第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

多应用智能卡平台和操作系统

吴 俊
(上海市经济和信息化委员会信息中心 上海 200125)

摘 要 智能卡可以安全地存取个人私密信息,提供包括密码服务和访问控制等多种服务。随着微电子技术的发展,多应用智能卡应运而生,并成为智能卡领域的发展方向。介绍了当前业界主流多应用智能卡平台和操作系统,即Java Card、GlobalPlatfrom、MULTOS、Smartcard.NET和BasicCard,着重说明了采用的架构和安全技术。

关键词 多应用智能卡,平台,操作系统,架构,安全技术
中图法分类号 TP316 **文献标识码** A

Multi-application Smart Card Platform and Operating System

WU Jun
(Shanghai Municipal Economic and Informatization Commission Information Center, Shanghai 200125, China)

Abstract Smart cards provide secure access to private personal information and many other services including cryptographic services and access controls. With the development of microelectronic technology, multi-application smart cards come into being and become the new tendency in the field. In this paper, currently five most popular multi-application smart card platforms and operating systems, which are Java Card, GlobalPlatform, MULTOS, Smartcard.NET and BasicCard, are introduced, and their architecture and security technology are underlined.

Keywords Multi-application smart card, Platform, Operating system, Architecture, Security technology

智能卡(Smart Card)为内嵌集成电路芯片的塑料薄片,包含微处理器、I/O接口和存储器。智能卡内存储持卡人的个人信息,提供支持认证(authentication)、完整性(confidentiality)和机密性(integrity)机制的密码服务和访问控制。

智能卡作为信息的存取设备,具有便携度高、安全性好等优点,现已在金融财务、社会保险、交通旅游、医疗卫生、政府行政、商品零售、休闲娱乐、学校管理等领域得到广泛应用。随着应用领域的拓展,智能卡需要提供的服务也越来越多元化,功能要求也越来越复杂,功能单一的单应用智能卡无法适应要求,可跨行业使用的多应用智能卡应运而生。

本文简述了智能卡的发展历程,并列举了目前业界主流的多应用智能卡平台和操作系统,分别就架构和安全技术进行介绍。

1 智能卡的发展历程

20世纪90年代初的智能卡硬件设备容量小,ROM容量通常只有1~3kB,RAM容量不到128B,EEPROM容量也只有1~2kB;软件平台由若干例程组成,支持简单的文件管理操作如数据读写等以及若干加密操作,使外界可以通过受控方式与智能卡通信,通信遵循ISO7816-4系列规范[1]。由于ROM对芯片容量的利用率高等原因,智能卡一般采用掩膜ROM技术把例程固化在ROM中,因此常被称为整体(Monolithic)系统。

到90年代中期,智能卡引入了智能卡操作系统(Smart Card Operating System, SCOS)的概念,用于分配系统资源并支持应用程序运行。然而此时大部分应用依旧以预先约定的结构固化在ROM中,留给后继应用开发的空间很小。发卡方出于安全目的对应用开发信息保密,缺乏必要的开发工具,应用开发者几乎无从下手。

智能卡微处理器技术持续发展,在设备容量、通信表现和运算效率等方面都有进步,使操作系统设计上的限制减少,产生了使用扩展表(Extension Table)扩展操作系统功能等新方法。随着技术的不断积累,90年代末期出现了开放的多应用智能卡平台,这种平台使用户可以在发卡后(post-issuace)下载应用到智能卡。发卡方提供一组应用程序设计接口作为框架,提供工具实现数据和代码共享,并使上层用户如服务提供方和持卡方等可以自行设计和加载应用。显然,可移植性、互操作性和安全性是多应用智能卡技术的要点,其中如何为应用提供安全且有约束的运行环境是重中之重。

2 多应用智能卡平台和操作系统

目前多应用智能卡技术的代表有Java Card、MULTOS、GlobalPlatform、SmartCard.NET和BasicCard等,其中MULTOS是智能卡操作系统,而Java Card、GlobalPlatform、SmartCard.NET和BasicCard是操作系统上的应用平台,其中Java Card和GlobalPlatform非常相近。

