第33卷 第20期 计 算 机 工 程 2007年10月
Vol.33 No.20 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)20—0156—03 文献标识码：A 中图分类号：TP393.08

# 一种柔性可信计算机模型与实现方法

周振柳[1]，陈 楣[1,2]，池亚平[3]，刘宝旭[1]，许榕生[1]
(1. 中国科学院高能物理所计算中心，北京 100049；2. 福州大学，福州 350002；3. 北京电子科技学院，北京 100070)

**摘 要：**基于可信计算组织提出的可信计算原理和安全技术规范，设计了一种柔性可信计算机模型(FTPC)，阐述了该模型的信任机制和实现方法。FTPC通过增强传统BIOS的安全功能，以BIOS核心代码为可信根核，将可信计算模块(TPM)封装成块设备，并通过计算机USB接口实现TPM与BIOS和操作系统的交互。FTPC采用实体的身份认证、完整性度量和密封存储等技术，无需改变现有计算机硬件体系结构即可支持可信计算，FTPC具有易实施和应用灵活的特点。

**关键词：**可信计算模块(TPM)；可信计算；柔性可信计算机；BIOS；用于度量的核心可信根

# Flexible Trusted PC and Its Realization

ZHOU Zhen-liu[1], CHEN Mei[1,2], CHI Ya-ping[3], LIU Bao-xu[1], XU Rong-sheng[1]
(1. Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049; 2. Fuzhou University, Fuzhou 350002; 3. Beijing Electronic Science and Technology Institute, Beijing 100070)

**【Abstract】** Based on the trusted computing group (TCG) specifications about trusted computing, a new type of flexible trusted PC (FTPC) is developed. The model and the trust transitive mechanism of FTPC are discussed. The trusted platform module (TPM) is an extension of USB port, and the legacy BIOS is enhanced to be the core root of trust for measurement (CRTM) in FTPC. The technologies, such as identity authentication of entity, integrity measurement of entity, and sealed storage, are employed in FTPC to support trusted computing. Without changing the PC's current hardware architecture, the FTPC is more easy and flexible to be implemented and applied than the TCG trusted PC.

**【Key words】** trusted platform module (TPM); trusted computing; flexible trusted PC(FTPC); BIOS; core root of trust for measurement (CRTM)

基于软件的信息安全基础解决方案存在一个包括4阶段的安全死循环周期：系统实现，发现缺陷，缺陷修补，发现新缺陷，不能从根本上解决信息安全问题。可信计算组织(trusted computing group, TCG)提出可信计算平台概念，以计算平台硬件安全可信为基础，以“信任传递”和“完整性度量”为手段，从硬件层安全着手解决信息安全问题[1]。

可信计算机是可信计算平台主要的终端计算设备。完全符合TCG规范的可信计算机的实现，要求对现有计算机软硬件体系结构进行较大改动：(1)可信计算模块(trusted platform module, TPM)通常要求和计算机主板集成；(2)操作系统能支持信任链传递和完整性度量。

因此，基于TCG规范的可信计算平台建设，其实际应用需要一个较长过程。另一方面，即使新的可信计算机面世，现有的PC机也不会被立即丢弃，会在较长时期内与新型可信计算机共存。

如何在不改变现有计算机硬件体系结构的情况下，方便地改造现有计算机成为可信计算设备，本文对这一问题进行了研究。

## 1 可信计算机原理和相关工作

TCG对可信的定义是：如果实体按照预先设定的方式运行，则实体是可信的。在可信计算环境中，所有实体都被要求是可信的，任何不能被证明是可信的实体都会被拒绝加入可信计算环境中。TCG定义通过“信任传递”和“完整性度量”机制保障计算平台的可信性和完整性不被破坏。

TCG从8个方面为可信计算平台开发制定了一系列技术规范[1]，可信计算机作为可信计算平台的主要终端设备，其相关原理和技术实现是本文关注的重点。

可信计算机由可信硬件系统和可信软件系统两部分构成。可信硬件系统包括物理硬件和固件，可信软件系统包括可信操作系统和可信应用软件。

可信计算机的核心部件是TPM。它是一个含有密码运算部件和存储部件的片上系统，提供密钥生成、加密解密、实体鉴别、数字签名等功能。TPM内部带有非易失性存储部件用来保存认证证书、私钥等秘密信息，并提供至少16个(platform configuration register, PCR)叠加存储可信平台的各种完整性度量值。

在可信计算机中，采用基于公开密码体制的数字证书实现实体的可信性认证，采用报文摘要和签名技术实现对软件、数据、环境配置等的完整性度量。

为防止私钥泄露，TPM提供对私钥的密封存储和运行时保护，私钥不离开TPM。可信计算机系统软件和应用软件所有与私钥有关的加解密、摘要签名等运算均通过标准接口交由TPM完成。

