第35卷 第23期 计 算 机 工 程 2009年12月
Vol.35 No.23 Computer Engineering December 2009
·安全技术· 文章编号：1000—3428(2009)23—0164—02 文献标识码：A 中图分类号：TP393

绑定式近场通信3GCOS安全性研究

刘志武[1]，李代平[1]，湛德照[2]，王 挺[1]，游剑锋[1]，周允强[1]，梅小虎[1]，郭鸿志[1]
(1. 广东工业大学计算机学院，广州 510090；2. 五邑大学，江门 529000)

摘 要：分析近场通信技术在应用上的安全问题和3GCOS系统的安全属性，针对卡的安全性问题提出解决方案。以3G的USIM卡为载体，采用近场通信技术把非接触的应用绑定在USIM卡上，在USIM卡中共存非接触应用的系统，并通过不同的接口实现方式与外界接触，实现不同的应用功能，制造出集成非接触应用的USIM卡。

关键词：3G通信；智能卡；卡操作系统；近场通信

Security Research of Bind Near Field Communication 3GCOS

LIU Zhi-wu[1], LI Dai-ping[1], ZHAN DE-zhao[2], WANG Ting[1], YOU Jian-feng[1],
ZHOU Yun-qiang[1], MEI Xiao-hu[1], GUO Hong-zhi[1]
(1. Faculty of Computer, Guangdong University of Technology, Guangzhou 510090; 2. Wuyi University, Jiangmen 529000)

【Abstract】This paper analyzes security problem of applying Near Field Communication(NFC) technology and 3GCOS system security-related issues, and proposes solution on the security problem. With 3G-USIM card as the carrier, using NFC technology to bind non-contact applications in USIM card, USIM card co-exist in the non-contact applications, systems and methods through different interface contact with the outside world to achieve different application functionality, which creates an integrated non-contact applications in USIM card.

【Key words】3G communication; smart card; card operating system; Near Field Communication(NFC)

随着3G时代的到来和移动电子商务的发展，手机不再局限于语音和短信功能，越来越多的数据应用应运而生，各国的研究机构和相关企业的研发部在不断开发新的产品。近场通信(Near Field Communication, NFC)[1]业务结合了近场通信技术和移动通信技术，实现了电子支付、身份认证、票务、数据交换、防伪、广告等多种功能，是移动通信领域的一种新型业务。近场通信业务改变了用户使用移动电话的方式，使用户的消费行为逐步走向电子化，从而建立了一种新的用户消费和业务模式。本文则采用NFC+USIM模式实现了绑定式近场通信3G智能卡操作系统3GCOS。

1 近场通信技术分析

近场通信由非接触式射频识别及互连互通技术整合演变而来，通过在单一芯片上集成感应式读卡器、感应式卡片和点对点通信的功能，利用移动终端实现移动支付、电子票务、门禁、移动身份识别、防伪等应用。在智能卡的发展中，安全问题是智能卡操作系统的核心部分，成为决定一个应用是否成功的重要因素。NFC应用存在链路层安全和应用层安全2个安全问题[2]。

(1)链路层的安全即NFC设备硬件接口间通信的安全。因为NFC采用的是无线通信技术，所以很容易被窃听。一方面窃听并不需要特殊的设备，另一方面标准是开放的，因此，攻击者能够轻松地解码监听到的信号。NFC设备的工作范围在10 cm以内，使得窃听设备与正在通信的设备之间的距离必须很近。由于同时受发起、目标和窃听设备的性能、功率等多方面影响，因此确切的距离很难确定。

(2)应用层安全包括数据的保密性和认证服务。数据的保密性是指信用卡、票据、个人身份等敏感数据可能根据不同的NFC应用而存储在移动设备中，以保证关键数据只能被合法的程序和用户访问。认证服务是指在应用过程中，移动设备往往还需要与其他设备或在线的服务进行交互，如电信运营商、银行交易支付系统，应在设备和服务提供者之间进行认证才能进行交互。

2 绑定式近场通信3GCOS的安全性

2.1 绑定式近场通信3GCOS

绑定式近场通信3GCOS可以实现3G移动业务通信、移动支付、电子票务、门禁、移动身份识别、防伪等应用。3G通信业务可以通过USIM卡、R-UIM卡实现。本文以USIM卡为载体，采用NFC技术实现绑定多应用功能，实现的系统结构如图1所示。

