

智能卡操作系统的测试技术

谢晶晶, 李代平, 郭 琨

(广东工业大学 计算机学院, 广东 广州 510006)

摘 要:智能卡操作系统是智能卡能够支持复杂且安全的应用的基础,目前智能卡操作系统的测试并没有形成成熟的模式。为了在智能卡操作系统的开发中能够对操作系统进行全面并充分的测试,根据智能卡操作系统的体系结构特点、状态转移过程和通信方式,结合软件测试中的理论方法及测试技术,从基本功能、防拔插及耐久性三方面对智能卡操作系统的测试进行研究,给出了智能卡操作系统的测试方案。在 EVDO 卡的测试中表明,该测试方案是可行的。

关键词:智能卡操作系统;测试用例;EVDO 卡

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2010)08-0021-04

Test Technology in Chip Operating System

XIE Jing-jing, LI Dai-ping, GUO Kun

(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: Chip operating system is basis of smart card capable of supporting complex and security applications. Now, the testing process of chip operating system has not been formed a mature mode. In order to develop chip operating system capable of operating in a comprehensively and fully tested. Based on the architecture of chip operating system features, state transition process and means of communication, combined with the theory of software testing methods and testing techniques, from basic features, anti-plug and durability of three aspects of testing a chip operating system research, present the test program of chip operating system. The feasibility of test scheme is proved by the testing in EVDO COS.

Key words: chip operating system (COS); test case; EVDO card

0 引 言

具有稳定、可靠的卡内操作系统是智能卡正常工作的基础,智能卡操作系统(Chip Operating System)控制外界与智能卡之间的通信,管理卡片的存储空间,并且在卡内对于各种命令进行处理,所以在 COS 开发过程中有必要对 COS 进行充分且全面的测试。

COS 的主要特点:它是一个专用系统;COS 一般是根据某种卡片的特点以及应用范围来设计开发的,具有高可靠性;COS 所要完成的功能需遵循相关的国际规范以及行业规范;支持同一应用类型的 COS 往往遵循同样的规范,这使得 COS 的测试有一定的重用性。

以上特点决定了常规的软件测试方法不能直接用于 COS 测试。

1 智能卡操作系统

1.1 COS 组成结构

COS 的主要功能是从智能卡传出和传入数据,控制执行相关的命令,管理维护文件系统,管理与执行加密算法。其结构可划分为两个层次:功能层和微内核层。

功能层主要实现 COS 的业务逻辑,包含通信管理、安全管理、命令解释、文件管理四大模块^[1]。

1)通信管理模块:对输入缓冲区中收到的数据进行奇偶校验,以及对分组长度等进行正确性判断,但不对其内容进行判断,以 ISO/IEC 7816-4 中有关命令结构作为判断的标准;接收经过命令处理、文件管理处理、安全认证后的数据,并按照 ISO/IEC 7816-4 中有关命令结构要求将其打包成完整的结果报文,放入到输出缓冲区,发送结果报文。

2)安全管理模块:接受通信管理模块的调度,并将处理后的信息返回给通信管理模块;对通信管理模块接收的数据进行安全验证,但不对其内容进行验证,若安全验证失败,则直接返回验证失败。

收稿日期:2009-12-09;修回日期:2010-03-01

基金项目:广东省广州市自然科学基金项目(2008-GX-015)

作者简介:谢晶晶(1986-),女,江西南康人,硕士研究生,研究方向为智能卡操作系统;李代平,教授,研究方向为智能卡操作系统、软件体系结构、并行计算。

3)命令解释模块:接受安全管理模块的调度,并将处理后的数据信息(与命令相对应的响应代码)返回给安全管理模块;需要作数据内容上的鉴别(检查命令的各项参数是否正确),然后执行相应的操作,完成对卡内有关数据的操作,若对数据内容鉴别未通过,则直接返回错误码给通信管理模块。

4)文件管理模块:接受命令管理模块的调度;数据在卡内是以文件形式存在的,文件管理模块须提供文件的建立、修改、删除等基本操作,文件访问的安全控制等。

微内核的主要功能^[2]:为上层的功能层提供硬件支持,实现终端与卡内硬件的通信。微内核分为接口层、驱动层,接口层为功能层提供服务,将功能层的服务请求转化成对驱动层的调用,为功能层提供统一的接口。驱动层主要实现对底层硬件的各种驱动操作。

