文章编号:1671 - 6833(2013)03 - 0098 - 04

基于 NFC 技术的智能海报安全实现

陈 静[1], 赵云雁[1], 张志鸿[1], 李 平[1,2]

(1. 郑州大学 信息工程学院, 河南 郑州 450001;2. 信息工程大学 密码工程学院, 河南 郑州 450001)

摘 要: 近场通信(Near Field Communication,NFC)智能海报是 NFC 技术主要应用之一,而如何保证智能海报中信息的安全成为了各应用厂商关心的主要问题. 首先,讨论了 NFC 标签和智能海报中存在的安全问题. 其次以校园快餐订餐系统为例,利用 NFC 标签技术及其记录类型设计了一种用于实现订餐功能的智能海报 NDEF(NFC Data Exchange Format)报文格式. 在此基础上,将 RSA 密钥体系应用于签名记录中实现了对智能海报中信息的签名,并详细描述了订餐信息读写模块的实现流程.

关键词: 近场通信;智能海报记录;签名记录;NFC 数据交换格式;校园订餐系统

中图分类号: TP311,TP309.2 **文献标志码**: A doi:10.3969/j.issn.1671 - 6833.2013.03.024

0 引言

传统的海报主要以纸质材料或显示屏等作为媒介实现信息的表达,其缺点是当用户想要记录海报的信息时,需要自己动手将信息记录下来. 而智能海报则实现了利用用户个人智能手机下载信息,甚至与用户交互的功能. NFC 技术因其兼容性和低成本等优点而成为实现智能海报的一种标准. 2008 年奥地利应用科学大学的 NFC 研究实验室推出了一种利用 NFC 技术的智能海报 ,通过将具有 NFC 功能的手机靠近海报上的标签(Tag),路人就可以扫描海报并下载有关奥地利 Hagenberg 旅游小镇的文字和图片.

随着 NFC 技术的成熟和推广以及智能海报的多功用性,越来越多的地方使用它作为信息的载体,如何保证智能海报内信息的安全随之也成了备受关注的问题. 标签制造厂商在标签的物理制作过程中遵循 ISO/IEC14443 协议,在硬件层解决其初始化和防冲突的问题以保证通信的安全. 刘志武等人[1-2]提出在 NFC 设备与智能海报通信过程中建立一个安全可信的通道,并在通信过程中采用加密协议来保证信息的安全.

笔者则利用签名记录实现了对智能海报中敏感信息的直接加密,将密钥体系和 JAVA API 中的加密算法引入智能海报. 以校园智能海报订餐系统(Campus Smart Posters Reservation System,CSPRS)为例说明 NFC 给出的标签数据格式,重点分析了 NFC 标签和智能海报中的安全问题,提出将 RSA 密钥体系应用于数字签名记录中来保证智能海报中的敏感信息不被篡改.

1 系统架构

CSPRS 应用涉及到三个角色:学校师生、快餐店和标签管理者. 学校师生利用拥有 NFC 功能的智能手机读取智能海报标签中的信息;快餐店将自己的订餐信息发布给标签管理者;标签管理者利用 NFC 读写器在标签中写入智能海报标签信息. 在该应用系统中,学校后勤处作为标签管理者在校园标签粘贴栏中安装标签并负责信息写入. 图 1 为该应用的技术架构.

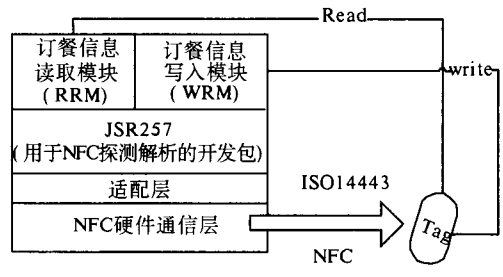

图 1 CSPRS 系统的技术架构

Fig. 1 The technical architecture of RRM

NFC 硬件通信层[3]主要由一个 NFC 控制器、

收稿日期:2012 - 11 - 20;**修订日期**:2013 - 01 - 07

基金项目:国家科技重大专项项目(2009ZX03001)

作者简介:陈静(1977 -),女,河南禹州人,郑州大学讲师,博士研究生,主要从事物联网、移动信息安全研究,E-mail:iej.chen@qq.com.

安全单元和天线构成的通信模块，安全单元根据应用需求不同可以选择 SIM、SD、SAM 或其他芯片. 架构上层的开发包则提供关于 NFC 数据交换格式(NFC data exchange format，NDEF)消息的探测方法和解析机制. CSPRS 中的订餐信息读取应用(Read Reservation Module，RRM)安装在用户的智能手机上，订餐信息写入应用(Write Reservation Module，WRM)放入管理员的 NFC 写卡器中. 两个基本应用模块的具体实现以及签名记录的使用将在本文随后的章节中介绍.

