(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 106709552 B
(45)授权公告日 2020.04.17

(21)申请号 201510791916.8

(22)申请日 2015.11.17

(65)同一申请的已公布的文献号
申请公布号 CN 106709552 A

(43)申请公布日 2017.05.24

(73)专利权人 上海复旦微电子集团股份有限公司
地址 200433 上海市杨浦区国泰路127号复旦国家大学科技园4号楼

(72)发明人 邬佳希 陆继承 王冬格 廖鹏 楼安琪 阚宏进

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 潘彦君 吴敏

(51)Int.Cl.
G06K 19/073(2006.01)

审查员 张盼

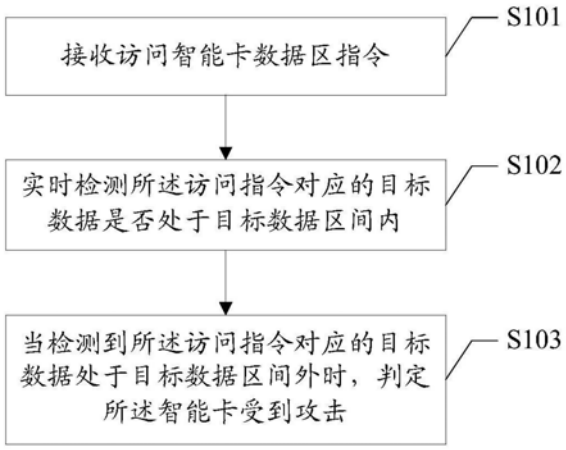
权利要求书3页 说明书8页 附图1页

(54)发明名称

智能卡安全防护方法及装置

(57)摘要

一种智能卡安全防护方法及装置，所述方法包括：接收访问智能卡数据区的指令；在对访问指令进行处理时，实时检测所述访问指令对应的目标数据是否处于目标数据区间内；当检测到所述访问指令对应的目标数据处于目标数据区间外时，判定所述智能卡受到攻击。采用所述方法及装置，可以有效降低智能卡的安全隐患。



CN 106709552 B

1.一种智能卡安全防护方法,其特征在于,包括:

接收访问智能卡数据区的指令;所述智能卡数据区包括以下至少一种:栈数据区、静态变量数据区以及对象字段数据区;

在对访问指令进行处理时,实时检测所述访问指令对应的目标数据是否处于目标数据区间内;当所述访问指令为对静态变量数据区进行访问的指令时,所述实时检测所述访问指令对应的目标数据是否处于目标数据区间内,包括:解析所述访问指令,获取所述访问指令携带的操作码和操作数,并获取所述操作码中包含的数据类型信息;获取所述访问指令对应的目标数据包的静态镜像信息;根据所述静态镜像信息,检测所述操作数对应的静态数据地址是否处于所述静态镜像信息对应的数据区间内;

当检测到所述访问指令对应的目标数据处于目标数据区间外时,判定所述智能卡受到攻击。

2.如权利要求1所述的智能卡安全防护方法,其特征在于,还包括:

实时获取所述访问指令涉及的数据类型,以及所述访问指令指向的目标数据的数据类型;

检测所述访问指令涉及的数据类型与所述目标数据的数据类型是否相同;

当检测到所述访问指令涉及的数据类型与所述目标数据的数据类型不同时,判定所述智能卡受到攻击。

3.如权利要求1或2所述的智能卡安全防护方法,其特征在于,在判定所述智能卡受到攻击后,还包括以下至少一种:发送报警信息;终止访问操作。

4.如权利要求2所述的智能卡安全防护方法,其特征在于,当所述访问指令为对所述栈数据区进行访问时,所述实时获取所述访问指令涉及的数据类型,包括:解析所述访问指令,获取所述访问指令携带的操作码和操作数,并获取所述操作码中包含的数据类型信息;

所述获取所述访问指令指向的目标数据的数据类型,包括:获取所述操作数对应的栈数据区中的目标数据的数据类型。

5.如权利要求4所述的智能卡安全防护方法,其特征在于,所述实时检测所述访问指令对应的目标数据是否处于预设范围内,包括:实时检测所述访问指令对应的目标数据是否处于所述栈数据区的预设范围内。

6.如权利要求5所述的智能卡安全防护方法,其特征在于,所述实时检测所述访问指令对应的目标数据是否处于所述栈数据区的预设范围内,包括:

当所述访问指令对应的操作包括压栈操作或弹栈操作时,实时获取与所述访问指令操作相关的数据单元的位置,检测所述数据单元的位置是否处于当前函数帧的操作数栈的上下边界;