1.2 COS 的状态转移过程

各功能模块在完成特定请求的过程中可能还需要向其他功能模块发出请求。各模块之间是调度请求和数据响应的关系,在一对关系中调度请求表现为模块的输出,数据响应表现为模块的输入,调度和响应都用事务表示,事务所代表的是一组数据,以及对数据的操作。

系统请求/响应过程中的状态转换图,如图 1 所示。

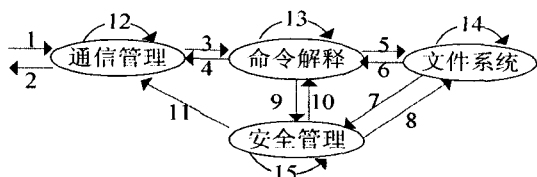


图 1 状态转换图

与其相对应的状态表,如表 1 所示。

表 1 状态转换表

| 状态 | 通信管理 | 命令解释 | 文件系统 | 安全管理 |
|------|-------|-------|-------|-------|
| 通信管理 | 事务 12 | 事务 3 | | |
| 命令解释 | 事务 4 | 事务 13 | 事务 5 | 事务 9 |
| 文件系统 | | 事务 6 | 事务 14 | 事务 7 |
| 安全管理 | 事务 11 | 事务 10 | 事务 8 | 事务 15 |

事务 1:智能卡收到终端的 APDU 请求;

事务 2:智能卡向终端发出的 APDU 响应;

事务 3:通信管理模块接收到 APDU 命令,进行校验后,调用命令解释模块对 APDU 指令进行处理;

事务 4:命令解释模块向通信管理模块返回处理后的数据或异常事件;

事务 5:命令解释模块在 APDU 命令的处理过程

中,需要访问文件而调用文件系统模块;

事务 6:文件系统模块将处理后的信息返回给命令解释模块;

事务 7:文件系统模块在对文件操作时需要进行安全控制时调用安全模块;

事务 8:安全管理模块在涉及安全性相关的文件时调用文件系统模块;

事务 9:命令解释模块向安全管理模块发出的响应事件;

事务 10:安全管理模块向命令解释模块发出的处理数据请求;

事务 11:安全管理模块向通信管理模块发出的响应事件或异常事件;

事务 12:通信管理模块为完成终端发出的 APDU 请求,向 COS 微内核发出的调用底层硬件接口请求;

事务 13:命令解释模块为完成安全管理模块请求,向 COS 微内核发出的调用底层硬件接口请求;

事务 14:文件系统模块为完成安全管理模块请求,向 COS 微内核发出的调用底层硬件接口请求;

事务 15:安全管理模块为完成安全管理模块请求,向 COS 微内核发出的调用底层硬件接口请求。

1.3 智能卡通信过程

智能卡与终端之间的通信是通过命令——响应对实现的。终端向卡发送命令(以 C-APDU 形式),卡收到命令后,由 COS 对接收的命令报文进行处理,然后将处理结果打包成响应报文(以 R-APDU 形式)返回给终端。

C-APDU 由两部分组成^[3]:一个必备连续 4 字节的命令头,用 CLA、INS、P1 和 P2 表示,以及一个可选的长度可变的条件体。在 C-APDU 中发送的数据的字节数由 1 字节的 Lc 定义,期望卡回送的 R-APDU 数据字段的最大字节数由 1 字节的 Le 指定,格式见图 2。

R-APDU 由两部分组成^[3]:可选的条件体以及必备的 2 字节状态码 SW1|SW2,格式见图 3。

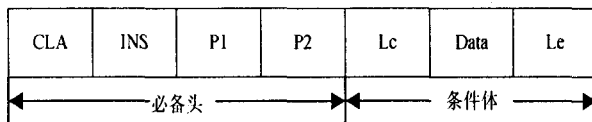


图 2 命令 APDU 格式

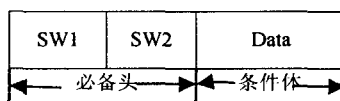


图 3 响应 APDU 格式

在智能卡上电复位之后, COS 便运行起来,开始

执行卡片的初始化工作,完成初始化的 COS 处于接收准备状态。COS 一旦查询到有命令输入,就采用已经被初始化的通信协议参数接收数据,数据全部接收后,存放在内存中命令的缓冲区中,启动命令处理流程,对命令报文进行语法检查,然后根据命令的类别以及应用的类别去执行相应的命令处理程序,命令处理完成后,将需要返回的数据存放在响应数据缓冲区中,与命令处理结果的响应状态码一起回送给终端。

