综述与评论 Review and Comment

智能卡安全性评估保护轮廓 PP 的研究

刘瑞玲,李代平
(广东工业大学 计算机学院,广东 广州 510090)

摘 要:在介绍智能卡安全性评估的相关知识后,重点分析了 EAL4+级智能卡保护轮廓中应包括的安全环境、安全目的和要满足的安全要求,指出了智能卡安全性评估保护轮廓发展的趋势,为下一步 PP 的开发实现做准备。

关键词:智能卡;EAL4+;保护轮廓
中图分类号:TP33 **文献标识码**:A

The study of the smart card security evaluation protect profile

LIU Rui Ling, LI Dai Ping
(School of Computer Science, Guangdong University of Technology, Guangzhou 510090, China)

Abstract: After introducing some knowledge raleted evaluation, this paper focuses on analysis the security environment, security objects and safety requirements which are included in the EAL4+ security evaluation protection profile. And then points out the development trend of the protection profile for the next implement of PP.

Key words: smart card; EAL4+; protect profile

目前智能卡应用已渗透到社会生活的各个方面,其在带给人们高效便捷生活的同时,安全性也倍受人们关注。因此,国内一些智能卡厂商通过对智能卡进行评估以提高智能卡的安全信誉。在进行智能卡产品安全性评估时,首先需要相关的指导性文档,其中位于高层抽象级的指导性文档是安全性评估保护轮廓 PP。它依据的是 GB/T 18336-2001《信息技术安全性评估准则》[1]。该准则的前身是国际通行的最先进的信息安全测评标准 CC[2](Common Crietira),即 ISO/IEC 15408。

1 PP 概述

1.1 概念介绍

要认识 PP,先介绍 CC 中的几个重要术语。

(1)评估对象 TOE(Target of Evaluation):评估申请方提供的被评估对象。

(2)安全组件包:多个安全要求组件构成一个安全组件包。安全组件包用于构造 PP 或 ST。

(3)保护轮廓 PP(Protect Profile):对于某一类 TOE 而言的高级抽象的安全要求说明书,与 TOE 的实现无关。

(4)安全目标 ST(Security Target):与 PP 类似,是针对某一特定安全产品而言,与 TOE 安全环境相关的安全要求与概要设计说明书,可以引用某个(些)PP。

(5)评估保证级 EAL(Evaluation Assurance Level):代表 TOE 的安全保证程度。CC 标准将 EAL 分为 7 级。

CC 标准由简介和一般模型、安全功能要求和安全保证要求 3 部分文档组成。其中,简介和一般模型相当于某一类 TOE 的 PP;安全功能要求根据 TOE 使用安全环境提出安全功能标准。相应地 CC 评估也分为 3 部分:PP 评估、ST 评估和 TOE 评估。若某一类种信息安全技术或产品通过 CC 评估,则意味着同时通过了这 3 部分评估。三者之间的评估顺序如图 1。

图 1 三种评估的顺序关系

鉴于 PP 评估在 CC 认证中的关键地位,要使智能卡产品顺利通过 EAL 评估,就有必要对智能卡的安全保护轮廓 PP 进行深入细致的研究。

PP 作为高层指导性文件,主要介绍 TOE 的安全环境、安全目的、安全要求和基本原理。安全要求包括安全功能要求 SFR(Security Functional Requirements)和安全保证要求 SAR(Security Assurance Requirements)。安全原理

指出安全环境、安全目的和安全功能之间的关系，如图2所示。

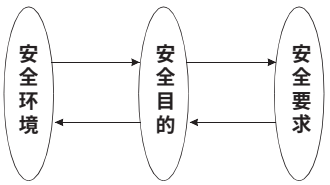

图2 PP安全原理图

1.2 PP分类

从不同的角度考虑，PP的分类不同：

(1)CC标准中将评估级别分为7级，因此，PP可以按评估级别分为7类，即为EAL1级PP，EAL2级PP等。

(2)由于PP是针对某一类TOE而定，因此PP就可以按TOE分类，如DBMS PP、防火墙PP、智能卡PP等。

(3)从TOE的安全环境角度看，PP可分为高风险环境(HRE)PP、中风险环境(MRE)PP和低风险环境(LRE)PP。

2 智能卡评估介绍

2.1 智能卡概述

智能卡也称为集成电路卡(Integrated Circuit Card)，即IC卡。智能卡的分类有多种，根据卡上集成电路的不同，可分为存储器卡、逻辑加密卡和CPU卡3种，由于CPU卡上的集成电路包括有片内操作系统COS(Card Operating System)，能存储并处理数据，所以CPU卡才是真正的智能卡(如无特殊说明，本文所讨论的智能卡均属CPU卡)。

2.2 智能卡安全性评估意义

智能卡的安全性非常重要。智能卡安全性评估是依照国内外行业相关安全技术标准，对智能卡生命周期各阶段的安全功能和安全保证进行评估，以确认该智能卡产品是否满足相应的安全要求。通过这一过程，可以促使生产者或开发商规范生产过程、节省人力物力资源，同时，也向用户和社会提供一个衡量智能卡产品安全性的客观标准。