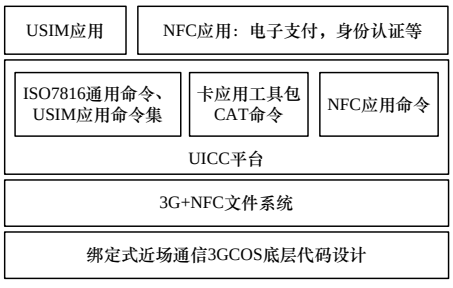

图1 绑定式近场通信3GCOS的结构

绑定式近场通信3GCOS中采用3G的UICC平台，支持USIM应用[3]、NFC应用。

基金项目：广州市越秀区自然科技基金资助项目(2008-GX-015)
作者简介：刘志武(1982－)，男，硕士研究生，主研方向：3G网络通信，智能卡，分布式并行计算；李代平，教授、博士；湛德照，工程师、硕士；王 挺、游剑锋、周允强、梅小虎、郭鸿志，硕士
收稿日期：2009-03-20 **E-mail：**l-zwu@163.com

2.2 USIM应用的安全性分析

(1)USIM 卡的安全鉴权

在 3G 通信系统中，USIM 卡采用双向鉴权机制，包含网络到 USIM 卡的鉴权以及 USIM 卡对网络的鉴权。比 2G 的单向认证更为安全，有效解决了卡与网络之间存在的问题。

USIM 卡的鉴权算法为非标准化算法[4]，运营商可以自行设计算法内核，但要满足一定的条件。本文采用 3GPP 推荐的基于 MILENAGE 算法[5]的鉴权算法，以 AES 算法为内核。鉴权算法包括一组算法：f0, fl, fl*, f2, f3, f4, f5, f5*。其中，f0 为随机数生成函数；fl 为消息认证码生成函数；fl*为重新同步消息认证函数；f2 在认证中用于计算期望响应值；f3 为加密密钥导出函数；f4 为消息完整性密钥导出函数；f5 为匿名密钥导出函数；f5*为重新同步匿名密钥导出函数。fl*和 f5*用于 MS 和网络失去同步的情况。

(2)加密算法

为防止破坏 USIM 应用和 NFC 应用接收和发送的数据的完整性和机密性[6]，以及保证卡内保存的重要数据的安全，USIM 卡通过用对称性加密算法、非对称性加密算法和散列算法等算法组合成 USIM 卡的 CryptoAPI 函数库。在 USIM 卡的 COS 运行时，调用这些 API 函数实现加解密、数据签名、校验、鉴权认证等功能，从而保证数据的完整性和机密性。针对 USIM 卡的加密算法 API 有利于解决卡的安全性、卡的内存空间不足、卡的运算效率等问题。

2.3 NFC应用的PKI认证

移动支付、电子票务、门禁、移动身份识别、防伪等应用认证方法一般采用 PKI 认证。基于 PKI 的身份认证技术主要包括数字签名、身份识别和信息的完整性校验等。PKI 是一种易于管理的、集中化的网络安全方案，支持多种形式的数字认证：数据加密，数字签字，不可否认，身份鉴别，密钥管理以及交叉认证等。PKI 可通过一个基于认证的框架处理所有的数据加密和数字签字工作。

3 安全性研究与安全实现

3.1 NFC安全问题的解决方法

(1) NFC 技术链路层安全问题[2,7]的解决

链路层安全问题的解决方案通过建立加密的安全信道很好地解决了窃听、篡改、插入等问题。因为不存在中间人攻击，所以在 NFC 的安全通信环境中，Diffie-Hellmann 协议可以很好地工作。

建立的安全信道中使用密钥交换协议，在通信双方间交换一个共享秘密值，并使用这些共享秘密值生成对称密码算法的密钥，然后使用该密钥对通信数据进行加密。在整个信道传输中，还需要建立一套完善的检测机制作为各项安全措施的基础才能实现 NFC 设备通信的安全。

