计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(2):71−76 [doi: 10.15888/j.cnki.csa.006193]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

Android 手机安全登录系统①

王振辉[1], 王振铎[2]

[1](西安翻译学院 工程技术学院, 西安 710105)
[2](西安思源学院 电子信息工程学院, 西安 710038)

摘　要: 针对 Android 手机应用软件登录中存在的设计缺陷和漏洞, 梳理并分析了目前手机登录系统技术和不足之处, 采用多因子 (账号、密码、验证码、登录位置、登录次数、人脸数据) 方案, 构建手机安全登录系统. 该登录系统由登录、注册、日志审计、微信提醒、找回密码等功能构成. 详细介绍了设计思想、技术路线、安全验证逻辑和日志审计功能, 实现了用户身份识别和登录行为审计, 为用户提供了一个安全性高、易用性强、成本低的解决方案.

关键词: 手机; 登录; 漏洞; 地图定位; 人脸

引用格式: 王振辉,王振铎.Android 手机安全登录系统.计算机系统应用,2018,27(2):71–76. http://www.c-s-a.org.cn/1003-3254/6193.html

Security Login System of Android Mobiles

WANG Zhen-Hui[1], WANG Zhen-Duo[2]

[1](School of Technology and Engineering, Xi'an Fanyi University, Xi'an 710105, China)
[2](School of Electronic and Information Engineering, Xi'an Siyuan University, Xi'an 710038, China)

Abstract: In view of the loopholes and defects in the application softwares of Android mobile phones, this paper analyzes the current solutions of mobile phone login system, using multi factor (account number, password and verification code, login numbers, login location, face recognition) scheme to build secure login system for mobile phones. The login system consists of login, registration, login audit, WeChat alerts, and it introduces the design ideology and technology route. It mainly introduces security verification logic and log audit function, the user identification and login behavior audit, to provide users with a safe, easy-to-use, and low cost solution.

Key words: mobile phone; login; loophole; map location; face

随着移动互联网技术的发展和"互联网+"国家战略的实施, 基于智能手机的电子商务、电子政务蓬勃发展, 手机应用软件逐渐普及. 这些手机客户端软件在给人们工作、生活带来极大便利的同时, 也带来了新的信息安全问题. 由于手机软件设计上存在的缺陷和漏洞及手机上驻留的木马后门程序造成的用户账户等隐私数据外泄, 财产损失等案例逐年增加[1,2].

登录系统作为应用软件的第一道屏障, 其缺陷严重程度和安全级别高低, 直接影响到系统安全评级. 信息系统中业务数据丢失和电子欺诈行为都是由于非法用户绕过了登录校验和利用了系统登录的缺陷[3].

针对上述问题, 国内外专家进行了深入研究, 并取得了不少研究成果. 主要采用的手段有针对用户账号、密码等数据的加密技术, 其次是为防止穷举攻击在账号和密码基础上增加验证码和登录验证次数限制[4–6]. 也有采用软硬件结合方法将用户登录信息存储到 SmartWatch2 设备上, 将用户登录数据和应用软件有效隔离, 同时, 允许用户在 SmartWatch2 上浏览、发送和删除用户登录信息, 从而达到保护手机应用登录信息的目的[7,8]. 此类解决方案采用硬件方式安全性高,

① 基金项目: 西安翻译学院科研团队 (XFU17KYTDB02);西安思源学院 2017 年度校级科研项 (XASY-B1712)
收稿时间: 2017-05-05; 修改时间: 2017-05-19; 采用时间: 2017-05-31

但由于携带不便, 有使用期限, 易丢失, 所有不适合移动环境使用[9]. Twitter 早期使用基于手机短信的验证, 但由于成本相对高, 易被攻击者劫持, 安全隐患大, 进而采用签入认证和批准请求双重认证系统, 但还是需要向用户推送消息, 用户体验不好[10,11]. 更多的研究, 将研究重点放在生物认证方面, 从指纹识别到人脸识别, 意图是解决人脑记忆密码的桎梏, 但由于 3D 打印技术的发展, 使得伪造指纹信息十分容易, 用户隐私更加难以保证. 人类脸部存在相似性和易变性, 识别算法的适应性有待提高, 采用人脸识别又会影响到登录性能, 所有实际应用较少[12−14]. 近期, 普利茅斯大学研究采用图像和数字编码代替依赖于硬件或软件的多因子验证方式或者密码, 此方式便于记忆, 开发成本低, 但操作界面多, 用户体验不好, 且仍存在猜测登录情况.

