Android 平台下文件透明加密技术的研究与实现

王艳敏,李永忠,吕少伟
(江苏科技大学 计算机科学与工程学院,江苏 镇江 212003)

摘 要:目前,透明加密技术在 Windows 平台下已经得到了广泛的应用,但在移动平台下的应用还有待探索。针对目前日益突出的手机数据安全问题,在对比分析了钩子透明加密和驱动透明加密这两种主要透明加密技术的基础上,设计了一种基于 Android 平台的文件透明加密系统。为了与传统手机加密系统区别开来,系统的身份验证环节被转移到 Android 手机自带的屏幕解锁环节上,有效提高了加密效率和用户体验。文中描述了该系统的总体设计方案和各个模块的设计方法,并给出了内核模块所使用的一些关键技术和重要的实现方法。测试数据表明,该系统能有效对手机应用程序和文件进行透明加密,同时又有较好的加密效率和用户体验。

关键词:透明加密;Android;文件安全
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2014)09-0137-04
doi:10.3969/j.issn.1673-629X.2014.09.031

Research and Implementation of File Transparent Encryption Technology Based on Android

WANG Yan-min, LI Yong-zhong, LÜ Shao-wei
(School of Computer Science and Engineering, Jiangsu University of Science and Technology, Zhenjiang 212003, China)

Abstract: Transparent encryption technology has been widely used in Windows now. However, it still needs some time in Android. Aiming at the increasingly prominent security problem of cellphone data, design a file transparent encryption system based on Android, on the basis of an analysis and comparison of Hook transparent encryption technology and Driver transparent encryption technology. In order to be different from traditional encryption systems used in cellphone, the authentication is shift to the course of Android's screen-unlocking, thus encryption efficiency and user experience are improved. The whole system design scheme as well as design methods of each model is described, and give the key technologies and important realization methods for internal core module. Test results show that this system can realize the transparent encryption of a cellphone's applications and files effectively with good encryption efficiency and user experience.

Key words: transparent encryption; Android; files security

0 引 言

Android 作为一个开源的移动平台操作系统,受到了越来越多的手机用户和手机开发者的青睐。Android 智能手机的迅速发展让手机应用和用户体验焕然一新,这在给现代人们的生活注入了新鲜活力的同时也引起了人们越来越多的担忧。手机作为日常生活和工作的重要数据载体,其安全问题日益突出。

目前,文件透明加密技术在 Windows 平台下已经得到了较为广泛的应用,市场上也出现了若干较为成熟的 Android 手机文件加密软件。但是这些软件要求用户在每次使用加密应用程序或者查看加密文件时都要进行验证,大大降低了加密效率和用户体验。本系统采用文件过滤驱动透明加密技术来完成对用户信息的保护,只需要一次身份验证,提高了加密效率和用户体验。

1 Android 体系结构

Android 系统的底层建立在 Linux 系统之上,该平台由操作系统、中间件、用户界面和应用软件 4 层组成,它采用一种被称为软件叠层(Software Stack)的方

收稿日期:2013-10-21 **修回日期**:2014-01-23 **网络出版时间**:2014-05-21
基金项目:江苏省高校自然科学基金资助项目(05KJD52006);江苏科技大学科研资助项目(2005DX006J)
作者简介:王艳敏(1991-),女,安徽阜阳人,硕士研究生,研究方向为智能网络理论与工程应用;李永忠,教授,研究方向为网络安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140525.1242.010.html

式进行构建[1]。这种软件叠层结构使得层与层之间相互分离,明确各层的分工。

Android 的架构主要由应用程序层(Application)、应用程序框架层(Application Framework)、函数库和运行时(Libraries、Android Runtime)、Linux 内核(Linux Kernel)组成[2]。应用程序层(Application)包括系统自带的和用户安装的应用程序,两者平等地访问 Android 提供的 API 框架。应用程序框架层(Application Framework)为应用程序层提供 API。函数库为应用程序框架提供 C/C++库,Android 运行时为应用程序框架提供 Android 核心库集和 Dalvik 虚拟机。Linux 内核提供了安全性、内存管理、进程管理等核心系统服务。

2 透明加密相关技术

所谓透明加密,是指在不改变用户操作习惯的情况下完成文件的加密和解密过程[3]。当系统监测到用户对受保护的文件进行读写操作时,将对文件进行解密操作,将明文传送给应用程序;当系统监测到用户对受保护的文件结束读写操作时,又将对文件进行加密操作,将密文传送存储设备进行存储。整个过程与文件的所在环境密切相关,环境一旦更改,加解密过程将无法完成,从而保证了对指定文件的保护。