目前可信计算机的研究一般将TPM绑定到主板。文献[4]通过在主板上集成嵌入式安全模块(embedded security module, ESM)实现了一种安全计算机，通过I/O端口操作控

**基金项目：**国家自然科学基金资助项目(90412017)；北京电子科技学院科研基金资助项目

**作者简介：**周振柳(1971－)，男，博士研究生，主研方向：网络安全，可信计算；陈 楣，硕士研究生；池亚平，副教授；刘宝旭，副研究员；许榕生，研究员、博士生导师

**收稿日期：**2006-10-28 **E-mail：**zhouzl@ihep.ac.cn

制和基于智能卡的认证控制增强计算机安全性能。文献[5]讨论了可信计算技术对可信操作系统的安全服务支持。文献[6]对改造 Linux 操作系统使之支持启动过程中的可信度量提出了设计和实现方案。文献[7]分析了计算机的启动过程，提出一种基于网络可信服务器的计算机可信引导方案。

以上工作主要集中在应用 TCG 的“信任传递”和“完整性度量”概念，对计算机软硬件进行局部安全增强和安全设计。本文提出一种新的柔性可信计算机模型 FTPC，能方便地改造现有计算机成为可信计算设备，其实现具有较大的灵活性。为在现有计算机和符合 TCG 规范的新型可信计算机共存环境下如何实现可信计算平台建设提供了一种新思路。

## 2 柔性可信计算机模型

柔性可信计算机模型立足于现有的计算机硬件体系结构，是 TCG 可信计算概念和技术在现有计算机硬件体系结构下的一种灵活的扩展应用模型。FTPC 模型改变一般在计算机主板上嵌入 TPM 模块的做法，将 TPM 封装成块设备并通过计算机 USB 接口实现与计算机的连接。通过对计算机 BIOS 的功能改造和安全增强，使 BIOS 在开机初始阶段支持 USB 通信和交互操作，由 BIOS 与 TPM 共同完成硬件平台设备的认证和其他固件与平台配置的完整性度量。FTPC 的结构模型如图 1 所示。

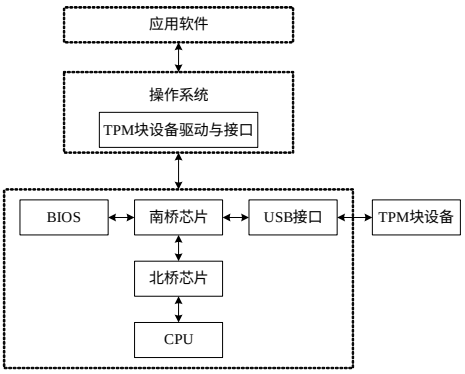


**图 1 FTPC 结构模型**

在柔性可信计算机模型中，不需要改变现有计算机主板体系结构，而是通过软件方式增强 BIOS 固件对可信计算的支持。现有计算机 BIOS 存储芯片普遍采用可软件读写的 FLASH 芯片，并且能提供足够大的容量，通过 BIOS 的安全增强实现对现有计算机的可信改造不仅是可行的，而且容易实施。BIOS 同时又是计算机开机上电最早执行的代码，增强 BIOS 使 BIOS 成为 FTPC 的核心可信根，进一步增强了 FTPC 的安全可信。

FTPC 中的 BIOS 增强，是在开机初始阶段让 BIOS 支持与 TPM 的双向身份认证，并与 TPM 交互，使 TPM 完成对平台中各种实体的身份认证和完整性度量。

在FTPC模型中，TPM与USB控制芯片集成构成TPM块设备，TPM块设备通过计算机USB接口和计算机相连接。FTPC中的TPM符合TCG的TPM 1.2 规范[3]。

柔性可信计算机的 BIOS 在开机最初阶段要与 TPM 块设备进行相互间的身份认证。如果认证失败，BIOS 停止计算机的启动过程。因此，当特定 TPM 块设备与计算机分离时，柔性可信计算机不能启动和使用。可见在 FTPC 中，TPM 在物理上与计算机主板是分离的，而在逻辑上是主板不可分离的一部分。

由于 TPM 不与计算机主板集成，当计算机的使用环境、用途、使用者等发生变化时，FTPC 能够更方便、灵活、快捷地适应这种改变。

基于 FTPC 模型的可信计算机，既支持不改变现有软硬件体系结构下实现有限可信，也支持符合 TCG 规范的软硬件体系结构下实现完全可信，其可信性是可扩展的。

## 3 柔性可信计算机信任机制

在 FTPC 中，用于度量的核心可信根 (core root of trust for measurement, CRTM)被设计成 BIOS 代码的一个组成部分。CRTM 是被无条件信任的根代码。计算机开机上电后，首先执行 CRTM 代码，然后由 CRTM 与 TPM 块设备共同完成对计算机启动、操作系统装载、操作系统和应用程序运行等剩余过程的信任度量。信任度量的内涵包括身份认证和完整性度量。

