

智能卡安全中间件的研究与开发^{*}

沈 仟 余 堃 周明天 宁显明

(电子科技大学-卫士通信信息安全联合实验室 成都610054)

摘 要 本文介绍了智能卡中间件的关键技术和层次结构模型。在此基础上结合其在金融领域的实际应用,提出各种层次模型的用例,并详述了层次和用例的服务功能以及屏蔽差异的关键技术。

关键词 智能卡,中间件,用例

The Research and Development of Middleware of Smart Card

SHEN Qian SHE Kun ZHOU Ming-Tian NING Xian-Ming

(Information Security United Lab, of UESTC-WESTONE, Chengdu 610054)

Abstract Key technology of middleware of smart card and its hiberarchic model are introduced. Based on its' application in the field of fianance, we raise some kinds of use case of layer models, and descript the service function of layers and use case and key technology in masking difference in detail.

Keywords Smart card, Middle ware, Use case

1 引言

在不远的将来,全球的各种电器以各种不同的方式连接成为一个网络。网络安全问题将变得尤为突出。使用智能卡可以很好解决网络时代的安全问题。借助智能卡上验证口令,存储密码,访问控制和进行加解密运算,存储用户的照片、指纹等生物信息,有助于构造一个安全的信息网络体系^[1,2]。

2 问题的提出

尽管智能卡在安全方面有着无可比拟的优势,但是往往智能卡及设备程序员又不得不面临着诸多智能卡、读写器和通信信道之间互不兼容的难堪局面^[5]。因此我们提出了全新的技术和观念——智能卡中间件。它可以使应用程序无缝地在各种智能卡、智能卡读卡器和通信信道上移植,有效地减少智能卡应用的开发工作,彻底地解决以前那种只要更换智能卡、智能卡读卡器和通信信道中的任何一种设备及相关的软件或软件库就必须从新修改程序甚至重新开发的问题。

3 智能卡中间件的体系结构

智能卡(smartcard)可分为:存储卡、逻辑加密卡、CPU卡以及近期发展的超级CPU卡。CPU卡通常本身就具有很强的硬件安全逻辑^[3],一般都能提供生成随机数、内外部认证、验证用户PIN、对称加密、非对称加密^[4],因此可以应用到银行金融系统^[8]。

中间件(middleware)就是处于操作系统软件与用户的应用软件的中间,是基础软件的一大类,属于可复用软件^[6,7]。概括地讲:中间件是一种独立的系统软件或服务程序,分布式应用软件借助这种软件在不同的技术之间共享资源,中间件位于客户机服务器的操作系统之上,管理信息网络资源和网络

通信。

智能卡中间件,就是处于应用层之下,在硬件设备(智能卡、读卡器、通信信道)之上的系统软件。它的主要功能是用来管理下层的软硬件资源,屏蔽其各种差异。智能卡中间件的体系结构如图1所示。

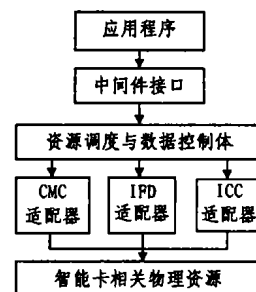


图1 系统体系结构

4 智能卡中间件的设计与实现

4.1 基于应用的物理模型

根据一个完整的应用服务,我们提出图1的智能卡中间件的应用模型。从这个模型中可以比较清楚地看到智能卡中间件在应用中所处的地位以及完整的应用层次结构。在这个应用模型中,智能卡中间件扮演着下层服务的总调度师以及为上层提供服务的职责。

模型说明:应用程序调用智能卡中间件提供的统一接口,它不用去关心特定的通信信道、智能卡读卡器、智能卡的差异。在程序初始化阶段智能卡中间件必须有一个自举的过程,这个过程可以通过读配置文件或通过读数据库有效获取下层通信信道、智能卡读卡器、智能卡的信息。上层形成API调用,智能卡中间件首先自举获取所需信息,形成加报头、报尾、

^{*}基金项目:国家863项目863-104-03-01课题资助。沈 仟 硕士研究生,主要方向:信息安全,PKI。余 堃 副教授,主要研究方向:分布式计算信息安全。周明天 博士导师,主要研究方向:中间件计算信息安全。宁显明 硕士研究生,主要研究方向:智能卡。