(2) NFC 技术应用层安全问题[2,8]的解决

应用层安全问题的解决方案是通过采用专用的安全芯片来保证 NFC 使用过程中的安全性。专用的安全芯片用硬件实现较复杂的加解密算法，并在芯片中存储密钥，本文主要采用 NFC+USIM 模式实现。USIM 卡的芯片上存储移动电话个人化数据、加密密钥等内容，可供电信运营商对客户身份进行鉴权论证。另外，USIM 还保存了 NFC 相关的移动商务应用程序和安全密钥，以解决应用层的安全问题。

3.2 NFC+USIM模式

NFC+USIM 模式以 3G 的 USIM 卡为核心[9]，把 NFC 的应用放在 USIM 卡中，作为 UICC 平台的一种应用，确保运营商有效控制和管理业务。业务逻辑层与射频(RF)层分离，业务逻辑由 USIM 卡管理，而射频由内置于手机的 NFC 芯片进行管理。采用此模式可以很容易地在 3G 手机卡上实现其他应用，如在 USIM 卡上添加电子支付应用，可使 USIM 卡具有通信、交通消费等功能。NFC+USIM 模式实现方法如下：

(1)UICC 平台支持多应用。UICC 平台由 USIM 应用和 NFC 应用的命令集和文件系统等组成，方便 NFC 应用的添加，如添加电子支付、身份认证等应用，则使 USIM 卡具备相关的功能。

(2)双界面卡。硬件采用双界面卡的解决方案，由一个微 CPU 芯片和一个与微 CPU 芯片相连的天线线圈组成，实现把接触式与非接触式接口集为一体，2 种接口共享 USIM 卡内的同一个微处理器、操作系统和 FLASH，NFC 应用的程序和数据储存在 USIM 卡中。当要用 NFC 应用时，外部读写器产生的电磁场向非接触界面提供能量，通过射频方式实现能量供应和数据传输。另外，非接触界面并不影响接触界面兼容接触式应用系统和读写机具。实现如图 2 所示。

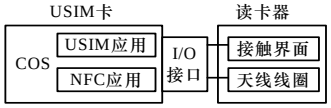

图 2 绑定式近场通信 3GCOS 的硬件结构

(3)安全实现。USIM 卡采用双向鉴权的认证方法，确保入网的安全性；通过文件安全访问机制防止文件的非法访问，有效保护了重要数据的安全。同时，绑定式近场通信 3GCOS 提供安全的逻辑通信和防火墙机制，各个应用能独立运行在一个安全的环境中。

本文研究的 NFC+USIM 模式已成功应用到华大电子股份有限公司和清华同方公司的芯片上，并且研究成果得到相关电信部门的鉴定，将应用于生产。

4 结束语

3G 网络和 NFC 技术在中国还没有得到广泛的应用，只有部分地区使用了近场通信业务，相应的技术在国内很薄弱。因此，本研究具有重大的意义。电信智能卡未来必将提供更大的存储容量、更高的通信速率、更强的计算能力以及更加完善的身份鉴权体系，电信智能卡的应用将会更广，但安全问题是关键。建立近场通信业务，进一步提高用户消费行为的电子化程度，将成为移动通信行业增值业务新的增长点。因此，需要进一步研究绑定式近场通信 3GCOS 及其安全性，给电信智能卡带来新的发展业务。

参考文献

[1] 许海翔, 伏京生. 近场通信技术拓展电信智能卡应用[J]. 今日电子, 2007, 12(12): 39-42.

[2] 吴思楠, 周世杰, 秦志光. 近场通信技术分析[J]. 电子科技大学学报, 2007, 36(6): 1296-1298.

[3] 3GPP TS 102.221-2007 Smart Cards; UICC-Terminal Interface; Physical and Logical Characteristics[S]. 2007.

[4] 3GPP TS 35.206-2007 3G Security Specification of the MILENAGE Algorithm: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions fl, fl*, f2, f3, f4, f5 andf 5*[S]. 2007.

[5] 3GPP TS 35.205-2007 3G Security; Specification of the MILENAGE Algorithm[S]. 2007.

[6] ISO7816-4. Security and Commands for Inter-changes[Z]. 2005.

（下转第 174 页）