当函数调用产生新的函数帧时,检测存放函数特征信息的栈顶是否超出新函数帧的操作数栈上边界;

当函数调用返回时,检测所述访问指令对应的栈顶信息弹出时是否超出整个栈的上边界。

7.如权利要求2所述的智能卡安全防护方法,其特征在于,所述检测所述访问指令涉及的数据类型与所述目标数据类型是否相同,包括:

当所述操作数对应的静态数据为引用类型时,检测所述静态数据是否处于所述静态镜

像信息对应的引用数据区间内；

当所述操作数对应的静态数据为基本数据类型时，检测所述静态数据是否处于所述静态镜像信息对应的基本类型数据区间内。

8.如权利要求2所述的智能卡安全防护方法，其特征在于，当所述访问指令为对所述对象字段数据区进行访问的指令时，所述检测所述访问指令涉及的数据类型与所述目标数据的数据类型是否相同，包括：

解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；

获取所述访问指令指向的对象的类信息；根据所述类信息获取所述对应的继承结构信息，以获取所述目标对象每层类结构中的引用类型数据以及基本类型数据；

根据所述操作数以及所述操作码中包含的数据类型信息，遍历每次类结构；当所述操作码中包含的数据类型信息为引用类型时，检测所述目标数据是否处于引用类型数据区间；

当所述操作码中包含的数据类型信息为基本数据类型时，检测所述目标数据是否处于基本数据类型区间。

9.如权利要求8所述的智能卡安全防护方法，其特征在于，所述实时检测所述访问指令对应的目标数据是否处于预设范围内，包括：

实时检测所述目标数据是否处于所述访问指令对应的对象的数据区间内。

10.一种智能卡安全防护装置，其特征在于，包括：

接收单元，用于接收访问智能卡数据区的指令；所述智能卡数据区包括以下至少一种：栈数据区、静态变量数据区以及对象字段数据区；

边界检测单元，用于对在对访问指令进行处理时，实时检测所述访问指令对应的目标数据是否处于目标数据区间内；当所述访问指令为对静态变量数据区进行访问的指令时，所述边界检测单元用于：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；获取所述访问指令对应的目标数据包的静态镜像信息；根据所述静态镜像信息，检测所述操作数对应的静态数据地址是否处于所述静态镜像信息对应的数据区间内；

判断单元，用于当检测到所述访问指令对应的目标数据处于目标数据区间外时，判定所述智能卡受到攻击。

11.如权利要求10所述的智能卡安全防护装置，其特征在于，还包括：类型检测单元，用于获取所述访问指令涉及的数据类型，以及所述访问指令指向的目标数据的数据类型，并检测所述访问指令涉及的数据类型与所述目标数据的数据类型是否相同；

所述判断单元还用于：当检测到所述访问指令涉及的数据类型与所述目标数据的数据类型不同时，判定所述智能卡受到攻击。

12.如权利要求10或11所述的智能卡安全防护装置，其特征在于，还包括：安全控制单元，用于在所述判断单元判定所述智能卡受到攻击后，发送报警信息，终止访问操作。

13.如权利要求11所述的智能卡安全防护装置，其特征在于，当所述访问指令为对所述栈数据区进行访问时，所述类型检测单元用于：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；以及获取所述操作数对应

