(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101930552 B
(45)授权公告日 2015.04.01

(21)申请号 201010255054.4
(22)申请日 2010.08.17
(73)专利权人 公安部第三研究所
地址 200031 上海市徐汇区岳阳路 76 号
(72)发明人 胡永涛 姚静晶 杭强伟 赵宏伟
(74)专利代理机构 上海天翔知识产权代理有限公司 31224
代理人 刘粉宝
(51)Int.Cl.
G06K 17/00(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 101741565 A,2010.06.16, 全文.
CN 101894235 A,2010.11.24, 说明书第 31,41,42 段,权利要求 4-7.

审查员 邓茜

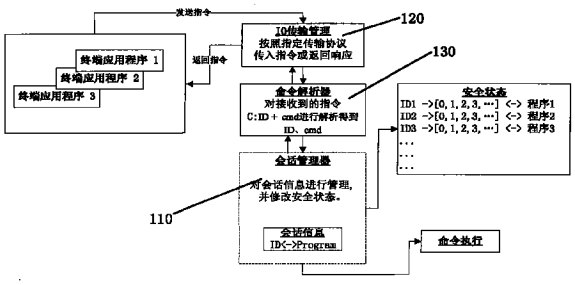
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种标识智能卡通信对象的方法

(57)摘要

本发明的目的在于公开一种标识智能卡通信对象的方法,在现有智能卡安全体系中,引入安全会话的概念,采用在一定时间内建立起智能卡与终端应用程序间的一种半永久性的、带有自动回收机制的、交互式的通信对象标识方式,将应用程序与自身发出的请求关联起来,从而使得智能卡可以同时与多个通信对象(如终端应用程序)进行安全通信;另外,安全会话一旦建立,就应当一直存在,直到终端应用程序操作结束,或者其他使得安全会话终止的情况出现;会话的安全性由安全会话对称密钥和安全会话公私钥对保护。



CN 101930552 B

1. 一种标识智能卡通信对象的方法，其特征在于，包括智能卡、传输管理器、命令解析器和安全会话管理器，安全会话管理器、传输管理器和命令解析器相互连接，传输管理器用于接收来自终端硬件的电气信号，转换成逻辑数据传递给命令解析器；将来自智能卡的响应信息以电气信号传递给终端硬件；命令解析器用于解析终端应用程序发来的指令，从中得到安全会话标识和指令内容；安全会话管理器用于管理安全会话标识 ID 的会话信息，并根据会话信息修改相应的安全状态；

它包括如下步骤：

终端应用程序发起安全会话，由终端应用程序产生随机数 R 作为安全会话标识，并将安全会话标识发送给智能卡的传输管理器，传递至命令解析器；命令解析器解析得到安全会话标识，然后执行创建会话工作，将安全会话标识发送给安全会话管理器；安全会话管理器产生安全会话标识 ID，将安全会话标识 ID 绑定，然后返回绑定的安全会话标识 ID 给终端应用程序，以此建立与终端应用程序的一个会话；当会话建立之后，终端应用程序访问智能卡时，由终端应用程序通过传输管理器发送安全会话标识 ID 和指令及指令的 hash 摘要；命令解析器在接收到带有安全会话标识 ID 的指令后，在安全会话管理器中验证当前安全会话标识 ID 是否合法；如果合法，则继续验证指令，进行命令执行；

所述安全会话是指在一定时间内建立的、在智能卡与终端应用程序间的一种半永久性的、带有自动回收机制的交互式的信息交换方式；

所述安全会话由设置在智能卡中的安全会话管理器管理，并根据安全会话标识和随机数生成的会话信息修改相应的智能卡的安全状态；

所述安全会话管理器的安全会话的生命周期包括安全会话初始化、安全会话通信和安全会话资源释放；当安全会话执行过程中发生错误，安全会话自动终止，安全会话管理器自动释放安全会话资源；安全会话的执行时间超过安全会话管理器的时间限制，安全会话自动终止，安全会话资源被释放；通信过程中掉电，安全会话管理器全部重置，安全会话资源被释放。

一种标识智能卡通信对象的方法

技术领域

[0001] 本发明涉及一种标识通信对象的方法，特别涉及一种计算机安全以及智能卡的应用安全领域，应用于终端与智能卡的安全通信方面的标识智能卡通信对象的方法。

背景技术

[0002] 智能卡作为一种保障电子政务、电子商务安全的手段，其应用范围越来越广；美国ROCKVILLE 市场调研组最新发布了关于智能卡的 RNCOS 报告，其报告表示在 2012 年智能卡市场将增长 13％，随之而来的问题是如何保障智能卡自身的安全，例如如何兼顾智能卡的可靠性和灵活性，如何兼顾智能卡在使用过程中的便利和数据安全等等。

