

智能卡 COS 安全性测试研究

李国俊^{1,2}, 董晶晶^{1,2}, 周 瑾^{1,2}

(1. 中国电子科技集团公司第十五研究所, 北京 100083;
2. 信息产业信息安全测评中心, 北京 100083)

摘 要:智能卡 COS 是智能卡中重要的软件控制部分,它控制着智能卡内部的数据通信和存储。智能卡 COS 的安全性是信息化应用健康有序进展的重要基础,因此,必须对智能卡 COS 进行科学全面的测试评价。文中首先描述了智能卡 COS 的组成结构;然后分析了智能卡 COS 需要保护的信息资产及其面临的安全威胁,在此基础上,提出智能卡 COS 在软件设计实现中需要考虑的安全机制,阐明如何构建智能卡 COS 安全性测试评价平台;最后,重点从安全功能测试和穿透性测试两个方面阐述了智能卡 COS 安全测试的关键技术。

关键词:智能卡;芯片操作系统;安全性测试

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2014)02-0164-04

doi:10.3969/j.issn.1673-629X.2014.02.040

Research on Security Test of Smart Card COS

LI Guo-jun^{1,2}, DONG Jing-jing^{1,2}, ZHOU Jin^{1,2}

(1. No. 15 Research Institute of CETC, Beijing 100083, China;
2. Information Technology & Security Test Evaluation Center, Beijing 100083, China)

Abstract: Smart card COS is an important software control part, which controls the smart card data communication and storage. Security of smart card COS is an important basis for the healthy and orderly development of information application, therefore, smart card COS must be tested comprehensively. Firstly, describe the structure of smart card COS. Then analyze information assets need to protect and security threat and risks of smart card COS. On the basis, propose security mechanisms need to be considered in the state of design and development of smart card COS, discuss the way to build the platform of security test and evaluation of smart card. At last, analyze the key technology of security test and evaluation of smart card from security function test and penetration test.

Key words: smart card; COS; security test

0 引言

智能卡是综合微电子、通信、计算机、密码等多种技术于一体的产品,随着信息技术和国内经济的快速发展,目前,智能卡在国内的应用已经遍布于移动通信、金融、社保、石油、身份证、城市一卡通、移动支付等众多的领域,已成为现代社会生活中不可或缺的重要部分。

智能卡芯片操作系统(Chip Operation System, COS)属于智能卡中的软件部分,它是搭载在智能卡芯片之上的嵌入式控制软件,它主要完成与外界的数据通信、身份鉴别、文件处理等功能,是智能卡应用得以

正确、安全实现的基础^[1-5]。由于其承担着重要的角色,特别是维护智能卡应用功能的正常运行,以及保障重要数据和密钥的安全性,因此,它的安全保证能力将直接影响着智能卡应用的安全稳健运行。

文中从测试验证智能卡 COS 的安全性的角度出发,首先分析了智能卡 COS 面临的威胁,提出了其需要具备的安全策略和机制,然后重点分析了安全性测试验证的内容和方法,为智能卡 COS 安全性测试提供借鉴。

1 智能卡 COS 结构

智能卡 COS 的主要功能是控制智能卡同外界的

收稿日期:2013-05-06

修回日期:2013-08-12

网络出版时间:2013-11-29

基金项目:国家质检公益性行业科研专项经费(201310033)

作者简介:李国俊(1978-),男,工程师,硕士,CCF 会员,国家金卡工程物联网应用联盟工作组成员,主要从事信息技术产品及软件的测试、智能卡产品 EAL4+级评估、标准与技术规范制定、信息安全咨询培训等方面的工作。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20131129.0826.004.html>

信息交换,分析接收到的指令进行处理,管理文件,执行加密及安全状态的管理^[6-8]。按照功能划分,智能卡 COS 的体系结构如图 1 所示。其中最主要的是通信传输模块、命令解释模块、安全管理模块和文件管理模块。