在 FTPC 中，通过对传统 BIOS 的改造，使 BIOS 的核心代码成为可信计算的 CRTM。对传统 BIOS 的改造，是通过在 BIOS 中嵌入功能模块实现的。

BIOS 中的 CRTM 包括：BIOS 自检代码，BIOS 基本硬件初始化代码，BIOS 中驱动 USB 的代码以及 BIOS 安全模块代码。BIOS 除包含 CRTM 外，还包括一些其他代码或数据模块。

系统加电，BIOS 首先执行 POST(power on self test)过程，然后对内存、芯片组等进行初始化，驱动 USB，执行 CRTM 的安全模块代码。这个过程是被无条件信任的。BIOS 安全模块执行后，利用 USB 通道与 TPM 进行双向身份认证。若认证失败，说明 TPM 块设备是非法的，停止启动过程。若认证成功，在继续调度执行 BIOS 中其他模块或扩展卡(如显卡、网卡、SCSI 卡等)ROM 中的代码前，BIOS 安全模块利用 TPM 对这些模块代码进行信任度量。这些模块执行后，控制权交回给 BIOS 安全模块。此后的每一个过程中代码执行前，都由上一过程对其进行信任度量，度量通过后才能进行控制权的转移。

FTPC 的信任机制如图 2 所示。

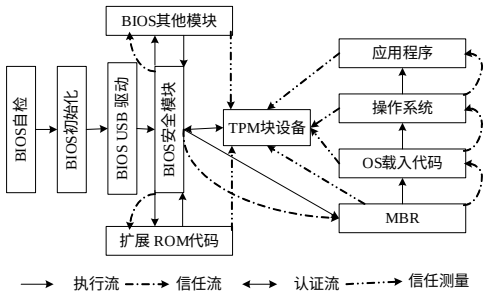


**图 2 FTPC 信任机制**

当然，在身份认证或信任度量失败时，也可允许计算机启动运行，进入弱可信或非可信运行状态。此时，可通过其他一些技术，让计算机功能受到一定的限制[4]。

## 4 柔性可信计算机实现

柔性可信计算机的实现，其主要采用的安全技术遵循 TCG 规范。其创新之处在于通过 BIOS 的安全增强和 TPM 与计算机主板的分离技术对可信计算机的灵活设计，解决了现有计算机与 TCG 可信计算机的硬件体系结构不一致的问题。

### 4.1 FTPC 的 BIOS 安全增强

在现有计算机硬件体系结构下，BIOS是计算机开机上电最先执行的代码，因此TCG定义的CRTM最适合存在于BIOS中。传统BIOS一般采用模块化结构，存储在FLASH芯片中的

BIOS二进制整体影像由几个到几十个不等数量的模块组成，每个模块完成相对独立的一组功能。因此，将传统BIOS整体作为CRTM显然是不合适的。通过对传统BIOS的功能细分，研究BIOS执行过程中每一过程的重要性和先后次序，FTPC将BIOS POST[8]和BIOS INITIAL[8]过程应包含的功能划分到CRTM中。

传统 BIOS 不提供对可信计算的支持。为了使 BIOS 中的 CRTM 代码在执行过程中能够与 TPM 块设备交互，FTPC 为 BIOS 新增加了 USB 驱动模块和安全模块。BIOS 的 USB 驱动模块支持 BIOS 中的 CRTM 在无操作系统环境下，通过计算机 USB 接口实现与 TPM 块设备的交互；BIOS 中的安全模块基于传统 BIOS 提供对可信计算的支持。两个模块既可以独立于 BIOS 设计编写，以符合 BIOS 格式的功能模块形式嵌入到传统 BIOS 中，也可在计算机出厂之初与 BIOS 整体提供。

BIOS 安全模块支持基于公开密码体制的数据加密、数字签名等功能。

### 4.2 FTPC 的 TPM 块设备

在 FTPC 中，TCG 组织定义的可信平台模块 TPM 被封装成块设备，通过计算机 USB 接口与计算机连接。但 TPM 块设备不同于普通的计算机外围设备，TPM 块设备参与计算机最初的 BIOS 引导过程并在计算机整个运行过程中提供信任度量。TPM 块设备在物理上与计算机主板分离，而在逻辑上实际是 FTPC 硬件平台不可分离的一部分。没有合法的 TPM 块设备，柔性可信计算机不能启动运行。

TPM 块设备结构包括：嵌入式 CPU，RAM，非易失性存储单元，随机数产生器，PKI 密钥产生器，RSA 协处理器，HMAC 和 SHA-1 代码引擎，USB 控制器，电源检测单元等。

