第35卷 第18期 计 算 机 工 程 2009年9月
Vol.35 No.18 Computer Engineering September 2009
·博士论文· 文章编号：1000—3428(2009)18—0022—03 文献标识码：A 中图分类号：TP309

一种基于智能卡的可信监视器程序实现方法

涂国庆
(武汉大学计算机学院，武汉 430079)

摘 要：智能卡的安全机制存在篡改存储数据或代码、拒绝服务攻击、重新编程等安全问题，其根源在于卡的合法应用环境发生了改变、正常应用操作序列发生了错乱或模仿。针对上述问题，结合智能卡应用与可信计算技术，提出一种对智能卡计算环境可信和行为可信的验证方法。通过智能卡COS的开发实现该可信增强的技术。该方法可提高金融卡应用的可信度。

关键词：可信计算；信任链；智能卡；监视器

Implementation Method of Trusted Monitor Program Based on Smart Card

TU Guo-qing
(Computer School, Wuhan University, Wuhan 430079)

【Abstract】The security mechanism of smart card can not dissolve some problems such as tampering the data or code, DoS attacks and re-programming. These problems are mainly caused by destruction of the card's application circumstance, by confusion or simulation of the operating sequence. By combinating of trusted computing technology and application of smart card, a method to verify the trustiness of the circumstance and actions on the card is present. The implementation for the method is introduced by the development of a kind of chip operating system on smart card, from which the trustworthiness of the financial card is enhanced effectively.

【Key words】trusted computing; trust chain; smart card; monitor

1 概述

1.1 智能卡简介

智能卡(Smart Card)又名IC卡(Integrated Circuit Card)，具有暂时或永久的数据存储能力以及加密及数据处理能力[1]。由于CPU卡中的集成电路包括CPU、EEPROM、随机存储器RAM以及固化的只读存储器ROM中的片内操作系统(COS)，因此构成了一个完整的计算机系统。COS建立在CPU、存储器等硬件之上，是管理芯片资源和实现安全保密的操作系统。它的主要功能是：控制智能卡和外界的信息交换，管理智能卡内的存储器，在卡内部完成各种命令的处理。COS系统由传输管理、文件管理、安全管理、命令解释4个功能模块及加密算法库组成。

1.2 监视器程序

智能卡系统由于具有成本敏感、资源有限、人机交互频繁等特点，在应用时更容易受到物理和逻辑攻击[2-3]，其攻击的防范重点往往要从指令行为的监控上进行考虑。因此，文献[4]提出了一种监视器子系统，其结构如图1所示。

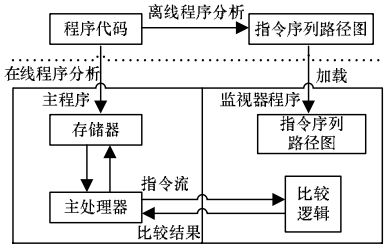

图1 嵌入式系统的监视器子系统

该系统通过对静态二进制代码进行分析，形成所有可能期望的指令序列路径图或状态转换图，由监视器子系统保存。在运行时，所有提交的指令系列都必须与预存的路径图比较，依据比较结果，可判断是否有非法操作系列存在，同时即可判断是否有攻击产生。一旦监视到这种情况发生，监视器就引起中断，终止当前处理器的指令执行过程，同时采取相应恢复措施。可见，只有按照一种期望的方式执行指令，才是合法指令流，这与可信计算理念是一致的。

2 可信增强的COS设计方法

本文从金融应用的智能卡COS架构进行安全改造，构筑一条包含软信任根的可信链，并通过该可信链实现对智能卡COS平台环境和COS操作指令行为的可信验证，以达到可信增强的目的。由于卡片资源有限，同时考虑到实际应用的通用性和成本，因此不专门向卡中增加额外的硬件芯片或电路，而是充分利用卡片本身的资源，从软件的角度模拟并设计出与可信计算相符的度量与存储机制，为以后真正包含TPM芯片的嵌入式系统的使用提供借鉴。

2.1 软信任根

可信计算平台通常包含专门的TPM芯片，其内部包含秘密存储和密码计算功能，平台的信任根源就是RTM(可信度

基金项目：国家“863”计划基金资助项目(2006AA01Z442, 2007AA01Z411)
作者简介：涂国庆(1974－)，男，讲师、博士研究生，主研方向：信息安全
收稿日期：2009-02-21 **E-mail：**tgq1001@yahoo.co