钩子透明加密(Hook)和文件过滤驱动透明加密是目前常用的两种透明加密技术。

2.1 钩子透明加密技术

钩子透明加密技术工作在应用层,结合使用 Windows API 函数和 Hook 消息处理机制[4]。通过 Windows 的钩子技术,监控应用程序对文件的打开和保存。打开文件时,先对密文进行解密再读入内存,以保证应用程序读到的是明文;保存文件时,先将内存中的明文进行加密再写入到磁盘中,如图 1 所示[5]。

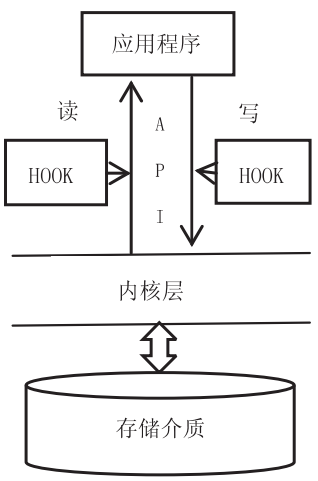

图 1 钩子透明加密拦截文件操作的层次

2.2 文件过滤驱动透明加密技术

驱动透明加密技术工作在 Windows 的内核层,主要依赖于 Windows 的文件系统驱动(IFS)技术[6]。文件系统驱动是把文件作为一种设备来处理的一种虚拟驱动。当文件系统驱动检测到用户对某种后缀文件进行操作时,对该文件进行加密/解密操作,从而达到加密的效果,如图 2 所示。

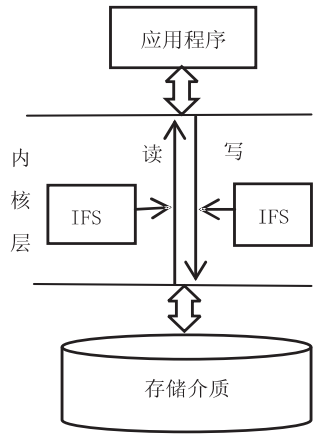

图 2 驱动透明加密拦截文件操作的层次

2.3 两种技术比较

综上所述,钩子透明加密技术开发容易,但与应用程序密切相关,容易因应用程序的改动和不同导致加密失败,而且容易被反 Hook 所破解。相比之下,文件过滤驱动透明加密技术开发难度较大,但因工作在受保护的内核层,运行速度较快,也较稳定。

3 透明加密系统设计与实现

3.1 总体设计思想

系统采用 MVC(Model, View, Controller)框架。Model(模型)接收控制器传来的控制信息,完成数据库或者文件的读写操作,以及加密解密操作。View(用户界面)主要实现与用户的交互,将用户的加密策略定制更新至相关数据库项。Controller(控制器)根据用户的加密策略定制更新监控列表,监控并接受列表内应用的数据读写操作,将相关信息传送至 Model。

加密算法采用了较为成熟的 DES 加密算法来实现文件的加密和解密。系统在手机开机时对用户进行身份验证。系统拦截到用户进行读取文件操作时,读出密文文件并解密,再将解密后的明文传送给应用层供用户读取;系统拦截到用户进行关闭文件的操作时,将明文文件进行加密,再存储到存储设备上。这样,用户就不用重复进行验证,保留了良好的操作体验,手机内的文件信息也得以保护。

3.2 功能模块设计

系统模块分为应用层模块和内核模块。其中,应用层模块主要完成加密策略定制和与用户的交互功能;内核模块则根据应用模块设置的加密保护策略完成读写监控、加密/解密、数据读写功能,如图 3 所示。

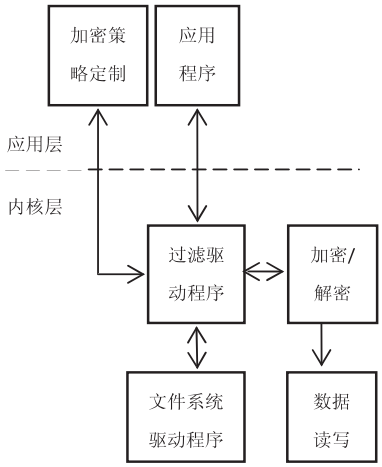

图 3　系统模块图

下面对内核模块重点功能的实现做介绍。

3.2.1　驱动层的文件读写监控实现

Android 平台的文件读写监控,实质上是指 Linux 文件系统中文件的实时读写监控[7]。在 Linux 文件系统中,文件是以文件信息节点(inode)的形式存在于内核之中的。内核通过对文件信息节点的管理来管理文件系统中的这些文件。每一个文件都有着与之对应的、唯一的文件信息节点。通过对文件节点的监控来实现对文件读写操作的监控,是一种非常有效且粒度很小的方法[8]。

