

基于标识符的 Android 客户端身份认证方案

王亚伟^{1,2,3}, 彭长根^{1,2,3}, 丁红发^{2,3,4}, 周凯^{1,2,3}

(1. 贵州大学计算机科学与技术学院, 贵州 贵阳 550025;

2. 贵州大学贵州省公共大数据重点实验室, 贵州 贵阳 550025;

3. 贵州大学密码学与数据安全研究所, 贵州 贵阳 550025;

4. 贵州大学数学与统计学院, 贵州 贵阳 550025)

摘要: 利用 Android 移动终端软硬件自有的标识符信息, 依靠 Android 系统这一可信第三方, 确保标识符信息的真实可信, 结合密码学中 Hash 函数以及异或、连接等运算构造出客户端应用的身份认证信息生成算法。通过对传统移动应用的账户注册和登录过程进行研究, 将身份信息的生成和验证过程放在服务器端, 使用户免去设置账户信息及口令这一繁琐且极易暴露隐私的过程, 完成一种新型的身份认证方案。最后, 对方案的安全性和效率进行了分析, 结果表明, 新的方案具有较强的安全性和较高的便捷性。

关键词: 标识符; Android 客户端; 认证模型; 身份认证信息生成算法

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00140

Identity authentication scheme of Android client based on identifiers

WANG Ya-wei^{1,2,3}, PENG Chang-gen^{1,2,3}, DING Hong-fa^{2,3,4}, ZHOU Kai^{1,2,3}

(1. College of Computer Science & Technology, Guizhou University, Guiyang 550025, China;

2. Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China;

3. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China;

4. College of Mathematics and Statistics, Guizhou University, Guiyang 550025, China)

Abstract: The Android mobile terminal's own identifier information was used, which was credibly ensured by the Android system, then combining the Hash function and operation such as xor or connection, an algorithm of authentication information generation for the Android client was created. The traditional mobile client's process of register and login were analyzed, putting the identity information generation and authentication on the sever. A novel authentication scheme was constructed, which made the users free from the cumbersome authentication process and privacy divulges. Finally, the security and efficiency of the scheme were analyzed. The results show that the new scheme has strong security and high convenience.

Key words: identifier, Android client, authentication model, algorithm of authentication information generation

收稿日期: 2016-09-24; 修回日期: 2016-12-29. 通信作者: 彭长根, peng_stud@163.com

基金项目: 国家自然科学基金资助项目 (No.61662009, No.61262073, No.61363068); 国家统计局全国统计科学研究重点基金资助项目 (No.2013LZ46); 贵州省统计科研基金资助项目 (No.201511); 贵州省哲学社会科学规划青年课题基金资助项目 (No.16GZQN06)

Foundation Items: The National Natural Science Foundation of China (No.61662009, No.61262073, No.61363068), The Key Project of National Statistical Scientific Research Project (No.2013LZ46), The Statistical Research Project of Guizhou Province (No.201511), The Youth Philosophy Social Sciences Planning Project of Guizhou Province (No.16GZQN06)

1 引言

随着移动互联网技术的飞速发展和广泛普及,移动端的电子商务、社交、娱乐和信息分享类服务在人们的生活中变得越来越重要^[1,2],并有赶超 Web 网站服务的趋势。然而,对于这些移动应用服务,用户账户注册和认证都是这些应用客户端必不可少的部分。因为只有通过用户账户的注册和认证,使用户拥有唯一的身份标识,服务提供者才可以记录用户的身份信息和使用数据,才能使用户随时随地,使用不同的方式查询、修改用户的个人数据或消费、享受服务^[3]。

