基于轻量级加密算法的手机短信加密软件①

李 悦[1], 李乾文[1], 王高丽[2], 李 玮[1]

[1](东华大学 计算机科学与技术学院, 上海 201620)
[2](华东师范大学 华东师范大学计算机科学与软件工程学院, 上海 200241)

摘 要: 针对 Android 智能手机的恶意软件正在迅速增长并危害手机用户的个人隐私和系统安全, 为了实现手机短信的隐私保护和秘密通信, 设计并开发了一款利用轻量级对称加密算法对短信进行加密发送的手机隐私保护软件. 该软件面向 Android 手机而开发, 具有软件开启密码保护、联系人导入、会话密钥设置、短信导入与加解密功能. 该软件为智能手机隐私泄露提供了一个可行的解决方案.

关键词: Android 应用开发; 手机隐私保护; 轻量级对称加密算法; 软件设计

Android Text Message Privacy Protection Software Based on Lightweight Symmetric Cryptography

LI Yue[1], LI Qian-Wen[1], WANG Gao-Li[2], LI Wei[1]

[1](School of Computer Science and Technology, Donghua University, Shanghai 201620, China)
[2](School of Computer Science and Software Engineering, East China Normal University, Shanghai 200241, China)

Abstract: The number of malicious software targeted on Android system is rapidly increasing. Therefore it is important to implement privacy protection software on smart phones. This paper introduces a new design and development of privacy protection software which encrypts the text message using lightweight block cipher encryption algorithm. This Android App provides software login protection, mobile contacts importing, conversation key setting, text message importing and message encryption and decryption features. This APP prevents the privacy leakage from the text message in Android devices.

Key words: Android application development; privacy protection; lightweight symmetric cryptography; software design

随着通信与计算机技术的不断发展和更新, 智能手机已然逐步演化成人们生活中不可或缺的工具之一, 除了基本的通话功能, 它还具备连接互联网、社交互动、多媒体、摄影、电子地图以及卫星定位等功能, 手机系统也越来越智能, 越来越易于操作, 用户能自行搜索、下载和安装第三方程序. 许多黑客和不法份子利用手机系统漏洞和巨大的手机用户群进行恶意软件的发布, 通过这些恶意软件进行非法信息收集, 这些信息包括个人的信用卡信息、个人隐私信息或者商业机密信息. 因此用于保护手机用户隐私的手机软件也应运而生.

1 设计背景

Android 的开源特性和优越的跨平台工作能力受到软件开发者和用户的喜爱, 因此该系统的市场占有率持续增长, 导致其逐渐成为大量恶意攻击者的首选目标之一. Android 平台中出现的一系列恶意软件会在软件安装时索取某些可能导致隐私泄露的 Root 权限, 使得用户在不留意的状况下被开启系统“后门”, 并通过联网上传或者短信外发等形式窃取用户隐私[1,2]. 因此移动终端的隐私保护是急需解决的信息安全问题[3-5]. 本软件可以将用户的接发短信以密文形式保存在手机上, 即使敌方窃取了手机中的短信(密文)也无法知道该短信的内容因为解密密钥只有用户知道, 而且解密密钥被用户的登录口令加密, 不法分子也无法从本地文件中找到解密密钥. 该软件适用于任何安装 Android 操作系统的手机.

① 收稿时间:2016-03-03;收到修改稿时间:2016-04-11 [doi:10.15888/j.cnki.csa.005436]

2 研究现状

目前, 手机上的短信技术是采用 GSM 标准[6], 明文传输, 短信息采用存储转发技术. 在 GSM 网络中, 短信都是明文传输, 只要对通信链路进行监听, 就可以获得用户的通信内容[7].

现今普遍流行的短信安全机制比较简单, 手机终端采取加锁机制, 在进入短信界面时, 增加一个登录界面, 输入密码, 若密码输入正确, 才能进入短信界面. 但短信还是以明文的形式保存在储存卡里, 利用软件反编译技术和口令破解技术就可以攻破这层防线并得到手机用户的机密信息. 攻击者也可以将窃取的手机直接连接电脑绕过加锁机制, 直接获取短信信息[8].

针对短信通信过程中的信息泄漏, 可采取的技术手段是对短信进行加密传输. 在电脑软件中, 有针对电子邮件加密的软件-PGP, PGP 是一个可以让我们的电子邮件拥有保密功能的应用. 我们可以将邮件加密, 除了邮件接收者能看到其内容以外, 其他人都无法解读. 一旦加密后, 信息看起来是一堆无意义的乱码. PGP 的出现与应用很好地解决了电子邮件的安全传输问题[9] . 它将传统的对称加密机制与公开密钥加密机制结合起来, 兼备了两者的优点. 使得信息的安全性有了很大的提高.