创建一张列表,将需要监控的对象存入表中,然后对监控对象进行监控,包括文件相应的打开、关闭、创建、删除等行为。并在相应的行为发生的时候向加密/解密模块发送相应的信息,以通知其进行相应的加密/解密操作。

3.2.2　DES 算法的实现

DES 算法是一种最通用的对称密钥算法,自出现以来一直作为非常安全的加密算法被用于各种数据的保护。该算法分别由初始置换函数 IP、自密钥 Ki 及获取、密码函数 F 和末置换函数 IP^{-1} 这四部分完成[9]。下面给出获得密钥功能函数。

函数 getKey 实现密钥获取功能:

```
public static Key getKey(byte[] arrBTmp, String alg){if(!(alg.equals("DES")||alg.equals("DESede")||alg.equals("AES"))){
System.out.println("alg type not find:"+alg);
return null;
}
byte[] arrB;
if(alg.equals("DES")){
arrB=new byte[8];
}
else if(alg.equals("DESede")){
arrB=new byte[24];
}
else{
arrB=new byte[16];
}
int i=0;
int j=0;
while(i < arrB.length){
if(j>arrBTmp.length-1){
j=0;
}
arrB[i]=arrBTmp[j];
i++;
j++;
}
Key key = new
javax.crypto.spec.SecretKeySpec(arrB, alg);
return key;
}
```

3.2.3　内核层 SQLite 读写的实现

在安卓平台中,数据的存储主要有文件系统、嵌入式数据库 SQLite、网络以及 Shared Perferences 等方式[10]。

对应用程序加密保护需要完成对 SQLite 的数据访问和读写。Android 类库提供了抽象类 SQLiteOpenHelper[11]。对数据库进行操作需要建立一个 SQLiteOpenHelper 类,以该类的对象对数据库进行添加、删除、更新、编辑等操作[12]。对于 SQLiteOpenHelper 类,设计了构造函数 MyDatabaseHelper。在该构造函数中,先调用父类的构造函数:super(context,name,factory,version);SQLiteOpenHelper 的构造函数:SQLiteOpenHelper(Context context,String name,CursorFactory factory,int version)[13]。context 指上下文对象,name 指数据库文件名字,factory 指 CursorFactory 的对象,version 表示数据库的版本[14]。

分别设置了 onCreate(SQLiteDatabase db),onUpgrade(SQLiteDatabase db,int oldVersion,int newVersion)来完成数据库的创建和更新功能。

3.3　系统工作流程图

系统工作流程图如图 4 所示。

4　系统测试

在 Android 2.3.3 上成功安装系统,可以对手机应用程序进行加密,成功实现对 SD 卡上 txt、doc 文件格式的透明加密功能。加密成功后,在本地手机上能够正常查看文件,通过电脑查看则为乱码。

5　结束语

测试结果显示,加密完成后,文件在本地手机上不

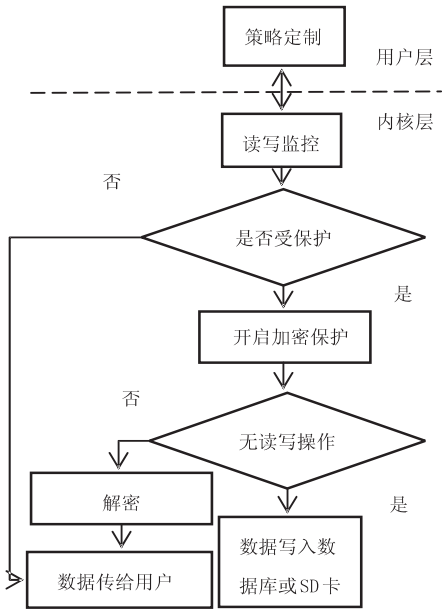

图 4 系统工作流程图

需要重复进行身份验证即可正常查看,在其他环境下则不能正常查看,成功实现了对文件的透明加密功能。文中的文件透明加密系统使用了文件过滤驱动技术,具有安全、稳定、高效的特点。但需要在此基础上引入数据控制和备份机制,才能最终形成一个完整的数据安全保护系统。

参考文献:

[1] 李 刚. 疯狂 Android 讲义[M]. 北京:电子工业出版社,2011.
[2] 刘彬彬,李永忠,舒 俊. Android 平台下的病毒原理分析及其防御技术研究[J]. 电子设计工程,2013,21(4):40-43.
[3] 梅凯珍,李永忠. 基于过滤驱动的局域网透明文件安全加密方法[J]. 计算机技术与发展,2012,22(4):238-241.
[4] 周道明,钱鲁锋,王路路. 透明加密技术研究[J]. 信息网络安全,2011(12):54-56.
[5] 王全民,周 清,刘宇明,等. 文件透明加密技术研究[J]. 计算机技术与发展,2010,20(3):147-150.
[6] 赵铭伟,毛 锐,江荣安. 基于过滤驱动的透明加密文件系统模型[J]. 计算机工程,2009,35(1):150-152.
[7] Ableson W F,Collins C,Sen R. Unlocking Android:a developer's guild[M]. Greenwich,Conn:Manning,2009.
[8] Darcey L,Conder S. Sams teach yourself Android application development in 24 hours[M]. Indianapoils,Ind:Sams Pub,2010.
[9] Stinson D R. The principle and practice of cryptography[M]. 3rd ed. Beijing:Electronic Industry Press,2009.
[10] 关东升,赵志荣. Android 开发案例驱动教程[M]. 北京:机械工业出版社,2011.
[11] 余 俊,袁家斌. 文件透明加密技术研究与实现[J]. 信息通信,2009(6):23-26.
[12] 张小川,陈 最,涂 飞. 基于过滤驱动的透明加密文件系统研究与实现[J]. 计算机应用与软件,2013,30(4):44-47.
[13] Hashimi S Y. Pro Android 2[M]. New York:Apress,2010.
[14] 胡 文. Android 嵌入式系统程序开发:基于 Cortex-A8[M]. 北京:机械工业出版社,2013.

(上接第 114 页)

研究[J]. 计算机技术与发展,2010,20(2):171-174.
[3] 刘 勇,曹明翠,罗志祥,等. SNMP 代理在光纤通道交换机上的嵌入式实现[J]. 光通信技术,2005,29(9):27-30.
[4] 葛永明,林继宝. 嵌入式系统以太网接口的设计[J]. 电子技术应用,2002,28(3):25-27.
[5] 王宜怀,刘晓升. 嵌入式系统-使用 HCS12 微控制器的设计与应用[M]. 北京:北京航空航天大学出版社,2008.
[6] 张裔智,赵 毅,汤小斌. MD5 算法研究[J]. 计算机科学,2008,35(7):295-297.
[7] 曾 金,毛燕琴,沈苏彬. 嵌入式流媒体服务器的设计和实现[J]. 计算机技术与发展,2011,21(7):81-84.
[8] 夏靖波,王 航,陈雅蓉. 嵌入式系统原理与开发[M]. 西安:西安电子科技大学出版社,2006.
[9] Dorigo M,Di Caro G,Gambardella L M. Ant algorithms for discrete optimization[J]. Artificial Life,1999,5(2):137-172.
[10] 陈兴文,刘 燕. 单片机应用系统硬件调试技巧[J]. 现代电子技术,2000(7):65-66.
[11] 顾 超,宋 宝,唐小琦. 总线式数控系统中 PCI 接口控制器的 FPGA 实现与应用[J]. 计算机应用,2011,31(2):565-567.
[12] 沈安东,王宜怀. 基于摩托罗拉 MCU 在线编程实验仪器的研制[J]. 实验技术与管理,2005,22(12):60-63.
[13] Padmanabhuni S,Singh V,Kumar K M S,et al. Preventing Service Oriented Denial of Service (PreSODoS):a proposed approach[C]//Proc of ICWS. Chicago:IEEE,2006:577-584.
[14] Wehrle K,Pahlke F,Ritter H. The Linux network architecture design and implementation of network protocols in Linux kernel[M]. Beijing:Tsinghua University Press,2007.
[15] Binnig C,Hildenbrand S,Faerber F. Dictionary-based order-preserving string compression for main memory column stores[C]//Proceedings of the ACM SIGMOD international conference on management of data. Providence:ACM,2009.

Android平台下文件透明加密技术的研究与实现

作者： 王艳敏， 李永忠， 吕少伟， WANG Yan-min， LI Yong-zhong， Lv Shao-wei
作者单位： 江苏科技大学 计算机科学与工程学院,江苏 镇江,212003
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(9)