以上登录方式存在的缺点是不能很好获取操作者个性信息, 来解决操作抵赖性问题, 不便于网络取证. 只有将登录者生物特征信息和操作手机特性信息有效收集, 才能真正避免能发现冒名登录而又无法查证的尴尬局面.

所以, 本文针对目前手机端应用软件登录系统存在的问题和漏洞, 为提高身份认证的安全性, 提出一种基于 Android 手机的安全登录子系统设计框架. 目标是实现用户身份验证及用户登录行为追溯, 防止非法用户冒名登录、篡改数据和电子欺诈等行为的发生. 在新的登录设计框架中采用多因子认证技术, 增加登录者信息和手机个性化信息的记录, 为登录审计和伪客户端程序检测提供依据, 在保证登录性能基础上, 进一步提高手机登录系统的安全性.

1 设计思想

多因子认证是在金融等安全性要求高的应用中经常使用的一种提升安全的方法, 它是在用户名/口令之外额外增加的一种认证措施.

多因子除包含了原有的用户名、密码、验证码外, 还可以增加登录次数、登录时间、手机验证码等信息. 本文为进一步提高安全级别, 又增加了 SIM 卡信息、手机 IMEI、登录位置、人脸特征等限制信息. 通过多因子认证 MFA 和服务器审计分析技术可以大幅度提升用户账户的安全性和管理灵活性.

首先, 通过采集账号、密码、验证码、登录次数等常规信息来匹配数据库中信息. 然后, 使用百度地图 API 和手机 GPS 定位技术来获取手机登录位置, 最后, 实施拍照, 采集登录人脸部信息, 常规信息登录成功后告知用户 (如: 登录名, 登录时间, 本日登录次数, 本月登录次数, 最后一次登录时间等). 地理位置和人脸信息隐式后台获取, 对用户透明, 用于用户登录审计. 由于人脸数据和地图定位在后台实现, 对操作用户而言是透明的, 具其具有强隐蔽性, 且不能删除, 故能避免非法用户有针对性的伪造和破坏.

2 登录系统设计

登录系统设计思想是对用户登录信息进行校验和记录, 以实现对用户操作行为的控制, 达到“事前检测、事中控制和事后审计”的安全目标. 应用 5W1H 分析法分析该系统重点要解决的问题包括: Who: 谁登录了系统, 需要采集个性化信息 (手机号, 人脸数据等). Where: 在哪里登录, 需要采集地理位置数据 (经纬度、省市、标志性建筑等). When: 什么时间进行了登录. What: 登录后做了什么, 采集操作对象数据 (客体信息和操作). Why: 为什么登录, 登录意图分析, 要进行事后分析. How: 登录方法, 是正常登录还是冒名登录、穷举攻击等.

上面是总体分析, 再结合目前登录系统存在的问题和缺陷, 进行问题合并、简化和求优, 设计了登录系统的核心验证功能, 以达到既能记录用户登录信息、手段、还可以明确系统的损失, 分析归纳用户登录意图, 从而有针对性的对数据对象进行保护. 图 1 为安全登录系统用户身份验证模型.

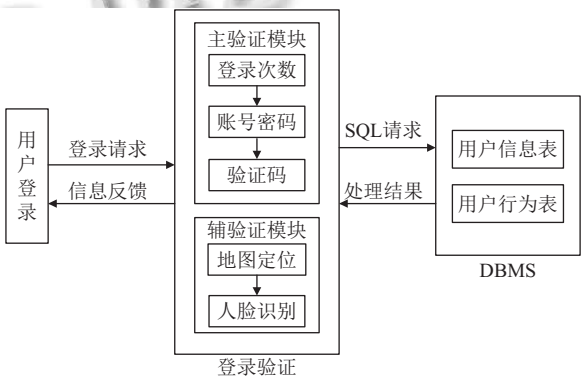

图 1 安全登录系统用户身份验证模型

3 登录系统实现

3.1 注册功能

用户注册功能是用户登录校验的前提. 用户下载企业级 APP 软件, 安装后运行的第一步就是注册, 通

过注册确定用户的信息和权限. 用户注册时, 首先通过用户名 (可以是邮箱或手机号), 来保证唯一性. 其次, 通过字母、数字、大小写、特殊符号等控制密码强度. 最后, 采用效率较高的非对称加密算法 MD5, 实现密码的密文存放. 用户注册信息保存在用户表中, 如表 1 所示.