的栈数据区中的目标数据的数据类型。

14.如权利要求13所述的智能卡安全防护装置，其特征在于，所述边界检测单元用于：实时检测所述访问指令对应的目标数据是否处于所述栈数据区的预设范围内。

15.如权利要求14所述的智能卡安全防护装置，其特征在于，所述边界检测单元用于：

当所述访问指令对应的操作包括压栈操作或弹栈操作时，实时获取与所述访问指令操作相关的数据单元的位置，检测所述数据单元的位置是否处于当前函数帧的操作数栈的上下边界；

当函数调用产生新的函数帧时，检测存放函数特征信息的栈顶是否超出新函数帧的操作数栈上边界；

当函数调用返回时，检测所述访问指令对应的栈顶信息弹出时是否超出整个栈的上边界。

16.如权利要求11所述的智能卡安全防护装置，其特征在于，所述类型检测单元用于：

当所述操作数对应的静态数据为引用类型时，检测所述静态数据是否处于所述静态镜像信息对应的引用数据区间内；

当所述操作数对应的静态数据为基本数据类型时，检测所述静态数据是否处于所述静态镜像信息对应的基本类型数据区间内。

17.如权利要求11所述的智能卡安全防护装置，其特征在于，当所述访问指令为对所述对象字段数据区进行访问的指令时，所述类型检测单元用于：

解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；

获取所述访问指令指向的对象的类信息；根据所述类信息获取所述对应的继承结构信息，以获取所述目标对象每层类结构中的引用类型数据以及基本类型数据；

根据所述操作数以及所述操作码中包含的数据类型信息，遍历每次类结构；当所述操作码中包含的数据类型信息为引用类型时，检测所述目标数据是否处于引用类型数据区间；

当所述操作码中包含的数据类型信息为基本数据类型时，检测所述目标数据是否处于基本数据类型区间。

18.如权利要求17所述的智能卡安全防护装置，其特征在于，所述边界检测单元用于：实时检测所述目标数据是否处于所述访问指令对应的对象的数据区间内。

智能卡安全防护方法及装置

技术领域

[0001] 本发明涉及智能卡技术领域，尤其涉及一种智能卡安全防护方法及装置。

背景技术

[0002] 智能卡技术由于其良好的可靠性和便携性，在金融、交通、医疗、教育等各领域得到日趋广泛的应用。在智能卡的应用场景日趋复杂的今天，各类信息攻击技术也在同步发展，因此其安全性的需求也日益得到重视。

[0003] Java智能卡以其支持后下载，多应用，跨平台的特性在各类环境下得到广泛使用和推广。随之而来的是，诸如恶意代码植入等软件攻击技术通过后下载的应用程序窥探Java智能卡的漏洞并进行数据篡改和破坏，已引起学术界和工业界的广泛研究。

[0004] 传统的Java智能卡，利用线下的字节码验证器(Byte Code Verifier，BCV)对即将烧录到卡上的应用程序文件进行安全性检查，若检查通过则允许应用程序文件烧录到卡上，否则给出报警信息。

[0005] 然而，上述方法无法对Java智能卡在出厂后安装的应用程序文件进行安全性检查，导致Java智能卡存在安全隐患。

发明内容

[0006] 本发明实施例解决的问题是如何降低Java智能卡的安全隐患。

[0007] 为解决上述问题，本发明实施例提供一种智能卡安全防护方法，包括：

[0008] 接收访问智能卡数据区的指令；

[0009] 在对访问指令进行处理时，实时检测所述访问指令对应的目标数据是否处于目标数据区间内；

[0010] 当检测到所述访问指令对应的目标数据处于目标数据区间外时，判定所述智能卡受到攻击。

[0011] 可选的，所述智能卡安全防护方法还包括：实时获取所述访问指令涉及的数据类型，以及所述访问指令指向的目标数据的数据类型；检测所述访问指令涉及的数据类型与所述目标数据的数据类型是否相同；当检测到所述访问指令涉及的数据类型与所述目标数据的数据类型不同时，判定所述智能卡受到攻击。

[0012] 可选的，在判定所述智能卡受到攻击后，还包括以下至少一种：发送报警信息；终止访问操作。

[0013] 可选的，所述智能卡数据区包括以下至少一种：栈数据区、静态变量数据区以及对象字段数据区。

[0014] 可选的，当所述访问指令为对所述栈数据区进行访问时，所述实时获取所述访问指令涉及的数据类型，包括：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；所述获取所述访问指令指向的目标数据的数据类型，包括：获取所述操作数对应的栈数据区中的目标数据的数据类型。

[0015] 可选的，所述实时检测所述访问指令对应的目标数据是否处于预设范围内，包括：实时检测所述访问指令对应的目标数据是否处于所述栈数据区的预设范围内。

[0016] 可选的，所述实时检测所述访问指令对应的目标数据是否处于所述栈数据区的预设范围内，包括：当所述访问指令对应的操作包括压栈操作或弹栈操作时，实时获取与所述访问指令操作相关的数据单元的位置，检测所述数据单元的位置是否处于当前函数帧的操作数栈的上下边界；当函数调用产生新的函数帧时，检测存放函数特征信息的栈顶是否超出新函数帧的操作数栈上边界；当函数调用返回时，检测所述访问指令对应的栈顶信息弹出时是否超出整个栈的上边界。

[0017] 可选的，当所述访问指令为对静态变量数据区进行访问的指令时，所述实时检测所述访问指令对应的目标数据是否处于预设范围内，包括：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；获取所述访问指令对应的目标数据包的静态镜像信息；根据所述静态镜像信息，检测所述操作数对应的静态数据地址是否处于所述静态镜像信息对应的数据区间内。

