基于 WPKI、DRM 与 TF Key 的智能手机安全存储系统

崔彦军[1,2,4],马艳东[1,2],李 杰[3],赵 政[4]
(1. 河北省科学院 应用数学研究所,河北 石家庄 050081;
2. 河北省信息安全认证工程技术研究中心,河北 石家庄 050081;
3. 河北大学 数学与计算机学院,河北 保定 071002;
4. 天津大学,天津 300072)

摘 要:为避免由智能手机丢失所引起的信息泄露的风险,提出了采用软硬件结合的智能手机信息安全存储的解决方案。本方案综合利用 WPKI 及 DRM 技术,并采用冀科 TF Key 作为硬件实现基础,为用户提供国密算法的加解密运算服务,以实现高强度的身份认证与加解密服务。由于明文只短时存在于内存,任何时刻不以文件的形式驻留于存储介质中;另外,由于本方案采用独立硬件冀科 TF Key 作为国密算法的加解密运算单元,因此,此方案可以为用户提供快速、高强度的安全保护。

关键词:无线公开密钥基础设施;数字版权加密保护技术;TF Key;双因素身份认证;非对称加密算法
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)05-0116-04
doi:10.3969/j.issn.1673-629X.2013.05.030

Secure Store System of Smart Mobile Phone Based on WPKI, DRM and TF Key

CUI Yan-jun[1,2,4], MA Yan-dong[1,2], LI Jie[3], ZHAO Zheng[4]
(1. Institute of Applied Mathematics, Hebei Academy of Sciences, Shijiazhuang 050081, China;
2. Hebei Authentication Technology Engineering Research Center, Shijiazhuang 050081, China;
3. Faculty of Mathematics and Computer, Hebei University, Baoding 071002, China;
4. Tianjin University, Tianjin 300072, China)

Abstract: In order to avoid the risk of information leakage caused by intelligent mobile phone loss, introduce the intelligent mobile phone information security storage solutions combined with hardware and software. This scheme takes advantage of WPKI and DRM, adopts TF Key as hardware realization basis, provides users with encryption and decryption operation service to achieve high strength identity authentication and encryption and decryption services. The information before encryption only exists in memory, not in storage medium in any other form at anytime. In addition, take JK TF key as encryption and decryption arithmetic unit in order to provide higher and faster safety protection for mobile users.

Key words: WPKI; DRM; TF Key; two-factor authentication; asymmetrical cryptography algorithm

0 引 言

智能手机功能强大,电子商务、网上银行、掌上办公、随身娱乐等等功能扩展及升级应用几乎无所不能,就如同一台连接到因特网的 PC 机。智能手机以其高智能性、超方便性为人们(尤其是需要强大商务功能的人士)提供了优质的服务。在现代生活中,智能手机已逐步成为人们日常交流沟通的主要通讯工具。

然而在享受智能手机给人们生产生活带来极大便利的同时,人们也不得不面临智能手机所带来的安全威胁,如手机遗失、手机病毒、恶意软件、垃圾短信侵扰等。手机病毒防范、垃圾短信拦截等领域已经有了较深入的研究[1,2],而手机遗失造成的信息泄露的威胁作为一个重要的安全问题正逐渐引起人们的关注。对个人用户来说,由于手机遗失而导致的隐私数据外泄

收稿日期:2012-08-06;**修回日期**:2012-11-13
基金项目:河北省科技支撑计划项目(12253570D)
作者简介:崔彦军(1971-),男,河北石家庄人,副研究员,主要研究方向为信息安全;赵 政,教授,博导,主要研究方向为数据库、网络、CIMS。

所造成的威胁最大;对企业用户来说,除了面对由于丢失智能手机本身所导致的敏感数据外泄之外,还得承受不法之徒利用智能手机非法接入企业 VPN(Virtual Private Network,虚拟专用网络)而导致的更为巨大损失。

鉴于智能手机市场的巨大商机,以及智能手机用户对信息安全产品的迫切需求,文中提出采用 WPKI(Wireless Public Key Infrastructure, 无线公开密钥基础设施)[3~5]、DRM(Data Rights Management,数字版权加密保护技术)[6,7]、TF Key(TransFlash Key,TF 卡)等先进技术为智能手机用户的重要信息提供高效强力的安全保护。