校验信息和 APDU 的数据包,称为 ICC 数据包,然后再形成 IFD 数据包,最后形成 CMC 数据包。

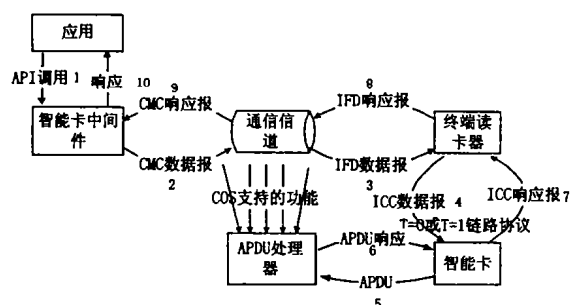


图2 基于应用的物理模型

然后按照图2所示的流程根据 API 调用在每个接口逐层地解析、剥离。最后 APDU 处理器在 COS 的控制下处理 APDU 数据包。

功能操作完成以后,按照逆向的过程形成 ICC 响应包,智能卡读卡器再根据 ICC 响应包构造 IFD 响应包,IFD 响应包可靠完整地通信信道传输到智能卡中间件,智能卡中间件根据已经得到的下层通信信道、智能卡读卡器、智能卡信息,完成对得到的 CMC 数据包的分析,最后给应用程序返回执行状态、得到的响应数据等。

4.2 智能卡中间件的四层模型(图3)

API 接口层:给上层应用提供统一的接口 API,为应用程序解释对 API 调用。同时把执行后的状态和得到的数据返回给应用程序;

智能卡子层:根据智能卡类型,形成 ICC 数据包;

智能卡读卡器子层:根据智能卡读卡器类型,将智能卡子层得到的 ICC 数据包加上 IFD 包头、IFD 包尾和校验形成 IFD 数据包;

通信信道子层:根据通信信道,将 IFD 数据包加上 CMC 包头、CMC 包尾和校验形成 CMC 数据包。

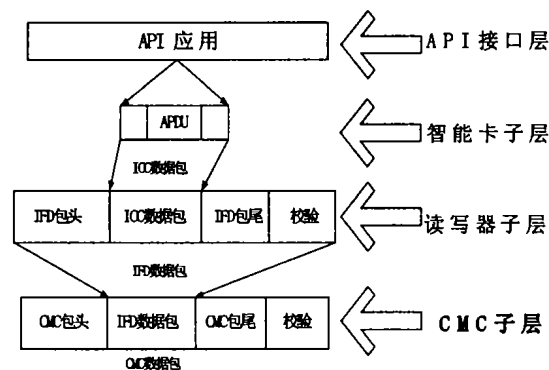


图3 智能卡中间件的四层模型

4.3 智能卡中间件的系统逻辑模型(图4)