2.1 Java Card

Java Card始创于1996年前后,为可以执行Java应用的

吴 俊 高级工程师,主要研究领域为信息安全、信息系统集成,E-mail:Leowoo519@hotmail.com。

智能卡。事实上,由于硬件限制等原因,Java Card 对 Java 语言的支持并不完全,Java Card 语言只是 Java 语言的子集。

2.1.1 架构

Java Card 架构[2]如图 1 所示,操作系统由通信协议、加密程序和文件系统等组成;Java Card 运行环境(Java Card Runtime Environment,JCRE)负责执行应用并保证各独立应用相互隔离[3],由 Java Card 虚拟机(Java Card Virtual Machine,JCVM)、应用程序设计接口(Application Programming Interface,API)和应用安装程序组成。

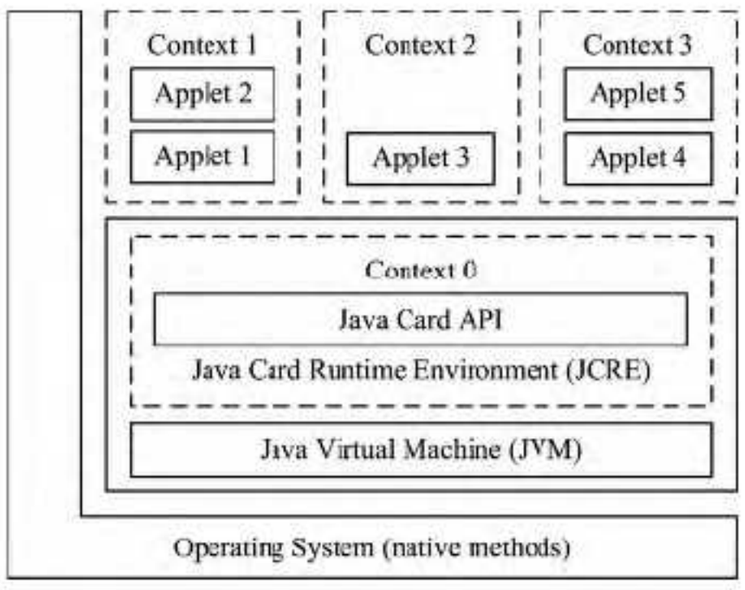

图 1 Java Card 架构

开发者使用 Java Card 语言编写应用,经过编译生成字节码,由 JCVM 解释生成机器码,使不同的智能卡可以执行相同的应用[4]。事实上,由于空间限制,JCVM 的加载、链接和字节码校验等功能通常被移至终端平台或工作站由专门的校验程序执行,卡端只有应用运行相关功能。Java Card API 分为 Java 核心类的小型子集和用于支持 Java Card 应用的框架 API(framework API),后者定义了用于应用的核心框架。

Java Card 规范不涉及智能卡及应用管理,如下载或删除应用等卡操作由附加组件卡管理器(Card Manager)实现。

2.1.2 安全技术

Java Card 安全性的基础是 Java 语言安全性。Java 语言继承了 C++语言面向对象技术的核心,舍弃了指针、运算符重载等容易引起错误的特性。Java Card 语言继承了这些优点,但同时也应注意 Java Card 语言没有垃圾收集(Garbage Colletion)等功能。

对于新应用,字节码校验器会检查应用是否越界使用资源等事项,生成的应用(Converted Applet,CAP)文件由发行方签名,经智能卡验签通过后加载。

Java Card 使用类似沙箱的策略实现实时校验,即 JCRE 为每个应用程序分配一个上下文(context),用于控制所分配对象的访问,上下文的边界通常被称为防火墙(firewall)。一个上下文内可以有多个应用程序和其他对象,如安全密钥等。防火墙创建了虚拟堆,同一上下文中各应用可以互相访问彼此的公开方法;不同上下文间,除非受访方法得到所属应用许可,否则禁止来自其他上下文中的应用访问。

2.2 GlobalPlatform

全球平台组织(GlobalPlatform)是跨行业的非营利组织,致力于开发、制定并公布在安全芯片上的技术标准。该组织的成员数在 2012 年过百,GlobaPlatform 现已成为业界主流多应用智能卡应用平台之一。

2.2.1 架构

GlobalPlatform 架构[5]如图 2 所示,底层为智能卡微处理器,其上一般为运行时环境(Run-Time-Environment,RTE),后者被认为是 GlobalPlatform 卡片规范(GlobalPlatform Card Specification,GPCS)和底层硬件间提供抽象层。典型的 RTE 包括智能卡操作系统、虚拟机和应用程序设计接口(API) 3 部分。API 为应用开发者提供 GPCS 中定义的基本功能,它也包括一些 ISO 7816-4 中定义的功能。