2　智能海报标签安全性分析

2.1　智能海报标签技术

标签作为 CSPRS 中智能海报的物理载体，造价低廉，应用广泛，并可重复使用. 利用 NFC 标签技术实现 CSPRS 中的智能海报功能，如图 2 所示[4].

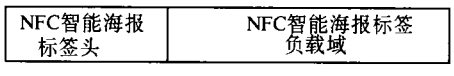

图 2　基本 NFC 智能海报标签格式

Fig. 2　The basic tag format of NFC smart posters

后勤中心将快餐店的订餐信息封装为智能海报标签的格式，写入标签. 用户需要先登录后勤中心的网站下载订餐信息读取软件和后勤中心的公钥，然后将智能手机靠近智能海报广告，就可得到快餐店的联系方式、订餐编号、折扣信息和信息有效期. 如图 3 所示，快餐店提供的信息是“tle = 0123456789，no = A11，disc = 65%，vali = 0930”. 其中 tle 表示快餐店的联系电话，no 为订餐编号，disc 是折扣信息，vali 是该信息的有效期.

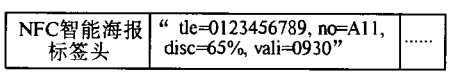

图 3　智能海报标签实例

Fig. 3　The instance of smart posters

2.2　智能海报标签的安全性分析

NFC 技术[5]虽然具有近距离通信的天然优势，但是无法保证订餐海报标签内的信息不被窃听或篡改. 一个非法 NFC 读写器有可能对一个未经安全保护的智能海报标签内容进行修改. 如果一个订餐海报标签被修改，用户将会被蒙蔽而去浏览一个看起来相似但有恶意导向的网页. 例如：在通过智能海报订餐时，电话号码有可能被另一个推销产品的号码代替以致用户买不到自己想要的快餐.

保证订餐海报标签的安全性，除了对它所处的物理环境安装必要的保护屏障外，更多的是要对订餐海报标签中的敏感信息采用必要的安全措施. 笔者提出一种方案：CSPRS 中后勤中心作为标签的统一管理者，所有提供快餐商家只有通过后勤中心才可以在标签上发布订餐信息. 这样系统可利用后勤中心的公私密钥实现标签信息的签名处理. 如果快餐店私自将自己的信息写入标签，RRM 应用会因为解密错误而报错，从而避免破坏者修改标签信息.

后勤中心从 CA 中心获取自己的私钥和公钥证书. 学生从校园网下载 RRM 应用安装在手机中，而后勤中心公钥证书同时被下载到手机的 SD 卡中. 在 WRW 应用中快餐店将订餐信息提供给后勤中心，后勤中心负责人利用写卡器将订餐信息、签名信息封装入 NFC 论坛给出的智能海报记录和签名记录中，并写入标签. 学生利用个人手机扫描标签，手机中已下载的 RRM 应用会自动分析标签的结构和内容，如果海报明文信息被篡改，则会因为与签名解密后的信息不一致而无法读取信息；如果破坏者试图修改签名信息，则会因为得不到后勤中心的私钥而签名无效. 分析可见，数字签名有效的保证了海报敏感信息不被篡改.

3　智能海报签名的实现

3.1　NFC 记录类型

在设备之间、NFC 论坛设备与标签之间以及标签之间封装交换信息的数据格式是 NDEF(NFC Data Exchange Format)消息，一个 NDEF 消息由一个或多个 NDEF 记录组成[7]. NFC 论坛给出多种不同的 RTD(Record Type Definition)，分别是：“U”URI 记录类型、“Sp”智能海报记录类型、“Sig”签名记录类型、“T”简单文本记录类型和“Gc”控制类型记录类型[7]. Sp 记录中必须包含一个 URI 记录[4].

如下图 4 所示，CSPRS 将快餐店提供给后勤中心的信息封装为 URL 记录，是明文记录.

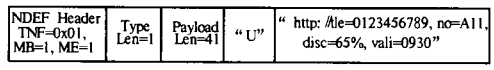

图 4　URI 记录

Fig. 4　The record of URI

然后将该记录封装为 NDEF 消息，如图 5 所示：

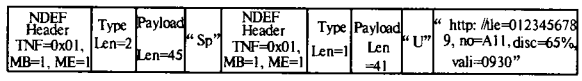

图 5　封装后的的智能海报消息格式

Fig. 5　The NDEF of packaged smart posters

两个封装操作是由 WRM 应用完成的,下一步笔者将实现该智能海报的数字签名.

