基于AKA协议的USIM卡安全研究与实现

欧阳小星,李代平,梅小虎,马海峰
(广东工业大学 计算机学院,广东 广州 510006)

摘 要:智能卡芯片存储了用户的敏感数据,提高智能卡的安全性与保密性显得至关重要,关系着运营商与用户的切身利益。通过对3G中认证和密钥协商协议(AKA)的安全性研究,阐述了USIM COS的安全特性,分析了3G的安全体系,对智能卡芯片操作系统的安全模块进行了体系结构设计,实现了AKA鉴权算法,对文件访问控制、报文鉴别和数据加密通信等进行设计。实验结果表明该系统符合国际标准和行业标准,运行稳定,能进行数据出错检测和数据恢复,安全高效。

关键词:通用用户识别模块;文件访问机制;芯片操作系统;鉴权算法
中图分类号:TP311.52 **文献标识码**:A **文章编号**:1673-629X(2010)06-0167-04

Research and Implementation of Security of USIM Card Based on Protocol of AKA

OUYANG Xiao-xing, LI Dai-ping, MEI Xiao-hu, MA Hai-feng
(College of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: The USIM card stores private sensitive defense data of user and it is very important to enhance the security and confidentiality of data. By researching the security of authentication and key management of 3rd communication, analyzing the ciphering mechanism and principle, design security module architecture of chip operating system, implement the authentication algorithm of AKA, and design a file access control mechanism, message authentication, data encryption for communication. Experiment results prove that the system is validated to accord with international standards and industry standards, run stably, effectively and safely.

Key words: USIM; file access mechanism; chip operating system; authentication algorithm

0 引 言

随着第三代移动通信技术的飞速发展和普及,3G智能卡芯片操作系统(COS)是一个崭新的系统,针对卡片上层出不穷的新的数据业务,特别是对数据安全性提出了很高的要求,要求智能卡应具有更高的安全性、良好的兼容性和可扩充性。而COS的安全是它的最核心部分,包括网络与用户的相互鉴权,以及对文件的访问操作控制、安全状态的更新、数据加密、解密及数据完整性校验保护等,防止非法行为的访问与接入,具备高安全性,是COS设计的重点,对保障智能卡成功广泛的应用具有重大的研究意义。

文中论述了基于AKA协议的USIM卡COS安全的研究与实现过程。

收稿日期:2009-10-21;**修回日期**:2010-01-02
基金项目:广东省广州市自然科技基金项目(2008-GX-015)
作者简介:欧阳小星(1980-),男,江西吉安人,硕士生,研究方向为3G智能卡的研发;李代平,教授,研究方向为智能卡芯片操作系统、网络并行计算。

1 USIM COS安全体系结构

USIM COS系统是智能卡内软件的核心,具有良好的可维护性、可伸缩性和高安全性,各模块之间具有弱耦合性,分工明确,但又协同合作,安全性控制良好。文中设计的系统模型结构如图1所示。