[0003] 智能卡的安全性是由其安全体系加以保障，对智能卡安全体系的研究目前主要集中在安全访问控制模型和设备认证模型等方面；智能卡的安全体系是智能卡的 COS(Card Operating System) 中一个极为重要的部分，包括三大部分：安全属性、安全状态以及安全机制；

[0004] 安全属性是智能卡执行某个指令所需要的一些条件，只有智能卡满足了这些条件，该指令才是可以执行的。

[0005] 安全状态是指智能卡在当前所处的一种安全级别，这种安全级别是在智能卡进行完复位应答或者是在其处理完某操作指令之后得到的。

[0006] 安全机制是安全状态实现转移所采用的转移方法和手段，通常包括通行字鉴别，密码鉴别，数据鉴别及数据加密等。

[0007] 按 ISO/IEC 7816 标准规定，智能卡中的数据在用户存储器中以树型文件结构的形式组织存放，智能卡的安全属性是和内部文件相关联的，具体是指对某个文件或者文件的一部分进行某种操作时必须达到的状态，有时称为访问权限；文件的访问权限是在文件创立时指定的，密钥的访问权限是在密钥写入时指定的；通过设置安全状态和安全属性，可以有效地控制文件的读写操作，从而保证数据的私密性。

[0008] 如图 1 所示，结合智能卡的安全体系和文件系统，现有的智能卡的应用控制流程如下：

[0009] 每个应用由一些具体的指令组成，这些指令通常都是对智能卡内文件的操作；指令的执行有一定的先后顺序，后一个指令的执行必须建立在前一个指令完成的基础上；

[0010] 和应用相关的每个智能卡文件拥有自己的安全属性，这些属性规定了指令对文件进行操作前应满足的安全条件；在一个指令的执行过程中，可以用文件当前已经满足的安全条件的集合来表示文件的安全状态；

[0011] 每个指令在访问某个具体文件前，必须符合一定的安全条件；一旦该条件被满足，指令就可以执行，并依据相应的安全机制改变文件当前的安全状态；

[0012] 当指令执行发生错误或者一个应用的所有指令都执行完毕，文件的安全状态被重置为初始安全状态。

[0013] 在应用结束前，随着指令的执行，文件的安全状态被改变，指令所具备的文件访问

权限逐步提升，以满足应用需要。

[0014] 在智能卡安全体系的具体内容里，大部分实现都是基于对智能卡的身份认证，以保证终端的安全；从智能卡的角度，也面临类似的安全问题，即如何保证当前发送指令的应用程序和上一次通过智能卡安全体系验证的应用程序是同一个，或者进行文件操作的指令是否是前一个改变文件操作模式的指令的合法后继操作。

[0015] 如图 1 所示，现有的智能卡安全体系并不能保障是同一个应用导致的状态迁移，从而可能存在以下攻击方式：

[0016] 旁路攻击：当合法进程以共享模式与智能卡交互、通过安全验证后，智能卡安全状态会保持一定时间，在应用操作结束前，非法进程就会利用已提升的操作权限访问智能卡，甚至替换卡内的密钥文件等，阻止合法操作的顺利进行；但是如果完全禁止共享模式，会影响多个应用同时对智能卡的访问。

[0017] 中间人攻击：攻击者通过各种技术手段将攻击软件或硬件装置放置在智能卡与终端的合法应用程序之间，在智能卡和真正的应用程序之间传递消息，同时监视、篡改它们之间通信的内容。

[0018] 综上所述，针对现有的智能卡安全体系存在的上述缺陷，特别需要一种标识智能卡通信对象的方法，以解决以上提到的智能卡的安全性问题。

发明内容

[0019] 本发明的目的在于提供一种标识智能卡通信对象的方法，针对现有技术的不足，解决现有技术中智能卡安全性的问题，基于非对称技术的智能卡安全会话机制，通过通信安全会话的方式，由完整的安全通信机制流程实现智能卡安全会话。

