文章编号:1671-8860(2010)05-0618-04　　**文献标志码**:A

可信密码模块软件栈兼容方案设计

张　兴[1,2]　黄宁玉[2]　祝　璐[2,3]

(1　信息工程大学电子技术学院,郑州市商城东路 12 号 450004)
(2　北京工业大学计算机学院可信计算实验室,北京市朝阳区平乐园 100 号,100124)
(3　武汉大学计算机学院,武汉市珞珈山,430072)

摘　要:提出了可信密码模块软件栈的兼容性设计方案,采用软件工程中的策略模式,在软件栈 TSS 基础上内置兼容解释器,对应用和 TCM 的交互进行数据流解析以及数据结构和授权协议的转换,为上层应用提供统一的服务接口。该方案使得基于 TPM 开发的可信应用不需修改或只需少量修改就可以应用于 TCM。测试表明,可信密码模块软件栈完成了应用层调用可信功能的透明转换,实现了应用兼容。

关键词:可信平台模块;可信密码模块;兼容性;软件栈;策略模式
中图法分类号:TP393

为了从体系结构上增强计算机的安全性,国际可信计算组织 TCG 推出了基于可信平台模块(trusted platform module,TPM)的一系列工业规范[1-3],旨在构建以 TPM 为核心的可信计算平台。由于 TPM 采用的密码方案在算法多样性、协议安全性等方面存在一定的局限性[4,5],所以中国分别推出了与 TPM 和 TSS 功能对应的可信密码模块(trusted cryptography module,TCM)和 TCM 服务模块(TCM service module,TSM)规范。文献[6]给出了针对应用兼容问题的改进方案,但只是从局部命令入手,没有给出整体的兼容架构,也没有实现面向应用的接口统一。

TCM 应用 SM2 公钥算法替代 TPM 的 RSA,带来了安全性、运算速度等方面的优势,也改变了 TCM 底层的相关命令[7],而底层命令的改变意味着应用层接口必须作出相应调整,从而引起兼容方面的问题。文献[5]研究了 TCM 授权协议,与 TPM 的授权协议存在很大不同,相应的接口协议也需要进行修改,存在兼容性问题。从密码算法、密码协议、证书管理角度看,TCM 与 TPM 存在很多不兼容的地方,但从应用角度看,只要应用接口统一,将芯片的可信功能提供给应用,就达到了兼容的目标。本文采用策略模式设计了一种新的可信密码模块软件栈。

1　可信密码模块软件栈

TCG 利用 TSS 为上层应用提供访问 TPM 的统一访问入口,对上层应用隐藏构建命令流的底层,管理 TPM 的资源,提供对 TPM 的同步访问[3]。IBM 发布了 TSS 的实现代码 TrouSerS,文献[8]对其进行了详细分析。

本文的基本思路是改进 TSS 以实现应用兼容,设计一种兼容的可信密码模块软件栈,内置兼容解释器,为 TCM 解释应用提交请求,并返回执行结果,通过对命令的映射、数据的解析以及对协议的转换,为应用屏蔽可信计算平台底层芯片的差异。

1.1　模块组成

借鉴 TSS 体系结构[5],本文设计的可信密码模块软件栈如图 1 所示,自顶向下为服务提供模块、核心服务模块、设备驱动库及设备驱动 4 个主体模块,其中分别位于服务提供模块和核心服务模块的两个兼容解释器是实现应用兼容的关键。

直接面向应用的是 TCM 软件栈顶层的服务提供接口,与 TSS 的 TSPI 保持一致。

收稿日期:2010-03-15。
项目来源:国家 863 计划资助项目(2006AA01Z440,2009AA012437);核安全与仿真技术国防重点学科实验室开放研究基金资助项目(HEUFN0801);国家 973 计划资助项目(2007CB311100)。