[0018] 可选的，所述检测所述访问指令涉及的数据类型与所述目标数据类型是否相同，包括：当所述操作数对应的静态数据为引用类型时，检测所述静态数据是否处于所述静态镜像信息对应的引用数据区间内；当所述操作数对应的静态数据为基本数据类型时，检测所述静态数据是否处于所述静态镜像信息对应的基本类型数据区间内。

[0019] 可选的，当所述访问指令为对所述对象字段数据区进行访问的指令时，所述检测所述访问指令涉及的数据类型与所述目标数据的数据类型是否相同，包括：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；获取所述访问指令指向的对象的类信息；根据所述类信息获取所述对应的继承结构信息，以获取所述目标对象每层类结构中的引用类型数据以及基本类型数据；根据所述操作数以及所述操作码中包含的数据类型信息，遍历每次类结构；当所述操作码中包含的数据类型信息为引用类型时，检测所述目标数据是否处于引用类型数据区间；当所述操作码中包含的数据类型信息为基本数据类型时，检测所述目标数据是否处于基本数据类型区间。

[0020] 可选的，所述实时检测所述访问指令对应的目标数据是否处于预设范围内，包括：实时检测所述目标数据是否处于所述访问指令对应的对象的数据区间内。

[0021] 本发明实施例还提供了一种智能卡安全防护装置，包括：

[0022] 接收单元，用于接收访问智能卡数据区的指令；

[0023] 边界检测单元，用于对在对访问指令进行处理时，实时检测所述访问指令对应的目标数据是否处于目标数据区间内；

[0024] 判断单元，用于当检测到所述访问指令对应的目标数据处于目标数据区间外时，判定所述智能卡受到攻击。

[0025] 可选的，所述智能卡安全防护装置还包括：类型检测单元，用于获取所述访问指令涉及的数据类型，以及所述访问指令指向的目标数据的数据类型，并检测所述访问指令涉及的数据类型与所述目标数据的数据类型是否相同；所述判断单元还用于：当检测到所述访问指令涉及的数据类型与所述目标数据的数据类型不同时，判定所述智能卡受到攻击。

[0026] 可选的，所述智能卡安全防护装置还包括：安全控制单元，用于在所述判断单元判定所述智能卡受到攻击后，发送报警信息，终止访问操作。

[0027] 可选的，所述智能卡数据区包括以下至少一种：栈数据区、静态变量数据区以及对象字段数据区。

[0028] 可选的，当所述访问指令为对所述栈数据区进行访问时，所述类型检测单元用于：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；以及获取所述操作数对应的栈数据区中的目标数据的数据类型。

[0029] 可选的，所述边界检测单元用于：实时检测所述访问指令对应的目标数据是否处于所述栈数据区的预设范围内。

[0030] 可选的，所述边界检测单元用于：当所述访问指令对应的操作包括压栈操作或弹栈操作时，实时获取与所述访问指令操作相关的数据单元的位置，检测所述数据单元的位置是否处于当前函数帧的操作数栈的上下边界；当函数调用产生新的函数帧时，检测存放函数特征信息的栈顶是否超出新函数帧的操作数栈上边界；当函数调用返回时，检测所述访问指令对应的栈顶信息弹出时是否超出整个栈的上边界。

[0031] 可选的，当所述访问指令为对静态变量数据区进行访问的指令时，所述边界检测单元用于：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；获取所述访问指令对应的目标数据包的静态镜像信息；根据所述静态镜像信息，检测所述操作数对应的静态数据地址是否处于所述静态镜像信息对应的数据区间内。

[0032] 可选的，所述类型检测单元用于：当所述操作数对应的静态数据为引用类型时，检测所述静态数据是否处于所述静态镜像信息对应的引用数据区间内；当所述操作数对应的静态数据为基本数据类型时，检测所述静态数据是否处于所述静态镜像信息对应的基本类型数据区间内。

[0033] 可选的，当所述访问指令为对所述对象字段数据区进行访问的指令时，所述类型检测单元用于：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；获取所述访问指令指向的对象的类信息；根据所述类信息获取所述对应的继承结构信息，以获取所述目标对象每层类结构中的引用类型数据以及基本类型数据；根据所述操作数以及所述操作码中包含的数据类型信息，遍历每次类结构；当所述操作码中包含的数据类型信息为引用类型时，检测所述目标数据是否处于引用类型数据区间；当所述操作码中包含的数据类型信息为基本数据类型时，检测所述目标数据是否处于基本数据类型区间。