目前,绝大多数用户账户的认证方式还是传统的用户名加账户口令的验证方式^[4,5],这种认证方式对服务提供商来说简单快捷、成熟稳定,但对用户来说不仅繁琐且存在大量的安全隐患。首先,由于用户账户名和密码是用户登录的唯一凭证,所以用户密码一旦泄露,将会对用户的隐私信息和财产安全造成巨大损失。虽然现今大多数大型互联网公司在用户设置密码时对密码的复杂程度都做出了限制,但由于各类应用和网站都需要注册账户,用户为了记忆方便,经常会将不同的账户设置成相同的密码。这样,攻击者通过社会工程学^[6]策略进行攻击,如“撞库”攻击^[7],使用户账户的安全性和个人信息的隐私受到极大威胁。其次,现今移动客户端服务商为了用户的方便,大多在用户第一次登录后默认下次自动登录,通过生成一个类似证书的信息“Token”作为用户以后认证的凭证^[8],如果用户的 Token 被攻击者盗取,则用户的身份就可以被攻击者随意使用,用户的账户财产和隐私信息会受到损害^[9]。再次,现今的互联网产品用户注册,用户需要填写用户名(经常会有用户名是否重复的验证)、密码(2次验证)、手机号等信息,这些繁琐的过程不仅影响用户的体验且经常会泄露用户的私人信息。最后,在账户注册过程中有些服务提供者为了用户的方便,提供手机号注册,授权 QQ、微信、微博等第三方社交账户注册等方式,这也导致了大量用户隐私信息被泄露^[10-12]。

文献[13]以 Android 系统为可信第三方实现了对 Android 软件身份信息的强制验证,解决了

Android 系统第三方登录中的漏洞问题,文献[14]提出了一种匿名认证密钥交换方案,这种方案可以抵抗多种攻击且计算开销更低,文献[15]通过使用 Android 设备和软件的一些标识符对 Android 智能终端进行识别。针对以上问题,本文提出了一种新的针对 Android 移动客户端的用户身份认证方案——通过组合移动终端特有的一些标识信息(如 IMEI 码、IMSI 码、设备型号),为移动终端生成一个身份信息,作为用户的账户身份认证标识,在服务器进行身份认证时,通过 Android 系统这一可信第三方获取这些标识符信息,保证信息的真实性和可信性,以此对客户端用户的身份进行认证。用户的注册和登录账户这一操作大大简化,且解决了上文提出的“撞库攻击”问题。

2 基础知识

2.1 撞库攻击

撞库攻击是指攻击者通过不断收集用户泄露的账户信息,构建一个对应的账户和口令数据表,然后用这些数据信息尝试常见的互联网网站或移动应用(如 QQ 账号、电子邮箱、微博)账户,从而得到用户其他账户的账号信息,窃取用户的隐私信息或侵害用户的个人财产。撞库攻击依赖于拖库,拖库是指攻击者利用欺诈、钓鱼等社工手段或漏洞、病毒等技术手段获取用户在一些小型网站或应用(因为这些网站的安全性或安全机制不够完善容易被攻击)中获取用户信息。对攻击者来说,拖库成功后撞库攻击就易如反掌。

2.2 标识符

本文所提到的标识符,主要是指 Android 移动终端的一些软硬件信息,这些信息有些是可以作为唯一标识的,如 IMEI 码^{注1}、IMSI 码^{注2}等。有些可以将 Android 终端作为简单的属性区分但并不唯一,如 Android 系统版本、手机型号等。将这些信息进行组合,即可作为某一客户端软件

注1: 国际移动装备标识码(IMEI, international mobile equipment identity)是由 15 bit 数字组成的“电子串号”,它与每台移动电话机一一对应,而且该码是全世界唯一的。

注2: 国际移动用户识别码(IMSI, international mobile subscriber identification number)是区别移动用户的标志,存储在 SIM 卡中,可用于区别移动用户的有效信息。

的身份信息,表1为一些标识符信息的介绍。

表1 标识符信息介绍

标识符名称	获取方式(以Java代码形式获取)	标识符内容
IMEI 码	getSystemService (TELEPHONY_SERVICE). getDeviceId()	18 bit 数字
IMSI 码	getSystemService (TELEPHONY_SERVICE). getSubscriber()	15 bit 数字
手机型号	android.os.Build.MODEL	字符串
系统版本号	android.os.Build.VERSION	字符串

