基于CPU智能卡技术的加油机系统设计

龚茜茹
(河南工业职业技术学院 计算机工程系,河南 南阳 473009)

【摘 要】针对M1智能卡存在着被复制和破解的风险,从实践出发,对基于CPU智能加油机系统的进行了详细的设计。包括智能卡芯片的选择、终端机系统整体设计、智能卡身份认证系统设计、在线交易的实现。最后对基于CPU智能卡技术加油机进行了详细的论证。

【关键词】加油机;RFID;CPU智能卡;安全;数字签名;设计
【中图分类号】TP311.521 【文献标识码】A 【文章编号】1673-1891(2013)02-01040-04

引言

业界通常认为,Mifare经典芯片(简称M1芯片)的安全性主要依赖其算法的安全性,虽然理论上认为M1芯片存在着安全隐患,但是一直没有证实。因此,以M1芯片为载体的一卡通在我国的各个行业得到广泛的应用。2008年,德国研究员亨里克·普洛茨和美国弗吉尼亚大学计算机科学在读博士卡尔斯滕·诺尔,在工程实践中破解了M1芯片安全算法[1]。因此,传统的M1卡为载体的加油机也急需升级。同时,由于时代的发展和业务的需要,传统的加油终端机显现出越来越多的缺点来:交易时没有使用电子签名进行身份认证,不符合《中华人民共和国电子签名法》;交易过程没有公证机构参与,很容易造成税收漏洞;无法与银行实现连接,不能使用电子银行;无法实现目前多种业务的综合经营。因此,从多种角度考虑,原来使用M1智能卡的自助加油终端,必然要对卡片和终端机进行升级。升级方案之一是改用更为安全的CPU智能卡来替代传统的M1卡[2]。

2 智能卡系统

2.1 卡片的选取

智能卡通常分为以M1卡为代表的普通智能卡(即逻辑加密智能卡)[3]和带有CPU和操作系统的CPU智能卡。除此之外,无源的RFID近年来也在各个行业也得到广泛的应用。

M1卡也就是Mifare卡。M1卡是我国各大中城市普遍使用的公交卡,学校使用的校园卡,公路使用的缴费卡,商场餐厅使用的消费卡。它占我国非接触智能卡市场的95%,发卡量在中国已超过1.5亿。由于存在已经证实的安全隐患,所以处于立即淘汰的地位。

RFID的大多数属于带有存储器的普通智能卡,使用中会涉及到隐私保护以及安全问题,由于无源RFID系统没有读写能力,所以无法使用密钥验证方法来进行身份验证。因此只能应用到对安全要求较低的场合,如门禁、公路收费等小额交易。

CPU智能卡内具有中央处理器(CPU)、随机存储器(RAM)、程序存储器(ROM)、数据存储器(EEPROM)以及片内操作系统COS(Chip Operating System)。由于CPU智能卡具有单独的COS(芯片操作系统)[4],并且可以灵活进行COS的裁剪和订制。因此,在芯片自身和COS层面提供了双重的安全保障。所以成为升级的必然选择。但是由于其价格较贵,需要设计终端机的读写设备,因此,其应用受到很大限制。

2.2 基于CPU智能卡技术的其它系统

目前,CPU智能卡在其它系统上已经开始应用。如预付费电表系统[3],水、电、气多表一卡管理系统[5],甚至还有非接触性的CPU智能卡系统[6]。由于使用了CPU智能卡,这些系统安全性高于使用其它卡片的系统。

2.3 基于其它技术的加油机系统

目前,加油站广泛使用51单片机控制的M1卡加油机系统[7],由于嵌入式技术的不断发展,出现了嵌入式控制的M1卡加油机[8]。这些加油机系统技术比较成熟,价格便宜。但是安全性无法得到保障,无法实现多种业务融合。