本文设计的 Android 短信加密软件借鉴了 PGP 的设计思想, 利用对称加密算法对手机短信进行加密传输, 只有拥有解密密钥的短信接收者可以解密密文短信. 这样可以解决短信在通信过程中的信息泄露.

3 轻量级加密算法设计

无线传感网和物联网的发展让轻量级加密算法的研究成为了一个研究热点, 许多轻量级加密算法在最几年被提出[10,11]. Android 短信加密软件采用新型轻量级分组加密算法(New Lightweight Block Cipher)对短信进行加密, 该算法在轻量级加密算法 LED 算法[12]的基础上对轮常量和 S 盒替换表[13]进行了优化.

New Lightweight Block Cipher 算法(NLBC)采用了和 AES 类似的 SPN 结构. 其加密轮数为 32 轮, 消息分组长度为 64 比特, 密钥分别支持 64 比特和 128 比特, 分别称为 NLBC-64 和 NLBC-128. 本文主要使用NLBC-64. NLBC 算法在第 1 轮之前进行一次轮密钥加, 以后每 4 轮进行一次, 轮函数包含 4 个步骤, 分别是轮常量加、S 盒替换、行移位、列混合. 其中非线性层为 16 个并行的 比特的 S 盒. 线性层为状态矩阵的第 j 行向左移 j 位(j=0,1,2,3). 与传统的 AES 算法相比, NLBC 算法采用了无密钥生成的策略, 轮密钥即为初始密钥, 从而提高了加密速度以及减小了硬件实现规模. NLBC 算法的结构如图 1 所示.

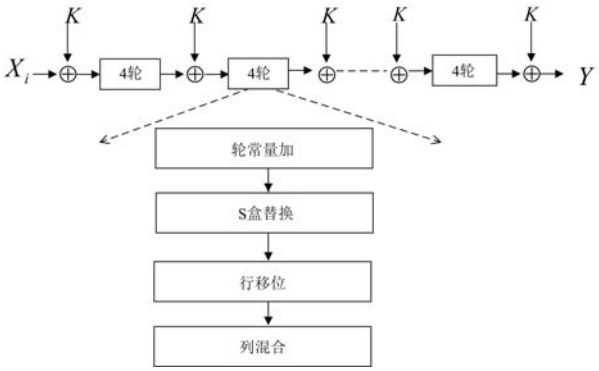


图 1　NLBC 算法结构

4 软件总体构架

针对手机短信在公开信道上的信息泄露和被窃听的威胁, 本文设计了一款短信加密软件, 该软件可以对短信进行加密发送并可在接收端对密文短信进行解密; 该软件为手机用户提供数据加密和隐私保护功能. 用户需要通过口令登录本软件来实现对短信的加密和解密, 软件保存了通讯录上手机联系人所使用的会话密钥, 软件会根据短信的联系人电话号码提取加密密钥对短信进行加密, 接收方收到密文短信后登录本软件, 根据短信的发送者电话号码导出解密密钥进行解密并生成明文格式的短信内容. 该软件实现的安全服务有以下四种:

1) 端对端加密

该软件的加密方式为端对端加密, 只有手机终端都安装了这款软件, 才能进行加密通信.

2) 加密对象的简短性

该软件的加密对象是手机短信以及用户通过手机或其他电信终端直接发送或接收的文字或数字信息, 用户每次能接收和发送短信的字符数是 160 个英文或数字字符, 或者 70 个中文字符. 所以加密后的密文长度不能与明文相差太多, 导致用户在发送短信时产生不必要的花费.

3) 加解密过程的透明性

在用户登录该软件进行发送和接收短信时, 加解

密过程对于用户是透明的. 在软件验证了用户的身份为合法后, 用户就可以发送和接受加密短信.

4) 密钥管理的安全性

该软件使用 Android 本地数据库 SQLite[14,15] 对密钥进行存储和管理. 在不使用该软件时, 将数据库加密, 这样就能阻止了非法用户窃取密钥, 从而打开相应的密文, 有效杜绝了因为密钥泄露造成的损失.

软件整体结构如图 2 所示.