2.3 智能卡安全要求

由于智能卡的功能和使用环境不同，所以对智能卡的评估需分级进行。如对医疗卡、社保卡、交通卡的评估属于低级别的，而对于电信卡、信用卡、现金卡等属于高级别的评估活动。目前国内评估机构——中国信息安全产品测评认证中心，对电信行业的SIM卡、UIM卡、PIM卡以及智能卡芯片开展的分级评估为EAL4+级。

EAL4+级又称为EAL4增强级，是在EAL4级的基础上提升了TOE安全保证要求的深度、广度和严格性。目前国际上开展的智能卡评估活动的保证级多数是EAL4+，也有智能卡通过了相应国家认证机构的EAL5+认证。

3 EAL4+级智能卡PP

CC规定了每级应具有的SFR，但没有明确规定每级EAL应包含哪些SFR，所以智能卡PP的主要任务是说明在预期的使用环境下的安全需求。可以根据智能卡安全使用环境来确定智能卡PP应包括的安全目的和安全要求，从而设计切实可用的智能卡PP。

3.1 智能卡安全环境

智能卡在整个生命周期中存在的敏感资产有用户的各种数据、系统应用数据、密钥、软件开发工具与技术等。智能卡务必要保护这些数据的私密性，所有可能危及到这类数据的行为或情况都要在保护轮廓中考虑到。智能卡PP需考虑的安全环境有3种。

3.1.1 假设

攻击者的能力(A.Attack)：假设攻击者有足够的时间，并具备智能卡所需的技术知识，拥有电脑和相关设备，动机可能有经济利益、政治利益或其他等。

用户权限(A.User)：假设用户拥有访问智能卡某些信息的权限。

管理者能力(A.Admin)：假设管理或使用智能卡的人胜任工作。

角色管理(A.Role_Man)：假设智能卡的开发者、发行者、管理者和使用者能被安全地管理。

外部数据存储(A.Data_Store)：假设能以安全的方式管理相关的外部数据。

生命周期管理(A.Life_Man)：假设智能卡的生命周期的每个阶段都被唯一标识，这样可以确保能通过标识信息追溯到生命周期的各个阶段。

密钥生成(A.Key_Gen)：假设智能卡应用系统中生成的密钥都是安全的。

3.1.2 威胁

智能卡面临的威胁主要有针对应用软件的威胁和对使用环境的威胁。在应用软件的使用过程中，如用户可能操作或引入错误数据而使卡内信息混乱，或攻击者反复使用某些数据或操作，通过观察卡的输出结果而获得卡的机密信息等威胁；在应用软件开发过程中，会面临保密数据泄漏、软件修改和开发工具失窃等威胁。

使用环境中由于不完善的控制程度或失窃造成密钥泄漏，使得攻击者在非法获得密钥后，就可以对卡内的信息和功能进行操作。管理者可能执行暴露智能卡安全功能或数据的操作而将智能卡置于危险境地。

3.1.3 组织安全策略

(1)数据访问：智能卡内的不同数据有不同的访问者，同一数据不同访问者有不同的权限。智能卡内数据应根据不同的使用者制定不同的访问规则。

(2)文件访问：智能卡内文件可能涉及不同的使用者，如系统集成商、智能卡发行者、用户等，对于文件的具体操作，需要不同的访问权限和规则。

(3)标识：智能卡内各文件应能唯一被标识。

(4)专业领域的信息技术标准：智能卡及其COS和

应用软件的设计都应符合国家标准、行业及组织的信息技术安全标准或规范。

(5)密码标准:智能卡中使用的密码或数据鉴别都必须与国家标准或行业规范相符合。

(6)配置管理:为了安全和便于管理,智能卡应使用配置管理工具管理所有代码。

3.2 智能卡安全目的

由于安全环境决定安全目的,所以智能卡 PP 中的安全目的应适应安全环境中的任何情况,具体见表 1、表 2 和表 3(限于篇幅,表 3 只列出了智能卡安全环境中部分威胁),即每种安全环境都有一个安全目的与之对应。表 1~表 3 中各组件的详细说明请见参考文献[4]。

表 1 与安全目的相关的威胁

威胁	对应的安全目的
用户错误 T.Us_Error	逻辑保护 O.Log_Prot
未授权操作 T.Ua_Op	逻辑保护 O.Log_Prot
对初始使用权的欺骗 T.First_Use	设置顺序 O.Set_Up
身份冒充 T.Impers	设置顺序,初始数据保护 O.Set_Up,OE.Init_Acs
非法访问 T.Access	数据访问控制 O.DAC
密码攻击 T.Crypt_Atk	密码 O.Crypt
联合攻击 T.Lnk_Atk	逻辑保护,审计 O.Log_Prot,O.Audit