1　基于 WPKI、DRM 及 TF Key 的智能手机安全存储系统

1.1　WPKI(Wireless Public Key Infrastructure,无线公开密钥基础设施)

WPKI 即“无线公开密钥基础设施”,它将互联网电子商务中的安全机制引入到无线网络环境中的一套遵循既定标准的密钥及证书管理平台体系,用它来管理在移动网络环境中使用的公开密钥和数字证书,有效建立安全和值得信赖的无线网络环境。WPKI 并不是一个全新的标准,它是传统的 PKI(Public key Infrastructure,公开密钥基础设施)技术应用于无线环境的优化扩展。WPKI 采用优化的椭圆曲线算法进行加解密;对数字证书采用压缩的 WTLS(Wireless Transport Layer Security, 无线安全传输层)证书格式来表示;并为了证书验证的高效率设置了短命证书机制。在使用短命证书机制中,对证书进行撤销已经没有意义,也就不需要查询证书的状态,减轻了资源有限的移动终端的负担。

由于 WPKI 具有保密性、完整性、真实性、不可抵赖性,WPKI 的应用消除了用户在交易使用中的风险,能够满足移动电子商务安全方面的要求。

1.2　DRM(Data Rights Management,数字版权加密保护技术)

DRM 技术通过对数字内容进行加密和附加使用规则对数字内容进行保护。其中,使用规则可以判定用户是否符合操作数字内容的条件。使用规则一般可以防止内容被复制或者限制内容的播放次数。通过授权列表和许可证表达文档的使用规则。每个用户或移动终端对应一个许可证,许可证中记录了用户的使用期限、次数等用户权限。系统对文件加密时根据授权列表形成加密文件,然后再对授权列表中的用户进行分发。对信息进行访问时,不仅要求用户合法(用户身份验证用 WPKI 实现)、具体的操作权限合法,还要求许可的使用期限、允许使用的次数等更详尽的信息。

1.3　基于 WPKI 与 DRM 的智能手机安全存储方案

为了避免由于智能手机存储的数据外泄而造成的巨大损失,以及基于对 WPKI 与 DRM 等技术的深入认知,文中提出采用 WPKI、DRM 等先进技术为智能手机用户的重要信息提供高效强力的安全保护的安全存储方案。

本方案为确保用户的身份合法,为智能手机用户设置一个 WPKI 的公钥证书,用于移动终端用户的身份认证、信息加解密、生成与验证数字水印等的技术实现。还可以用硬件信息与用户信息共同生成标识码,将此码作为证书主题信息。证书验证通过后,再将证书中的标识码与实际的硬件信息及用户信息进行比对,只有符合才表明该移动终端拥有信息的访问权。

利用 Windows Mobile 文件系统的分层驱动模型,通过自定义的文件系统过滤驱动程序,能够拦截任何试图对文件系统的访问操作,并根据规则预先进行处理。文件操作跟踪与实时透明加密技术就是基于此原理,对 Windows Mobile 文件系统的过滤功能进行扩展,一是进行数据读写的控制,作为防信息泄漏软件的基础;二是用于文件系统的透明附加功能,在文件写过程中对数据进行加密,读过程中自动解密。

用户对文件进行访问时,必须经过文件驱动,所有需要防护的数字文档新建、拷贝甚至通过网络传输时,都被监控和强制加密。访问这些文件时,只有符合系统安全规则的用户或移动终端才能正确解密。明文只短时存于内存,任何时刻不以文件的形式驻留于存储介质。而这些加密、解密与安全规则验证都是在用户无知觉的情况下进行。

1.4　基于 WPKI、DRM 及 TF Key 的智能手机安全存储系统

考虑到现有智能手机的计算能力有限,于是本系统建议将所有的极其消耗资源的身份认证及加解密计算都由智能手机自身迁移至独立的系统硬件中。这样,不仅可以将计算能力不强的智能手机从繁重的加解密计算中解脱出来,加解密计算由专门的硬件实现,速度快、系统消耗小,还可有效地减少用户的等待时间。