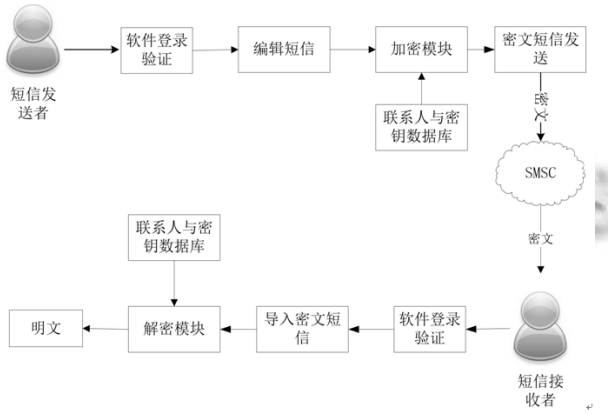


图 2 软件结构示意图

5 程序设计流程

本软件主要有四大功能模块组成, 分别为登录密码模块, 短信收发模块, 信息加解密模块和密钥管理模块(如图 3 所示).

图 3 功能模块示意图

登录密码模块主要实现验证登录用户功能; 短信收发模块主要实现短信的正常收发功能并且附带短信监听; 数据加解密模块是主体模块, 主要实现短信内容加密与解密的功能; 联系人密钥管理模块主要包括了密钥的增删查改以及数据库安全性管理等一系列操作.

5.1 登录模块

该模块包括用户注册和用户验证:

5.1.1 用户注册

第一次进入本软件, 会出现用户注册界面. 注册时, 用户需按照相应的约束条件来设计登录口令. 口令必须大于 6 位且不能单纯的是数字, 设计的口令通过 MD5 散列函数进行压缩加密, 得到的结果保存在 password 文件中. 注册成功后, 注册页面不再出现, 即确保用户唯一的唯一性.

5.1.2 用户验证

注册成功后, 转入登陆页面, 用户输入登录口令, 经过 MD5 散列函数计算出散列值, 与数据库中保存的散列值比较, 若两者相同则认证通过, 继续进一步操作; 若不同, 无法通过认证, 则继续返回登陆界面. 输入错误口令超过三次后程序自动关闭.

5.2 密钥与联系人管理模块

这款手机短信加密软件综合考虑内存消耗, 速率等问题, 采用对称密码算法, 因此在数据库中仅需设计保存一张表, 即联系人信息表(姓名, 密钥, 电话号码). 每次添加联系人成功后, 软件自动将联系人的完整信息保存在 SQLite 数据库中. 联系人管理主要包括查找某个或所有联系人, 添加联系人, 编辑联系人, 删除联系人操作. 我们为后台数据库中的联系人表取名 contact.

本系统的数据库程序设计包括一个 DBOpenHelper 类, contact 类, DBkey 类. DBOpenHelper 主要用于建立、更新和打开数据库. contact.java 用于获得和设置 contact 表各字段的值. 该类中包含了五个私有成员: id, name(姓名), phone(电话号码), key(密钥), flag, 分别对应 contact 表中 id, name, phone, key 字段和一个用于检测添加联系人和编辑联系人时数据库中是否存在相同电话号码的标志符 flag. DBkey 类主要包括对联系人的增、删、查、改操作的函数. add(contact con)函数用于添加联系人, update(contact con, String phone)函数用于根据联系人的电话号码来编辑联系人, find(String phone)函数用于根据联系人的电话号码来查找一位联系人, getcontacts()函数用于查找所有联系人.

5.3 信息加解密模块

这款短信加密软件采用第 4 节介绍的 NLBC 加密

算法对短信进行加密. 短信加密的步骤如下:

(1) 导入短信明文字符串和加密密钥(编码格式任意, 消息长度任意);

(2) 将输入的消息和密钥字符串转换为十六进制

(3) 按照算法要求对转换后的消息和密钥进行填充;

(4) 按照算法要求对填充后的消息和密钥进行分割或截取;

(5) 产生子密钥;

(6) 轮函数处理明文消息块和子密钥, 获得密文块;

(7) 采用 ECB 加密工作模式对密文分组进行合并;

算法的解密过程是加密过程的逆, 在此就不再重复.

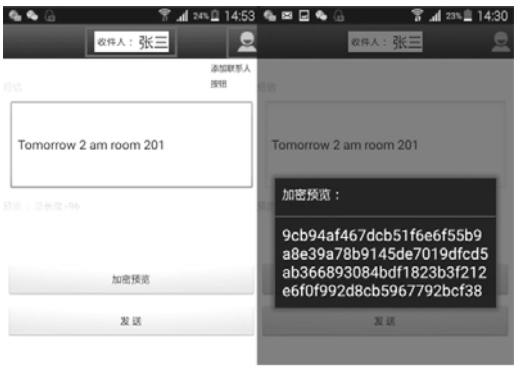
6 功能实现

该软件初次登录时, 将会要求用户设置登录密码. 因为该软件限定用户唯一性, 即只能手机拥有者使用, 所以不需要添加用户名. 注册完成后, 再次登录该软件时, 将会显示登录页面.