[0020] 本发明所解决的技术问题可以采用以下技术方案来实现：

[0021] 一种标识智能卡通信对象的方法，其特征在于，它包括如下步骤：

[0022] (1) 终端应用程序发起安全会话，产生随机数作为安全会话标识；

[0023] (2) 将生成的安全会话标识做映射，然后将安全会话标识返回到终端应用程序；

[0024] (3) 当终端应用程序访问智能卡时，需要将指令和安全会话标识一起发送到智能卡并由智能卡解析得到指令；

[0025] (4) 智能卡根据接收到的信息来决定是否允许终端应用程序访问。

[0026] 在本发明的一个实施例中，所述安全会话是指在一定时间内建立的、在智能卡与终端应用程序间的一种半永久性的、带有自动回收机制的交互式的信息交换方式。

[0027] 在本发明的一个实施例中，所述安全会话由设置在智能卡中的安全会话管理器管理，并根据安全会话标识和随机数生成的会话信息修改相应的智能卡的安全状态。

[0028] 在本发明的一个实施例中，所述安全会话管理器的安全会话的生命周期包括安全会话初始化、安全会话通信和安全会话资源释放。

[0029] 进一步，当安全会话执行过程中发生错误，安全会话自动终止，安全会话管理器自动释放安全会话资源。

[0030] 进一步，安全会话的执行时间超过安全会话管理器的时间限制，安全会话自动终止，安全会话资源被释放。

[0031] 进一步，通信过程中掉电，安全会话管理器全部重置，安全会话资源被释放。

[0032] 本发明的标识智能卡通信对象的方法主要具有如下优点：

[0033] 1、通信的唯一性，即在一个安全会话里，与智能卡通信的对象（如终端应用程序）是确定的，不同的安全会话 ID 标明不同的通信对象，来自同一终端的不同的应用程序对应不同的安全会话。

[0034] 2、通信状态的一致性，在智能卡和多个应用程序通信时，保持安全会话状态的一致性是很重要的；否则，当用户在一个新的、而不是一开始保存安全会话信息的应用程序提交访问请求的时候，智能卡会因为无法获知原来的安全会话状态而产生问题。

[0035] 本发明的标识智能卡通信对象的方法，在现有智能卡安全体系中，引入安全会话的概念，采用在一定时间内建立起智能卡与终端应用程序间的一种半永久性的、带有自动回收机制的、交互式的信息交换方式，将应用程序与自身发出的请求关联起来，从而使得不同的应用程序的安全会话是相互独立的；另外，安全会话一旦建立，就应当一直存在，直到应用程序操作结束，或者其他使得安全会话终止的情况出现；会话的安全性由安全会话对称密钥和安全会话公私钥对保护，实现本发明的目的。

[0036] 本发明的特点可参阅本案图式及以下较好实施方式的详细说明而获得清楚地了解。

附图说明

[0037] 图 1 为现有的智能卡安全体系的应用工作的流程图；

[0038] 图 2 为本发明的标识智能卡通信对象的方法的智能卡的结构框图；

[0039] 图 3 为本发明的标识智能卡通信对象的方法的工作流程示意图。

具体实施方式

[0040] 为了使本发明实现的技术手段、创作特征、达成目的与功效易于明白了解，下面结合具体图示，进一步阐述本发明。

[0041] 实施例

[0042] 如图 2、图 3 所示，本发明的一种标识智能卡通信对象的方法，它包括如下步骤：

[0043] (1) 终端应用程序发起安全会话，产生随机数作为安全会话标识；

[0044] (2) 将生成的安全会话标识做映射，然后将安全会话标识返回到终端应用程序；

[0045] (3) 当终端应用程序访问智能卡时，需要将指令和安全会话标识一起发送到智能卡并由智能卡解析得到指令；

[0046] (4) 智能卡根据接收到的信息来决定是否允许终端应用程序访问。

[0047] 在本发明中，智能卡 100 由安全会话管理器 110、传输管理器 120 和命令解析器 130 构成，安全会话管理器 110、传输管理器 120 和命令解析器 130 互相连接。