2 智能卡操作系统测试方案

COS 测试主要包括基本功能、防拔插、兼容性以及耐久性测试^[4]:

(1) COS 基本功能的测试,主要包括文件的测试、命令功能、命令的执行情况、命令出错处理等;

(2) 由于智能卡在实际应用中往往会涉及到对一些敏感数据的操作,因此必须针对在 COS 与终端进行交互的过程中被意外事件中断时其自动恢复能力进行测试,即防拔插测试;

(3) 智能卡的使用寿命是有限的,对存储介质的过度损耗是导致智能卡损坏的主要原因,但可以采用软件优化来均衡对存储介质的访问从而延长智能卡的使用寿命,因此在 COS 测试中需要对智能卡进行耐久性测试;

(4) 智能卡与终端之间进行正常通信的前提是它们遵循相同的协议,因此在 COS 的测试中需对协议的实现情况进行测试,即协议测试。

COS 测试总体上采用增量测试的方法,各项内容与测试阶段^[5]对应见表 2。

表 2 COS 检测项

| 测试项 | 描述 | 测试阶段 | 测试技术 |
|----------|--------------------------|----------------|------|
| COS 基本功能 | 命令功能、命令出错处理、文件测试 | 单元测试、集成测试、系统测试 | 灰盒测试 |
| 防拔插 | 测试因断电而使操作意外中断后智能卡的自动恢复功能 | 系统测试 | 黑盒测试 |
| 耐久性 | 检验卡片在多次擦写后能否正常工作 | 系统测试 | 黑盒测试 |
| 协议一致性 | 检验智能卡与终端是否遵循相同的协议 | 系统测试 | 黑盒测试 |
| 兼容性 | 检测智能卡与相应终端能否正常通信 | 验收测试 | 黑盒测试 |

2.1 COS 基本功能测试

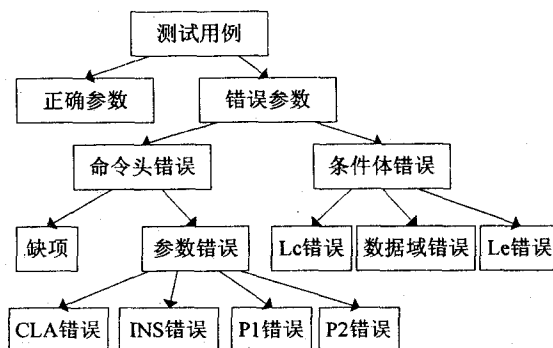
灰盒测试^[6]结合了白盒测试和黑盒测试,软件需求规格说明书是测试用例^[7,8]的设计依据,也是验证软件满足其功能需求的依据,在对需求和结构进行覆盖分析时须使用同样的测试用例。灰盒测试是发现软件潜在缺陷的非常有效的技术手段^[9]。对于 COS 基本功能的灰盒测试方法如下:测试人员根据 ISO/IEC

7816-4 标准以及具体的需求规范进行测试用例设计,对已有测试进行覆盖分析来进一步扩充测试用例以确保测试的充分性,对于需求的覆盖率一般要达到 100%,而对于结构的覆盖率达到所要求的即可。

从智能卡所遵循的 ISO/IEC 7816-4 规范入手设计 COS 的测试用例,ISO/IEC 7816-4 规范的主要内容包括:在接口设备与智能卡之间的通信中所传送的报文、命令和响应的内容;在处理交换用的行业间命令时,在接口处所看到的数据文件的结构;卡内数据文件的访问方法;定义卡内数据文件访问权限的安全体系结构。这些都可用模拟终端发送特定的命令序列给 COS,然后根据 COS 执行命令的结果来进行测试。

智能卡与终端是以 APDU 为基本单元通信的, COS 功能测试主要关注工作流程、命令参数、安全状态、状态码和响应数据。因而对 COS 基本功能测试的对象就是 APDU 序列。