3 系统整体设计

系统采用基于公网的在线电子交易系统,由加油机、数据中心和公共网络组成。

3.1 加油终端机的结构

3.1.1 传统加油机结构

由于实现功能比较简单,加上原来计算机价格比较昂贵(相对于单片机和当时的劳动力价格),因此,传统的加油终端多为51单片机控制的终端。

这种加油机的工作原理非常简单[7],即在保证

收稿日期:2013-04-22
作者简介:龚茜茹(1978-),女,河南南阳人,讲师,计算机科学工程硕士,研究方向为计算机应用。

油泵、油气分离器、计量器等部件保持原有的结构和性能不变的情况下,通过主控板(或者单片机或者计算机)完成加油机的自我检测、加油计量、定量控制、显示加油数据、执行键盘命令等多项工作,从而带动油泵和油枪、完成加油任务。

3.1.2 CPU智能卡加油终端机的结构

CPU智能卡加油终端机的总体结构与传统的加油终端机类似,电气控制部分采用相同的结构,计算机控制部分、供电部分以及显示部分,进行改进[9]。

改进后的CPU智能卡加油机的计算机控制部分硬件结构如图1所示。

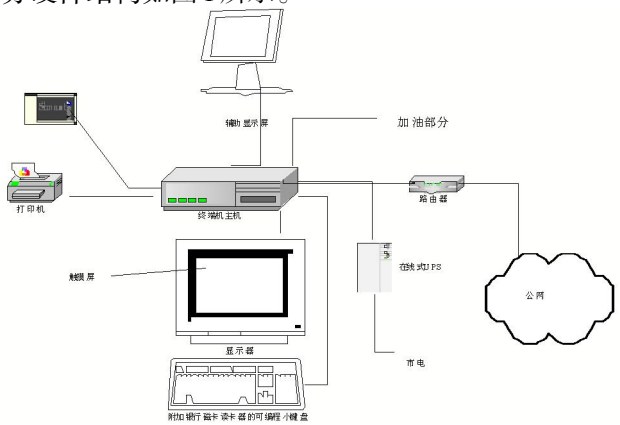

图1　加油终端机结构图

3.2 交易系统的结构

为了保证数据的安全,终端机和数据中心采用VPN进行连接。如果需要,VPN可以移动环境使用[10]。

整个终端机交易系统的结构如图2所示。

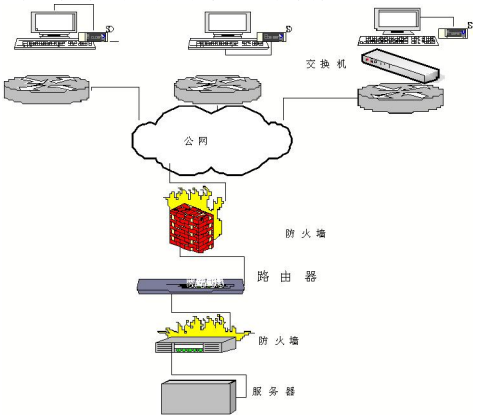

图2　交易系统结构图

该系统由终端机、通信网络和数据中心组成。加油机中的数据,经过VPN加密之后,通过路由器、防火墙接入公网。

4 硬件的选择

4.1 终端机机箱选择

采用专门定制的高强度主机机箱。在主机机箱的外部,任何外部设备的端口都被封闭到机箱内部,外部不能直接使用。比如USB、键盘接口。该主机箱安装特殊的主机锁,并且加有易碎标签,保证没有授权的用户不能打开机箱。这样,只要主机没有被非法破坏,只有数据中心维护人员才可以打开机箱。

4.2 键盘和鼠标的选择

采用专门的可编程小键盘和触摸屏。系统不直接支持普通的键盘。可编程键盘是一种可以根据需要随时定义功能的小键盘。可以把必要的功能定义到合适的按键(或者组合)上,不必要的功能不进行定义。这样,用户的操作比较简单,可以用简单的按键代替PC键盘上复杂的操作。同时,恶意的用户很难进行除了可编程小键盘定义功能之外的操作。

4.3 主板的选择

主板采用工控机主板。加油站工作环境非常恶劣,高温、潮湿加上存在加油混合气体,对系统的正常工作造成了极大威胁。由于系统对稳定性要求比较高,一般的PC机主板在温度和湿度以及电路发生变化时,工作可能不太稳定。工控机的技术指标比一般的主板高出很多,缺点是价格比较高。