量根)，往往存放在 TPM 的秘密存储区[5]，称之为硬件形态的信任根源。

考虑卡片的实际情况，本文提出软信任根的概念。其思路就是将 COS 内核、卡片关键文件以及芯片主要参数等信息的完整性值作为卡片信任链的信任根源，存于卡片 NVM(Not Volatile Memory)的 OTP 区(One Time Programming Zone)，该值在卡片初始化时写入，在其后的卡片生命周期都不能更改，称之为软信任根 SRTM(Soft-based RTM)。本文对软信任根的度量不是通过 TPM 实现的，而是由一种软度量模块 STMM(Soft-based Trust Measurement Module)的代码实现的，这种软度量模块代码存放于卡片提供的 NVM 的 ROM 区。

2.1.1　使用依据

软信任根在卡片中能够充当信任根源的理论与实用依据在于：

(1)卡片 NVM 的 OTP 区一旦写入便不能更改，在保障物理可靠时认为足够可信。

(2)软信任根在卡片本身的 BOOTROM 代码执行完后(卡片的硬件自检完全通过后)，在进入 COS 核心代码执行之前才开始度量。其目的是为了追加验证芯片的完整性并对即将执行的 COS 的完整性进行检测，从而为其后的具体应用提供可信软件平台。

(3)软度量模块 STMM 对软信任根 SRTM 进行验证，若验证通过，则初始化卡片的安全状态为某一初值 S_0，该状态值与普通卡片登录 MF 的安全状态初值不同，且将它作为由 MF 切换到 ADF 的状态机中的唯一合法起始状态(如 S_0－>S_x)。换而言之，若由 MF 切换到 ADF 的状态变换不是以 S_0 为起点，会遭到应用中的访问控制或者监视器程序(2.2 节)拒绝。可见，软信任根的验证操作不可被旁路。

2.1.2　完整性收集与度量

软信任根 SRTM 的完整性数据来源主要和卡片本身特征以及 COS 代码有关，可选用以下参数作为软信任根计算完整性值的数据来源：芯片唯一序列号，产品标识符，发行商标识符，制造商标识符，COS 版本号，COS 内核代码校验和，初次发行日期，主文件(MF)头，软度量模块，监视器程序。

软信任根的完整性度量方法首先利用完整性检测算法对上述选定的参数或数据文件进行校验，将校验值编号并在初始化卡片时写入 OTP 区。当卡片上电进入 COS 应用之前，重复上面的过程，并得到新的校验值。将这 2 组校验值逐一进行比较，如果结果一致，则系统环境安全、核心文件完整；若不一致，说明系统核心文件有可能被非法篡改和破坏，或者进行了非法移植。该检测过程主要是监控系统环境和核心文件的数据信息的变化，是进入 COS 平台之前的一个基本可信的验证过程。

2.2　信任链机制

TCPA 的信任链往往从一个物理的可信根源 CRTM 开始检测，逐级向后传递系统的控制权，整个过程都离不开 TPM 芯片的度量、存储和报告[6]。本节在软信任根的基础上分析可信的传递，对应了 TCPA 信任链的 POST(上电自检)后的阶段。这一阶段主要是对 COS 代码、卡片文件以及应用操作行为进行度量，而且缺乏具体的 TPM 芯片，主要采用替代的软度量模块和监视器程序(Monitor)实现，同样能较好地实现可信的验证。其可行性基于以下具体因素：

(1)代替 TPM 芯片，采用 NVM 中划出的若干可信存储区存储可信的初值，该可信区与 DDF(含 MF)一一对应，对用户来说是屏蔽和透明的，实现了 TPM 芯片的秘密存储功能。

(2)软度量模块 STMM 首先对软信任根 SRTM 的完整性(含 STMM 自身的完整性及 Monitor 的完整性)进行度量，以确定能否进入 COS 平台；其后，STMM 继续对卡片各个应用下的应用完整性值进行度量，以确定能否进入具体的应用。这些应用完整性值主要来源于每个应用下的文件结构、应用核心代码和可信策略表等信息，称之为 AIVM(Application Integrity Value for Measurement)。