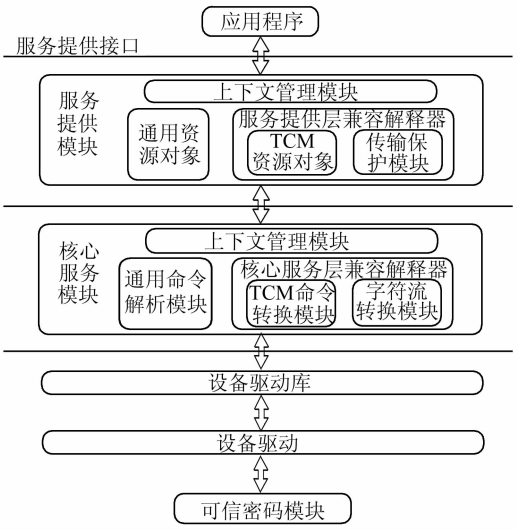

图 1　可信密码模块软件栈

Fig. 1　TCM Software Stack

TCM 软件栈为每个应用程序提供一个服务提供模块,该模块包含上下文管理模块、通用资源对象和服务提供层兼容解释器。上下文管理模块为应用创建会话。通用资源对象提供 TCM 中与密码操作无关的资源映射,可通用于 TSS 和 TCM 软件栈。服务提供层兼容解释器包括 TCM 资源对象和传输保护模块。TCM 资源对象为 TCM 中特有的资源,将应用提供的涉及密码属性的参数解释成与 TCM 密码方案匹配的资源对象,传输保护模块将交互过程解释为 TCM 可识别的授权协议,提供必要的密码功能服务。

与平台上可同时存在多个服务提供模块相比,TCM 软件栈只包含一个核心服务模块。该模块包含上下文管理模块、通用命令解析模块及核心服务层兼容解释器。上下文管理模块管理多个服务提供模块对 TCM 的同步访问。通用命令解析模块为 TCM 中不涉及密码方案的功能提供支撑服务,可通用于 TSS 和 TCM 软件栈。核心服务层兼容解释器包括 TCM 命令转换模块和字符流转换模块,前者将对 TPM 命令的请求解释成对 TCM 中功能相应命令的请求,转换所需参数,后者根据与 TCM 交互的授权协议解析传输中的字符流。

设备驱动库和设备驱动与硬件相关,设备驱动库为核心服务模块提供标准化接口,以访问不同的 TCM 芯片,设备驱动面向 TCM 进行读写操作,是可信计算平台上直接访问 TCM 的惟一入口。

1.2　基于策略模式的设计思想

以 TSS 为基础,采用策略模式设计思想[10]将算法封装,使系统更灵活,并易于扩展。

在策略模式的框架下设计 TCM 软件栈,如图 2 所示,将 TSS 中每条支撑访问 TPM 的命令抽象成一个策略,保持策略与其环境的接口不变,策略中封装与 TCM 的密码服务相匹配的算法。以设置授权数据 Tspi_Policy_SetSecret 命令为例,其核心步骤是为对象的授权数据计算杂凑值 obj_policy_set_secret。在 TSS 中,该策略封装 SHA1 算法,而在 TCM 软件栈中,则将该策略对象中封装的算法替换成 SM3。

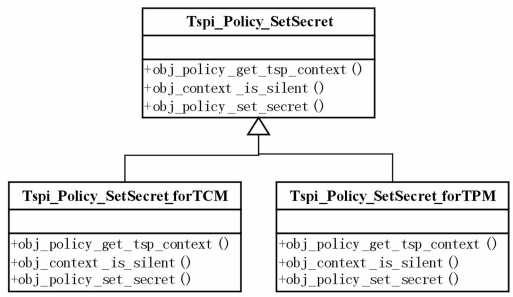

图 2　策略模式的一个实例

Fig. 2　An Instance of Strategy Pattern

1.3　可信密码模块软件栈的实现

如图 3 所示,核心服务模块以守护进程的形式实现,启动后,处于监听等待状态,当接收到服务提供模块处理过的数据后,通过系统调用新建一个线程,在该线程空间中,进一步解析接收到的命令参数等信息,再通过硬件设备驱动与芯片交互,最后将芯片的执行结果通过软件栈顶层接口返回给应用,结束线程。

根据 TCM 密码方案,TCM 软件栈中的 PCR 和哈希值对象的长度定义为 256 位,密钥则分别定义 SM2 密钥和 SMS4 密钥,SM2 密钥结构中包含公钥、加密的私钥、Fp 域的系统参数等,而 SMS4 密钥则包含加密的私钥以及创建时需要的初始向量等参数。执行授权协议的过程中,使用 SMS4 算法加密敏感数据,使用 SM3 算法对参数进行哈希,使用 SM2 算法验证 TCM 的签名。数据传输过程中,将针对 TPM 的命令解释成 TCM 中功能相对应的命令,结合参数的个数和长度,根据协议的具体步骤构建和解析字符流。