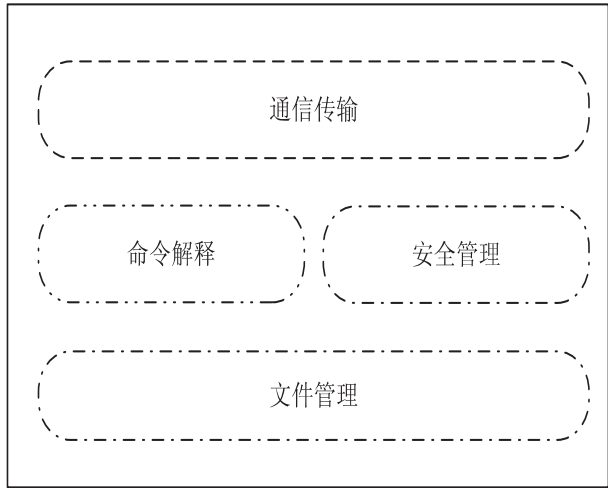


图 1 智能卡 COS 组成结构

(1)通信传输模块:通信传输模块依据智能卡所使用的通信协议,对读写设备发出命令通过接触式或非接触式接口进行接收。同时,把对命令的响应按照传输协议的格式发送出去。传输模块负责智能卡和接口设备之间的数据通信,在正确地接收到命令后交给下一个功能模块进行处理。

(2)命令解释模块:对接收到的每条命令的命令头做语法分析,分析和检查命令参数的正确性,如果参数不正确将返回过程字节给通信管理模块,然后根据命令要求分别调用安全管理模块或文件管理模块。命令执行完后,负责将安全管理模块的应答数据返回给通信管理模块,并最终由通信管理模块发送给卡读写设备。

(3)安全管理模块:主要实现如下 3 个功能,即鉴别、数据加解密、文件访问的安全控制。鉴别是通过智能卡和读写设备进行单向或双向的身份认证;智能卡 COS 通过密码算法及密钥管理系统产生的过程密钥来对数据进行加解密;文件访问的安全控制通过读写更新的控制来实现。安全管理是对从传输模块传入的数据进行安全控制及管理。

(4)文件管理模块:智能卡 COS 通常在应用下建立文件,通过对文件的操作和访问来实现应用管理。在数据操作前,安全管理模块根据文件的访问条件检查当前的安全状态,以确定操作的可行性,只有满足文件的访问条件才可以对该文件进行操作。例如对文件进行访问,首先要对比文件的安全状态和当前全局状态机的数值,当对比结果符合要求时,则允许对文件访问,否则不允许访问。

2 智能卡 COS 安全威胁分析

智能卡 COS 面临着多种可能的安全威胁,必须充分对安全威胁进行分析,并采用合适的安全机制进行抵御,以达到保护智能卡资产的目的。

2.1 资产

首先,对于智能卡 COS,其需要保护的资产包括^[9]:

- 1)用户数据(例如智能卡持有者使用的数据);
- 2)系统数据(例如软件的开发者、发行者使用的与安全相关的数据);
- 3)应用数据(例如网络连接接口参数、系统参数、初始化数据、智能卡的预个人化和个人化数据);
- 4)各种密钥或口令。

2.2 面临的威胁分析

然后,分析对智能卡 COS 构成的威胁情况,具体见表 1。

表 1 智能卡 COS 威胁列表

威胁名称	内容描述
用户错误	智能卡 COS 的授权用户可能通过引入错误数据或进行了不当操作等,危及智能卡的安全特性
未授权操作	攻击者可能通过未授权操作智能卡 COS 来探测或修改智能卡的安全特性。如在智能卡 COS 中存在未公开的命令或功能,对这些命令或功能的未授权操作会危及智能卡的安全特性
命令操纵	攻击者可能异常地使用软件命令非法获得存储器内容。例如,通过执行越界请求或使用畸形的命令格式
强制重置	攻击者可能通过不正常中断方式使智能卡进入不安全状态
缺陷插入	攻击者可能通过反复地插入选定的数据或错误,并观察相应的输出结果,从而获得重要信息
重放攻击	攻击者可能通过重用合法鉴别数据旁路安全机制或探测智能卡嵌入式软件信息
审计失败	如果审计失败,那么攻击者可能通过重复探测来获取存储器内容,或改变智能卡 COS 的安全功能的关键要素
身份冒充	攻击者可能冒充智能卡的授权管理员或用户而非法获得智能卡 COS 信息
非法访问	每个授权角色都有特定的权限来访问智能卡 COS 分配或指定的区域及其包含的信息,如果访问超出规定权限,会导致安全相关信息的暴露