3.2 智能海报数据格式中签名范围的讨论

签名记录可以是针对一个记录、一组记录或者整个消息的.假设是对图 5 中整个智能海报消息进行签名,签名将附加到最后,"SP"记录头中 ME 位将包含在签名范围内.如果不修改该 ME 位的值,签名记录无效;如果修改该值,则无法形成一个完整的智能海报消息,故不建议针对 MB 和 ME 位进行签名处理.有效载荷域作为实际数据的存储地址,是数字签名的核心保护对象.类型域决定负载域的类型,所以也要保证 Type field 的完整性.类型长度域和负载长度域如果得不到保护而被随意修改,该应用将无法准确定位负载域的字节数.综上所述,一个消息的有效信息位都需要得到保护.笔者将对图 5 中除智能海报消息头外的字节进行签名,即类型长度域、负载长度域、类型域和整个 URI 记录.

3.3 实现数字签名

NFC 论坛协议[8]给出的数字签名记录内封装了版本、签名和证书链 3 个数据结构.如图 6 所示,"Signature"域放签名后数据,"Certificate Chun"域放公钥证书.

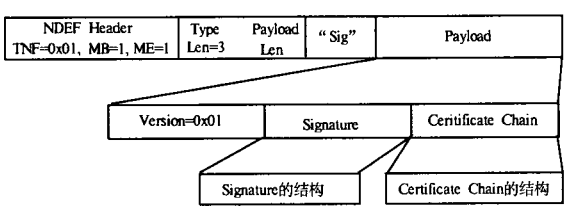

图 6 签名记录格式

Fig. 6 The NDEF of signature

"Sig"记录将与 URL 记录并列放入"Sp"记录的负载域中.

WRM 模块的功能包括:订餐信息的封装,签名记录的添加,以及标签管理者将消息写入标签,如图 7 所示.智能海报的实际编码是 ASCII 编码,通过编码转化后利用应用协议数据单元(Application Protocol Data Unit, APDU)指令写入标签[9].需要签名的字节首先经过 SHA 计算获得摘要,再利用 RSA 算法获得签名.将签名放入 Signature 结构中,完成签名记录的封装.最后重新对 URI 记录和签名记录进行封装,生成一个完整的具有签名记录的 NDEF 消息,写入标签.

RRM 模块是安装在用户手机中的应用模块,主要功能是读取并解析 NDEF 消息[10]、分析签名数据以及判断信息是否完整未被篡改,流程如图 8 所示.