2.3 Hash 函数

Hash 函数是把任意长度的输入,通过相应的散列算法,转换为固定长度的输出,输出的结果就是散列值。由此可知,Hash 函数是一种将任意长的消息压缩成特定长度的消息摘要的函数。由于散列算法的过程是不可逆的,所以 Hash 函数是单向的,除此之外,Hash 函数还有抗冲突性和分布均匀性等特点。

本文提到的加盐 Hash 函数是指在对消息去消息摘要前,消息要按照某种规则加入随机数或时间戳等内容,这样就解决了由于摘要值一成不变而容易受攻击的问题。

3 基于 Android 系统的身份信息生成算法

身份信息算法的安全性依赖于标识符信息的安全与可信,如果不能保证标识符信息的真实可信,身份信息的生成则无意义。基于 Android 系统这一可信第三方,应用在获取标识符时必须通过系统调用获取,如表1所示的系统调用代码,由于恶意应用无法绕过系统调用来获取这些信息,这样就充分保证了标识符信息的安全性。

在保证标识符的安全性后,身份信息算法的安全性也就得到了极大的保证。用户身份信息的生成算法主要有2个部分构成:一是作为数据的标识符信息,二是作为运算符或者函数的运算符和函数符号信息。数据包括2个部分,可以作为唯一标识的标识符信息,如IMEI码和IMSI码,剩下的就是不能作为唯一标识的标识符信息,如手机型号或者系统版本号等信息。运算符和函数包括异或和连接运算,以及Hash函数、字符转二

进制函数,下面给出以上信息的定义。

R_n 为可以作为唯一标识的标识符信息, n 值代表不同标识符信息。

W_n 为不能作为唯一标识的标识符信息, n 值代表不同标识符信息。

$\oplus$ 为异或运算。

$\parallel$ 为连接运算。

H 为 Hash 函数,可以对信息进行压缩获取其摘要。

C 为将字符串或数字转换成二进制码的函数。

F 为身份信息生成算法。

T 为时间戳生成算法,Hash 函数的加盐。

方案的详细介绍及举例说明如下。

假设取出4个标识符信息,分别为用户移动终端的IMEI码 User_IMEI、SIM卡唯一标识 User_IMSI、手机型号 User_Model 和手机系统版本 User_Version。定义 User_IMEI 和 User_IMSI 分别为 R_1 和 R_2 ,定义 User_Model 和 User_Version 为 W_1 和 W_2 ,则身份信息生成算法如下。

$$F = H(C(R_1) \oplus C(W_1 \parallel W_1 \parallel T)) \parallel R_2 \quad (1)$$

$$F = C(R_2) \oplus C(W_2 \parallel W_1) \oplus H(C(R_1 \parallel T)) \quad (2)$$

式(1)将2个非唯一的标识符和时间戳通过连接运算合并,然后将其通过函数 C 转换成二进制码,通过和唯一标识符的 R_1 的二进制码进行异或运算,这样既减少了消息的长度又保证了最终得到的摘要值的唯一性,而且由于加入了时间戳,保证了标识符信息的动态变化,大大增强了安全性。这里的时间戳函数 T 还可以换做随机数生成函数,并且“加盐”的动态变化可以根据移动应用的安全需求来进行适当的调整,大大算法增强了灵活性和效率。同理,式(2)用另一种方式保证了消息的长度适当,并且加盐,最终得到的身份认证信息也是唯一且安全的。

式(1)的核心代码如下。

```
public String getIdentifyInfo() {
    TelephonyManager mTelephonyMgr
    = (TelephonyManager)
    this.getSystemService(Context.TELEPHONY_
    SERVICE);
    String imsi = mTelephonyMgr.
```

```

getSubscriberId();
    String imei = mTelephonyMgr.get-
DeviceId();
    String version = android.os.Build.
VERSION.SDK;
    String model = android.os.Build.
MODEL;
    int r1 = Integer.parseInt(imsi);
    int r2 = Integer.parseInt(imei);
    String time = System. currentTi-
meMillis() + "";
    int result = r1 ^ (Integer.parseInt
(version + model + time));
    return bytesToHexString((result+ "").
getBytes()) + r2;
}
public static String bytesToHexString
(byte[] src) {
    StringBuilder stringBuilder = new
StringBuilder("");
    if (src == null || src.length ≤ 0)
    {
        return null;
    }
    for (int i = 0; i < src.length; i++) {
        int v = src[i] & 0xFF;
        String hv = Integer. toHex-
String(v);
        if (hv.length() < 2) {
            stringBuilder.append(0);
        }
        stringBuilder.append(hv);
    }
    return stringBuilder.toString();
}