3 安全机制要求

为了抵御这些安全风险,达到保护智能卡 COS 资产的目的,智能卡 COS 软件产品应实现相应的安全机制。

1)标识鉴别(Identification and Authentication)。

智能卡 COS 应鉴别用户身份,以判定软件相关操作的可执行性。对于必须明确身份后方可执行的动作应首先进行用户身份标识鉴别,且对于鉴别过程应进行敏感信息保护,防止信息泄露,同时,对于鉴别的次数应进行安全控制。

2)访问控制(Access Control)。

智能卡 COS 中通常应实现主体对客体的访问控制,包括管理受控主体对受控客体执行的操作列表,以及通过软件将用户数据传输到安全控制范围之外时的控制措施。智能卡 COS 应对受控主体和受控信息之间存在的经由受控操作产生的信息流进行控制。如文件读写访问控制和命令访问控制机制的实现。

3)安全审计(Security Audit)。
智能卡 COS 应能够对初始化操作记录进行审计,并唯一性标识智能卡 COS 的标识和版本号。另外还要防止这些审计信息被篡改。此外,对于外部潜在侵害事件应能够检测和发出告警动作。

4)安全功能保护(Security Function Protection)。
智能卡 COS 应具有功能恢复的功能,能够在异常状态发生时自动保存到一个安全状态,如在文件更新或密钥更新时突然发生掉电异常,安全功能能保证恢复到一个正确状态。

智能卡 COS 应能够分离不同安全域,能够保证安全策略不被旁路,能够防止重放攻击。

5)安全管理(Security Management)。
智能卡 COS 应具有安全管理功能,安全管理主要包括安全功能行为的管理、安全属性的管理、安全功能数据的管理、安全功能数据限值的管理等。

4 安全性测试

4.1 测试目的

对于智能卡 COS 的安全性测试,主要目的是验证其面临的安全威胁得到了妥当的解决^[10]。那么,也就是要验证智能卡 COS 产品实现的安全机制是否被正确恰当的实现。那么要完成安全机制的测试验证,应从两方面进行深入透彻的测试实施。

其一,安全功能测试(Security Function Test),即是要从安全功能实现的角度测试验证是否达到规定的安全要求;

其二,穿透性测试(Penetration Test),即是从攻击者的角度测试验证已实现的安全机制是否能够抵御一定级别的攻击。

4.2 测试体系建立

要构建智能卡 COS 安全测试体系,应从以下方面考虑,包括测试标准、测试规范、测试用例,以及测试工具环境等。从而立体地构建智能卡 COS 安全性测试评价平台,为智能卡 COS 产品提供安全测试服务。具体关系如图 2 所示。

4.3 安全功能测试

针对智能卡 COS 安全功能进行测试,主要验证智能卡 COS 安全机制是否实现,是否能够在保密性、完整性、可用性等方面达到一定的安全水平。

因此,从安全功能角度对智能卡 COS 进行测试验证,主要从几个具体的角度验证安全机制的正确性和全面性。具体测试验证应从各个安全机制细分具体测试指标分别详细验证其安全性。安全功能测试分类结构如图 3 所示。



