“十二五”重点图书

# 可信链度量与测评

张 帆 徐明迪 杨 飏 著

学术专著

西安电子科技大学出版社
http://www.xduph.com

# 可信链度量与测评

张 帆　徐明迪　杨 飏　著

西安电子科技大学出版社

## 内容简介

可信计算是一种信息系统安全新技术，它关注于终端安全，从硬件和软件底层入手，针对信息系统综合采取措施，以增强系统的安全性。目前，可信计算已经成为国内外信息安全领域的一个新热点，并已取得了令人鼓舞的成绩。

可信计算具有三大基本功能：完整性度量、完整性存储和完整性报告。其中，完整性度量功能又是完整性存储功能和完整性报告功能的基础。为了实现完整性度量功能，可信计算组织TCG定义了可信链技术。能否实现完整、安全的可信链，直接关系到整个可信计算平台能否正常运行。目前，研究人员从不同角度对可信链进行了深入研究，但仍有不少开放问题有待解决。本书重点针对可信链的两个重要组成部分——完整性度量和安全性测评，从理论和实践两方面作了介绍。

全书共分五章：第一章，可信计算；第二章，可信启动完整性度量；第三章，应用程序完整性度量；第四章，可信链测评；第五章，总结与展望。

本书可以作为高年级本科生、研究生的教材，也可以作为可信计算研究人员和工程技术人员的参考书。

**图书在版编目(CIP)数据**

**可信链度量与测评**/张帆，徐明迪，杨飚著. —西安：西安电子科技大学出版社，2011.12
ISBN 978-7-5606-2694-9

Ⅰ. ①可… Ⅱ. ①张… ②徐… ③杨… Ⅲ. ①计算机安全—安全技术—研究生—教材
Ⅳ. ①TP309

**中国版本图书馆 CIP 数据核字(2011)第 230430 号**

策　　划　马乐惠
责任编辑　阎　彬　马乐惠
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　西安文化彩印厂
版　　次　2011 年 12 月第 1 版　　2011 年 12 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印 张 8
字　　数　186 千字
印　　数　1～2000 册
定　　价　20.00 元
ISBN 978-7-5606-2694-9/TP・1310

**XDUP 2986001-1**

# 前　言

21世纪是信息的时代。随着科技的飞速发展，信息技术已经深入到人们生活的方方面面，社会信息化程度空前提高，大大改变了人们的生活方式。但是与此同时，危害信息安全的事件也在不断发生，信息安全已经成为一个重要的国家和社会问题。从全球来看，世界发达国家和地区均将信息安全提高到战略高度。2009年，美国成立了“网站司令部”，并于2010年5月21日正式运行。“网站司令部”是隶属于美国战略司令部的下级联合司令部，其重要职责和功能就是要确保美国夺取制网权。在“网战司令部”的基础上，美国五角大楼于2011年拟出台一份关于网络战争的新战略文件，根据这一新战略，从外国向美国计算机系统发起的攻击将被视为战争行为，美国将对此类攻击进行包括传统军事打击在内的报复。无独有偶，欧盟也于2011年成立了“网络安全保障小组”，其任务是防范和应对黑客袭击，确保欧盟机构电脑网络的安全。同年，日本防卫省也决定建立一支专门的“网络空间防卫队”，以防备黑客攻击，加强保护机密信息的能力。英国在2009年出台了首个国家网络安全战略，并在2011年宣布拟成立英版的“网络司令部”。可见，信息安全已经成为国家综合国力竞争的焦点之一，可以这样说，谁走在了信息安全的前列，谁就占领了信息安全领域国家竞争的战略制高点。因此，必须采取措施确保并增强我国的信息安全。

在长期的信息安全研究过程中，人们逐渐认识到，信息安全是一项系统性的工作，只有从信息系统整体入手，才能比较有效地确保信息系统的安全性。就信息系统整体而言，其安全的基础是信息系统硬件安全和操作系统安全，密码和网络安全等则是关键技术。因此，要保证信息系统的安全性，就必须从芯片、主板、BIOS、操作系统和终端做起，从硬件和软件的底层做起，并结合密码和网络安全等关键技术，综合采取措施。正是这一思想催生了可信计算，并促进了可信计算的蓬勃发展。