```

算法主要运用 Hash 函数、异或和连接等运算, 极大地提高运算效率, 且有效地缩短了身份信息长度, 减小服务器的存储压力和计算消耗。算法设计原则为将唯一标识符和非唯一标识符进行混淆, 再加入一个变量时间戳经过 Hash 函数的压缩, 然后再对唯一标识符或其摘要进行连接运

算, 由于加入了时间戳, 可以抗重放攻击, 并且可以定期对用户身份信息进行更新, 充分保证了用户账户的唯一性和安全性, 如式(1)和式(2)所示。另外, 算法的自定义空间也很大, 应用开发者可以通过不同的标识符信息取摘要的加盐操作, 也可以自定义构造不同的生成算法。

4 传统用户注册、登录方案及其弊端

4.1 传统的用户注册、登录方案

用户通过输入不重复用户名或邮箱、手机号码等信息作为用户账户, 并需要输入 2 次密码以保证用户密码的正确性, 通常用户在提交信息后还需要通过邮箱验证链接或者短信验证码来确认用户的注册合法性。在此过程中如果用户不使用邮箱或手机号码作为用户的账户名(由于大多数应用开发者将用户名作为用户身份数据表的主键), 则用户需要繁琐地寻找用户名, 直到找到一个与数据库不重复的用户名, 通常用户再次登录难以记起设置的用户名。如果用户使用邮箱或手机号码进行注册, 则难免会导致个人信息的泄露。用户注册的大致流程如图 1 所示。

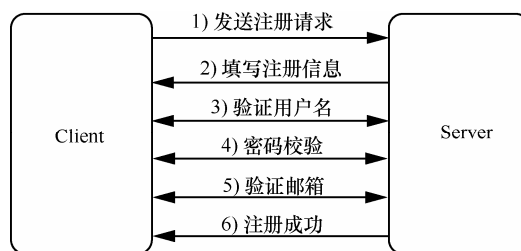


图 1 用户注册流程

用户首次登录需要输入用户名和密码, 客户端将用户名和密码传给服务器, 服务器验证成功后, 用户登录成功, 否则需要重新登录。在以后的登录过程中大多用户会默认选择自动登录, 服务器会在第一次成功登录后生成一个 Token, 并将此 Token 返回给客户端, 以后客户端只需用 Token 请求数据即可, 无需再次使用用户名和密码。

4.2 方案弊端

从图 1 的用户注册流程中可知, 传统的用户注册和登录方案过程较繁琐, 与现阶段移动互联网追求优质用户体验的目标有较大差距。要抵御

前面提到的“拖库攻击”，最好的方法就是每一个账户使用不同的口令，但这样的后果是用户不得不记忆大量的用户名和密码，一些不经常使用的移动应用会使用户陷入每次登录都要找回密码的尴尬境地。但如果用户采取在登录时使用记住密码这一功能，则具有较大的安全隐患。文献[13]指出了移动客户端记住密码这一功能存在的安全隐患，如果攻击者盗用了服务器用于认证用户的 Token 则可以伪造用户的身份，进而使用户的隐私信息和财产安全受到损害。

5 解决方案及分析

针对传统登录认证方案所存在的问题，利用移动终端标识符可以作为唯一身份信息特性，结合密码学中的 Hash 函数和一些基本变换方法将这些标识符组合起来形成用户的强身份识别信息，将这一身份信息作为移动客户端用户的身份。在认证过程中，标识符的信息需要通过 Android 系统的系统调用获取，防止攻击者对标识符信息进行伪造的隐患，保证了用户身份信息的仿伪造性，用户在以后的登录过程中也不需进行账户和密码输入的繁琐过程，更加安全。为了介绍方案的运行过程，本文给出以下基本定义。