用户需要在软件里添加保密联系人并设置和他对话的加解密密钥, 软件可以通过导入功能, 导入现有的联系人方便用户操作, 添加联系人和对应加密密钥的解密如图 4 所示.

图 4　机密联系人和会话密钥添加界面

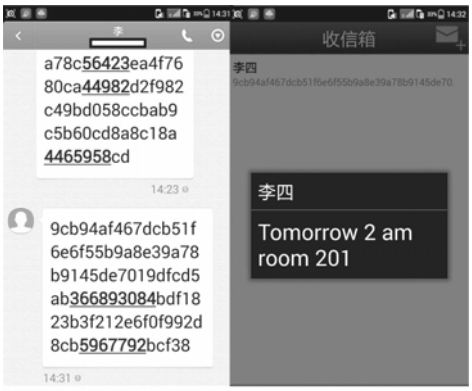
编辑短信, 先按“添加联系人”键, 添加联系人, 点击后, 返回图 5(a)界面, 获取收件人的电话号码和密钥, 在编辑框中编辑完短信后, 即可点击“发送”, 如果用户想预览发送的密文, 可点击“加密预览”查看密文, 如图 5(b)所示.



(a) 编辑短信　　(b) 加密预览

图 5　发送短信界面

通过点击收件箱就可以查看收到的短信如图 6(a)所示. 点击密文短信就会自动跳出明文如图 6(b)所示, 因为软件通过联系人姓名自动调取与该联系人的会话密钥并解密, 不需要再输入解密密钥方便用户使用.



(a) 收信箱界面　　(b) 解密界面

图 6　收信箱和解密界面

7 结语

本文详细介绍了基于新型轻量级对称加密算法的 Android 短信加密软件的设计理念、整体架构和设计流程. Android 手机短信加密软件为手机短信提供了一个安全通道使短信以密文形式在网络中传输并以密文形式在手机端保存, 即使手机丢失, 也不会导致手机敏感信息的泄露. 今后我们还会在这个软件的基础上继续设计开发手机通讯录、图片以及多媒体文件的加密保护功能, 从而实现全方位的 Android 手机隐私保护.

参考文献

1 边悦,戴航,慕德俊.Android 恶意软件特征研究.计算机技术与发展,2014,11(24):178–181.

2 彭国军,李晶雯,孙润康,肖云倡.Android 恶意软件检测研究与进.武汉大学学报(理学版),2015,1(61):20–33.

3 Yan L, Yin H. DroidScope: Seamlessly reconstructing the OS and Dalvik semantic views for dynamic Android malware analysis. Proc. of the 21st USENIX Security Symposium. 2012.

4 张玉清,王凯,杨欢,方喆君,王志强,曹琛.Android 安全综述.计算机研究与发展,2014,51(7):1385–1396.

5 Shabtai A, Fledel Y, Kanonov U, Elovici Y, Dolev S, Glezer C. Google Android: A comprehensive security assessment. Security & Privacy, IEEE, 2010, 8: 35–44 .

6 马玉春,孙冰,王建明.GSM 模块的综合应用研究.计算机应用与软件,2008,25(2):68–70.

7 Delac G, Silic M, Krolo J. Emerging security threats for mobile platforms. Mipro, 2011 Proc. of the International Convention. Opatija, Croatia. 23-27 May. 2011. 1468−1473.

8 刘人杰.手机短信安全与应用研究.硅谷,2012.6:91–133.

9 邓惠洁,姜明富.电子邮件系统 PGP 的加密原理与安全性分析.现代计算机(专业版),2010,14:31–43.

10 杨威,万武南,陈运,张言涛.适用于受限设备的轻量级密码综述.计算机应用,2014,34(7):1871–1877.

11 陈平,廖福成,卫宏儒.对轻量级密码算法 MIBS 的相关密钥不可能差分攻击.通信学报,2014,35(2):190–194.

12 Guo J, Peyrin T, Poschmann A, et al. The LED blockcipher. Proc. of the International Workshop of Cryp-Tographic Hardware and Embedded Systems (CHES 2011). 2011.

13 刘景伟,韦宝典,吕继强,王新梅.AES S 盒的密码特性分析.西安电子科技大学学报,2004,2:255–259.

14 林培杰,朱安南,程树英.Android 数据库 SQLite 性能优化,2014,23(4):193–196.

15 倪天龙,张贤高,王培.数据库 SQLite 在嵌入式系统中的应用.单片机与嵌入式系统应用,2006,10:25–37.