首先需要针对标准以及需求规范中描述的每个命令的 APDU 设计测试用例,由于命令解释模块首先对命令缓冲区中 APDU 的 4 个字节的必备头进行接受分析处理,因此对各个命令可依据图 4 所示的测试用例树来设计测试用例。



测试时,判断命令执行结果是否正确的主要依据是 COS 执行 APDU 命令后返回的状态码,在 COS 中定义了 4 种状态:

1) State-Response: 命令执行完后,把命令执行的结果存储在 Get Response 专用缓冲区中,并且卡回送的状态码被设为 61XX,它通知终端发出 Get Response 命令来获取数据;

2) State-Success: 命令成功执行时返回的状态,该状态不需要终端再使用 Get Response 命令来获取数据;

3) State-Error: 在执行命令过程中出现了异常情况时返回的状态,这时会向终端回送错误代码,包括命令的参数出错和在执行命令过程中出现的存储空间、安全状态等错误;

4) State_Timeout: 在接收 Lc 长度的数据的过程中发生超时, 则返回该状态, 此时不需要向终端回送错误代码。

在 EVDO 卡的测试中, 以 SELECT 命令为例, 依据图 4 设计测试用例, 如表 3 所示。

表 3 测试用例

| | 测试用例 | 描述 | 期望结果 |
|----------|-----------|--|--------------------------------------|
| SELECT-1 | 正常测试 | 分别对 3F00、3F00 下的 EF 进行 SELECT 操作, 并用 GET RESPONSE 取得文件信息 | 返回正确的状态字, 使用 GET RESPONSE 能取得正确的文件信息 |
| SELECT-2 | 错误的 CLA | CLA 取 00-0F 以及 A1-FF | 执行 SELECT 失败, 返回错误状态字 6E 00 |
| SELECT-3 | 错误的 INS | P3=00、01 以及从 03 取到 DD | 执行 SELECT 失败, 返回错误状态字 6D 00 |
| SELECT-4 | 错误的 P1、P2 | P1 从 01 取到 FF P2 从 01 取到 FF | 执行 SELECT 失败, 返回错误状态字 6B 00 |
| SELECT-5 | 错误的 P3 | P3=00、01 以及从 03 取到 FF | 执行 SELECT 失败, 返回错误状态字 67 00 |
| SELECT-6 | 错误参数组合 | 取各个参数的错误组合 | 执行 SELECT 失败, 返回适当的错误状态字 |
| SELECT-7 | EF 文件不存在 | 对不存在的 DF、EF 进行 SELECT 操作 | 执行 SELECT 失败, 返回状态字 94 04 (文件未发现) |

对命令功能的测试主要是测试各命令之间的相互关系以及命令序列所完成的功能。根据 ISO 7816-4 中规定的命令执行时需要满足的条件及有关命令间的相互关系, 描述执行命令序列的过程, 然后以非正常和正常事件作为输入来设计测试用例。

在 EVDO 卡的测试过程中, 利用团队自主开发的自动化测试^[10]工具, 引入脚本技术^[11,12], 实现 COS 测试的自动化, 大大地提高了测试的效率。引入自动化测试技术具有如下优势:

1) 使测试可以快速准确地进行, 减少人为的操作失误, 更多更频繁地运行测试脚本, 使得脚本的执行效率高于手工测试, 缩短发布产品的时间;

2) 对新版本的程序运行已有的测试脚本, 特别是在程序更新较频繁时, 自动化测试可以在短时间内测试已有的脚本;

3) 更好地利用资源, 使繁琐的任务自动化可提高测试的准确性以及测试人员的积极性, 从而使测试人员能有更多精力来设计更好的测试用例;

4) 自动化测试可通过重复执行相同的测试脚本来

获得测试的可重复性和一致性。

2.2 防拔插和耐久性测试

防拔插测试主要检测因突然断电而使操作中中断后智能卡能否自动恢复。主要涉及的是在正常环境下执行正确的命令序列, COS 写 FLASH 时, 突然断电, 智能卡能够保证卡内的数据依然具有完整性。若命令未能成功执行, 验证卡内数据与命令执行前是否完全一致, 若一致则表示卡片的防插拔功能是有效的。