智能卡应用进程,基于智能卡中间件提供的服务,完成特定的功能的进程。

智能卡中间件 API,提供给用户的接口,用户通过调用这些接口,完成其所需要的功能。

智能卡中间件资源管理调度和数据控制体,这是整个系统的核心部分,将完成对智能卡、智能卡读卡器以及通信信道以及各配置文件等资源的管理,同时完成相应的数据控制功能。

CMC 适配器、IFD 适配器和 ICC 适配器,这是智能卡中间件资源管理调度和数据控制体的中间部分,分别对通行信

道、读写器和智能卡进行配置管理。

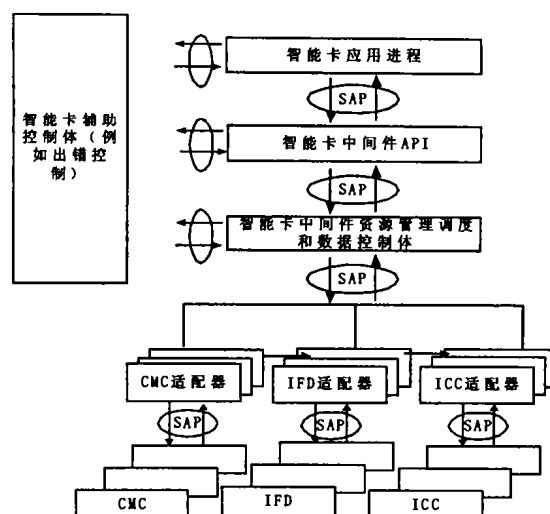


图4 系统逻辑模型

5 系统用例分析

我们定义的系统用例有:系统主用例分析(图5)、智能卡数据通信用例分析、智能卡读写器通信服务用例和通信信道服务用例,下面做简单叙述。

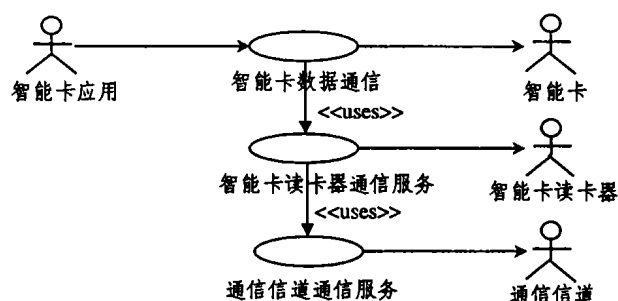


图5 系统主用例图

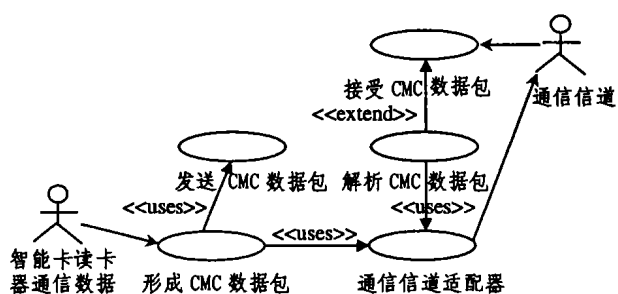


图6 CMC 用例图

这里我们定义的角色都是为了屏蔽这一层设备或者环境的差异而专门抽象出来的。经过中间件的屏蔽,使用者可以不管具体的差异直接可以对下层进行操作访问。“智能卡应用”这个角色,其实是向用户提供的平台,即通用 API,而不管 IFD、ICC、CMC 等的差异性。其它的角色“智能卡数据通信”、“智能卡读写器通信服务”、“通信信道”这些对用户来说感觉并不存在,确实,这从另一方面也体现了智能卡中间件的作用,用户用不着管设备或通道有什么功能、电气特性、提供什么功能。系统设计中,可详细了解每个抽象的角色分别提供什么具体的服务。我们以 CMC(通信信道)提供的服务来说明:

对用户来说根本不需要知道具体应用中通信信道的参数、电气特性、服务等。

“形成 CMC 数据包”使用案例旨在准确而安全封装以得到 CMC 数据包,因为在 WINDOWS 系统模式、UNIX 系统模式和 UNIX 终端模式下形成 CMC 数据包的方式不尽相同。这样通过通信信道适配器提供的服务生成统一标准的 CMC 数据包。

“发送 CMC 数据包”使用案例完成 CMC 数据包的发送,发送的数据将被硬件设备通信信道、智能卡读卡器和智能卡一层一层地进行解析,最后成为符合 ISO7816 规定格式的 APDU 从而被智能卡执行,完成相应的功能和服务。篇幅关系,其它的角色功能即用例省略。

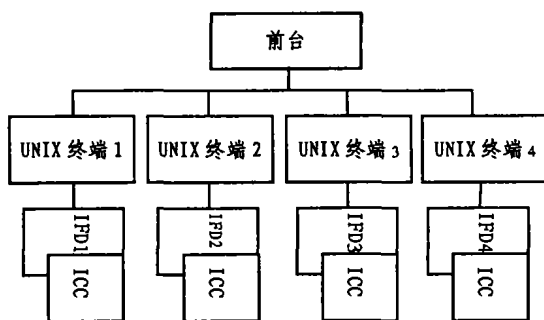


图7 应用案例系统结构

(上接第88页)

7 实验

实验的目的是测试系统是否能识别和正确抽取所要的关系信息。首先,我们定义了课程-教师关系,并输入一些课程名和人名作为训练数据,建立一个关系模型。然后从 www.princeton.edu/index.shtml 开始,搜索了该网站的1196个链接,下载了5111张网页作为测试数据。

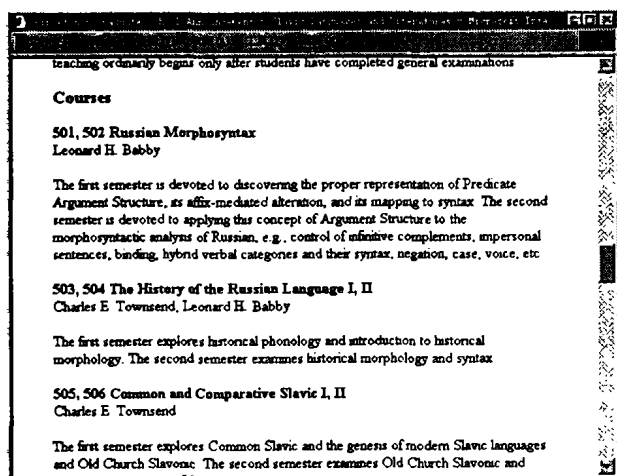


图5 无列名的列表

最初测试时我们分别设 $\delta_{ST}=0.3$, $\delta_{TE}=0.2$, $\delta_{PT}=0.1$, k_1, k_2 和 k_3 为 $1/3$, 阈值为 0.5 , 实验系统能准确识别网页上编写比较规则的列表结构(如图2、3、5), 并正确地抽取带有列标题的列表中的关系元组。如图2中列表, 由于列名含有两个实体的关键字, 其语义可信度达最大, 为1, 其第一列与课程实体的相似度大于其他列与课程实体的相似度, 第八列与教师实体的相似度也大于其他列与课程实体的相似度, 并且两者均大于 0.5 , 所以, 系统准确地从中抽取课程-教师元组。像图5这