[0034] 可选的，所述边界检测单元用于：实时检测所述目标数据是否处于所述访问指令对应的对象的数据区间内。

[0035] 与现有技术相比，本发明实施例的技术方案具有以下优点：

[0036] 在接收到对智能卡数据区访问的访问指令时，检测访问指令对应的目标数据是否处于目标数据区间内。当访问指令对应的目标数据处于目标数据区间外时，判定智能卡受到攻击，从而可以实时地检测智能卡是否遭到攻击，降低智能卡的安全隐患。

[0037] 进一步，通过比较访问指令涉及的数据类型以及目标数据的数据类型，当二者不同时，则判定智能卡遭到攻击，可以更进一步地降低智能卡的安全隐患。

附图说明

[0038] 图1是本发明实施例中的一种智能卡安全防护方法的流程图；

[0039] 图2是本发明实施例中的一种智能卡安全防护装置的结构示意图。

具体实施方式

[0040] 对于传统的Java智能卡，通常利用线下的字节码验证器(Byte Code Verifier，BCV)对即将烧录到卡上的应用程序文件进行安全性检查，若检查通过则允许应用程序文件烧录到卡上，否则给出报警信息。然而，若用户在使用Java智能卡时下载一些应用程序，而一些来自未知信息源的应用程序中可能携带有病毒程序，现有的Java智能卡检测方法并不能对用户自行下载的程序进行安全性检测，导致Java智能卡存在安全隐患。

[0041] 在本发明实施例中，当接收到对智能卡数据区访问的访问指令时，检测访问指令对应的目标数据是否处于目标数据区间内。当访问指令对应的目标数据处于目标数据区间外时，判定智能卡受到攻击，从而可以实时地检测智能卡是否遭到攻击，降低智能卡的安全隐患。

[0042] 为使本发明实施例的上述目的、特征和优点能够更为明显易懂，下面结合附图对本发明的具体实施例做详细的说明。

[0043] 本发明实施例提供了一种智能卡安全方法检测方法，参照图1，以下通过具体步骤进行详细说明。

[0044] 步骤S101，接收访问智能卡数据区指令。

[0045] 在本发明实施例中，智能卡数据区可以包括栈数据区、静态变量数据区以及对象字段数据区三种数据区。接收到的访问指令可以是对上述三种数据区中的任一数据区或多个数据区进行访问的指令。

[0046] 步骤S102，在对访问指令进行处理时，实时检测所述访问指令对应的目标数据是否处于目标数据区间内。

[0047] 在本发明实施例中，可以实时检测访问指令对应的目标数据是否处于目标数据区间内。目标数据可以是指访问指令指向的数据，目标数据区间可以是在实际应用中预先设定的用于存储目标数据的地址区间。例如，目标数据为数据A，在实际应用中，数据A应存储在地址区间B内。

[0048] 在正常情况下，当访问指令为正常的访问指令时，访问指令对应的目标数据理论上应处于目标数据区间内。若处于目标数据区间之外，则可以判定存在异常情况。

[0049] 因此，在对访问指令进行处理时，可以判断访问指令对应的目标数据是否处于预设目标数据区间内。当访问指令对应的目标数据处于目标数据区间内时，判定访问指令为合法指令，当前智能卡未存在被攻击的情况；当访问指令对应的目标数据未处于目标数据区间内时，则执行步骤S103。

[0050] 步骤S103，当检测到所述访问指令对应的目标数据处于目标数据区间外时，判定所述智能卡受到攻击。

[0051] 在本发明实施例中，如前所述，若目标数据未处于目标数据区间内时，则可以判定当前访问指令可能为非法指令，因此可以判定智能卡受到攻击。

[0052] 例如，目标数据为数据A，在正常情况下，数据A存储在地址区间B内。在对访问指令

进行处理的过程中，若检测到数据A处于地址区间B内，则可以判定访问指令为合法指令；若检测到数据A未处于地址区间B内，则判定智能卡当前受到攻击。

[0053] 在本发明实施例中，当智能卡受到攻击时，可以立即终止访问指令对应的访问操作。当终止访问操作后，还可以发送相应的报警信息，来告知用户当前智能卡受到攻击，并向用户指示是哪个应用程序对应的访问指令为非法的，以告知用户哪个应用程序存在安全隐患。

[0054] 由此可见，在接收到对智能卡数据区访问的访问指令时，检测访问指令对应的目标数据是否处于目标数据区间内。当访问指令对应的目标数据处于目标数据区间外时，判定智能卡受到攻击，从而可以实时地检测智能卡是否遭到攻击，降低智能卡的安全隐患。