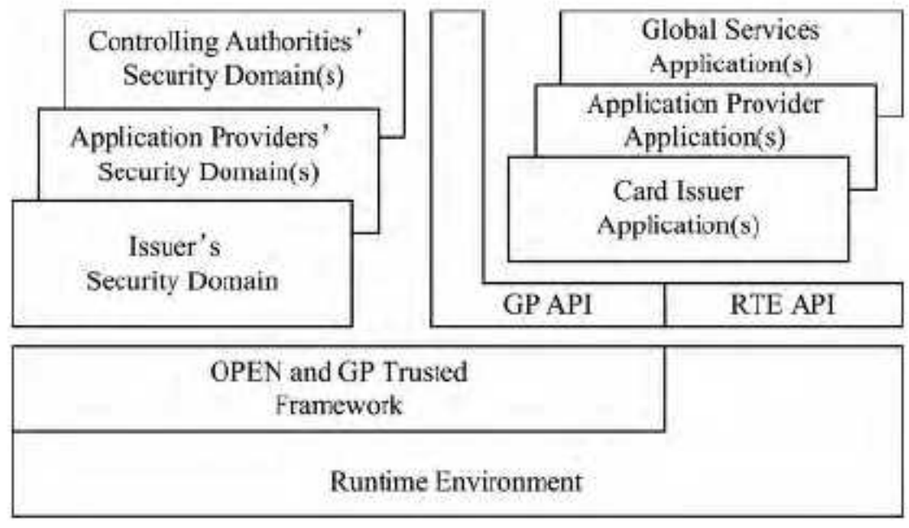

图 2 GlobalPlatform 架构

安全域(Security Domain)依据现有的 3 种卡外授权机构,分为发卡方、补充和授权管理者安全域,其中发卡方安全域为卡片上首要的、强制性存在的安全域,是卡片管理者在卡片内的代表;补充安全域为卡片上次要的、可选择存在的安全域,是应用供应方或发卡方及其代理方在卡片内的代表;授权管理者安全域为一种特殊类型的补充安全域,是授权管理者在卡片内的代表,可以存在一个或多个。

GlobalPlatform 环境(GlobalPlatform Enviroment,OPEN)的主要功能包括向应用提供 API、命令转发、应用选择、逻辑通道管理和卡片内容管理(Card Content Management)等,与发卡方安全域和持卡方验证服务(Cardholder Verification Method Services)共同组成卡片管理器(Card Manager),后者是 GlobalPlatform 智能卡的中央控制实体。

2.2.2 安全技术

(1)安全域

安全域负责提供各类安全服务,包括密钥管理、加密解密、针对其提供者的应用进行数字签名验签。发卡方、应用供应方、授权管理者等卡外实体可以由新的安全域代理实现从其他实体区隔离所需密钥。

(2)卡片内容管理

卡片目录管理是实现智能卡安全下载应用的重要先决条件,包括加载文件数据块散列值(Load File Data Block Hash)、加载文件数据块签名(Load File Data Block Signature)、委托管理令牌(Delegated Management Tokens)和收条(Receipts)。

加载文件数据块散列值用于向 GlobalPlatform 加载数据时验证加载文件数据块的完整性。

加载文件数据块签名是由卡外实体产生的认证数据值,作为加载文件数据块散列值的数字签名并附着在加载文件的数据鉴别块中,每个加载文件附有一个或多个数据鉴别块。向卡片加载文件时,每个存在的数字签名必须由恰当的安全域进行验证,即数据鉴别模式验证。

委托管理令牌是发卡方对加载、安装、让渡和删除等委托管理操作创建的签名，使发卡方可以控制其发行卡片的内容变化，该令牌必须由恰当的安全域进行验证。

收条是应用供应方已经对卡片内容进行改变的证据，由恰当的安全域在委托管理时创建。

(3)GlobalPlatform 安全通道协议(GlobalPlatform Secure Channel Protocols)

GPCS 在 ISO 7816-4 相关协议之上定义了自己的安全通信协议。安全通道会话用于卡片与外界通信中的实体认证及随后的加密保护。

安全通道可以用于所有 GlobalPlatform 敏感操作。

2.3 MULTOS

MULTOS 是开放标准，由智能卡业界众多厂商组成的 MULTOS 联盟(MULTOS Consortium)推动，现已成为世界范围内最流行的多应用智能卡应用平台。