表 2 与安全目的相关的假设

假设	对应的安全目的
攻击者能力 A.Attack	逻辑保护,防信息泄漏 O.Log_Prot,O.I_Leak
用户权限 A.User	数据访问控制,文件访问控制 O.DAC,O.FAC
管理者能力 A.Admin	管理者能力 OE.Admin
角色管理 A.Role_Man	角色管理 OE.Role_Man
外部数据存储 A.Data_Store	数据存储 OE.Data_Store
生命周期管理 A.Life_Man	生命周期管理 O.Life_Man
密钥生成 T.Key_Gen	密钥生成 OE.Key_Gen

表 3 与安全目的相关的组织安全策略

组织安全策略	对应的安全目的
数据访问 P.Data_ACC	数据访问控制 O.DAC
文件访问 P.File_Acc	文件访问控制 O.FAC
标识 P.Ident	标识 O.Ident
专业领域的信息技术标准 P.IT_Std	专业领域的信息技术标准 O.IT_Std
密码标准 P.Crypt_Std	密码 O.Crypt
配置管理 P.Con_Cont	配置管理 O.Con_Cont

表 4 安全要求组件和对应的安全目的、安全环境

安全要求	安全目的	安全环境
安全告警	O.Log_Prot	A.Attack,T.Lnk_Atk,T.Us_Error,T.Ua_Op
潜在侵害分析	O.Audit	T.Lnk_Atk
密钥生成	O.Crypt	T.Crypt_Std
产生支持和接收程序	O.Ident,O.Con_Cont	P.Ident
模块化	O.IT_Std	P.IT_Std
明确定义的开发工具	O.IT_Std,O.Life_man	P.IT_Std,A.Life_Man
中级抵抗力	O.Log_Prot,O.I_Leak	A.Attack,T.Lnk_Atk,T.Us_Error,T.Ua_Op

3.3 智能卡安全要求

智能卡安全要求是指针对安全环境而提出的要求。智能卡 PP 中安全要求组件也分为安全功能要求组件和安全保证要求组件。

3.3.1 安全功能要求组件

安全告警:当检测到潜在的安全侵害时,智能卡应能采取相应措施将危害降到最低。

审计并分析潜在侵害:智能卡应能用一定的规则去监控审计事件,并根据这些规则指示出对智能卡的潜在侵害,如用户进入系统时需要身份认证或用户签名等,都是为了实现事后追查和安全审计。

密钥的生成、访问和运算:智能卡密钥生成所用的算法必须与国家法规和行业标准相一致,密钥访问必须有严格的方法。

无过度损失的自动恢复:当不能从失败或服务中断自动恢复时,智能卡安全功能应进入一个安全状态,并确保数据或客体在无过度损失的情况下恢复到初始状态。如当用户在向智能卡内写数据时突然断电,则智能卡应能确保卡内数据的安全,并在下次使用时功能正常。

3.3.2 安全保证要求组件

智能卡安全保证要求组件包括:部分配置管理自动化组件、产生支持和接收程序组件、安全加强的高层设计组件、模块化组件和描述性低层设计组件等。

3.4 智能卡安全原理

智能卡中的安全环境、安全目的和安全要求是相互关联的[5]。表 4 给出一部分安全要求与安全目的、安全环境的对应关系。

4 智能卡 PP 发展趋势

(1)智能卡 PP 开发流程化。PP 的开发涉及多方面内容,工作量极大。如果能够通过有效方法使开发过程趋于流程化,则不仅会使开发时间大大缩短,而且开发产品 PP 将更令人满足。

(2)智能卡安全环境规范化。从之前的描述中可知,智能卡的安全环境是 PP 开发及评估的基础和前提,并且智能卡的安全环境具有相似性。因此,安全环境的规范化将会使智能卡 PP 的开发更标准、高效。

(3)HRE PP 的研究开发。目前国内对智能卡开展的安全性评估大多是在

EAL4+,属于中风险PP。随着智能卡的普及,人们对智能卡的安全期望值会更高,届时,必将需要更高风险的PP以适应技术发展的需要。

优质的智能卡PP对安全性评估有着重要的意义和作用,本文通过对智能卡安全性评估保护轮廓PP的研究及PP的发展展望,希望对下一步智能卡PP的开发有所帮助。同时也希望有助于其他的信息安全产品或技术PP的开发。

参考文献

[1] 国家技术监督局.GB/T 18336-2001.信息技术安全技术信息技术安全性评估准则[S].北京:中国标准出版社,2001.

[2] Common Criteria for Information Technology Security Evaluation. Version 2.1.ISO/IEC 1548, CCIB-99-031,1999.

[3] 穆肇骊,赖华添,耿静.信息安全技术电信智能卡安全技术要求.中国信息安全产品测评认证中心,1999.

[4] 李守鹏,徐长醒,付敏,等.信息安全技术智能卡嵌入式软件安全技术要求(EAL4增强级).GB/T 20276-2006,2006.

[5] 中国信息安全测评中心分级文档编写指南EAL4.V2.0.EAL4+认证编写指南[S].北京:中国信息安全测评中心,2008.

(收稿日期:2009-11-06)

作者简介:

刘瑞玲,女,1982年生,硕士研究生,主要研究方向:3G智能卡的开发、并行计算。