表 1 用户信息表

序号	列名	类型	长度	主键	说明
1	uid	字符	20	是	用户账号
2	uname	字符	20		姓名
3	email	字符	30		注册邮箱
4	phone	字符	11		验证手机号
5	pwd	字符	20		密码
6	status	字符	10		账号状态
7	right	字符	10		权限

3.2 密码找回

密码忘记时, 用户通过提供个性化数据 (手机号, 身份证号, 邮箱等) 获取原密码或重置密码, 但需经管理员审计. 本文中注册邮箱的作用是用户注册后, 激活账号. 找回密码采用更为安全的手机验证码, 通过手机短信发送给最终用户. 为了保证密码安全, 找回的密码在登录系统后, 必须修改为新密码.

3.3 登录验证功能

登录验证是登录过程的核心, 校验步骤如下:

(1) 用户输入账号、密码、验证码, 点击登录按钮.

(2) 检查验证码和登录次数是否正确, 如不正确提示或退出应用, 正确执行 (3).

(3) 从用户信息表中比对账号, 正确后获取用户密码、权限和状态, 如状态为已登录、停用、未激活状态, 则提示用户. 否则, 执行 (4).

(4) 将用户输入的密码用 AES-RSA 混合算法加密和获取的密码进行比较, 如正确根据用户权限进行业务系统, 同时把该用户的状态更新为已登录.

(5) 获取用户登录时地理信息和头像, 存入登录审计表.

3.4 日志审计

登录日志审计功能的主要作用是通过记录登录者使用的账号、登录时间、地理位置、人脸数据来实现嫌疑人跟踪. 用户登录行为数据保存在操作审计表中, 如表 2 所示.

通过该日志表, 可以浏览和统计某个用户时间段内登录次数、登录位置和登录成功与否等信息, 从而帮助用户自查和管理员审核系统受攻击程度. 拍照和写日志采用异步进程提交, 以保证登录系统的用户体验. 本文操作类型只针对登录行为审计, 用户如有更高安全要求, 也可以扩展操作类型的取值, 如: 登出、付款、转账等操作. 该表数据是非法用户跟踪的有效凭证, 所有一次写入后, 不能做修改和删除操作.

表 2 操作审计表

序号	列名	类型	长度	主键	说明
1	id	数值	10	是	登录序号
2	utype	字符	10		操作类型
3	uid	字符	20		用户账号
4	utime	时间			时间
5	uaddr	字符	50		地理位置
6	phoneid	字符	15		手机IMEI
7	Phonenumber	字符	11		手机号
8	simid	字符	50		SIM卡号
9	photo	二进制			面部图像
10	flag	字符	4		成功标识

3.5 微信提醒

微信基本上成为我国手机用户人手一份的“碎片化”社交软件, 由于受众面广, 不需要运营商支撑, 已逐步取代了短信的作用, 所以可以使用企业短信提醒功能, 提示用户, 告知其登录行为, 已减少业务数据的安全风险.

4 关键技术

4.1 软件防钓鱼

针对恶意应用以伪造目标应用登录界面的方式进行钓鱼攻击的行为[15], 本文使用软件校验码技术来进行预防. 在手机登录 Activity 的 OnCreate 事件中, 除了加载指定的布局文件外, 还连接到后台服务器读取该软件版本所对应的校验码. 后台数据库 MySQL 的软件校验码表中存取了各版本所对应的软件校验码. 表 3 是软件验证码表的数据结构.

表 3 软件校验表

序号	列名	类型	长度	主键	说明
1	id	数值	10	是	编号
2	vid	字符	20		版本号
3	vname	字符	50		软件名
4	vcode	字符	50		验证码
5	note	字符	50		备注

软件验证码由软件发行时间戳和 APK 文件字节数组合而成, 并用非对称加密算法 MD5 加密, 一份存

在数据库表记录中, 另一份存放在 APP 应用配置文件中. 为防止 APK 被反编译, 可以对 APK 进行加壳和数字签名操作.