[0055] 在本发明实施例中，在接收到访问智能卡数据区指令后，还可以实时获取访问指令涉及的数据类型，并将访问指令涉及的数据类型与访问指令指向的目标数据的数据类型进行比较。当访问指令涉及的数据类型与目标数据的数据类型相同时，则可以判定访问指令为合法指令；当访问指令涉及的数据类型与目标数据的数据类型不同时，则可以判定访问指令为非法指令，此时智能卡可能受到攻击。

[0056] 下面对本发明上述实施例中提供的智能卡安全方法防护方法在三种智能卡数据区中的执行流程进行说明。

[0057] 在本发明实施例中，当访问指令为对栈数据区进行访问的指令时，可以先将智能卡中的随机存储器(Random Access Memory，RAM)的栈空间存储一倍，使得堆栈上的每个单元的长度均扩充一倍。即将一个2字节长度的单元扩充到4字节长度，新增的2个字节用于存放该单元存储的数据的类型信息。

[0058] 在对栈数据区进行访问时，可以实时地对栈数据区的访问过程中涉及的数据进行边界检查。

[0059] 假设RAM中的栈结构的地址增长顺序是自下而上的，通常在智能卡系统里，用到的栈是一个双向栈，即函数调用时创建的函数帧是自下而上生长，而函数的特征信息会被保存到栈顶，是自上而下生长。

[0060] 当访问指令对应的操作为压栈操作时，可以实时检测压栈操作涉及的数据单元的位置是否超出当前函数帧的操作数栈的上边界。当超出上边界时，则可以判定当前智能卡遭到攻击；当未超出上边界时，则可以判定当前访问指令为正常指令。

[0061] 当访问指令对应的操作为弹栈操作时，可以实时检测弹栈操作涉及的数据单元的位置是否超出当前函数帧的操作数栈的下边界。当超出下边界时，则可以判定当前智能卡遭到攻击；当未超出上边界时，则可以判定当前访问指令为正常指令。

[0062] 此外，当进行函数调用时会创建新的函数帧，而之前旧的函数帧的特征信息会被保存到栈顶。可以实时检测存放函数特征信息的栈顶是否超出新函数帧的操作数的上边界。当超出上边界时，判定当前智能卡遭到攻击。

[0063] 类似地，当函数调用返回时，需要将当期访问指令对应的函数帧清除，恢复其调用者的帧。此时，可以检测调用者的栈顶信息被弹出时，是否超出整个栈的上边界。当检测到弹出的栈顶信息超出整个栈的上边界时，判定当前智能卡遭到攻击。

[0064] 在对栈的访问增加边界检查的同时，还可以对栈的访问增加类型检查。对数据单元内的数据进行读操作和写操作时，均需要满足数据类型匹配原则。对于任意涉及栈操作

的访问指令，可以对其进行解析以获取对应的操作数和操作码。对操作数对应的栈数据区中的目标数据的数据类型与操作码中包含的数据类型进行比较，当二者相同时，可以判定访问指令为合法指令；当二者不同时，判定当前智能卡遭到攻击，立即终止程序并报错。

[0065] 当访问指令为对静态变量数据区进行访问的指令时，也可以对静态变量数据的访问增加边界检查和类型检查。

[0066] 在具体应用中，对静态变量的访问指令涉及到智能卡上某个数据包对应的静态镜像。按照预设的对访问指令的解析方式，将访问指令定位到数据包C后，可以获取数据包C的静态镜像信息。

[0067] 在本发明实施例中，数据包C的静态镜像信息可以包括：数据包C的静态变量存储的地址区间、数据包C内包含有引用类型的静态变量的数量等。通过数据包C的静态镜像信息对访问指令进行边界检查和类型检查。

[0068] 当对访问指令进行解析后，获取到的操作数对应的静态数据地址位于数据包C的静态镜像的地址区间内时，可以判定边界检查成功，也即当前访问指令为合法指令；否则，判定边界检查失败，也即当前访问指令为非法指令。

[0069] 当获取到的访问指令的操作数对应的静态数据是引用类型，且位于静态镜像的引用数据区间内时，可以判定类型检查成功，也即访问指令涉及的数据类型与目标数据类型相同，当前访问指令为合法指令。当获取到的访问指令的操作数对应的静态数据是基本数据类型，且位于静态镜像的基本类型数据区间内，则可以判定类型检查成功，也即访问指令涉及的数据类型与目标数据类型相同，当前访问指令为合法指令。否则，视为类型检查失败，当前访问指令为非法指令。