图 2 测试体系构成示意图

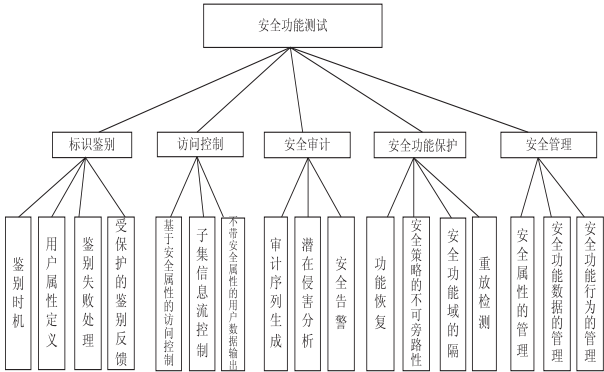


图 3 安全功能测试分支结构图

1)标识鉴别(Identification and Authentication)。

应测试验证智能卡 COS 是否能够针对用户的类别和属性进行鉴别,主要是对用户的身份进行标识和鉴别。特别是验证智能卡 COS 对用户或管理员的身份属性的定义,在执行安全动作前的身份鉴别,鉴别失败时的安全处理能力,以及鉴别过程中的敏感信息的保护方式等。

2)访问控制(Access Control)。

应测试验证智能卡 COS 的访问控制策略和信息流控制策略,主要包括文件访问控制和命令访问控制策略,以及数据传输时的信息流控制策略。

应测试智能卡 COS 是否能够基于安全属性对文件进行访问控制,在每个文件的文件头信息中都存储有该文件能够被操作的权限,包括读、写、更新、失效和恢复等条件。智能卡 COS 实行阶段化的管理,不同的人员在不同的阶段可以执行不同的命令,因此应测试是否能够基于生命周期对命令访问进行控制。数据的读出和写入在智能卡中通常有多种模式,如明文、密文

或校验等,应测试是否能够基于多种传输模式对信息流操作进行控制。另外,有时还要求输出的用户数据不带安全属性。

3)安全审计(Security Audit)。

应测试验证智能卡 COS 是否能够唯一性标识其本身,包括型号和版本等信息,并能够防止审计记录信息被篡改。另外,应测试智能卡 COS 对安全侵害事件的检测能力,并能够发出适当的告警信息。

4)安全功能保护(Security Function Protection)。

应测试验证智能卡 COS 的安全功能自我保护能力,包括在异常状态发生时是否能够恢复到一个安全已知的状态。测试智能卡 COS 是否能够将不同主体和客体的安全域进行分离,并能够保证安全策略强制执行,而不被旁路,如鉴别策略、访问控制策略、审计策略等。测试验证智能卡 COS 是否能够防止非法用户的重放攻击。

5)安全管理(Security Management)。

应测试验证智能卡 COS 的安全管理能力,包括是否能够控制授权角色对安全功能行为进行管理,是否能够基于授权角色对安全属性、安全功能数据、安全功能数据限值等进行管理控制。

4.4 穿透性测试

穿透性测试是指以未经授权的动作绕过某一系统的安全机制的方式,检查数据处理系统的安全功能,以发现信息安全问题的手段。

针对智能卡 COS 进行穿透性测试,将主要从以下几个方面进行^[11]。

a)旁路,包括攻击者能够避开安全强制措施所采取的任何手段。

b)篡改,包括基于攻击者试图影响安全功能或机制行为(即破坏或使失效)的任何攻击。

c)直接攻击,包括确认或推翻所声称的最小功能强度时必需的任何穿透性测试的标识。

根据以上要求,构建穿透性测试列表。通常可能执行的穿透性测试内容如表 2 所示。

根据开发者实现的防护措施,穿透性测试列表可能进行适当的增减,比如裁剪列表中的已有测试内容或增加新的穿透性测试项目,以及调整已存在攻击测试项等^[12]。设计定义穿透性测试列表的方法如图 4 所示。

从通常的观点来看,智能卡 COS 某些攻击是已知的。依赖于智能卡 IC 和软件应用的特征,特定的策略、特定的参数可能需要被调整。对智能卡(源代码, IC)的分析将帮助提供一些信息来调整工具。例如, DPA 可能被使用在 DES 的不同地方, DPA 通过获取波形,从中提取感兴趣的特征并利用它们,适用的处理方

法须依赖于 IC 特征信号。不同的安全性测试评价级别有不同的相应攻击潜力级别,它们之间重要差异是脆弱性分析方法。例如从脆弱性搜索,脆弱性分析,重点脆弱性分析,方法脆弱性分析到高级方法脆弱性分析。