C 为用户客户端。

S 为客户端服务器。

DB 为客户端服务器的数据库。

AS 为客户端 C 所依赖的 Android 操作系统。

F 身份信息的生成算法。

5.1 用户注册

新解决方案的用户注册过程对客户端使用者来说较简单，只需要单击注册等待服务器生成并存储用户身份信息，然后验证用于管理自身账户的邮箱即可。注册过程中较复杂的生成并存储用户身份部分由客户端服务器完成，服务器需要获取标识符信息，并将通过标识符信息生成用户身份信息存储至服务器数据库。

用户注册模型如图 2 所示，具体步骤如下。

1) 用户打开 Android 客户端，进入注册页面，单击注册按钮对客户端服务器发起新账户注册的请求。

2) 服务器收到请求后，要求客户端将用户移

动终端的 IMEI、IMSI、设备型号和系统内核等标识符信息传输至服务器端。

3) 客户端收到请求以后，通过 Android 系统的系统调用获取用户移动终端的相关标识符信息。

4) 客户端将这些信息通过与后台服务器的安全信道传输给后台服务器。

5) 后台服务器将这些信息运用软件开发者所定义的，包含加盐 Hash、连接和异或的算法生成用户的身份认证信息。

6) 服务器将生成的身份信息存储至后台服务器。

7) 服务器端通过客户端要求用户填写验证邮箱，后台服务器对发送给用户邮箱的验证码验证成功以后，提示用户账户注册成功。

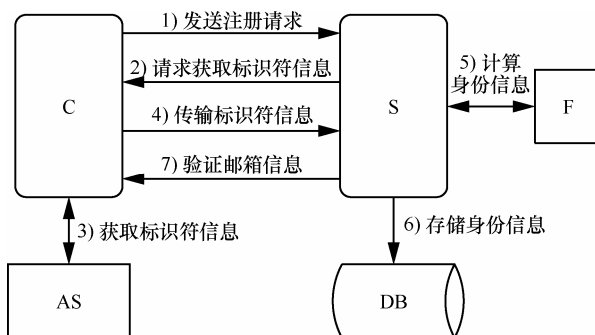


图2 用户注册模型

5.2 用户登录和验证

新用户的登录和验证方案要比传统的登录方案更加高效、安全。由前面注册的过程可知，移动应用的服务器端已经存储了用户的身份认证信息，用户登录时需要重新获取用户移动终端的 IMEI、IMSI、设备型号和系统内核等标识符信息，经过自定义算法的处理后对身份信息进行验证。

用户登录和验证模型如图 3 所示，具体步骤如下。

1) 用户打开客户端，单击登录按钮向服务器端发起登录和身份验证请求。

2) 服务器收到请求后，要求客户端传输移动终端的标识符信息。

3) 客户端通过 Android 系统的系统调用获取标识符信息。

4) 客户端将信息传输至服务器端。

5) 服务器端将接收到的标识符信息通过约

定好的自定义算法得出最终的身份信息。

6) 服务器将此身份信息在数据库进行匹配。

7) 将匹配结果返回给客户端, 客户端收到登录请求的结果。

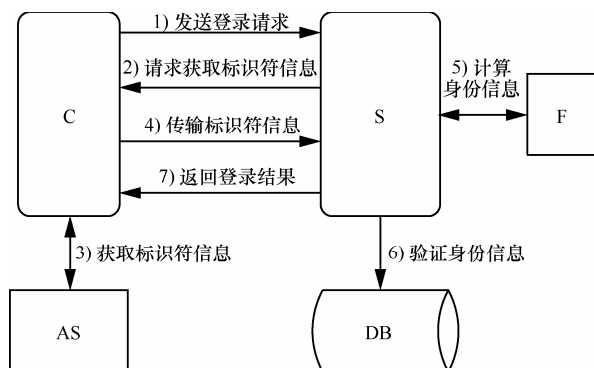


图3 用户登录和验证模型

5.3 用户账户管理

在用户注册时, 要求用户进行邮箱验证。这一做法主要用于解决用户更换设备、设备丢失或多设备登录等问题。若用户设备丢失, 用户可以立即通过邮箱冻结原有账户, 当然, 在此过程前需要用户对原有账户的所有权进行验证。验证成功后, 用户可以重新使用新的设备进行注册, 注册成功后原有账户则失去效用。