[0048] 传输管理器 120 的主要功能是接收来自终端硬件的电气信号，转换成逻辑数据传递给命令解析器；将来自智能卡的响应信息以电气信号传递给终端硬件。

[0049] 命令解析器 130 的主要功能是解析终端应用程序发来的指令，从中得到安全会话标识和指令内容。

[0050] 安全会话管理器 110 的主要功能是管理安全会话标识 ID 的会话信息，并根据会话信息修改相应的安全状态。

[0051] 终端应用程序发起安全会话，由终端应用程序产生随机数 R 作为安全会话标识，并将安全会话标识发送给智能卡 100 的传输管理器 120，传递至命令解析器 130；命令解析器 130 解析得到安全会话标识，然后执行创建会话工作，将安全会话标识发送给安全会话管理器 110；安全会话管理器 110 产生安全会话标识 ID，将安全会话标识 ID 绑定，然后返回用安全会话标识 ID 给终端应用程序，以此建立与终端应用程序的一个会话；当会话建立之后，终端应用程序访问智能卡 100 时，由终端应用程序通过传输管理器 120 发送安全会话标识 ID 和指令及指令的 hash 摘要；命令解析器 130 在接收到带有安全会话标识 ID 的指令后，在安全会话管理器 110 中验证当前安全会话 ID 是否合法。如果合法，则继续验证指令，进行命令执行。

[0052] 在本发明中，安全会话管理器 110 的安全会话的生命周期包括安全会话初始化、安全会话通信和安全会话资源释放。

[0053] 在安全会话的初始化阶段，智能卡生成终端应用程序的标识 ID，用于区分不同的终端应用程序。安全会话有一定的生存时间，安全会话管理器既可以定义不同的安全会话生存时间，也可以对所有的安全会话实行统一的生存时间限制。

[0054] 安全会话的最后一个阶段是安全会话的资源释放。除了终端主动终结一个安全会话的情况外，以下任意一种情况出现时，安全会话资源就被释放：

[0055] 1、当安全会话执行过程中发生错误，安全会话自动终止，安全会话管理器 110 自动释放安全会话资源；

[0056] 2、安全会话的执行时间超过安全会话管理器 110 的时间限制，安全会话自动终止，安全会话资源被释放；

[0057] 3、通信过程中掉电，安全会话管理器 110 全部重置，安全会话资源被释放。

[0058] 本发明的智能卡安全会话系统，在终端应用程序与智能卡之间建立安全会话，能够解决旁路攻击、中间人攻击的问题；在普通智能卡的应用中，如网上银行使用的 U 盾、市民卡、社保卡等，终端与智能卡的交互过程不存在会话机制，智能卡无法确定当前的终端处于何种状态，所以可能无法避免旁路攻击行为；本发明的智能卡安全会话系统通过加入安全会话机制，在一定程度上能够防止非法终端程序以旁路方式或中间人方式访问智能卡内部信息。

[0059] 以上显示和描述了本发明的基本原理和主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的只是说明本发明的原理，在不脱离本发明精神和范围的前提下，本发明还会有各种变化和改进，这些变化和改进都落入要求保护的本发明范围内，本发明要求保护范围由所附的权利要求书及其等效物界定。