结束语 智能卡作为 IT 产业中最热门的工具, 其独有的特性: 便携性、高度安全性和抗损的数据存储功能等, 使得它成为近年来发展最快的一个分支。为了将多样性的智能卡应用抽象的简单而诞生了智能卡中间件。

江西省建设银行柜员卡系统采用基于 PKI 技术的强安全体系, 而本智能卡中间件是整个安全体系机构中重要的部分。操作员需要通过智能卡从终端登录, 交易过程中也需要用智能卡进行身份识别或用卡直接产生签名。案例系统结构如图7所示。

通过该中间件系统的应用大大降低了上层应用开发的时间, 将程序员从诸多类似重复的劳动中解放出来。

参考文献

- 1 Schneier B, Shostack A. Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards, Oct. 1999
- 2 David Michal W, Kouichi S. Security issues for contactless smart cards. Lecture Notes in Computer Science, 1998
- 3 Anon. Smart-card microcomputers for high-security applications. Hitachi Review n SPECIAL ISSUE July 2001
- 4 Poggi A, Rimassa G, Turci P. What agent middleware can (and should) do for you. Applied Artificial Intelligence, 2002, 16(9-10): 677~698
- 5 宁显明. 智能卡中间件: [硕士论文]. 成都: 电子科技大学, 2002
- 6 TongSEC V1.0 安全中间件白皮书. 北京: 东方通科技公司
- 7 秦志光, 周世杰, 刘锦德. 智能运输系统中的中间件技术. 电子科技大学学报, 2002, 31(2): 168~172
- 8 黄文贵. 电子商务安全与智能卡. 中国数据通讯网络, 2000, 7: 150~152

样无列名的列表, 按上述设置, 其语义可信度及列与实体的相似度较低。于是, 我们动态调整系数, 对无列名的列表结构, 降低列名对计算结果的影响。对图5, 最后识别的结果是: 第二列(由“Russian Morphosyntax”, “The History of Russian Language I, II”等组成)与课程最相似, 第三列(由“Leonard H. Babby”, “Charles E. Townsend, Leonard H. Babby”等组成)与教师实体最相似。最后, 我们从所下载的网页中抽取1061个关系元组。

结束语 本文提出了一种识别和抽取 Web 列表中的关系信息的方法, 该方法是基于语义和数据特征的, 可用来收集 Web 上的关系数据, 以便进一步分析处理。初步实验结果表明, 本方法是可行的, 它能较准确地识别和抽取编写比较规则的、特别是有列名的 Web 列表中的关系信息, 对于无列名的列表结构, 采用半自动的方法, 效果比较好, 如何自动且准确地识别和抽取无列名的列表中的关系信息, 还须进一步研究和实验。

参考文献

- 1 Hammer J, Hector Garcia-Molina, Svetlozar Nestorov, Ramana Yerneni, Merkus M. Breuning, and Vasilis Vassalos. Template-based wrappers in the TSIMMIS system. In: Proc. of ACM SIMOD Conf. on Management of Data, Tucson, Arizona, 1998
- 2 Gruser J-R, et al. Wrapper generation for web accessible data source. In: Proc. of the CoopIS, 1998
- 3 Kuserick N, et al. Wrapper induction for information extraction. IJCAI-97, pp. 729~737
- 4 Brin S. Extracting patterns and relations from the World-Wide Web. In: Proc. of the 1998 Intl. Workshop on the Web and Databases, 1998
- 5 Agichtein E, Gravano L. Snowball: Extracting Relations from Large Plain-Text Collections. In: Proc. of the 5th ACM Intl. Conf. on Digital Libraries, 2000
- 6 Wu Yangyang, Yokota H. A method of recognizing tables and lists on the Web. In: Proc. of Int. Conf. on Communication, Internet, and Information Technology (CIIT 2002), USA, pp. 479~485
- 7 Lin D. An information-theoretic definition of similarity. In: Proc. of intl. conf. on machine learning. Madison, Wisconsin, 1998