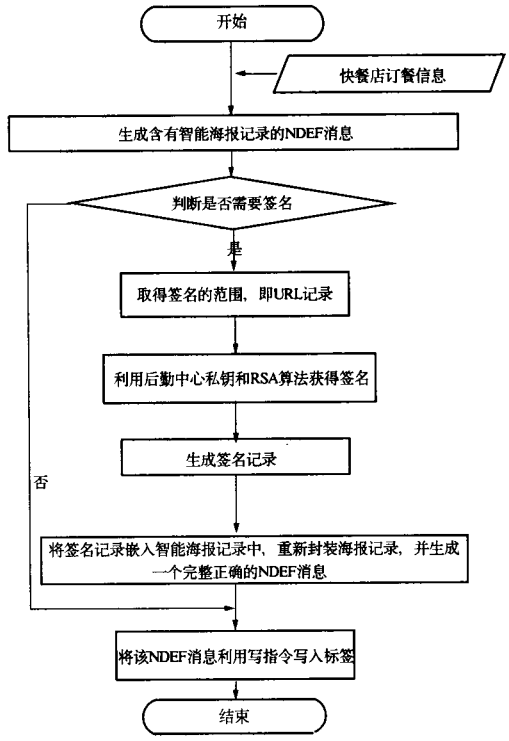

图 7 WRM 模块流程图

Fig. 7 The flow of WRM

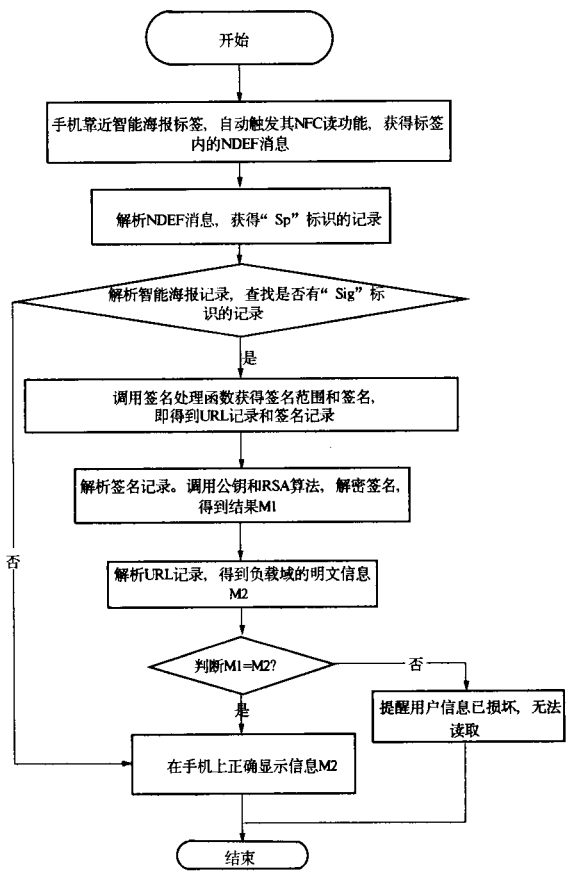

图 8 RRM 模块流程图

Fig. 8 The flow of RRM

RRM模块在探测到一个NDEF消息时将被自动触发,用户可以选择是否对探测到的标签进行读取.读取标签信息后,识别带有"Sig"标识的记录,从中得到签名.模块调用之前存入手机的标签管理者公钥和RSA算法解密签名[11-12],得到解密后的信息M1.将M1和URI记录负载域中的明文信息M2对比,若一致,则用户可成功读取订餐信息;若不一致,则RRM模块提示用户:"信息已损坏,无法读取!".

在结束签名记录的相关处理动作后,利用Action记录可以打开用户手机的浏览器浏览该快餐店网站信息;也可以打开SMS功能实现订餐短信发送;还可以将读取到的订餐信息转化为一个书签保存在用户手机中,当他到快餐实体店消费时,出示信息即可.

4　结论

笔者以校园快餐店订餐为应用背景,利用NFC实现了CSPRS的整个系统架构,将订餐信息放入智能海报中,便于用户随时随地读取信息.另外从标签信息易被篡改以及签名范围的角度分析了该应用的安全性,利用NFC论坛签名记录实现了对信息的签名处理,并给出了具体实现流程.下一步的工作是研究关于智能海报中更多记录类型的应用,以及各种签名算法的实现和比较.

参考文献:

[1] 刘志武,李代平,湛德照,等.绑定式近场通信3GCOS安全性研究[J].计算机工程:2009(35):164-165.

[2] 刘姗姗.近距离通信安全研究[J].中国新通信:2010,12(9):30-31.

[3] HUTTER M, TOEGL R. A trusted platform module for near field communication [C]//2010 Fifth International Conference on Systems and Networks Communications. NewYork:IEEE Press,2011:136-141.

[4] NFC. Forum. Nfcforum - ts - smartposter_rtd_1.0 [S].2006.

[5] ROLAND M, LANGER J. Digital signature records for the nfc data exchange format[C]. Near Field Communication (NFC) 2010 Second International Workshop, NewYork:IEE Press, 2010,10 : 71-76.

[6] 陈卓,阮鸥,沈剑.网络安全编程与实践[M].1版.北京:国防工业出版社,2008:8-36.

[7] NFC Forum. Nfcforum - ts - ndef_rtd_1.0[S].2006.

[8] NFC. Forum. Nfcforum - ts - signature_rtd_1.0 [S].2006.

[9] CHENG Hsu-chen, LIAO Wen-wei, CHI Tian-yow, et al. A secure and practical key management mechanism for NFC read-write mode[C]//Advanced Communication Technology (ICACT),2011 13th International Conference, NewYork: IEEE Press, 2011: 1095-1100.

[10] MARKUS K. Digital signatures on nfc tags[D]. Stockholm, Sweden: Reyal Instinte of Technology (KTA), 2009.

[11] 余桂贤,赵志强,薛阳,等.基于数字签名的安全电子商务交易系统的实现方法[J].华北科技学院学报,2010,7(2):89-93.

[12] 胡延军,仲亚丽,袁莎莎.云计算和自由视点视频相结合的实时监控系统[J].徐州工程学院学报:自然科学版,2012,27(1):65-70.

Security Implementation of Smart Posters Based on NFC

CHEN Jing[1], ZHAO Yun-yan[1], ZHANG Zhi-hong[1], LI Ping[1,2]

(1. School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China; 2. School of Cryptography Engineering, Information Engineering University, Zhengzhou 450001, China)

Abstract: Smart poster is one of the main application of NFC(Near Field Communication) technology, while the security of its payload is concerned by all users. First, the security problems of the NFC tags and smart posters are discussed in the paper. And then the Campus Smart Posters Reservation System (CSPRS) is proposed in the paper, which uses NFC tags and NFC record types to form the smart poster NDEF message for reservation. The RSA encryption scheme is used to signature the smart posters' payload and the implementation flows of reservation information reading and writing modules are described in detail in this paper.

Key words: NFC; smart poster; signature record; NDEF; CSPRS