4.4 小票打印机的选择

小票打印机采用专门的高精密度打印机。小票是交易的凭证之一,也是开具发票的依据,由于属于自助打印,为了防止伪造小票,所以采用高精度打印机。该打印机可以打出极其细微的保密字母。在每种票据上,每张票据上都有对应的英文字母,每换一批票据,对应的英文字母就会被更换。该字母只有在高倍放大镜下才能看到。

4.5 显示屏的选择

由于终端机的特殊工作环境,显示器采用工业级的嵌入式显示器,与普通显示器相比,工业显示器在整机稳定性(包括使用时间、抗干扰等)、制作材料上有很大差别。

5 终端机登录系统的实现

智能卡登录系统完成管理用户登录工作。当用户向读卡器中插入智能卡的时候,系统读取卡的内容并进行验证,如果验证通过则允许用户登录系统,如果验证失败则向用户提示相关信息。

5.1 卡片认证实现

要实现卡片身份认证工作,首先要完成智能卡的配置工作和智能卡内容的设计,然后编写合适的智能卡认证PAM模块,最后进行配置就可以完成智能卡认证工作了[11][12]。

5.2 智能卡身份认证系统工作流程

本智能卡身份认证系统工作流程如图3所示。

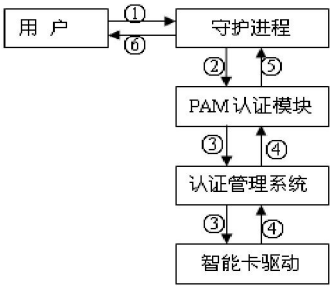

图3 身份认证系统工作流程

6 在线交易的实现

随着燃油税的推行,在加油系统设计过程中,引入可信任的第三方成为当务之急。如果交易过程没有采用可信任第三方作为交易的公证机构,当发生纠纷时极容易引起人们的置疑。所以客观上需要可信任第三方公证机构的出现。

图4是有可信任第三方参与的交易系统的结构图[13,14]。

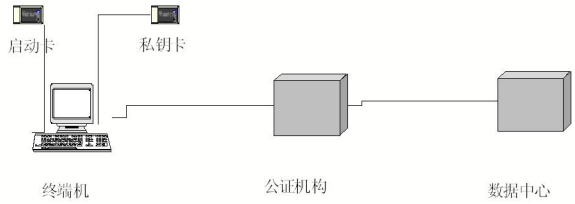

图4 有可信任第三方参与的交易系统

其实,这是一个有仲裁的数字签名系统。在终端机中,私钥卡保存用户的私钥,也就是用户使用的智能卡。假定用户卡为X,数据中心为Y,公证机构为A。在系统中,X、Y之间都有对方的公钥和相应的用户信息,可以使用公证机构颁发证书来证明自己的身份。具体过程如下:

X->A: IDx||EKRx[IDx||EKUy(EKRx[M])]

A->Y: EKRa[IDx||EKUy[EKRx[M]]T]

解释如下:当发送交易信息M的时候,首先用户卡内部对M进行加密,然后在计算机内部用Y的公开密钥EKUy对消息进行加密,形成一个经过签名且保密的消息。然后将启动卡的ID号码(唯一的不可以更改的号码)和本信息用KRx加密后一起发给公证机构A。

A:验证X签名的有效性。如果有效,则通过KRa加密之后发送报文,报文上添加有公证机构的时间戳。同时,A备份密文和时间戳。

数据中心Y在收到消息后,先用KUa解密,得到A的ID号码和时间戳;检查ID号码和公钥的对应关系,如果正确则解密得到正确格式的交易信息。

7 基于CPU智能卡技术加油机的论证

在加油机的设计中,与传统使用单片机或者嵌入式M1智能卡的加油机相比,使用CPU智能卡技术的Linux加油机具有以下优点:

7.1 符合法律规定

按照2005年4月1日生效的《电子签名法》的要求,交易必须有符合法律规定的载体:比如使用智能卡[15]。可信任第三方的引入,可以有效避免燃油税的实施带来的税收风险。