智能卡的使用寿命是有限的, 对智能卡的插拔次数决定了智能卡的物理寿命, 一般来说, 约在 1 万次左右; 而数据存储器的擦写次数决定了集成电路芯片的寿命, 各厂家生产的芯片其指标是不同的。故而必须对智能卡实施耐久性测试, 检验存储器的擦写次数是否会因为日常使用而超出芯片存储器擦写的最大值。对文件的操作是使用智能卡时主要涉及的内容, 因而需要模拟日常使用智能卡的行为, 对所有文件的访问频率进行统计, 找出具有相对较高访问频率的那些文件, 在个人化过程中分散存储这些文件, 避免某一块存储区域擦写过度, 均衡整个存储器的擦写。

3 结束语

根据 COS 的特点给出了 COS 的测试方案, 对于每个测试项给出了其测试的方法和技术。在测试中, 结合对测试结果的分析, 进一步补充测试用例。在 EVDO 卡的开发中按照文中的测试方案进行了测试, 经反复测试, 开发的 EVDO 卡通过了第 3 方测试, 该卡正应用于生产。

参考文献:

- [1] 张利华. 智能卡操作系统开发中的测试技术[J]. 计算机工程与设计, 2004, 25(6): 901-902.
- [2] 游剑锋, 汤荣江, 李代平, 等. 智能卡操作系统结构研究[J]. 现代计算机, 2009(1): 11-13.
- [3] International Electrotechnical Commission. International Standard ISO/IEC 7816-4. Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 4: Interindustry Commands for Interchange[S]. 1998.
- [4] ETSI TS 131. 122 Technical Specification Group Core Network and Terminals, Universal Subscriber Identity Module (USIM) Conformance Test Specification[S]. 2007.
- [5] 吴进波, 王志标. 软件测试技术研究[J]. 咸宁学院学报, 2006, 26(3): 98-99.
- [6] Kaner C, Falk J, Nguyen H Q. 计算机软件测试[M]. 第 2 版. 王峰, 陈杰, 喻琳, 译. 北京: 机械工业出版社, 2004.

(下转第 28 页)