[0070] 相类似地，当访问指令为对对象字段数据区进行访问的指令时，也可以对对象字段数据区的访问增加边界检查和类型检查。

[0071] 在实际应用中，在对对象字段数据的访问指令执行之前，已经有对象引用数据预先被存储到栈上。该对象引用按照预定义的规则被解析成相对应的对象地址。读取对象地址上定义的对象头，获取该对象对应的类信息以及包信息。根据类信息可以获取相关的继承结构信息，以及当前类的引用类型数据个数。依据上述信息划分当前对象的字段区间，包括每层类结构里的引用类型数据和基本类型数据。根据访问指令中的操作数以及操作码中包含的数据类型信息，遍历每层类结构，包括各种子类结构以及根结构。

[0072] 当操作码中包含的数据类型信息为引用类型时，检测目标数据是否处于引用类型数据区间。当目标数据处于引用类型数据区间内时，判定类型检测成功。当操作码中包含的数据类型信息为基本数据类型时，检测目标数据是否处于基本数据类型区间内。当目标数据处于基本数据类型区间内时，判定类型检测成功。

[0073] 当目标数据处于访问指令对应对象的数据区间内时，可以判定边界检查成功；否则，判定边界检查失败。

[0074] 可以理解的是，在本发明实施例中，既可以只通过判断访问指令对应的目标数据是否处于目标数据区间内来获知智能卡是否受到攻击，也可以只通过判断访问指令涉及的数据类型与目标数据的数据类型是否相同来获知智能手机是否受到攻击。还可以同时通过判断访问指令对应的目标数据是否处于目标数据区间内，以及数据类型与目标数据的数据类型是否相同，来共同获知智能卡是否受到攻击。

[0075] 参照图2，给出了本发明实施例中的一种智能卡安全防护装置20，包括：接收单元201、边界检测单元202以及判断单元203，其中：

[0076] 接收单元201，用于接收访问智能卡数据区的指令；

[0077] 边界检测单元202，用于对在对访问指令进行处理时，实时检测所述访问指令对应的目标数据是否处于目标数据区间内；

[0078] 判断单元203，用于当检测到所述访问指令对应的目标数据处于目标数据区间外时，判定所述智能卡受到攻击。

[0079] 在具体实施中，所述智能卡安全防护装置20还可以包括：类型检测单元204，用于获取所述访问指令涉及的数据类型，以及所述访问指令指向的目标数据的数据类型，并检测所述访问指令涉及的数据类型与所述目标数据的数据类型是否相同；

[0080] 所述判断单元203还可以用于：当检测到所述访问指令涉及的数据类型与所述目标数据的数据类型不同时，判定所述智能卡受到攻击。

[0081] 在具体实施中，所述智能卡安全防护装置20还可以包括：安全控制单元205，用于在所述判断单元判定所述智能卡受到攻击后，发送报警信息，终止访问操作。

[0082] 在具体实施中，所述智能卡数据区可以包括以下至少一种：栈数据区、静态变量数据区以及对象字段数据区。

[0083] 在具体实施中，当所述访问指令为对所述栈数据区进行访问时，所述类型检测单元204可以用于：解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；以及获取所述操作数对应的栈数据区中的目标数据的数据类型。

[0084] 在具体实施中，所述边界检测单元202可以用于：实时检测所述访问指令对应的目标数据是否处于所述栈数据区的预设范围内。

[0085] 在具体实施中，所述边界检测单元202可以用于：当所述访问指令对应的操作包括压栈操作或弹栈操作时，实时获取与所述访问指令操作相关的数据单元的位置，检测所述数据单元的位置是否处于当前函数帧的操作数栈的上下边界；当函数调用产生新的函数帧时，检测存放函数特征信息的栈顶是否超出新函数帧的操作数栈上边界；当函数调用返回时，检测所述访问指令对应的栈顶信息弹出时是否超出整个栈的上边界。