为此,开发了具有独立知识产权的智能手机专用的密码外设:冀科 TF Key。该 TF Key 的工作原理如图 1 所示。

本 TF Key 选择 TF 卡结构作为密码外设的载体,并在其基础之上嵌入国产安全芯片,从而为手机提供高性能密码运算能力。其中,本 TF Key 中采用的国产安全芯片具备如下特点:

(1)采用了功耗低、面积小的处理器。

(2)集成了 MPU(Micro Processor Unit,微处理器)、RSA(公钥加密算法)[10]、DES(Data Encryption Algorithm,数据加密算法)、SM1(商密 1 号算法)、SM2(商密 2 号算法)、SM3(商密 3 号算法)、SSF33 对称加密算法、HRNG(High Quality Random Number Generator,高质量随机数发生器)和安全保护模块等多种安全模块。

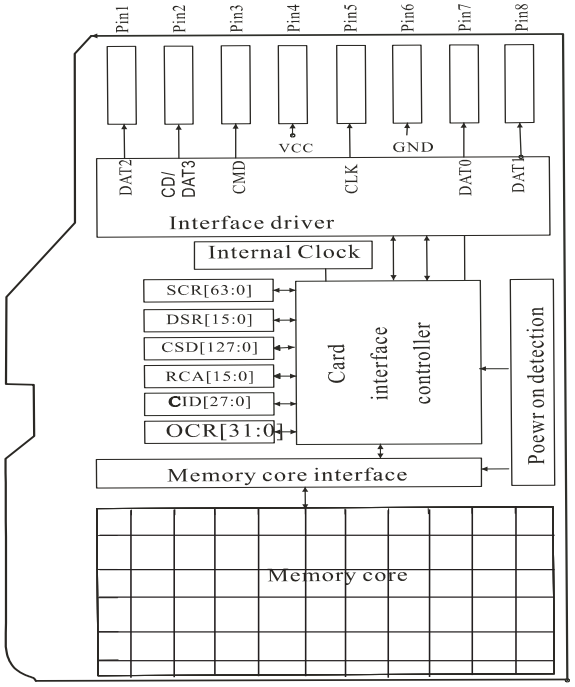

图 1 冀科 TF Key 原理图

(3)提供了丰富的外围接口,如 USB2.0(全速)、ISO7816、SPI(Serial Peripheral Interface,串行外围接口)、UART(Universal Asynchronous Receiver/Transmitter,通用异步接收/发送器)、GPIO(General Purpose Input Output,通用输入输出接口),可应用于 USB Key、安全 TF 卡、RF-SIM(Radio Frequency-Subscriber Identity Module,基于射频技术的用户身份识别模块)、智能卡、终端加密机等多种安全产品。

冀科 TF Key 为一个存储类设备,在手机上使用时不需要安装额外的驱动程序,从而大大简化了应用的复杂性。任何一个安装有客户端应用程序的智能手机均可利用该加密卡进行密码运算。即使没有安装客户端应用程序的手机上,该加密卡也可作为一个加密存储设备为用户提供私有信息的安全保护。冀科 TF Key 的工作流程原理如图 2 所示。

本产品在三个层次上为智能手机用户的信息安全提供保护。

硬件层:TF 接口的加密卡同时提供密码运算功能和数据加密存储功能,配合数字证书可以建立起完善的身份认证体系,从而避免非法用户对设备的滥用。

片内操作系统(COS,Chip Operating System):片内操作系统作为冀科 TF Key 的核心部分,为用户提供应用服务接口、系统调用接口、高级系统服务接口和基本系统服务接口。通过这些功能接口,冀科 TF Key 才能正确执行完成命令解析、数据传输、密码运算、密钥管理、Flash 管理等功能,从而为用户提供可靠的保护。该片上操作系统的功能列表如图 3 所示。