TPM块设备设计遵循TCG TPM 1.2 规范[3]，支持USB 2.0 协议。

### 4.3 FTPC 的软件系统支撑

FTPC 在操作系统核心层提供对 TPM 块设备的驱动，在系统服务层提供调用 TPM 进行可信计算的服务。

现有操作系统不提供对可信计算的支持。柔性可信计算机使用非可信操作系统的情况下，应该在操作系统安装完后利用 BIOS 安全模块和 TPM 设备对操作系统环境进行初始化信任度量，以保证操作系统在以后运行过程中的完整性。

FTPC模型主要为适应现有的计算机硬件体系结构而提出。当采用可信操作系统时，FTPC的软件支撑符合TCG的TSS规范[1]。

### 4.4 FTPC 的可信初始化算法

以实体 $B$ 代表 BIOS 的安全模块，实体 $T$ 代表 TPM 块设备。FTPC 硬件平台可信初始化算法描述如下：

(1)基于PKI，为$B$和$T$分别生成一对秘钥，设$B$的公钥为$E_B$，私钥为$D_B$；$T$的公钥为$E_T$，私钥为$D_T$。

(2)公钥$E_T$和私钥$D_B$写入$B$中，将$B$嵌入到BIOS中。

(3)公钥$E_B$和私钥$D_T$存储到$T$中。

(4)$B$ 判断 FTPC 状态，若平台已经进行过可信初始化，则结束；否则继续下一步。

(5)$B$ 与 $T$ 进行双向身份认证，认证过程为

$B$ to $T$: $E_T(R_B)$

$T$ to $B$: $E_B(R_B, R_T, K)$

$B$ to $T$: $K(R_T)$

$R_B$和$R_T$为$B$和$T$为该次认证产生的随机数，$K$是$B$和$T$共享的通信密钥。$E_X()$表示以实体$X$的私钥进行加密。任何一方认证失败，则中断初始化过程。

(6)$B$ 采集 BIOS 其他模块代码和扩展 ROM 代码并提交给 $T$ 进行完整性度量，$T$ 保存这些模块代码完整性度量的结果。设代码数据为 $code$，根据 HMAC 方法计算 $code$ 的摘要鉴别码：

HMAC=$H(K \text{ xor } opad, H(K \text{ xor } ipad, code))$

(7)初始化完成后，B 和 T 更新各自的平台状态值

如果在柔性可信计算机上安装运行不支持可信计算的操作系统，则对软件系统平台在安装完成的最初阶段也要进行软件系统平台的可信初始化，方法参考硬件平台的可信初始化算法。

## 5 小结

基于 TCG 规范的可信计算平台建设，需要对现有的计算机硬件体系结构和软件体系结构进行较大的改动，其实际应用需要一个较长过程。另一方面，非可信计算环境向完全可信计算环境迁移过程中，现有计算机将会与可信计算机有一个长期共存的过程。因此，在不改变现有计算机硬件体系结构的情况下，方便地改造现有计算机成为可信或有限可信的计算设备，对于可信计算的发展和应用存在实际意义。

本文从 TCG 规范和技术入手，提出柔性可信计算机模型 FTPC。通过对传统 BIOS 软件在功能和安全性能方面的增强，使得 TPM 与计算机在物理上分离，在逻辑上则是不可分割的整体。FTPC 模型既能支持在现有计算机软硬件体系结构下实现可信计算，也为符合 TCG 规范的可信计算机硬件体系结构设计提出了一种新的思路。下一步的工作，是进一步细化操作系统引导、运行中的各个环节的研究，使信任度量更全面完善，在现有软硬件条件下进一步提高 FTPC 实现的可信度。

## 参考文献


1 TCG. TCG Infrastructure Architecture Version 1.0[Z]. [2006-06-13]. https://www.trustedcomputinggroup.org.

2 TCG. TCG PC Client Specific Implementation Specification for Conventional BIOS Version 1.2[Z]. [2006-06-13]. https://www.trustedcomputinggroup.org.

3 TCG. TCG TPM Specification Version1.2[Z]. [2006-06-13]. https://www.trustedcomputinggroup.org.

4 张焕国, 毋国庆, 覃中平, 等. 一种新型安全计算机[J]. 武汉大学学报(理学版), 2004, 50(S1): 1-6.

5 黄　强, 沈昌祥. 可信计算技术对操作系统的安全服务支持[J]. 武汉大学学报(理学版), 2004, 50(S1): 15-18.

6 方艳湘, 黄　涛. Linux 可信启动的设计与实现[J]. 计算机工程, 2006, 32(9): 51-53.

7 黄　涛, 沈昌祥. 一种基于可信服务器的可信引导方案[J]. 武汉大学学报(理学版), 2004, 50(S1): 12-14.

8 陈文钦. BIOS Inside-BIOS 研发技术剖析[M]. 中国台湾: 旗标出版股份有限公司, 2001.