2.3.1 架构

MULTOS 架构[6]如图 3 所示，底层为智能卡微处理器，多应用操作系统(Multi-Application Operating System, MAOS)提供输入输出、通信协议、加密算法和文件系统管理等基本功能项，驻留在 MAOS 上的虚拟机称为应用抽象机(Application Abstract Machine, AAM)，负责提供应用运行环境、内存管理和应用的下载和删除。

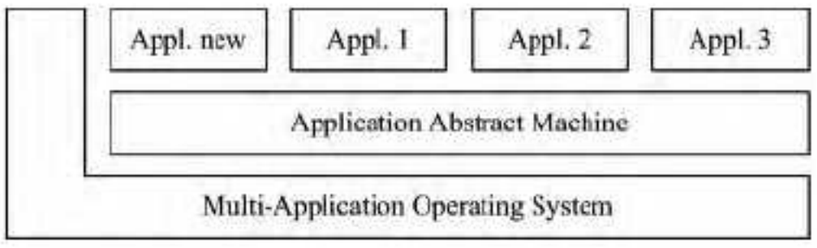

图 3 MULTOS 架构

MULTOS 仅支持单线程，即同一时间只能有一个应用，且应用间没有通信协议，即所有应用都是严格隔离的。

2.3.2 安全技术

MULTOS 独有的安全技术包括执行应用的虚拟机 AAM 和 MULTOS 安全方案(MULTOS security scheme)，如密钥管理中心(Key Management Authority, KMA)等，用于保护芯片、应用代码和数据。

(1)虚拟机 AAM

MULTOS 应用的开发语言一般为 C 或 Java，经编译生成 MULTOS 可执行语言(MULTOS Executable Language, MEL)字节码，由虚拟机解释执行。对于非法指令及尝试内存访问，虚拟机会拒绝操作，同时所有卡上应用操作停止运行。执行时校验(Execution-time Checking)可以保证应用安全运行，同时防止其他应用访问其数据。

(2)KMA

KMA 为启用智能卡、批准加删应用和注入传输密钥等操作提供了安全途径。KMA 使用非对称密钥，私钥存储在卡内，用于解密来自发卡方和 KMA 的信息，私钥不出卡。只有在给出匹配证书的条件下用户才能进行加删应用等操作，操作所需的证书由发卡方向 KMA 申请得到。

2.4 Smartcard.NET

Smartcard.NET 是由 Hive-Minded 开发的智能卡上.NET平台，它的出现有助于实现智能卡与 Microsoft 计算机系统和设备间安全的网络连接。

2.4.1 架构

Smartcard.NET 是具有互操作性的多应用多语言平台，架构[7]如图 4 所示，开发者可以在 C#、C++、Visual Basic (VB)、J# 和 JavaScript 等中任意选择并使用最合适的语言编写应用，代码经过编译生成.NET 码，由虚拟机解释执行。

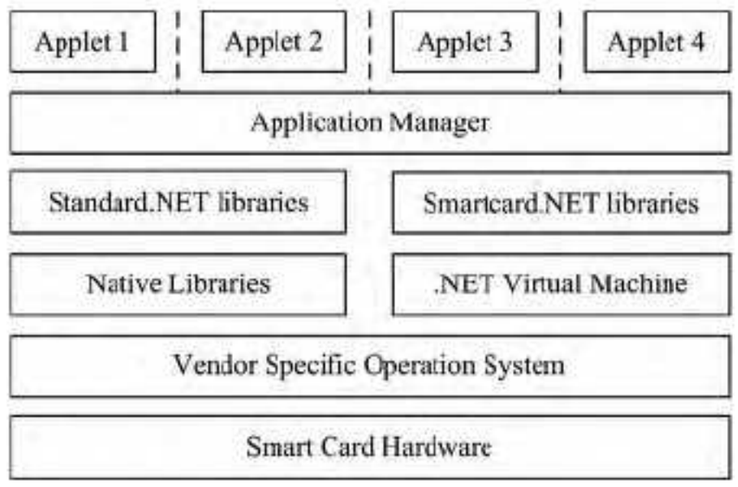

图 4 Smartcard.NET 架构

目前平台已经支持流、64 位整数和代码检验，并提供垃圾回收机制，但依旧不支持浮点数。

2.4.2 安全技术

Smartcard.NET 中的 NCFS 文件系统(.NET Enabled SmartCard FileSystem)类似 Windows 平台的 NTFS 文件系统，提供用户级访问控制和线程级访问控制。