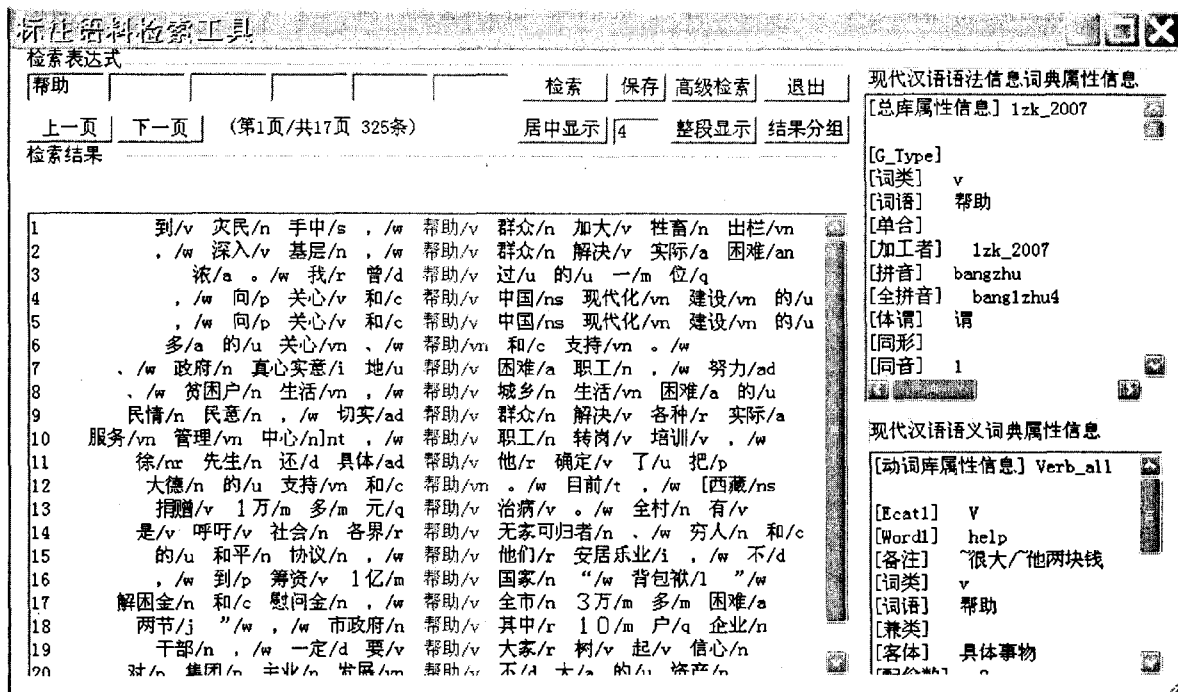


图 3 语料库与词典的交叉参照图

利的支持。

切分单位在查询中是孤立的,今后努力的主要方向是在当前切分单位的基础上获取其相关的搭配单位。例如“苹果/n”,希望能得到其左边的“很/d”、“大/a”和“的/ud”等修饰信息^[6~11]。此外,考虑到切分单位不等同于词典词,因此如果获取不到相应切分单位的属性信息,可以对切分单位进行处理,例如“企业经营/者/n”,可以分析为“企业/n”、“经营/n”、“者/k”,从词典获取各个部分的属性返回。这样可以使得本系统模块得到更大的改进,更好地服务于汉语语言学本体研究和教学研究。

参考文献:

- [1] 俞士汶,朱学锋,王惠,等. 现代汉语语法信息词典详解[M]. 第2版. 北京:清华大学出版社, 2003.
- [2] 王惠,詹卫东,俞士汶. 现代汉语语义词典规格说明书[J]. 汉语语言与计算学报, 2003, 13(2): 159 - 176.
- [3] 俞士汶,段慧明,朱学锋,等. 北京大学现代汉语语料库基本加工规范[J]. 中文信息学报, 2002, 16(5): 49 - 64.

(6):58 - 65.

- [4] 俞士汶,段慧明,朱学锋,等. 北大语料库加工规范:切分词性标注·注音[J]. 汉语语言与计算学报, 2003, 13(2): 121 - 158.
- [5] 俞士汶,段慧明,朱学锋,等. 综合型语言知识库的建设与利用[J]. 中文信息学报, 2004, 18(5): 1 - 10.
- [6] 陈素萍,谢丽聪. 一种文本特征选择方法的研究[J]. 计算机技术与发展, 2009, 19(2): 112 - 115.
- [7] Suarez A, Palomar M. A Maximum Entropy - based WSD System[J]. COLING, 2002, 2: 960 - 966.
- [8] 张燕平,徐庆鹏,苏守宝,等. 一种基于贪婪覆盖的文本分类方法[J]. 计算机技术与发展, 2009, 19(1): 74 - 76.
- [9] 刘琼,李宝敏. 一种果品领域本体库的构建方法[J]. 计算机技术与发展, 2009, 19(1): 197 - 199.
- [10] Nivre J. MaltParser: A Language - independent System for Data - driven Dependency Parsing[J]. Natural Language Engineering, 2007, 13(2): 95 - 135.
- [11] Otero P. Learning Bilingual Lexicons from Comparable English and Spanish Corpora[C] // Proceedings of MT Summit XI. [s.l.]: [s.n.], 2007: 191 - 198.

(上接第 24 页)

- [7] 尚冬娟,郝克刚,葛玮,等. 软件测试中的测试用例及复用研究[J]. 计算机技术与发展, 2006, 16(1): 69 - 72.
- [8] 马瑞芳. 计算机软件测试方法的研究[J]. 小型微型计算机系统, 2001, 24(12): 2211 - 2213.
- [9] RTCA/DO - 178B. Software Consideration in Airborne Systems and Equipment Certification[M]. USA: Radio Technical Commission for Aeronautics, Inc, 1992.
- [10] 张克东,庄燕滨. 软件工程与软件测试自动化教程[M]. 北京:电子工业出版社, 2002.
- [11] 周章慧,王同洋. 智能卡操作系统自动测试中的脚本技术[J]. 计算机工程与设计, 2008, 29(8): 2068 - 2071.
- [12] 蒋云,赵佳宝. 自动化测试脚本自动生成技术的研究[J]. 计算机技术与发展, 2007, 17(7): 4 - 7.