2　兼容性分析与测试

2.1　兼容性分析

在底层芯片不兼容的前提下,应用兼容的实现主要取决于芯片上层支撑软件提供的服务可以兼容,即服务接口一致以及密码属性可映射。

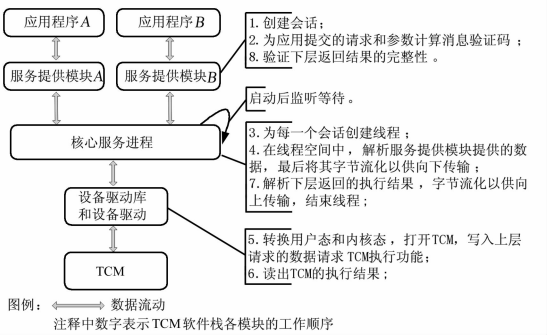

图3 TCM软件栈的实现

Fig. 3 Implementation of TCM Software Stack

借鉴文献[9,10]的接口兼容模型和信号匹配模型，本文给出了支撑服务兼容的形式化模型，定义支撑软件提供的支撑服务为 $S=(O, T, A)$，其中，O 表示接口的操作；T 表示接口参数的数据类型；A 表示服务所包含的密码属性。

定义1 支撑服务兼容：

$$C(S_X,S_Y)\Leftrightarrow C_{\text{op}}(O_X,O_Y)\wedge C_{\text{type}}(T_X,T_Y)\wedge C_{\text{attr}}(A_X,A_Y)$$

C 表示括号中的两个参数具有某种兼容关系；$C(S_X,S_Y)$ 表示采用密码方案 X 和 Y 的支撑服务兼容，当且仅当它们的接口操作兼容、接口参数数据类型兼容并且密码属性兼容。

鉴于软件栈的特点，本文简化了操作兼容，O_X 与 O_Y 相等时，$C_{\text{op}}(O_X,O_Y)$ 为真，即两个操作具有相同的标识符时，则认为它们兼容。

考虑接口参数类型 $T(t_1, t_2, \cdots, t_n)$，其中 t_i 分别表示每个参数的数据类型，T 的兼容性取决于每个参数的兼容性。

定义2 参数数据类型的兼容。对于 $T_X(t_1, t_2, \cdots, t_n)$ 和 $T_Y(t'_1, t'_2, \cdots, t'_m)$，有：

$$C_{\text{type}}(T_X,T_Y)\Leftrightarrow \forall\, 1\leqslant i\leqslant n, C(t_i,t'_i)\wedge n=m$$

与操作兼容相似，将接口参数数据类型兼容简化为接口参数数量相同，且每个对应参数类型相同。

由接口信息得到的密码方面的属性集合包括密钥大小、密钥用途及加密方案等。

定义3 密码属性的兼容：

$$C_{\text{attr}}(A_X,A_Y)\Leftrightarrow \exists\, f: A_X\rightarrow A_Y$$

f 是一个映射，使相同类型或相同用途的算法的密码属性形成对应关系。当 $\text{dom}(f)=A_X$ 时，f 是完全映射，X 提供的功能不会在 Y 中缺失；当 f 是双映射时，X 中的每个属性都能在 Y 中得到对应的属性，且只有一个，反之亦然。

2.2 兼容性测试

参考开源项目 TPM-Emulator，仿真了 TPM 和 TCM 模块，按上述设计思想，以 IBM 开源软件 TrouSerS 为基础，实现了 TCM 软件栈。然后让相同的可信应用调用 TPM 和 TCM 仿真模块，比较调用结果。如图4所示，应用程序分别通过 TrouSerS 和 TCM 软件栈访问 TPM_Emulator 和 TCM_Emulator 请求，获取相同的功能服务。实验结果表明，应用不需修改或者较少修改即可获取 TPM 或者 TCM 中相对应的服务。

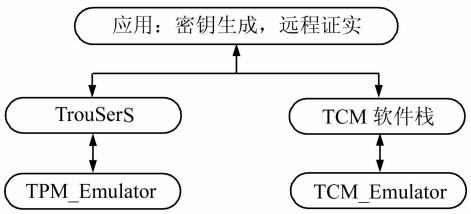

图4 应用兼容测试

Fig. 4 Experiment for Compatibility

表1给出了本文提出的 TCM 软件栈与 TSS、TSM、文献[6]提出的软件栈方案的功能比较，表中，√、×分别表示方案具备或不具备某个功能特性。从表1可发现，本文提出的 TCM 软件栈可支撑应用对 TCM 的访问，并可确保基于 TPM 开发的应用不需针对 TCM 进行修改，增加了底层芯片以及软件栈支撑服务的差异对应用的透明性，在满足安全的前提下实现了对应用的兼容。