可信计算具有完整性度量、完整性存储和完整性报告三大基本功能。其中，完整性度量功能又是完整性存储功能和完整性报告功能的基础。能否实现完整、安全、可靠的完整性度量功能，关系到整个可信计算平台的可信性。这是因为：如果完整性度量功能存在功能缺失或者安全漏洞，则整个可信计算平台将部分或者全部地处于不可知甚至不可信的状态，由此将进一步妨害完整性存储功能和完整性报告功能的正常运行，最终会导致整个可信计算平台失去“可信”的基础。因此，对完整性度量功能展开理论研究，并进而实现完整、安全、可靠的完整性度量功能，是可信计算平台必须解决的核心问题之一。作为实现完整性度量功能的关键技术，对可信链技术展开深入研究具有重要的理论和现实意义。

可信链是一项复杂的工作，它定义了从可信度量根核(CRTM)开始，逐步到基本输入输出系统(BIOS)、操作系统加载器(OS Loader)、操作系统(OS)，最后到应用程序(Applications)和网络(Networks)的可信度量与可信传递过程。在这个过程中，包含了可信度量根核、相关证书、TPM/TCM驱动、完整性度量、完整性度量结果存储与集成、可信链恢复、可信链安全性测评等一系列相关工作。本书针对其中的两个重要组成部分——

完整性度量和安全性测评，从理论和实践两方面进行了研究，其中的部分研究成果得到了实际应用。

本书共分五章：第一章，可信计算；第二章，可信启动完整性度量；第三章，应用程序完整性度量；第四章，可信链测评；第五章，总结与展望。其中，第一章、第二章由张帆和杨飏编写，第三章由张帆编写，第四章由徐明迪编写，第五章由张帆和徐明迪编写。全书由张帆统稿。

在本书的理论研究和书稿写作过程中，得到了武汉大学计算机学院、武汉瑞达信息安全股份有限公司和杭州电子科技大学通信工程学院各级领导、同事和朋友的关心和帮助；西安电子科技大学出版社的马乐惠和阎彬老师对于本书的定稿和出版也付出了非常辛苦的劳动。作者在此一并表示由衷的谢意！

本书的三位作者在理论研究、系统实现和书稿写作的过程中，先后分别参与并受到了以下项目及基金的支持：国家 863 高科技研究与发展计划“面向复杂系统的需求建模方法的研究与实现”(2007AA01Z85)、国家 863 高科技研究与发展计划“可信计算平台安全测评关键技术与原型系统研究”(2007AA01Z411)、国家自然科学基金(60872092)、国家信息安全特色专业建设项目(GK090104003)、浙江省科协育才计划(ZX090206003)和武器装备预研基金(9140A15040211CB3901)。在此一并表示感谢！

由于作者水平有限，书中难免会有不妥之处，恳请读者理解和批评，并欢迎读者提出宝贵的意见。作者在此先表示感谢！

张帆　徐明迪　杨飏

2011 年 6 月于杭州电子科技大学

# 目　录

# 第一章 可信计算

## 1.1 可信计算简介

随着信息产业的高速发展，信息技术深入到了人们生活的方方面面。但是与此同时，危害信息安全的事件也在不断发生，对国家、社会和个人的信息安全构成了巨大的威胁。目前，世界发达国家均将信息安全提升到了国家战略地位，从某种程度上来讲，谁站在了信息安全的前列，谁就占据了国家战略竞争的先机。因此，必须采取措施来保障我国的信息安全，并大力开展信息安全研究，促进信息安全产业化。

对于一个信息系统而言，其安全性的基础是硬件安全和操作系统安全，密码和网络安全等是关键技术。只有从信息系统的硬件和软件底层做起，并从整体上采取措施，才能比较有效地确保信息系统的安全性[1]。