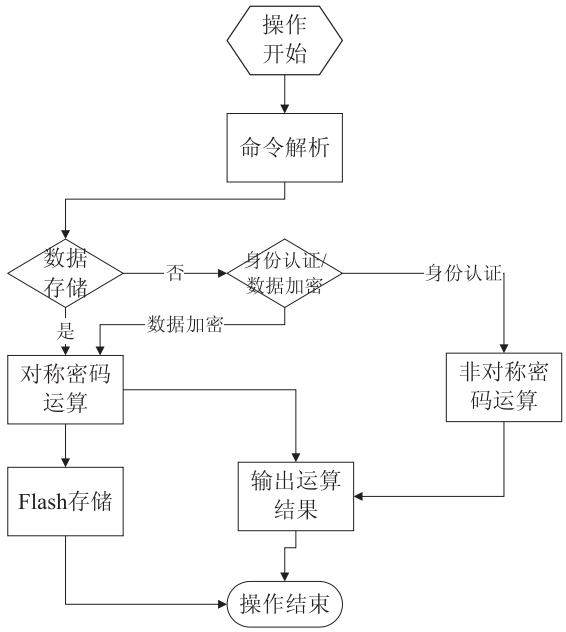

图 2 TF Key 的工作流程原理图

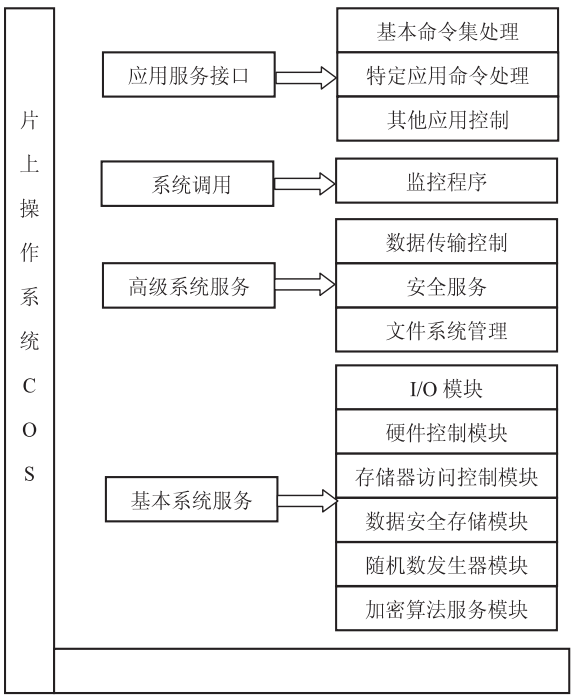

图 3 冀科 TF Key 的 COS 功能列表

应用层:为用户提供数字证书申请、使用、签名/验证、加密/解密等相应功能的 API(Application Programming Interface,应用程序编程接口)接口。客户端应用软件通过 MS CSP(Microsoft Cryptographic Service Provider,微软加密服务提供程序)或 PKCS(Public Key

Cryptography Standards,公开密钥密码标准)#11 接口对加密卡进行访问,建立手机信息安全体系。

本系统正是利用了冀科 TF Key 所提供的高效的身份认证、高强度的加解密服务,实现了基于 WPKI 与 DRM 等技术的智能手机信息安全存储系统。由于采用的是由国家密码管理局指定的 SM1、SSF33 等对称加密算法与 RSA、ECC(Elliptic Curve Cryptography,椭圆曲线加密算法)[9,10]非对称加密算法,并且所有算法都是由冀科 TF Key 硬件实现,因此,本系统可为智能手机用户提供安全、高效、快捷的加解密服务。

2　结束语

随着移动通信技术的迅猛发展,集通讯、电子商务、网上银行、掌上办公、随身娱乐等于一身的智能手机也迅速普及。在人们享受智能手机给生产生活带来的极大便利的同时,也逐渐认识到智能手机安全问题也越来越成为制约智能手机广泛应用的重要因素。