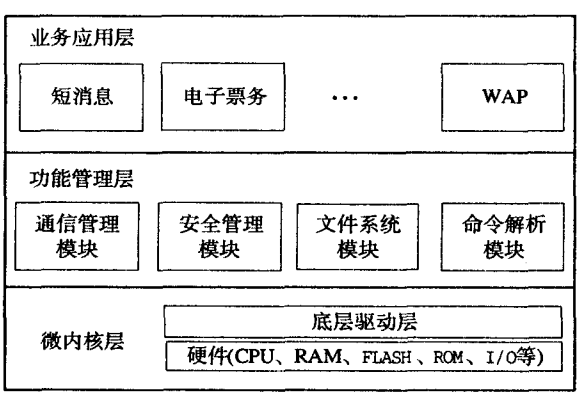

图1 USIM COS系统结构模型

其中,微内核层是根据硬件芯片的差异性,对不同芯片的驱动进行分析和编写,抽取其共同部分,生产时只需底层驱动程序的移植,便于上层代码的复用、移植

和扩展;通信管理模块负责与外界的数据通信,依据通信协议负责接收命令与返回响应数据,同时对命令接收的正确性采取奇偶校验、累加和分组长度检验等手段做出判断,不涉及信息内容的正确性校验;文件系统模块根据 ISO/IEC 7816 - 4 规范组织文件系统的逻辑结构,实现物理存储,完成文件系统初始化、更新、检索、创建、删除等操作;命令解析模块主要分析接收到的命令的可执行性,检查命令中的各项参数是否正确等,根据相应的命令类别 INS 执行相应的命令功能;安全管理模块是智能卡 COS 系统的核心部分,安全体系一般包含安全状态、安全属性、安全机制,主要实现网络与用户的相互鉴别与核实,数据的加密与解密,文件访问的安全控制,安全算法的实现,安全报文的传输等。鉴权的过程是终端向 USIM 卡发送鉴权命令,USIM 卡向终端产生响应数据,依靠多次交互实现鉴权。每个文件都有专门的安全访问规则,只有满足了安全规则的外部命令才允许执行此文件。USIM 的安全体系与一般智能卡的安全体系基本一致,但在实现上有一定的差别,其基本工作原理如图 2 所示[1]。

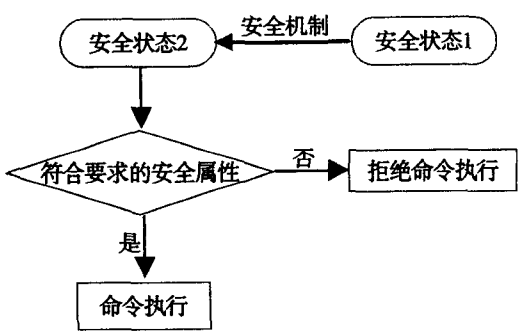

图 2 COS 安全体系

2 USIM 的认证与密钥协商机制分析设计

2.1 认证与密钥协商协议

USIM 卡系统执行认证与密钥协商协议 AKA[2],参与认证与密钥协商的主体包括用户终端 MS/USIM、访问网络 VLR/SN、归属网络 HLR/HE。AKA 采用双向的鉴权方式,用户和网络相互鉴权,二者共享秘密密钥 K,并且只存储在 USIM 卡和鉴权中心 AuC 中。另外,USIM 和 HE 各自跟踪计数器 SQN_{MS} 和 SQN_{HE} 以支持认证同步。SQN_{HE} 对于每一个用户都不同,保存在 HLR/AuC 中,SQN_{MS} 则保存在 USIM 中,是 USIM 接收到的最大序列号值。具体的认证与密钥协商机制如图 3 所示[2~4],执行步骤如下:

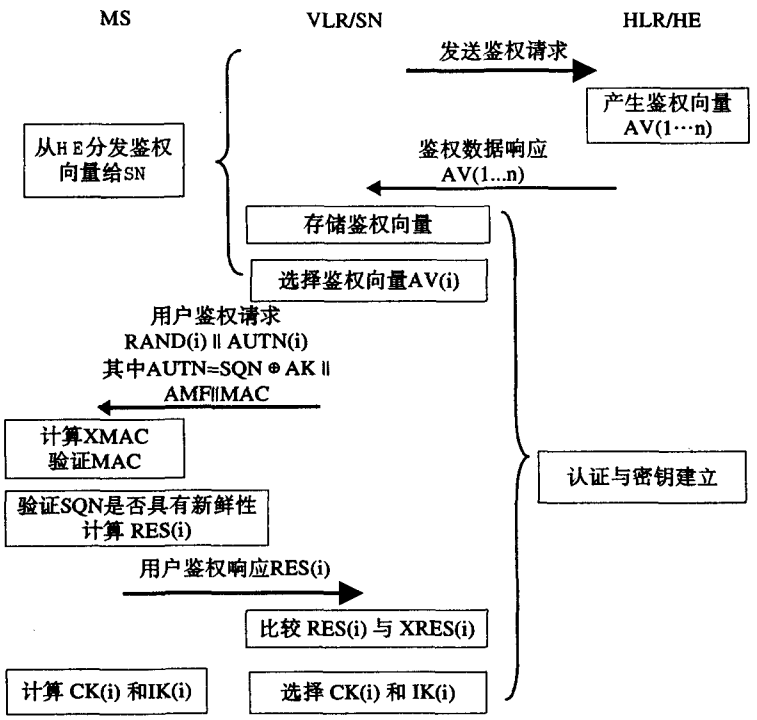

图 3 USIM 系统认证与密钥协商机制 AKA

1) HLR/HE 收到 VLR/SN 发送的鉴权请求,产生鉴权向量 AV,并通过响应的方式,返回 n 个有序队列的鉴权向量给 VLR,其中 AV 由 RAND(随机数)、XRES(期望响应)、CK(加密密钥)、IK(完整性密钥)、AUTN(鉴权令牌)构成。