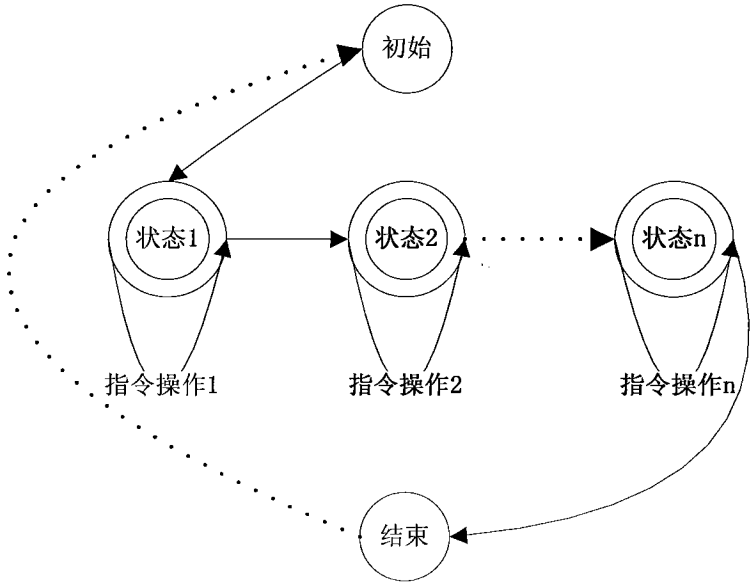

初始
状态1
状态2
状态n
指令操作1
指令操作2
指令操作n
结束

图 1

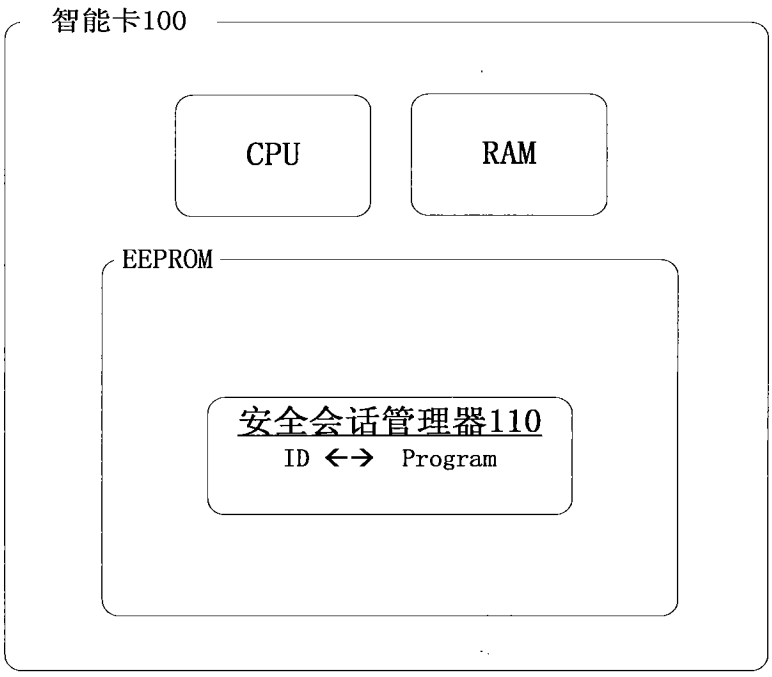

智能卡100
CPU
RAM
EEPROM
安全会话管理器110
ID ←→ Program

图 2

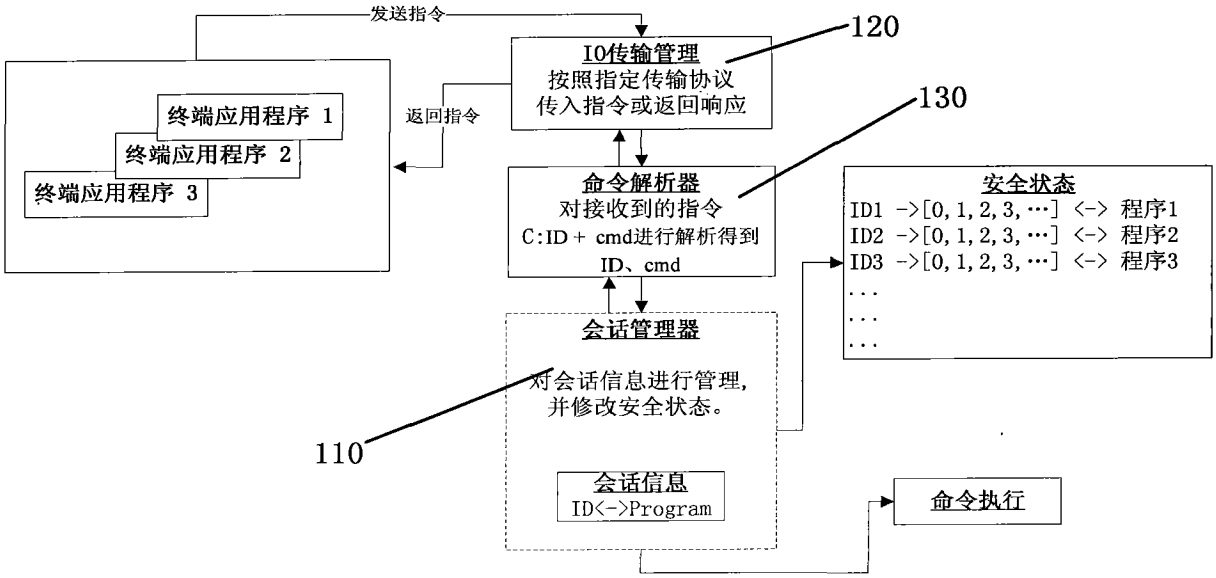

发送指令
IO传输管理
按照指定传输协议
传入指令或返回响应
120
返回指令
终端应用程序 1
终端应用程序 2
终端应用程序 3
130
命令解析器
对接收到的指令
C:ID + cmd进行解析得到
ID、cmd
安全状态
ID1 ->[0, 1, 2, 3, …] <-> 程序1
ID2 ->[0, 1, 2, 3, …] <-> 程序2
ID3 ->[0, 1, 2, 3, …] <-> 程序3
...
...
...
会话管理器
对会话信息进行管理,
并修改安全状态。
110
会话信息
ID<->Program
命令执行

图 3