如果用户需要在不同的设备进行登录, 则可以进行二次注册, 通过邮箱认证原有账户的所有权, 然后在新的设备上注册, 最终2个不同身份信息的设备在数据库中对应的是同一用户账户。

5.4 方案分析

本文的新方案与传统的登录方案相比有以下优点。

1) 便捷的注册和登录。新方案实现了用户的无密码账户生成, 即用户在使用一个新的移动应用后不需要进行以前繁琐的账户注册, 且账户验证不需要设置用户名和口令, 也不需要暴露各种用户隐私信息, 大多数工作将由服务器端完成。用户只需要通过一个邮箱验证, 极大地改善了用户体验。

2) 安全性和效率提高。根据文献[13]所述, 标识符由 Android 系统这一可信第三方的系统调用获取, 防止了标识符信息被攻击者伪造的风险。攻击者如果不能伪造使服务器信任的标识符信

息, 则无法通过身份认证。身份信息由标识符信息通过包含加盐 Hash、连接和异或运算的算法处理得出, 且处理过程在服务器端, 身份信息的生成和认证效率较高, 并可抵抗重放攻击。由于方案不需要密码、账户以及其他用户隐私信息, 用户信息是和设备直接联系的, 攻击无法对用户进行拖库撞库, 所以方案可以抗撞库攻击。

3) 自定义性高。本文方案的关键在于自定义算法的设计, 由于从 Android 系统获取的移动终端的标识符信息种类繁多, 根据以上给出的算法设计原则, 软件开发者的设计灵活性较强, 很容易就可构造出具有强身份识别特性且高安全的身份信息生成算法。

6 结束语

本文提出了一种新型的基于 Android 移动终端标识符的客户端登录认证方案, 方案通过 Android 系统调用可信的移动终端标识符信息, 通过可以自定义的身份信息生成算法, 在服务器端完成用户身份信息的生成和验证, 使用户在使用移动应用的登录注册功能时获得更好的用户体验, 且具有更好的安全性。

在大数据的今天, 免去用户账户和密码设置, 极大地保护了用户的隐私, 且可以抵抗撞库攻击。下一步, 将针对不同安全级别的应用场景和用户安全性需求进行分析, 对方案认证过程的效率问题进行深入的分析和优化。

参考文献:

- [1] 吴吉义, 李文娟, 黄剑平, 等. 移动互联网研究综述[J]. 中国科学: 信息科学, 2015(1):45-69.
WU J Y, LI W J, HUANG J P, et al. Summary of mobile Internet[J]. Scientia Sinica Informationis, 2015(1):45-69.
- [2] 罗军舟, 吴文甲, 杨明. 移动互联网: 终端、网络与服务[J]. 计算机学报, 2011, 11:2029-2051.
LUO J Z, WU W J, YANG M. Mobile Internet: terminals, networks and services[J]. Chinese Journal of Computer, 2011, 11:2029-2051.
- [3] 刘鑫洋, 王菁, 韩博洋. 面向移动客户端的数据服务推荐策略研究[J]. 小型微型计算机系统, 2015, 8: 1752-1757.
LIU X Y, WANG J, HAN B Y. Data services for mobile clients the strategy[J]. Journal of Chinese Mini-Micro Computer Systems, 2015, 8: 1752-1757.
- [4] 王崇霞, 朱艳琴. 一种动态口令身份认证协议的设计与研究[J]. 计算机工程与应用, 2010, 46(18):71-73.
WANG C X, ZHU Y Q. Design and research of dynamic password