表 2 穿透性测试项列表

攻击测试项	测试描述
软件攻击	用软件的手段实现对智能卡的攻击,多数软件攻击是从源代码的分析着手
信息收集	试图以协议开发者不期望的方式使用协议,首先收集信息,然后改变通信进而获得秘密数据或其他资源
编辑指令	攻击者修改通信序列中的指令,以观察卡是否给出非预期的响应
直接协议攻击	攻击者试图向智能卡发送其当前状态不期望收到的指令
中间人攻击	攻击者隐藏在正在进行有效通信的两个实体之间的通信路径上,攻击者在任何一方面伪装成有效的另一方
重放攻击	攻击者捕获到感兴趣的消息后,经过篡改重新发送该消息
旁路鉴权或访问控制	对驻留在智能卡上的数据进行未授权的访问,执行不符合被处理数据对象或操作系统的当前生命周期状态的操作
缓冲区或堆栈溢出	通过运行恶意应用所产生的缓存溢出或堆栈溢出实现该攻击

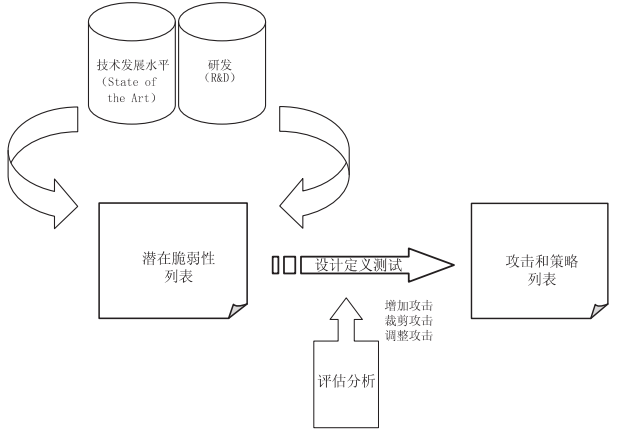


图 4 穿透性测试列表的产生

5 结束语

智能卡 COS 的安全性是抵御面临的安全威胁,保护其相关资产安全的重要基础。文中通过分析智能卡 COS 面临的安全风险,提出智能卡 COS 在软件设计实现中需要考虑的安全机制,然后重点分析了测试验证智能卡 COS 安全性的两个方面,并分别讨论了两方面测试的关键技术及方向,为深入开展智能卡 COS 产品的安全性测试评估提供指导借鉴。

参考文献:

[1] 王爱英. 智能卡技术[M]. 第 2 版. 北京:清华大学出版社, 1996.

[2] Rankl W, Effing W. 智能卡大全[M]. 王卓人,王 锋,译. 北京:电子工业出版社,2002.

[3] 杨志峰,王志新. 智能卡的操作系统: COS[J]. 现代电子技

迭代检索掩码,同时固定其他,然后在下次迭代检索第二个,然后再检索第一个,这个循环不断直到算法收敛。但它不是这种情况下提出的算法,在每个迭代同步修改两个阶段,这种变化会导致更快的收敛速度和较高的恢复质量。四个算法的目标图像以及所述迭代图像之间的均方误差和相关系数,分别由式(5)和式(6)定义。表1所示A及B分别是在100次迭代的效果,显然结果与图3得到的是一致的。需要指出的是,虽然图3(c)和图2、图3(d)和图2之间的相关系数似乎都等于1,但其对应的MSE有很大的不同。如表1显示CIFT算法得到的迭代图像质量显著高于其他方法,得到最好的最有效搜索策略。

表1 四种算法在100次迭代下均方误差与相关系数的比较

Algorithm	A	B	C	CIFT
MSE	0.006 2	0.001 77	4.354×10^{-11}	$1.086 7 \times 10^{-18}$
R	0.987 1	0.996 4	1.0	1.0