用户登录前, 首先从应用的配置文件中读取加密的软件验证码数据和后台数据库中的软件验证码进行比较, 如正确进行用户校验, 否则, 提示用户软件存在异常.

4.2 地图定位

系统中地理位置信息的获取, 需要对地址进行定位和反地址编码. 开发时获取当前地理位置可以采用三大地图 API: 百度地图 API、高德地图 API、腾讯地图 API. 鉴于百度地图控件更适应国内城市地理信息, 且资料更新最快, 登录系统中采用百度地图 API 实现 LBS 定位和反编码等功能, 实现步骤如下:

(1) 注册百度开发者.

(2) 获取 API key.

(3) 下载百度地图 SDK 开发包.

(4) 在 Android 项目中引用百度 SDK.

(5) 在清单文件中添加开发者密钥和所需权限.

(6) 布局文件中隐式添加地图控件.

(7) 程序文件中添加地图事件处理逻辑, 获取用户所处的经纬度信息和标志性建筑.

4.3 人脸信息获取

人脸信息获取主要用于登录行为审计. 通过使用手机前置摄像头抓拍用户脸部信息和操作环境来帮助系统和用户能够随时查询自己的账号被冒名登录的情况. 由于系统只是异步采集人脸数据而未对人脸数据信息训练和对比, 所有不会对用户登录性能有所影响.

在 Android 手机中使用 Camera API 实现人脸信息采集, 步骤如下:

(1) 在 AndroidManifest.xml 文件中, 增加 SD 卡外部存储功能和用户手机拍照权限, 并定义自动对焦和摄像特性.

(2) 布局文件中添加一个不可见的 surfaceView.

(3) 根据 SurfaceView 获得固定器 Holder.

(4) 设置固定器的 SurfaceHolder.Callback.

(5) 打开前置摄像头开始拍照, Callback 里面有拍照数据, 这些 byte[]数据通过流读取技术写入数据库图片字段, 也可以根据 BitmapFactory 变成 Bitmap 图片.

4.4 手机个性化信息获取

每台手机和电脑一样都有标识自己身份的唯一识别信息. 电脑有 CPU 号、硬盘号、网卡 MAC、IP 地址等. 手机有硬件标识 IME 和用户标识 SIM 卡. 所以, 可以采集这些唯一标识来进行行为追溯.

IMEI (International Mobile Equipment Identity) 国际移动设备身份码和每部手机一一对应. 由于每部手机的 IMEI 号是唯一的, 所有可以作为手机用户身份认证的个性化数据. 在 Android 语言包中, TelephonyManager 类提供了手机硬件信息的操作方法. 操作步骤如下:

(1) 在项目清单文件 AndroidManifest.xml 中增加访问设备状态的权限 READ_PHONE_STATE.

(2) 通过获取 TelephonyManager 对象实例, 调用 getDeviceId 方法获取 IMEI.

在模拟器中运行时, getDeviceId 方法返回总是 000000000000000, 所以应在实际手机中测试.

另外, TelephonyManager 类还提供了获取手机号码, SIM 卡号等方法, 这些都可以成为用户登录行为追溯的个性化数据.

4.5 AES 与 RSA 混合加密算法

登录系统中, 用户密码的可控能力将直接影响到系统可靠性, 也直接影响到整个系统的运作效率和信任度. 为保障用户账户安全性, 解决信息窃取问题. 采用 AES、RSA 两种加密算法的混合算法对用户密码进行加密. AES 加密算法是对称分组加密算法, 用于取代 DES, 其处理效率高, 适于明文加密. RSA 算法是秘钥管理算法的代表, 是不对称加密算法, 用公钥加密, 私钥解密, 秘钥管理性能优异. 本文综合发挥 AES 和 RSA 的优点实现 AES-RSA 混合加密算法. 使用 AES 对称密码体制对密文加密, 同时使用 RSA 不对称密码体制来传送 AES 的密钥, 就可以加解密实现. 流程如图 2, 图 3 所示.