随着理论和实践的发展，人们已经逐渐认识到，大多数的安全隐患来自微机终端，因此，要保证信息系统安全，首先必须保证微机的安全性。而要保证微机的安全性，就需要从芯片、主板等基础硬件和 BIOS、操作系统等基础软件两方面综合采取措施。正是这一思想催生了可信计算，并促进了可信计算的蓬勃发展[1]。

### 1.1.1 可信计算的基本概念

本节对可信计算的一些基本概念予以说明。

(1) TPM 和可信计算机。与普通计算机相比，可信计算机最大的特点就是在它的主板上嵌入了一个安全模块——可信平台模块(Trusted Platform Module，TPM)。在 TPM 的内部封装了可信计算平台所需要的大部分安全服务功能，用来给平台提供基本的安全服务。同时，TPM 也是整个可信计算平台的硬件可信根，是平台可信的起点。作为平台的硬件可信根，TPM 受到了严格的保护：从物理上来说，TPM 具有防攻击、防篡改和防探测的能力，能够保护 TPM 本身以及其内部数据不被非法攻击。图 1.1 给出了 TPM 的主要结构。

图 1.1 中各个部分的含义如下。I/O 部件管理信息通过总线的流通，完成协议的编码和译码，并发送消息到各个部件。Cryptographic Co-Processor 是密码协处理器，用来实现加密、解密、签名和签名验证。TPM 采用 RSA 公钥密码，也允许使用 ECC 或者 DSA。HMAC Engine(HMAC 算法引擎)实现 HMAC 的计算，其计算依据是 RFC2104 规范。SHA-1 引擎(SHA-1 Engine)用来计算部件的 SHA-1 哈希摘要。Opt-In 是一组选项开关。

Non-Volatile Memory 是非易失存储器，主要用于存储密钥、证书、标识等重要数据。Key Generation 是密钥产生部件，用来产生 RSA 的密钥对和对称密码的密钥等。RNG(随机数产生部件)用来产生随机数，作为 TPM 的随机源。Power Detection(电源检测部件)管理 TPM 的电源状态和平台的电源状态。Execution Engine 是执行引擎，它包含 CPU 和嵌入式软件，通过软件的运行来执行接收到的命令。Volatile Memory 是易失性存储器，是主要用于 TPM 的工作存储器。

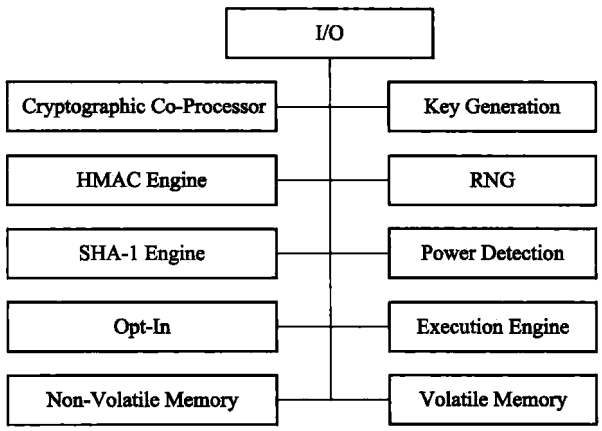


图 1.1 TPM 硬件结构

(2) 可信的定义。关于可信的定义目前还存在着一定的争议。就 TCG(可信计算组织)而言，他们是从行为的角度定义可信的，即：一个实体是可信的，如果它的行为总是以预期的方式，朝着预期的目标。其关注的主要是完整性属性。因此，从 TCG 的角度而言，可以认为：可信≈完整性。国内也有观点认为：可信≈可靠＋安全[1-2]。文献[1]中指出：由于可信计算系统要能够提供系统的可靠性、可用性、信息和行为安全性，因此，其可信包括许多方面，例如正确性、可靠性、安全性、可用性、效率等。但是，系统的安全性和可靠性是现阶段可信最主要的两个方面，因此，可信可以简称为：可信≈可靠＋安全。