7.2 操作系统的安全

目前国内大量使用window平台,Windows Server 2003提供了智能卡身份验证的技术的支持,国内不少厂家也提供了相应的硬件产品(eKey),使得智能卡在windows领域的使用非常方便。但是,windows的稳定性非常不适合电子交易,而层出不穷的病毒和木马给交易带来了很大的风险。基于系统安全、知识产权等方面的考虑,开源的linux系统平台成为不错的选择。

7.3 交易本身的安全

电子交易的虚拟性,必然要求交易本身要具有完整性和不可抵赖性。在本系统中,使用带有公证的数字签名系统,具有完整性和不可抵赖性。

7.4 可扩展性

由于嵌入式技术的迅猛发展,以arm为代表的嵌入式芯片占领了很多控制市场。嵌入式芯片低价格、低功耗、开发成本低,因此非常适合更关注成本和功耗的领域使用。但是由于其性能比较差(如广泛使用的arm9,其主频只有203M),可扩展性差(每个应用都要单独开发),因此不适合承载多种业务加油机的使用。

8 结束语

毋庸置疑,由于M1卡遭到破解,包括加油站在内的电子交易系统受到空前的威胁,CPU智能卡即将成为主流。但是,目前快速推广却困难重重。首先,由于在国内传统M1卡没有真正遭到实质性破解的案例;其次,很多公司在竞争中形成了利益联;从加油机交易系统本身来说,也存在着不够成熟、成本过高的问题;另外外部环境也不够理想:例如,央行迟迟没有实现类似“支付宝”的交易工具,公证机构也没有现成的公证模型,没有全国统一的数字签名系统等等。但是,新技术必然要替代老的技术,CPU智能卡加油机未来必将得到大规模的推广使用。

注释及参考文献:

[1]张洁.关于CPU卡安全性能的研究[J].计算机时代,2011(10):18-19.

[2]佟秋利.CPU卡或成主流[J].中国教育网络,2009(7):15-17.

[3]陈作炳,张鸿宇,陈燕飞,等.CPU卡技术及应用系统设计研究[J].武汉理工大学学报,2002(9):85-87.

[4]Bruce Schneier著.应用密码学[M].北京:机械工业出版社,1999.

[5]袁怀民.基于智能卡的多表一卡管理系统的研究[J].计算机工程,2007(11):247-248.

[6]张建军,包国峰,马一兵.FM1208非接触CPU卡读写系统的研制[J].单片机与嵌入式系统应用,2009(12):56-59.

[7]吴生武.IC卡加油机结构组成及其应用[J].计算机与现代化,2004(6):109-110.

[8]邢远秀,于继武,方明.嵌入式加油机刷卡系统的研究与开发[J] .武汉理工大学学报,2006,30(5):923-926.

[9]向婕.嵌入式加油站前庭控制器研究及设计[D].重庆大学,2008.

[10]张平,纪阳.移动泛在业务环境及其体系架构设计的挑战[J].北京邮电大学学报,2005:(5):1-3.

[11]Mario Strasser and Martin Saegesser, smartcard-login Documentation.2001.[DB/OL].[2007-09-01] http://www.kernel.org/pub/Linux/libs/pam/

[12]ISO. SmartCard standard.2003.[EB/OL]. 2007 .7. http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx.

[13]孙萧寒.基于可信第三方的即开型电子彩票方案[J].信息安全与通信保密,2009(8):65-66.

[14]卿斯汉.安全协议20年研究进展[J].软件学报,2003(10):1740-1752.

[15]中华人民共和国电子签名法.[Z/OL].2005.7. http://www.miit.gov.cn/.

Refueling System Design based on CPU Integrated Circuit Card Technology

GONG Qian-ru

(Department of Computer Engineering, Henan Polytechnic Institute, Nanyang, Henan 473009)

Abstract: For the risk of being copied and cracked of M1 IC card, a detailed design is made for the refueling system based on CPU IC. It includes the choice of the IC card chip, terminal overall system design, CPU IC authentication system design and the realization of online transactions. Finally, a detailed argumentation is made on the refueling system based on CPU IC technology.

Key words: Refueling; RFID; CPU IC card; Security; Digital signature; Design