.NET 虚拟机使用应用域(Application Domain)隔离运行中的应用并防止访问非公开数据。

2.5 BasicCard

2.5.1 架构

ZeitControl 开发的 BasicCard 由 $T=0$ 字节级(byte-level)通信协议、指令调度程序、内置指令、虚拟机和类似 PC 上基于目录的文件系统和浮点运算器组成。值得一提的是，目前业内仅 BasicCard 可以直接支持浮点数操作[8]。

通过网络开发者可以免费获得完整的 BasicCard 开发环境。开发者可以使用 ZeitControl Basic(ZC-Basic)语言编写应用，经过编译生成 P-code，由虚拟机解释执行。为使开发者可以快速编写终端和卡端应用，BasicCard 工具箱免费提供封装了 ISO-7816 协议的 API。BasicCard 还提供若干插件库用于支持后续拓展和升级。

2.5.2 安全技术

BasicCard 通过验证电子签名实现安全加载新应用，并为应用间的隔离和通信提供途径。

BasicCard 提供了一个加密算法库用于保证卡上应用和终端程序安全通信，算法有用于认证加密的 EAX 和用于信息验证的 OMAC[9]。

结束语 随着物联网和智慧城市的发展，支持多应用的智能卡将成为今后智能卡应用发展的趋势。

从本文可以看出，多应用智能卡可内置若干应用，通过嵌入式操作系统支持不同应用的加载与运行。操作系统作为应用运行时环境，通过虚拟机等核心部件实现可移植性、互操作性和安全性。作为业界先行者，GPCS 定义了安全的可互操作的多应用智能卡平台的各种业务逻辑，Java Card 可以看成是带有 JRE 的 GlobalPlatform。MULTOS 继承了 Java Card 的基本思想，但更着重于互操作性以及多应用管理如执行代

码和加删应用等操作的安全性。

综上所述，通过分析现有各种多应用智能卡的架构，结合具体的应用要求，开发适合各行业发展要求的多应用智能卡产品，将成为今后智能卡技术研究和开发的重点方向。

参 考 文 献

[1] ISO/IEC 7816-4:2005(E). Identification cards--integrated circuit cards--Part 4:organization, security and commands for interchange [S]. Switzerland: ISO/IEC, 2005

[2] Chen Zhi-qun. Java card technology for smart cards: architecture and programmer's guide[M]. Boston: Addison-Wesley Longman Publishing Co., Inc., 2000

[3] Oracle and/or its affiliates. Java card 3 platform runtime environment specification, classic edition version 3.0.4[EB/OL]. http://www.oracle.com/technetwork/Java/Javacard/specs-jsp-1364 30.html, 2013-09

[4] Oracle and/or its affiliates. Java card 3 platform virtual machine specification, classic edition version 3.0.4[EB/OL]. http://www.oracle.com/technetwork/Java/Javacard/specs-jsp-136430.html, 2013-09

[5] GlobalPlatform Inc. GlobalPlatform card specification version 2.2[EB/OL]. http://www.win.tue.nl/pinpasjc/docs/GPCardSpec-v2.2.pdf, 2013-09

[6] MULTOS. An introduction to MULTOS [EB/OL]. http://www.multos.com/uploads/MULTOS-8-page-brochure.pdf, 2013-09

[7] Mayes K, Markantonakis K. Smart cards, tokens, security and applications[M]. New York: Springer-Verlag, 2008

[8] ZeitControl cardsystems GmbH. The compact, enhanced, and professional BasicCards version 4.50[EB/OL]. https://dspace.ist.utl.pt/bitstream/2295/49097/1/BasicCrd.pdf, 2013-09

[9] ZeitControl cardsystems GmbH. Overview[EB/OL]. http://www.basiccard.com/index.html?overview.htm, 2013-09

(上接第 476 页)

管自动化系统"网络环境安全"为"中等风险"程度。

表 3 融合结论

融合次数	m(L_1)	m(L_2)	m(L_3)	m(L_4)	m(L_5)
1	0.031	0.220	0.508	0.241	0
2	0.017	0.142	0.561	0.280	0
3	0	0.086	0.780	0.069	0
4	0	0.074	0.913	0.013	0