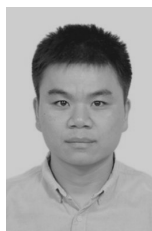
- user authentication protocol[J]. Computer Engineering and Applications, 2010, 46(18):71-73.
- [5] 邓飞, 朱莹. 基于口令的客户端/服务器认证协议[J]. 计算机工程与应用, 2015, 20:72-76.
DENG F, ZHU Y. The client/server authentication protocol based on a password[J]. Computer Engineering and Applications, 2015, 20: 72-76.
- [6] 马明阳. 针对社会工程学攻击的防御技术研究[D]. 北京: 北京邮电大学, 2015.
MA M Y. Research on defense technology against social engineering attacks[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.
- [7] 数据安全再爆重磅炸弹 12306 数据泄露事件确认为撞库攻击[J]. 信息安全与通信保密, 2015, 1:17.
Safety critical blockbuster 12306 data leak identified as collision attack[J]. Journal of Library and Communication Security, Information Security, 2015, 1:17.
- [8] 王鹏, 唐西铭, 王勇, 等. 一种基于手机令牌和 NFC 技术的身份认证系统[J]. 武汉大学学报(理学版), 2013,5:403-410.
WANG J, TANG X M, WANG Y, et al. A mobile phone token-based authentication systems and NFC technology[J]. Journal of Wuhan University (Natural Science Edition), 2013,5:403-410.
- [9] CHOI J, CHO H, YI J. Personal information leaks with automatic login in mobile social network services[J]. Entropy, 2015, 17(6):3947-3962.
- [10] LIU D, COX L P. VeriUI: attested login for mobile devices[C]//The Workshop on Mobile Computing Systems & Applications. 2014:1-6.
- [11] 程瑶, 应凌云, 焦四辈, 等. 移动社交应用的用户隐私泄露问题研究[J]. 计算机学报, 2014,1:87-100.
CHENG Y, YING L Y, JIAO S B, et al. Mobile social application privacy leaks[J]. Chinese Journal of Computer, 2014, 1:87-100.
- [12] 牛犇, 李凤华, 华佳烽, 等. 移动网络中场景关联的隐私保护机制研究[J]. 网络与信息安全学报, 2016, 2(1):31-42.
NIU B, LI F H, HUA J F, et al. Research on scenario-based mechanism in privacy-aware mobile networks[J]. Chinese Journal of Network and Information Security, 2015, 2(1):31-42.
- [13] 董超, 杨超, 马建峰, 等. Android 系统中第三方登录漏洞与解决方案[J]. 计算机学报(自然科学版), 2016,3:582-594.
DONG C, YANG C, MA J F, et al. The vulnerabilities and solutions of third-part login services in Android system[J]. Chinese Journal of Computer (Natural Science Edition), 2016,3:582-594.
- [14] LU Y, LI L, PENG H, et al. Robust anonymous two-factor authenticated key exchange scheme for mobile client-server environment[J]. Security & Communication Networks, 2016, 9(11):

1331-1339.

- [15] 王研昊, 马媛媛, 杨明, 等. 基于隐性标识符的零权限 Android 智能终端识别[J]. 东南大学学报(自然科学版), 2015, 6: 1046-1050.

WANG Y H, MA Y Y, YANG M, et al. Zero permission Android device identification based on implicit identifiers[J]. Journal of Southeast University (Natural Science Edition), 2015, 6:1046-1050.

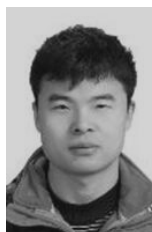
作者简介:



王亚伟 (1990-), 男, 河南洛阳人, 贵州大学硕士生, 主要研究方向为密码学与安全协议。



彭长根 (1963-), 男, 贵州锦屏人, 博士, 贵州大学教授、博士生导师, 主要研究方向为密码学与信息安全、大数据隐私保护。



丁红发 (1988-), 男, 河南南阳人, 贵州大学讲师, 主要研究方向为密码协议、数据安全。



周凯 (1991-), 男, 浙江衢州人, 贵州大学硕士生, 主要研究方向为密码学与可信计算。