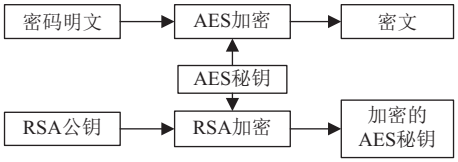

图 2 AES-RSA 算法加密流程图

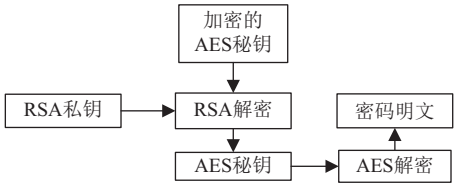

图 3 AES-RSA 算法解密流程图

5 原型系统及实验分析

为验证该改进的登录子系统的可靠性和安全性, 笔者结合西译通手机软件进行了部署与测试. 西译通是毕业学生为母校开发的一款集校园新闻、信息查询、招生宣传为一体的手机 APP 软件. 该 APP 主要面向学生和教师使用. 为保证后台数据安全, 该系统实现了对用户登录验证, 并记录了登录时间、登录地点、登录者头像等信息, 便于操作审计. 图 4 为该系统部署图.

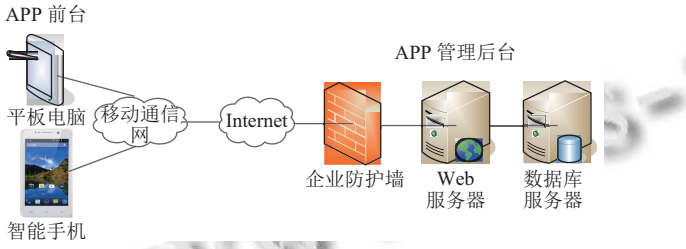

图 4 西译通系统部署图

由于增加了登录行为审计, 故用户可以查看时间段内登录行为的审计信息, 这些数据对所有用户来说是只读的, 从而可以真实追溯历史信息. 图 5 为用户某次登录信息界面截图 (前置摄像头无时显示无照片图片).

目前, 手机拍照、地理位置获取等个性化信息收集功能一般新款手机自带安全软件和 360 手机卫士中都有体现. 但一般企业工具类 APP 中应用较少, 只在支付宝中人脸支付功能中体现, 且客户无法方便的查询到详细的个人登录隐私数据. 随着手机应用的日益普及和移动商务的飞速发展, 企业级 APP 涉及支付和个人隐私数据的场景会越来越多, 在此类 APP 登录系统中集成这些功能与进行二次开发显得日益紧迫. 本文在西译通软件中集成了这些元素, 相当于在客户 APP 中集成了小型个人安全中心. 除用户自身可以查看自己登录行为外, 后台管理员也可以使用后台审计报警功能, 根据登录频度对比统计出时间段内登录异常的用户, 并推送消息给用户, 提示用户加以检查和干预.

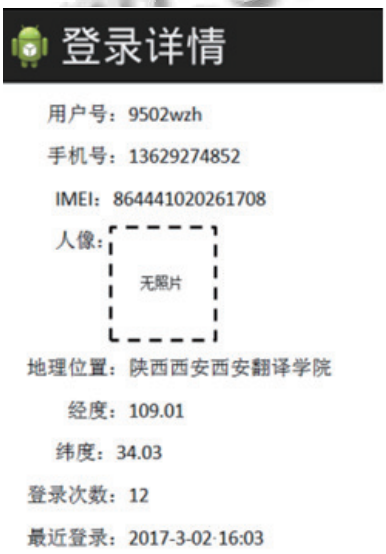

图 5 登录详情界面

下面是与安全性要求较高的手机银行 APP 的登录安全功能进行对比的结果. 如表 4 所示.

表 4 登录系统对比分析

	手机银行APP	原型系统	对比分析
登录方式	首次登录, 除账号、密码外需要手机校验码	每次均需要账号、密码和验证码	前者需要手机短信支持、且易造成穷举攻击
加密方式	3DES数据加密	AES-RSA混合加密	后者既考虑加密效率也考虑加密性能
多终端登录	仅招行支持, 消息提示	不支持, 消息提示, 记录登录日志	基本一致, 后者更细粒度
日志功能	仅记录登录账号、时间、手机号	除账号、时间外还记录位置、人像等信息	后者日志信息更详细
审计自助	无	有	前者只能由管理后台审计, 后者用户自己可以查询和取证

通过比较分析, 本文设计的登录系统相对于目前手机中使用的登录系统有以下优点:

(1) 提出了验证与审计相结合的安全管理模式.