基于同样的专家评分结果，采用模糊评价算法得到 5 个评价等级 $L_i=(L_1, L_2, \cdots, L_5)$ 的概率分别为(0, 0.142, 0.731, 0.065, 0.062)。建立折线图比较两种评价结论，由图 1 可得如下结论：两种评价方法评估值变化趋势具有一致性，但 DS 证据理论评价值在等级 L_3 即中等风险处取得较大概率，可信度更高，说明 DS 证据方法更能确定风险发生可能等级。对等级 L_1、等级 L_5，DS 证据理论评估值均为 0，表明在定义的低风险和高风险两个等级处 DS 证据理论均排除了其存在的可能性，而模糊评估方法在 L_5 处仍存在评估取值，且 L_4 等级的评估值与 L_5 等级评估值趋于一致，无法对两者进行有效区分。可见 DS 证据理论结论具有更准确、更有效地取得有效评估等级的能力。

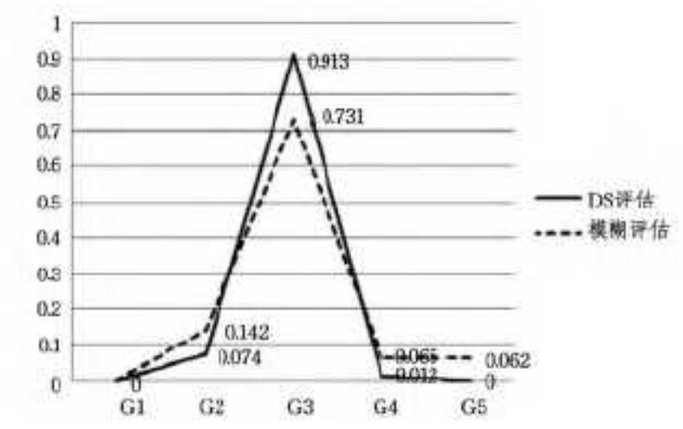

图 1 两种评价方法的风险等级比较

依此方法可以对空管自动化系统的"系统平台安全"、"人员管理安全"设计合理的评价因素。采用多位专家评价结果进行有效融合得到各方面的评价结果，为管制单位空管自动化系统信息安全程度评估提供客观的评判结论。

结束语 本文分析了影响空管自动化系统信息安全的各项因素，为实施客观准确的信息安全评估提出了评价体系。考虑切实的可实施性，评价过程仍采用了传统的专家评分方法，但结合 DS 证据融合理论，可使得该方法的评价结论更准确有效。本方法评价过程直观简易，在实际信息安全评估过程中具有可操作性。

参 考 文 献

[1] 中国民用航空局. 民用航空空中交通管理管理系统技术规范 MH/T 4018.1[S]. 2004

[2] 中国民用航空总局. 中国民航空管系统安全管理体系建设与实施指南[S]. IB-TM-2010-003, 2013

[3] 张文涛. 一种基于业务信息流的空管信息系统安全评价指标体系[J]. 计算机安全, 2009(4): 15-20

[4] 马兰, 吴志军, 潘雯. 民航 ATM 信息系统安全性评价指标体系的研究[J]. 微计算机信, 2010, 26(3): 39-43

[5] 中华人民共和国国家质量监督检验检疫总局. 信息安全风险评估规范 GB/T 20984-2007[S]. 2007

[6] 李大海. 民航空管网络与信息安全管理体系的构建研究[D]. 天津: 天津大学, 2009

[7] 潘雯. 民航 ATM 系统安全性评价指标体系的研究[D]. 天津: 中国民航大学电子信息工程学院, 2008

[8] 田春岐, 邹仕洪, 王文东, 等. 一种新的基于改进型 D-S 证据理论的 P2P 信任模型[J]. 电子与信息学报, 2008, 30(6): 1480-1484

[9] 韦勇, 连一峰, 冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2009, 46(3): 353-362

[10] 石波, 谢小权. 基于 D-S 证据理论的网络安全态势预测方法研究[J]. 计算机工程与设计, 2013, 34(3): 821-825

[11] Shafer G. A Mathematical Theory of Evidence [M]. Princeton: Princet on University Press, 1976

[12] 中华人民全国信息安全标准化技术委员. 信息系统安全等级保护定级指南 GB/T 22240-2008[S]. 2008