2) VLR 选择下一个鉴权向量,并发送 RAND 和 AUTN 给用户,每一个 AUTN 包括:序列号 SQN,鉴权管理参数 AMF 和校验信息 MAC。

3) USIM 计算出匿名密钥 AK,由它恢复被隐藏的 SQN 序列值。

4) USIM 计算期望消息校验码 XMAC,与 AUTN 中的 MAC 进行比较,如果两者相同,转步骤 5;否则,发送用户鉴权失败信息给 VLR,USIM 鉴权过程终止。

5) USIM 验证序列号 SQN 是否在正常的范围内,如果 SQN 正常,转步骤 6;否则 USIM 发送同步失败消息给 VLR,USIM 鉴权过程终止。

6) 计算响应数据 RES,并发送给 VLR;VLR 将收到的 RES 和 XRES 进行比较,如果两者匹配,VLR/SN 认为鉴权成功。

7) 最后,USIM 计算出 CK 和 IK,两者密钥被 USIM 与 VLR 传送给执行数据加密和完整性功能的实体。

2.2 AKA 算法内核

AKA 协议中用到的算法为非标准化算法,由运营商自行设计,3GPP 给出了基于以 AES 算法为内核的

MILENAGE 算法集来设计与实现 AKA 算法。USIM 与 AuC 采用 AES 作为内核,采用 10 轮,分组长度和密钥长度均为 128 比特的 AES 实现 AKA 算法内核,AKA 包括一组 8 个算法:f0、f1、f1*、f2、f3、f4、f5、f5*,各算法的作用如下[5~6]:

1)f0,随机数产生函数;

2)f1,消息认证码生成函数,MAC = f1k(SQN ‖ AMF ‖ RAND);

3)f2,期望响应值计算函数,XRES = f2k(RAND);

4)f3,加密密钥产生函数,CK = f3k(RAND);

5)f4,完整性密钥产生函数,IK = f4k(RAND);

6)f5,匿名密钥导出函数,IK = f5k(RAND)。

网络端利用以上算法得到鉴权令牌 AUTN = SQN ⊕AK ‖ AMF ‖ MAC,以及鉴权向量 AV = RAND ‖ XRES ‖ CK ‖ IK ‖ AUTN。另外 f1*,f5 算法主要用于 MS 和网络需要重同步的 MAC 及 AK 产生情况。

2.3 SQN 新鲜性验证

3G 网络为了保证终端与网络服务端的通信同步,有效防止重放攻击,在 USIM 卡中保存前 $n-1$ 个接收的序列号 SQN_{MS},与网络端的 SQN_{HE} 比较,验证 SQN_{HE}的新鲜性,SQN 由 SEQ ‖ IND 构成,IND 代表着 6 比特的索引号,指示 USIM 中 SQN_{MS}(IND)值[2]。首先,判断网络侧的 SQN_{HE}是否大于 USIM 卡中的 SQN_{MS}(IND);如果大于,则 SQN_{HE}和 SQN_{MS}(IND)与 △的和比较,设 $SEN_{MS} = SQN_{MS}(IND) + \triangle$,其中,△值要足够的大,以确保不被攻击,文中取△为 2^{28}[2];如果 SEN_{MS}大于或等于 SQN_{HE}值,说明 SQN_{HE}具备新鲜性,USIM 与网络同步成功,否则同步失败。当 SQN 具备新鲜时,判断是否大于先前保存在 USIM 卡中 SQN_{MS}的最大值,如果大于,用此新鲜值替换 SQN_{MS}。