(3)结合基于状态机的可信策略表检测指令系列的可信性，实现了对操作行为的可信度量功能。

(4)选用具备非对称加密协处理器、随机数发生器、加密加速器及安全传感器等安全组件的卡片，这些安全组件完全可以代替 TPM 芯片进行相应的安全计算。

(5)本信任链虽然缺乏对系统加载之前阶段的可信度量，但考虑到智能卡芯片和读写设备本身的安全特性及在应用时的可靠性保障措施，在 COS 系统加载前，敏感信息是不可能从卡片泄漏的。

综上所述，含软度量模块的信任链结构见图 2 实线部分的描述，其中，STMM 是软度量模块；SRTM 为软信任根；AIVM 为应用完整性值；Monitor 为监视器程序。BOOTROM 为芯片启动自检代码。各部分在芯片存储器的存储分布情况如图 3 所示。

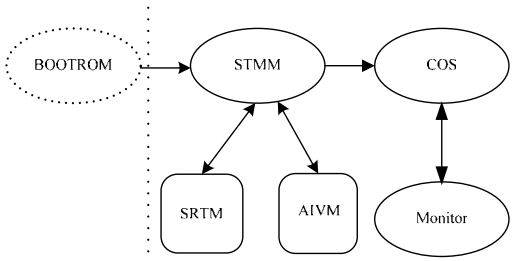

图 2　含软度量模块的信任链结构

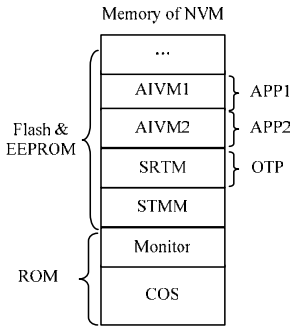

图 3　度量参数存储分布

结合图 2 与图 3，有 3 个问题需要指出：

(1)软度量模块和监视器程序在系统中唯一存在，其完整性由软信任根度量。

(2)软度量模块对每个应用下的文件结构、核心代码、可信策略表的完整性进行校验并检测是否与对应的预置初值相符，以决定能否进入该应用。预置初值保存于每个应用下的可信存储区中。

(3)在进入应用之后，监视器程序结合该应用下的可信策略表对涉及安全状态改变的所有指令或指令序列进行监视，以确保操作行为的可信。

2.3　可信验证机制

这种可信增强的智能卡操作系统重点为行为和计算环境

的可信方面提供有效的验证手段，以保障用户行为达到预期的目的。

(1)计算环境可信保障：智能卡 COS 的计算环境主要是指使用和执行 COS 的应用环境。在上文指定了软信任根，只有对该软信任根中的关键参数进行完整性验证后才能够进入各具体应用，而这些参数正好反映了卡和卡操作系统的基本特征，可以认为是一种最基本的平台计算环境。在验证这种平台计算环境可信之后，才能将信任传递给下一个可信模块，即软度量模块。软度量模块负责对卡的所有应用进行完整性验证，包含对应用下的文件结构、应用核心代码以及可信策略的完整性值进行验证，以确定能否进入该应用。这一阶段实际上是对具体应用计算环境的可信认证。

(2)行为可信保障：本文在对智能卡 COS 进行安全增强时，提出一种基于状态机的监视器程序，它与应用下的可信策略表结合，专门负责监视指令的执行过程/操作行为是否可信。该监视器的基本工作原理如图 4 所示。

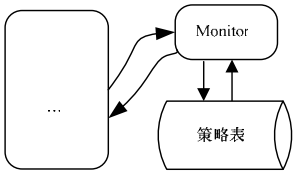

图 4　监视器工作原理

监视器主要包含中断输入接口、响应输出接口及决策模块。其中，中断输入接口负责接收来自主程序(应用代码)的可信度量请求；决策模块进行查表，依据可信策略表的策略作出判断，并由响应输出接口输出给主程序。实际上，监视器程序与主程序共用 CPU 和其他资源，以中断的方式运行，在硬件上没有要求卡片增加任何设施，只是为了提高中断请求速度，借用了芯片的某个安全传感器位(称为行为度量请求位(Action Measurement Request, AMR))来触发监视器的中断请求。