表1 本文提出的方案与其他方案的功能比较

Tab. 1 Function Comparison

	TSS	TSM	文献[7]软件栈	TCM软件栈
支撑基于TCM开发的应用获取TCM服务	×	√	√	√
支撑基于TPM开发的应用获取TCM服务	×	×	×	√
针对其他算法的灵活扩展性	×	×	×	√

3 结 语

本文针对应用兼容问题设计了可信密码模块软件栈，该软件栈在 TSS 基础上内置兼容解释器，实现了基于 TPM 开发的应用程序无需修改或少量修改即可调用 TCM 的可信功能。并在开源软件 TrouSerS 的基础上，借鉴策略模式的思想设计实现了 TCM 软件栈。通过 Linux 平台上的仿真实验以及各相关方案之间的比较分析，验证了本文所提出的可信密码模块软件栈面向应用的兼容性。在今后的研究中，将进一步完善可信密码模块软件栈的设计。

参 考 文 献

[1] Trusted Computing Group. TCG Specification Architecture Overview[OL]. http://www.trustedcomputinggroup.org/files/resource_files/AC652DE1-1D09-3519-ADA026A0C05CFAC2/TCG_1_4_Architecture_Overview.pdf,2007

[2] Trusted Computing Group. TPM Main Part 1 Design Principles Specification Version 1.2. [OL]. http://www.trustedcomputinggroup.org/resources/tpm_main_specification/mainP1DPrev103.zip,2007

[3] Trusted Computing Group. TCG Software Stack Specification Version 1.2 Level 1 Errata A [OL]. http://www.trustedcomputinggroup.org/files/resource_files/6479CD77-1D09-3519-AD89EAD1BC8C97F0/TSS_1_2_Errata_A-final.pdf,2007

[4] Bruschi D, Cavallaro L, Lanzi A, et al. Replay Attack in TCG Specification and Solution[C]. The 21st Annual Computer Security Applications Conference, Washington D C, USA, 2005

[5] Zhang Xing, Zhang Xiaofei, Shen Changxiang. A New Authorization Protocol for Trusted Computing [C]. The 1st International Symposium on Data, Privacy and E-Commerce, Oakland, CA,2007

[6] 刘毅,沈昌祥. 一种可信软件栈的兼容性改进方案[J]. 武汉大学学报(理学版), 2009,55(1): 57-61

[7] Zhang Xing, Zhou Ming, Zhuang Junxi, et al. Implementation of ECC-Based Trusted Platform Module[C]. Machine Learning and Cybernetics, Hong Kong, China, 2007

[8] Catherman R, Munetoh S, Nakamura T. TrouSerS-An Open-source TCG Software Stack Implementation [OL]. http://sourceforge.net/projects/trousers/,2007

[9] Zaha J M, Geisenberger M, Groth M. Compatibility Test and Adapter Generation for Interfaces of Software Components[M]. Berlin: Springer-Verlag, 2004: 318-328

[10] Zaremski A M, Wing J M. Signature Matching: A Key to Reuse[M]. New York: ACM Press, 1993: 182-190

第一作者简介:张兴,高级工程师,主要研究方向为信息安全、可信计算。

E-mail:zhangxing99@sohu.com

Design of Compatibility Scheme on TCM Software Stack

ZHANG Xing[1,2]　*HUANG Ningyu*[2]　*ZHU Lu*[2,3]

(1 Institute of Electronic Technology, Information Engineering University, 12 East Shangcheng Road, Zhengzhou 450004,China)

(2 School of Computer Science and Technology, Beijing University of Technology, 100 Pingleyuan, Chaoyang District, Beijing 100124,China)

(3 School of Computer, Wuhan University, Luojia Hill, Wuhan 430072,China)

Abstract: Due to the differences of cryptography and key management model between TCM and TPM, an application which is developed based on TPM could not access TCM through existing software without modification. To solve this problem, we propose a new TCM software stack. It supplies a uniform interface orienting to applications for shielding the difference of chips. Compatibility explainer, the key component of TCM software stack, converses commands and data structures, constructs and resolve information string during the authorization protocols. The design of TCM software stack is guided with strategy pattern and its implementation is based on a TSS instance and the interface definition of TSPI. Through the emulation of TCM software stack and comparison with other related work, the result shows that the compatibility problem has been solved.

Key words: TPM; TCM; compatibility; software stack; strategy pattern

About the first author: ZHANG Xing, senior engineer, majors in information security and trusted computing.

E-mail: zhangxing99@sohu.com