鉴于隐私数据外泄对个人用户及企业用户都会造成不可估量的损失,同时,考虑到现在智能手机有限的计算能力,文中研制了基于 WPKI、DRM 及冀科 TF Key 的智能手机信息安全存储系统。该系统充分利用 WPKI 与 DRM 中成熟的技术,借助独立的冀科 TF Key 作为运算单元,实现身份认证及加解密运算功能。该安全存储系统可为用户提供由国家密码管理局指定的 SM1、SSF33 等对称加密算法与 RSA、ECC 等非对称加密算法,提供保护的高效的身份认证及高强度的加解密服务,使智能手机用户在享受本系统带来的高强度的安全保护的同时,又不必饱受漫长的等待之苦。本系统特别适用于对安全性要求较高的电子商务、网上银行、网上购物等 3G 应用场合。

参考文献:

[1] 桂佳平,周雍恺,沈　俊,等. 基于智能手机恶意代码防范模型的研究[J]. 计算机技术与发展,2010,20(1):163-166.

[2] 宋　杰,党李成,郭振朝,等. Android OS 手机平台的安全机制分析和应用研究[J]. 计算机技术与发展,2010,20(6):152-155.

[3] 张　玮. 移动电子商务安全中 WPKI 证书查询机制研究[D]. 北京:北京邮电大学,2007.

[4] Chen Lunyong, Li Chunqing. Discussion and Application of WPKI Technology[J]. Modern Applied Science,2007,4(1):50-54.

[5] 张跃进,谢　昕,黄德昌. 基于 WPKI 的 3G 认证方案的研究与实现[J]. 华东交通大学学报,2008,25(3):88-91.

[6] 范科峰,莫　玮,曹　山,等. 数字版权管理技术及应用研究进展[J]. 电子学报,2007(6):133-141.

[7] Pucella R,Weissman V. A Logic for Reasoning about Digital Rights[C]//Proceedings of 15th IEEE Computer Security Foundations Workshop (CSFW'02). [s. l.]:[s. n.],2002:282-294.

[8] 黄　成,汪海航. 智能卡在 WPKI 中的应用研究[J]. 计算机技术与发展,2007,17(12):154-156.

[9] 李　姜. 基于 ECC 的组合公钥技术的研究与实现[D]. 太原:太原理工大学,2007.

[10] Afreen R,Mehrotra S C. A Review on Elliptic Curve Cryptography for Embedded Systems[J]. International Journal of Computer Science & Information Technology,2011,3(3):84-103.

(上接第 115 页)

vey of information security[J]. Science in China Series:E (Information Security),2007,37(2):129-150.

[3] 刘　皖,谭　明,郑　军. 基于平台可信链的可信边界扩展模型[J]. 计算机工程,2008,34(6):32-34.

[4] 胡中庭,韩　臻. 操作系统安全可信链的研究与实现[J]. 信息安全与通信保密,2007(2):47-49.

[5] Shen Changxiang,Zhang Huanguo,Feng Dengguo,et al. Survey of Information Security[J]. Science in Chian Series F,2007,50(3):273-298.

[6] 张京楣,金　妍. 基于对等网络的信任模型[J]. 济南大学学报(自然科学版),2002,16(4):46-47.

[7] 杨　涛,陈福接,沈昌祥. 一个安全操作系统 S-UNIX 的研究与设计[J]. 计算机学报,1993,16(6):409-415.

[8] Bell D E,LaPadula L J. Secure computer systems:mathematical foundations[R]. Bedford, MA:Electronic Systems Division,Air Force System Command,Hanscom AFB,1973.

[9] 陈志平,雷　航,杨　霞,等. 嵌入式安全操作系统的研究和实现[J]. 计算机工程,2007,33(1):83-85.

[10] 陈幼雷. 可信计算模型及体系结构研究[D]. 武汉:武汉大学,2006.

[11] 吴兴勇. 嵌入式操作系统安全保障技术研究[D]. 成都:电子科技大学,2003.

[12] 刘威鹏,张　兴. 基于非传递无干扰理论的二元多级安全模型研究[J]. 通信学报,2009,30(2):52-58.

[13] 王　飞,刘　毅,李　勇. 基于无干扰原理的终端安全模型研究[J]. 武汉大学学报:信息科学版,2008,33(10):1092-1094.