监视器需要借助于可信策略表进行可信判断，本文设计了一种实用的可信策略表，见表 1。

表 1　可信策略表

状态切换	序列计数器	指令序列	目的地址
$S_i \longrightarrow S_j$	5	I_1, I_2, I_3, I_6, I_8	0x01F0
$S_i \longrightarrow S_k$	7	I_1, I_2, I_4, I_6, I_9	0x0380
$S_j \longrightarrow S_m$	6	I_3, I_6, I_8, I_9	Null
…			

在表 1 中，“状态切换”栏目列出了所有合法的安全状态切换形式；“序列计数器”和“指令序列”分别记录了从初始状态变换到某一目标状态所经过的关键指令步骤数和所有关键指令的操作码；“目的地址”记录了该指令序列操作中要访问的存储器的物理地址。COS 主程序中的安全状态切换(如由状态 A 切换到状态 B 记为：$S_A \rightarrow S_B$)触发监视器中断，监视器工作流程如下：

(1)当 COS 主程序中的某个指令执行引起安全状态发生改变或切换，说明系统在执行与安全相关的操作，这时会引起安全传感器的 AMR 位置位，触发监视器中断，即请求监视器进行行为可信度量。

(2)监视器接收到 AMR 中断后，开始执行行为可信度量的服务程序。首先读取当前状态 S_B 以及前一状态 S_A，得到 $S_A \rightarrow S_B$，并由 $S_A \rightarrow S_B$ 作为索引查找可信策略表的状态切换栏目，如果在策略表中不能查到与 $S_A \rightarrow S_B$ 相符的项，说明操作为非法行为，转出错处理；如果找到对应项，假定为第 k 项，继续下一步骤。

(3)监视器读取当前序列计数器值(Sequence Counter Value, SCV)，假如该值为 m，监视器比较策略表中第 k 项的序列计数器值，如果不符，转出错处理；否则继续下一步。

(4)监视器读取最近的指令队列并从该队列中分析是否有访存操作，若有，记访存的物理地址 $PA=x$，若没有访存操作，记 PA=Null；假如队列中最近的指令序列为 $Ir(I_1, I_2, \cdots, I_n)$，而在策略表中的第 k 项的“指令序列”为 $\mathrm{Is}(I_1, I_2, \cdots, I_m)$，若 $Ir(I_1, I_2, \cdots, I_n)$包含且匹配于 $Is(I_1, I_2, \cdots, I_m)$，转下一步；否则，转出错处理。

(5)监视器读取策略表中第 k 项的“目的地址”值，并将其与第(4)步中记录的 PA 值比较，若不相同，转出错处理；否则，转下一步。

(6)监视器清除安全传感器的 AMR 位，结束中断服务过程，控制权移交主程序。

另外，出错处理的步骤包含：清除安全传感器的 AMR 位，给出警告，退出系统应用，或者重启芯片，甚至锁定应用直至锁定卡片。当然，这些强制处理的选择基于用户的安全决策机构。

3　结束语

智能卡操作系统的软信任根记录了平台环境的静态数据和代码的完整性，对其进行度量很好地解决了平台环境的可信认证。对于智能卡应用时的动态行为，即操作指令序列，采用一种监视器程序结合预存的可信行为策略对其实时监控，实现了关键安全行为的可信验证，从而达到行为的可预期性。开发和测试实验证明，该软信任根与监视器子系统占用系统存储空间很少，对系统性能影响不大，以较低成本达到了较好的效果。

参考文献

[1] 王爱英. 智能卡技术[M]. 北京: 清华大学出版社, 1996.

[2] Koopman P. Embedded System Security[J]. Embedded Computing, 2004, 37(7): 95-97.

[3] David D H, Schaumont P. Securing Embedded Systems[J]. IEEE Security & Privacy Magazine, 2006, (4)3: 40-49.

[4] Mao Shufu, Wolf T. Hardware Support for Secure Processing in Embedded Systems[C]//Proceedings of DAC'07. San Diego, California, USA: [s. n.], 2007.

[5] 张焕国. 可信计算研究进展[J]. 武汉大学学报: 理学版, 2006, 52(10): 513-518.

[6] TCG Main Specification Version 1.2.2[Z]. (2003-10-10). https://www. trustedcomputinggroup.org.

编辑　张正兴