(3) 信任的属性。文献[1]中指出，信任具有以下属性：

• 信任是一种二元关系，它可以是一对一、一对多(个体对群体)、多对一(群体对个体)或者多对多(群体对群体)的。

• 信任具有二重性。信任既具有主观性又具有客观性。

• 信任不一定具有对称性，即 A 信任 B，但是 B 不一定信任 A。

• 信任可度量。信任有程度之分，可以划分等级。

• 信任可传递，但是不绝对，并且在传递过程中可能有损失。传递的路径越长，损失可能越大。

• 信任具有动态性。信任与环境(上下文)和时间因素相关。

(4) 信任的获取。信任的获取有直接和间接两种方法。有时候，信任还可能一级一级地传递，由此就构成了信任链。

(5) 可信根。可信根是可信计算平台的基础之一。根据 TCG 规范，一个可信计算平台包含三个可信根，分别是可信度量根(Root of Trust for Measurement，RTM)、可信存储根(Root of Trust for Storage，RTS)和可信报告根 (Root of Trust for Report，RTR)。这

三个根都必须是绝对可信的，它们分别是可信计算平台进行完整性度量、存储和报告的基础和起点。在实现的时候，必须从硬件、软件以及管理上确保这三个根的绝对可信。

(6) 完整性度量、存储和报告。所谓的完整性度量是指：通过一定的技术，获取整个平台(硬件或软件)的完整性特征的过程。在度量的过程中，需要把度量的结果记录下来，这个记录的过程就是完整性存储的过程。通常，完整性存储需要执行两方面的操作：第一，把度量结果保存到位于主机内存的度量日志(Measurement Log，ML)中；第二，把度量的结果集成到平台配置寄存器 (Platform Configuration Register，PCR)中。通常，PCR 位于可信平台模块 TPM 的内部并受到 TPM 的严格保护。当第三方需要判断该平台可信性的时候，完整性报告功能可以把通过完整性存储功能所保存下来的平台完整性度量结果发送给第三方，由第三方自主判断平台的可信性。

(7) 可信支撑软件。可信支撑软件(TCG Software Stack，TSS)是可信计算平台上 TPM 的支撑软件。TSS 的主要作用是为应用软件提供兼容已购可信平台模块的开发环境。

(8) 可信网络连接。可信网络连接(Trusted Network Connection，TNC)的主要目的是确保网络访问者的完整性。通过网络访问请求，搜集和验证请求者的完整性信息，依据一定的安全策略对这些信息进行评估，决定是否允许请求者与网络连接，从而确保网络连接的可信性。

### 1.1.2 国外可信计算的发展

1983 年，美国国防部制定了世界上第一个可信计算机系统评价准则 TCSEC。在 TCSEC 中，第一次提出了可信计算机和可信计算基(Trusted Computing Base，TCB)的概念，并把 TCB 作为系统安全的基础。

1999 年，IBM、HP、Intel 和微软等国际知名 IT 企业联合发起成立了可信计算平台联盟(Trusted Computing Platform Alliance，TCPA)。2003 年，TCPA 改组为可信计算组织 TCG。TCPA 和 TCG 的出现形成了可信计算的高潮。目前 TCG 已经制定了一系列的可信计算规范。

2002 年，微软提出了“Palladium”计划，关注于数字版权的问题，后来改为更平和的 NGSCB(Next Generation Secure Computing Base)[3]。NGSCB 从下至上依次分为三层：最底层为安全硬件支持模块(Secure Support Component，SSC)，提供必要的密码支持和安全存储功能；中间层为运行在操作系统内的 Nexus，它是 NGSCB 的核心组件，负责为上层应用提供 SSC 的访问和各种安全功能支持；最上层为 NCA(Next Computing Agent)，它是 Nexus 为应用程序提供的一个用户态代理进程，应用程序通过该进程与 Nexus 交互，获取所需的安全服务。目前 NGSCB 已经在 Vista 中得到应用。