整个 USIM 卡鉴权过程实现的伪代码描述如下:

```
USIM AUTHENTICATION BEGIN
    writeUART(&INS,1);
    readUART(DAT, LEN) ; //首先读写串口,读取 APDU 带出的 DATA 数据,即鉴权数据 RAND||AUTN
    memcpy(rand,DAT+1,0x10) ; //取网络端发送的 128 bits 随机数 RAND
    memcpy(autn,DAT+18,0x10) ; //取 128 bits 认证令牌数据 AUTN
    memcpy(sqnandak,autn,0x06) ; //取 SQN⊕AK
    memcpy(amf,autn+6,0x02) ; //取 AMF
    memcpy(mac,autn+8,0x08) ; //取 MAC
    f2345 (key, rand,res,ck,ik,ak) ; //执行算法 f2,f3,f4,f5,计算出 RES,CK,IK,AK
    sqn=sqnandak^ ak ; //由 AK 恢复出 SQN
    f1(key,rand,sqn,amf,xmac) ; //计算出消息认证码 MAC
    if(memcmp(mac,xmac,8) = 0) //鉴权检测,校验 MAC
    {
    if(compareSQN(sqn) = 1) //验证网络传送的 SQN 是否在正常范围内
    {
    send_auth_re_data(res,ck,ik) ;//发送鉴权成功的响应数据,返回 RES,CK,IK
    }
    else
    { //同步失败! 发送错误报文 AUTS
    memcpy(sqn,sqnandak,6) ;
    milenage_auts(key, rand,auts,SQNmax) ;//由 f1*,f5*,生成错误报文,同时把先前成功接收的 SQN 最大值传给网络进行重同步
    }
    else
    {
    send_auts(rand,auts); //校验 MAC 不相等,发送错误报文 AUTS
    }
USIM AUTHENTICATION END
```

3 文件访问控制设计

USIM 卡的文件访问机制采用 PIN 引用关联实现安全访问规则与文件关联,并采用有效的安全访问规则编码,提高空间利用率。通过对各个文件访问规则的归纳、分析,发现不同的文件之间存在安全访问规则相同的情况,且编成记录号。对规则采用扩展方式编码进行引用关联,实现了访问规则对不同文件的共享,减少对存储空间的需求。扩展方式的编码采用 TLV 结构实现[7],即"标识 + 长度 + 值"的方式,把不同文件操作、安全条件和 PIN 码关联起来,组成一条访问规则,直接存放在访问规则存取文件 $ER_{ARR}0_X2F06$ 中,且在文件的 FCB 头信息中只标识访问规则记录号。当操作文件时,首先找到文件 FCB 中的访问规则记录号,然后,根据此记录号去 0_X2F06 文件中存取相应访问规则,从规则中获取具体的文件操作需校验哪个 PIN 值。本设计构造的文件访问条件控制能够很好地保护用户的私密数据,对非法访问进行限制。USIM 卡 COS 的文件系统的 FCB 结构设计如下:

```
Typedef struct
{
    unsigned short fileId ; //文件标识
    unsigned short fileSize ; //文件大小
    unsigned char fileDes[4] ; //文件描述符
    unsigned char firstRecordNum ; //指向第几条记录是第一条记录,用于环形文件
```

```
    unsigned char lifeCycstatus ; //生命状态
    unsigned char noOfDF ; //当前目录下的 DF 数目
    unsigned char noOfEF ; //当前目录下的 EF 数目
    unsigned char arr_ num ; //访问规则记录号(只保存文件 2F06 下的记录号)
    unsigned long parentDirAddr ; //当前目录的父目录
}FCB ;
```

4 仿真测试

USIM 卡的鉴权过程是 USIM 卡安全最核心的部分,关系到 USIM 与网络是否能正常安全通信。文中在华大微电子提供 HED－IC51 仿真器对 CIU51G256 芯片进行仿真,采用自行开发的 APDU 执行工具,根据返回状态字和数据,验证 AKA 的鉴权是否正确。