评估收敛,设置的趋同标准 $R = 0.988$ 。这些算法都在相同初始条件下测试。在这个模拟中,算法A需要124.63 s和632次迭代,算法B需要25.72 s和100次迭代,算法C需要3.97 s和15次迭代,分别驱动 R 这个临界值。相对而言,达到同样的阈值CIFT算法只需要2.358 s和9次迭代。显然,作为在前文的评论,C和D有更快的收敛速度。相应的算法的MSE如下:算法A为 $9.834 5 \times 10^{-4}$,算法B为 1.7×10^{-3} ,算法C为 1.3×10^{-3} ,CIFT算法为 $6.456 2 \times 10^{-4}$ 。然而,如果迭代过程继续进行,直到MSE不再有任何减少,这个值则是完全不同的。

3 结束语

文中提出级联迭代傅里叶变换(CIFT)算法在光学安全应用相位掩模的设计。CIFT算法与以往的方法相比,调整了两个相位掩码同步分布以及扩大搜索空间,

因此有更快的收敛速度和更好的恢复图像的质量。该算法分为两个阶段掩码,作为安全系统密钥编码目标图像,这些密钥被分配到不同的人能获得较高的安全水平。

参考文献:

[1] 王永瑛. 基于计算全息和迭代傅里叶变换算法的光学图像加密技术的研究[D]. 济南:山东大学,2007.

[2] 乌 旭. 基于随机相位编码的加密与防伪技术研究[D]. 大连:大连理工大学,2006.

[3] 丛长平. 信息安全中的光学加密及数字水印技术[D]. 大连:大连理工大学,2009.

[4] 王永瑛,王玉荣,杨永斌. 用迭代傅里叶变换算法实现光学分级图像加密[J]. 中国激光,2006,33(10):1360-1364.

[5] 赫明钊,曹良才,谭峭峰. 基于级联分数傅里叶变换系统的数字水印技术[J]. 光学学报,2009,29(10):2709-2715.

[6] 贾丽娟,刘正君. 基于随机分数傅里叶变换的双图像加密算法[J]. 光子学报,2009,38(4):1020-1024.

[7] 吴克难,胡家升,乌 旭. 信息安全中的光学加密技术[J]. 激光与光电子学进展,2008,45(7):30-38.

[8] Réfrégier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics letter, 1995,20(7):767-769.

[9] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. Optics letter,2000,25(12):887-889.

[10] Javidi B, Horner J L. Optical pattern recognition for validation and security verification[J]. Optical engineering,1994,33(6):1752-1756.

[11] Javidi B, Sergeant A. Fully phase encoded key and biometrics for security verification[J]. Optical engineering,1997,36(3):935-942.

[12] Weber D, Trolinger J. Novel implementation of nonlinear joint transform correlators in optical security and validation[J]. Optical engineering,1999,38:62-68.

+++++ (上接第167页)

术,2005,28(8):91-93.

[4] 李金良. 智能卡操作系统(COS)编程语言及编译器系统设计与实现[J]. 中国集成电路,2005(11):67-69.

[5] 李 翔. 智能卡研发技术与工程实践[M]. 北京:人民邮电出版社,2003.

[6] 张志刚,赵 奎. 智能卡操作系统研究和实例分析[J]. 企业技术开发,2005,24(9):18-20.

[7] ISO 7816-3. Identification cards integrated circuit(s) cards with contacts-Part 3:Electronic signals and transmission protocols[S]. [s. l.]:International Electrotechnical Commission, 1997.

[8] 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.

[9] GB/T20276-2006. 信息安全技术智能卡嵌入式软件安全技术要求(EAL4增强级)[S]. 2006.

[10] CCDB-2010-03-001. Smartcard evaluation[S]. 2010.

[11] Common methodology for information technology security evaluation[S]. 2009.

[12] CCDB-2009-03-001. Application of attack potential to smartcards[S]. 2009.

作者: [李国俊](#), [董晶晶](#), [周瑾](#), [LI Guo-jun](#), [DONG Jing-jing](#), [ZHOU Jin](#)
作者单位: [中国电子科技集团公司第十五研究所, 北京 100083; 信息产业信息安全测评中心, 北京 100083](#)
刊名: [计算机技术与发展](#)

ISTIC

英文刊名: [Computer Technology and Development](#)

年, 卷(期): [2014\(2\)](#)

本文链接: http://d.wanfangdata.com.cn/Periodical_wjfz201402041.aspx