[0086] 在具体实施中，当所述访问指令为对静态变量数据区进行访问的指令时，所述边界检测单元202可以用于：

[0087] 解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；

[0088] 获取所述访问指令对应的目标数据包的静态镜像信息；

[0089] 根据所述静态镜像信息，检测所述操作数对应的静态数据地址是否处于所述静态镜像信息对应的数据区间内。

[0090] 在具体实施中，所述类型检测单元204可以用于：

[0091] 当所述操作数对应的静态数据为引用类型时，检测所述静态数据是否处于所述静态镜像信息对应的引用数据区间内；

[0092] 当所述操作数对应的静态数据为基本数据类型时，检测所述静态数据是否处于所述静态镜像信息对应的基本类型数据区间内。

[0093] 在具体实施中，当所述访问指令为对所述对象字段数据区进行访问的指令时，所述类型检测单元204可以用于：

[0094] 解析所述访问指令，获取所述访问指令携带的操作码和操作数，并获取所述操作码中包含的数据类型信息；

[0095] 获取所述访问指令指向的对象的类信息；根据所述类信息获取所述对应的继承结构信息，以获取所述目标对象每层类结构中的引用类型数据以及基本类型数据；

[0096] 根据所述操作数以及所述操作码中包含的数据类型信息，遍历每次类结构；

[0097] 当所述操作码中包含的数据类型信息为引用类型时，检测所述目标数据是否处于引用类型数据区间；

[0098] 当所述操作码中包含的数据类型信息为基本数据类型时，检测所述目标数据是否处于基本数据类型区间。

[0099] 在具体实施中，所述边界检测单元202可以用于：实时检测所述目标数据是否处于所述访问指令对应的对象的数据区间内。

[0100] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：ROM、RAM、磁盘或光盘等。

[0101] 虽然本发明披露如上，但本发明并非限定于此。任何本领域技术人员，在不脱离本发明的精神和范围内，均可作各种更动与修改，因此本发明的保护范围应当以权利要求所限定的范围为准。

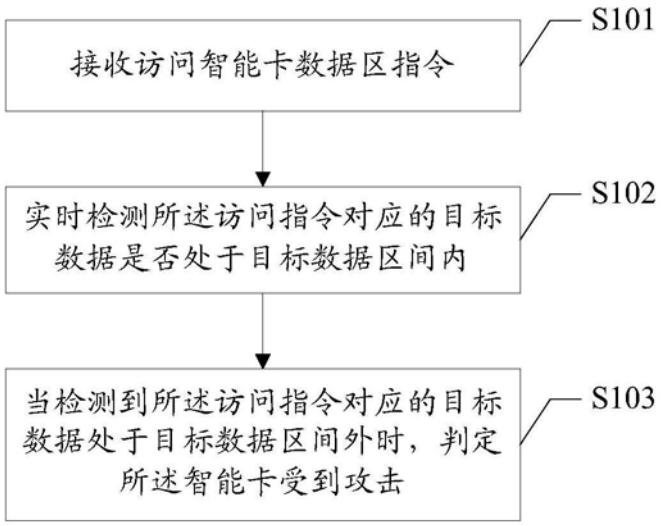

接收访问智能卡数据区指令
S101
实时检测所述访问指令对应的目标数据是否处于目标数据区间内
S102
当检测到所述访问指令对应的目标数据处于目标数据区间外时，判定所述智能卡受到攻击
S103

图1

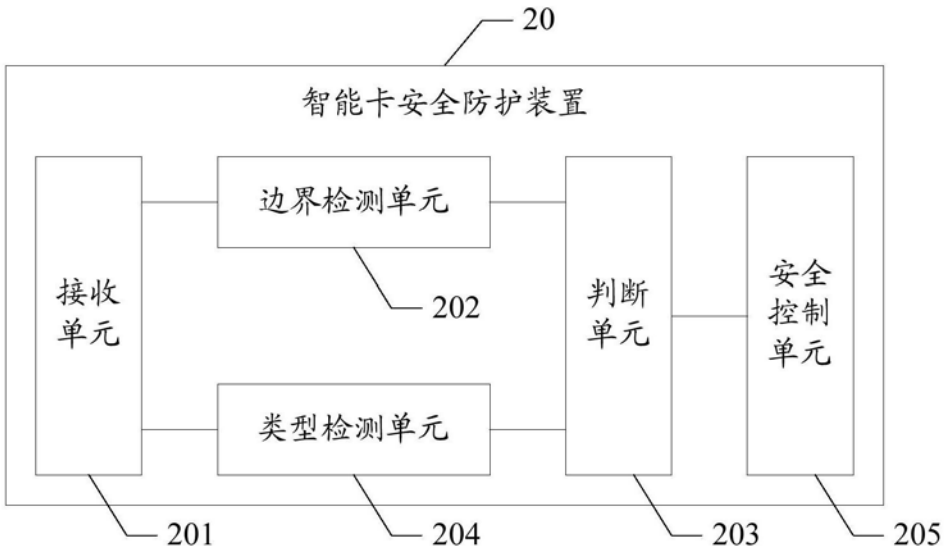

20
智能卡安全防护装置
接收单元
边界检测单元
202
类型检测单元
判断单元
安全控制单元
201
204
203
205

图2