(2) 使用多因子多重验证技术提高登录安全级别.

(3) 操作可追溯性和防抵赖性. 不仅管理员可以查看用户登录行为, 用户自己也可以查看自身账号登录行为.

(4) 精细化的行为审计查询和分析. 对管理员提供

了针对不同操作类型、账号、时间段、地理范围的审计记录的查询和有效分析, 及时找出可能的攻击行为.

6 结语

随着“互联网+”国家战略的推进和移动互联网技术的飞速发展, 手机应用不断丰富的同时, 用户信息安全也时刻面临新的挑战. 为了便于处理已有安全威胁和应对新的未知安全风险. 本文分析了目前手机应用登录系统存在的缺点, 利用手机定位技术和拍照特性, 设计了一款集注册认证、登录验证、登录审计为一体的用户登录子系统, 有效管理用户登录行为, 并进行了原型系统实现和安全性验证. 首先, 使用软件校验技术, 避免钓鱼软件的使用, 然后采用账号、密码、验证码、登录次数等多因子保证登录事前检测和事中控制, 又进一步使用地图定位、刷脸技术、登录时间、时间段登录次数等多因子技术, 实现了用户登录的事后审计. 不足之处是由于地图 API 精度和摄像受像素等因素影响, 采集的登录位置和人脸数据会有一定偏差. 总之通过验证和审计相结合的登录技术, 既可以帮助管理者评估系统安全性, 也可以成为个人用户审计自身账户安全的得力助手. 该解决方案用户体验好, 性能优, 安全性强, 为用户开展基于手机的商务活动提升了安全级别.

参考文献

1 董超, 杨超, 马建峰, 等. Android 系统中第三方登录漏洞与解决方案. 计算机学报, 2016, 39(3): 582–594. [doi: 10.11897/SP.J.1016.2016.00582]

2 吴琼. 基于 Android 平台手机客户端登录破解的研究与分析. 农业网络信息, 2016, (5): 60–61.

3 王振辉. 一种安全登录子系统的设计与实现. 科学技术与工程, 2012, 12(22): 5624–5629. [doi: 10.3969/j.issn.1671-1815.2012.22.045]

4 Terry RF. Creating and using a specific user unique id for security login authentication: US 20140173273. [2014-06-19]

5 Agrawal VK, Bharti RK, Parihar B. Password authentication with secured login interface at application layer. International Journal of Computer Science & Network Security, 2014, 14(9): 82–85.

6 周小红, 周建伙. MD5 加密算法在注册及登录验证模块中的应用. 工业控制计算机, 2015, (11): 118–119. [doi: 10.3969/j.issn.1001-182X.2015.11.051]

7 黄少川, 谭毓安, 马忠梅, 等. 基于 SmartWatch2 的手机 App 登录信息保护研究. 单片机与嵌入式系统应用, 2016, (3): 12–15.

8 Buck BJ. Method and system for managing user login behavior on an electronic device for enhanced security: US 2014/0165169A1. [2016-04-05]

9 杨海, 赵文涛, 张乃千, 等. 基于 USB Key 的 Windows 凭据提供登录系统的设计与实现. 计算机科学, 2014, 41(S2): 371–374, 398.

10 Twitter 增强 iPhone、Android 帐户安全登录功能. 工业设计, 2013, (6): 29.

11 Geil PW. Login security with short messaging: US 8712453. [2014-04-29]

12 刘妍, 金鑫, 赵耿, 等. 基于高效隐秘汉明距离计算的安全人脸识别. 计算机工程与设计, 2016, 37(9): 2327–2331.

13 吴贤平. 基于指纹识别和 CAS 的单点登录模型技术研究. 计算机应用研究, 2012, 29(4): 1381–1383, 1390.

14 梁丽雯. 手机指纹登录争议不断. 金融科技时代, 2016, (6): 102–103.

15 徐强, 梁彬, 游伟, 等. 基于 SURF 算法的 Android 恶意应用钓鱼登录界面检测. 清华大学学报 (自然科学版), 2016, 56(1): 77–82.