将个人化密钥写入 USIM 卡中,取值[8]为 K＝465b5ce8b199b49faa5f0a2ee238a6bc,APDU＝0088008 12210 23553CBE9637A89D218AE64DAE47BF351055 F328B43577B9B94A9FFAC354DFAFB3,其中 DATA 域包含 128 比特的 RAND 和 128 比特的 AUTN 值,即 48 比特的 SQN,16 比特的 AMF,64 比特的 MAC。鉴权成功的响应数据为 DB08A54211D5E3BA50BF10B40 BA9A3C58B2A05BBF0D987B21BF8CB10F769BCD7510 44604127672711C6D3441,其中 DB 代表成功执行 3G 鉴权[7~10],64 比特的 RES,128 比特的 CK 和 IK 值。鉴权结果如图 4 所示。

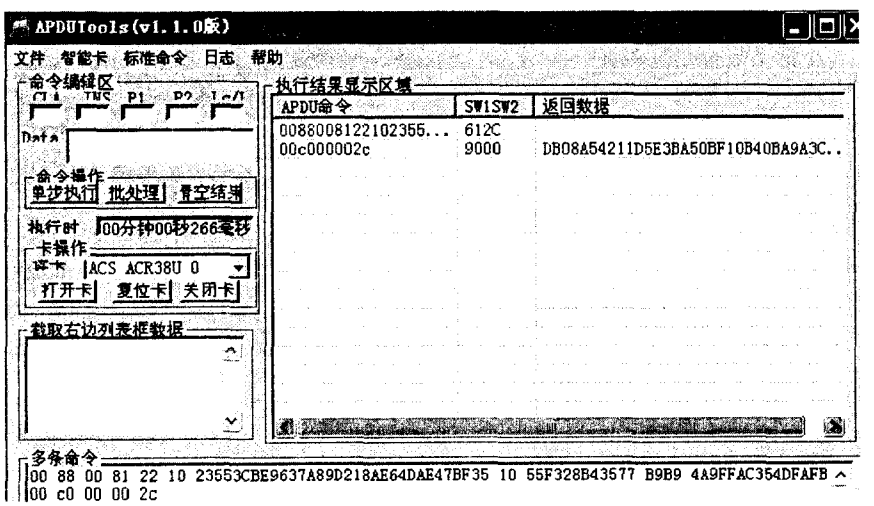

图 4 USIM 卡的鉴权仿真与测试

5 结束语

通过对 3GPP 技术规范和智能卡行业标准的研究,分析了 USIM 卡 COS 的安全管理机制,并成功设计和实现了基于 3G 网络的 USIM 卡 COS。该 COS 严格遵照 3G 标准,提供了用户与网络的相互鉴权,及数据的保密性和完整性保护机制,其安全性较高,并成功地应用于华大微电子 CIU51G256 芯片上,有利于国内的 3G 通信研究和发展。

参考文献:

[1] 刘志武.3G 智能卡 COS 安全的研究与实现[D].广州:广东工业大学图书馆,2009:21－22.

[2] ETSI TS 133.102,V7.1.0,Universal Mobile Telecommunications System (UMTS);3G security; Security architecture [S]. France: European Telecommunications Standards Institute,2006.

[3] 赵春泽.UICC 安全特性研究及实现[J].重庆邮电大学学报,2008(10):557－560.

[4] 崔宏伟.3GUSIM 卡的安全控制[J].山西电子技术,2006(6):45－57.

[5] 3GPP TS 35.205, V8.0.0,3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1 *, f2, f3, f4, f5 and f5 *;Document 1: General[S]. France : the 3rd Generation Partnership Project,2008.

[6] ETSI TS 102.221,V7.8.0,Smart Cards; UICC－Terminal interface; Physical and logical characteristics[S]. France: European Telecommunications Standards Institute,2007.

[7] 刘志武,李代平,容伟斌,等.3G 网络 USIM 卡的安全研究与实现[J].现代计算机,2008(7):16－19.

[8] 3GPP TS 35.208 ,V8.0.0,3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1 *, f2, f3, f4, f5 and f5 *;‖Document 4: Design Conformance Test Data[S]. France: the 3rd Generation Partnership Project,2008.

[9] 中国移动通信企业标准.USIM 卡技术规范[S].北京:中国移动通信集团公司,2008.

[10] 马奇学.WCDMA 网络的 USIM 卡研究与实现[D].北京:北京邮电大学图书馆,2005.