场景。为了解决可穿戴设备拥有者转换场景下可能遇到信道安全问题,设计了一个拥有者转换方案。安全分析表明本方案可抵御传统的信道攻击和拥有者转换场景下的特殊攻击。实验分析表明本方案具有较高的执行效率与实际应用的可行性。

参考文献:

- [1] MCCRINDLE R J, WILLIAMS V M, VICTOR C R, et al. Wearable device to assist independent living[J]. International Journal on Disability and Human Development, 2011, 10(4): 349-354.
- [2] BIANCHI V, GROSSI F, DEMUNARI I, et al. MuSA: a multisensor wearable device for AAL[C]//2011 Federated Conference on Computer Science and Information Systems. 2011: 375-380.
- [3] WAHBAH M, ALHAWARI M, MOHAMMAD B, et al. Characterization of human body-based thermal and vibration energy harvesting for wearable devices[J]. IEEE Journal on Emerging & Selected Topics in Circuits & Systems, 2014, 4(3): 354-363.
- [4] DE S T M, SANTOS H M D, DE M A. et al. Wearable authentication device with biometrical intrusion prevention system[J]. User. Iformatik.uni, 2006, 31(10): 2660-2664.
- [5] LYER M S, MONDAL P, KIRAN V V S, et al. Wearable device for

- health care applications[C]//2013 Texas Instruments India Educators' Conference. 2013: 91-96.
- [6] WANG Z, HUANG Z. Wearable health status monitoring device for electricity workers using ZigBee-based wireless sensor network[C]//2014 7th International Conference on IEEE Biomedical Engineering and Informatics (BMEI). 2014: 602-606.
- [7] ZHENG Y, DING X, POON C, et al. Unobtrusive sensing and wearable devices for health informatics[J]. IEEE Transactions on Biomedical Engineering, 2014, 6(15): 1538-1554.
- [8] MATSUBARA M, OBA T, KADONE H, et al. Wearable auditory biofeedback device for blind and sighted individuals[J]. IEEE Multimedia, 2015(1): 68-73.
- [9] GORMAN B M. VisAural: a wearable sound-localisation device for people with impaired hearing[C]//Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility. 2014: 337-338.
- [10] FONTANA J M, MUHAMMAD F, EDWARD S. Automatic ingestion monitor: a novel wearable device for monitoring of ingestive behavior[J]. IEEE Transactions on Biomedical Engineering, 2014, 61(6): 1.
- [11] GRUEBLER A, SUZUKI K. Design of a wearable device for reading positive expressions from facial EMG signals[J]. IEEE Transactions on Affective Computing, 2014, 5(3): 227-237.
- [12] LYONS K, PROFITA H. The multiple dispositions of on-body and wearable devices[J]. Pervasive Computing IEEE, 2014, 13(4): 24-31.
- [13] OJALA S, KEINANEN J, SKYTÄ J. Wearable authentication device for transparent login in nomadic applications environment[C]//The 2nd International Conference on Signals, Circuits and Systems. 2008: 1-6.
- [14] PERIASWAMY S C G, THOMPSON D R, DI J. Ownership transfer of RFID tags based on electronic fingerprint[C]//Proceedings of the 2008 International Conference on Security & Management, Las Vegas, Nevada. 2008: 14-17.
- [15] SAITO J, IMAMOTO K, SAKURAI K. Reassignment scheme of an RFID tag's key for owner transfer[J]. Lecture Notes in Computer Science, 2005, 3823: 1303-1312.
- [16] KULSENG L, YU Z, WEI Y, et al. Lightweight mutual authentication and ownership transfer for RFID systems[C]//Proceedings of 2010 International Conference on Computer Communications. 2010: 1-5.
- [17] OSAKA K, TAKAGI T, YAMAZAKI K, et al. An efficient and secure RFID security method with ownership transfer[C]//2006 International Conference on Computational Intelligence and Security. 2006: 1090-1095.
- [18] SONG B. RFID tag ownership transfer[C]//Proceedings of Workshop on RFID Security, Budapest. 2008.
- [19] KAPOOR G, PIRAMUTHU S. Single RFID tag ownership transfer protocols[J]. IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews, 2012, 42(2): 164-173.
- [20] MUNILLA J, PEINADO A, YANG G, et al. Enhanced ownership transfer protocol for RFID in an extended communication model[EB/OL]. <http://eprint.iacr.org/2013/187.pdf>
- [21] CHEN C L, CHIEN C F. An ownership transfer scheme using mobile RFIDs[J]. Wireless Personal Communications, 2013, 68(3): 1093-1119.

作者简介:



胡舜（1990-），男，湖南娄底人，暨南大学信息科学技术学院硕士生，主要研究方向为移动信息安全。



翁健（1976-），男，广东茂名，暨南大学信息科学技术学院教授、博士生导师，主要研究方向为密码学与信息安全。



刘家男（1992-），男，河南周口人，暨南大学信息科学技术学院硕士生，主要研究方向为密码学、加密数据搜索。

收录声明

本刊对发表的文章,拥有出版电子版、网络版版权,并拥有和其他网站交换信息的权利。本刊支付的稿酬中已经包含上述费用。

Chinese Journal of Network and Information Security has the copyright to publish electronic edition, online edition of the published articles, and has the right to exchange information with other sites. The expenses have been included in the fee paid by editorial department.

道德声明

本刊发表的论文是作者独立取得的原创性研究成果,无一稿多投;论文内容不涉及国家机密;未曾以任何形式用任何文种在国内外公开发表过;论文内容不侵犯他人著作权和其他权利。若发生一稿多投、侵权、泄密等问题,论文作者将承担全部责任。

The authors of *Chinese Journal of Network and Information Security* guarantee that their submitted article is original and contains nothing confidential. The said article is only submitted to *Chinese Journal of Network and Information Security*. The said article has not been published before and has not been submitted elsewhere for print or electronic publication consideration. The said article is no way whatever a violation or an infringement of any existing copyright or license from the third party. Otherwise, the authors of the said article shall take the blame for the violation or infringement of the related copyright and the leakage of secrets.

读者信箱:

cjnis@bjxintong.com.cn

官方微信:



网络 Chinese Journal of
Network and Information Security
信息安全学报

2015 年 12 月 15 日出版

定价：30.00 元

ISSN 2096-109X