2003 年，Intel 正式发布了支持 Palladium 的“LaGrande” 技术，简称 LT。其核心是在原来硬件基础上增加一层可信机制，保护 PC 免遭基于软件和硬件的攻击。LT 将改进 CPU 的结构和指令集，改进芯片组结构，以支持内存保护和进程隔离，同时对输入输出设备进行保护。目前，Intel 已将 LT 更改为可信执行技术(Trusted eXecution Technology，TXT)[4]。

2006 年，欧盟启动了名为“开放式可信计算(Open Trusted Computing)”[5]的可信计算研究计划。其目标是开发一个源代码公开的基于 TPM 的安全操作系统，开发基于安全操

作系统和遵循相关协议的软件，开发 OpenTC 原型应用，以使民众能使用用户自主控制的、可信安全的信息设备。

目前，可信计算已经成为许多国际学术会议的重要议题。国外许多芯片厂商也推出了自己的可信平台模块芯片。几乎所有的品牌笔记本电脑和台式机都安装了 TPM 芯片。多家网络技术企业的产品都支持 TNC 体系结构。可信计算产品已经走向了应用。

### 1.1.3 国内可信计算的发展

我国的可信计算“起步不晚，水平不低，成果可喜，已经站在了国际可信计算的前列”[1]。

2000 年 6 月，武汉大学和武汉瑞达公司合作，开始研制安全计算机。2004 年 10 月，他们所研制的安全计算机通过了国家密码管理委员会主持的技术鉴定。这是我国第一款自主研制的可信计算机，这种计算机[6-7]在系统结构和主要路线上与美国可信计算组织 TCG 的可信 PC 规范是一致的，并且在技术上有所创新，有些地方也有差异。这一产品被国家科技部等四部委联合认定为“国家级重点新产品”，并在我国政府、公安、银行、军队等多部门得到了实际应用。

2004 年 6 月在武汉召开了中国首届 TCP 论坛。2004 年 10 月在解放军密码管理委员会的支持下，在武汉大学召开了第一届中国可信计算学术会议。

2005 年联想集团的 TPM 芯片和可信计算机研制成功。同年，兆日公司的 TPM 芯片也研制成功。这些产品都通过了国家密码委员会的鉴定和认可。

2006 年我国进入制定可信计算规范和标准的阶段。在国家密码管理局的主持下，我国制定了《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与结构规范》两个规范。

2007 年在国家信息安全标准委员会的主持下，我国开始制定一系列的可信计算标准，包括芯片、主板、软件、可信网络连接等。国家自然科学基金委员会启动了“可信软件重大研究计划”。深圳中兴集成电路公司的“可信计算机密码模块安全芯片”和联想公司的“可信计算密码支撑平台”通过了国家密码管理局的认证。

2008 年中国可信计算联盟 CTCU 成立。在国家 863 计划支持下，武汉大学研制出我国第一款“可信 PDA”和第一个“可信计算平台测评系统”。

2009 年瑞达公司的“可信计算机密码模块安全芯片”通过国家密码管理局的认证。基于这一新芯片的可信计算机也推出上市。

我国的可信计算事业进入了蓬勃发展的阶段，可信计算技术与产品得到了国际同行的高度评价，我国已经站在了国际可信计算领域的前列。

## 1.2 可 信 链

可信计算平台具有三大核心功能：完整性度量、完整性存储和完整性报告。其中，完整性度量功能又是完整性存储功能和完整性报告功能的基础。如果完整性度量功能存在功能缺陷或安全缺陷，则可信计算平台就无法将其当前的信任状态如实地反映给对方，从而

导致整个可信计算平台就无法“可信地”工作。本节所介绍的可信链正是实现完整性度量的关键技术。

TCG 给出的可信链定义[8]如下(参见图 1.2)：

CRTM→BIOS→OS Loader→OS→Applications

其中，CRTM 称为可信度量根核(Core Root of Trust Measurement)。根据 TCG 规范，作为度量起点的可信度量根核 CRTM 应该是绝对可信的，理想情况下它应该存储在 TPM 内部，受到 TPM 的严格保护，但是在实现时它往往存储在另外的固件中。有时候，CRTM 就是 BIOS 里面的一小块代码。

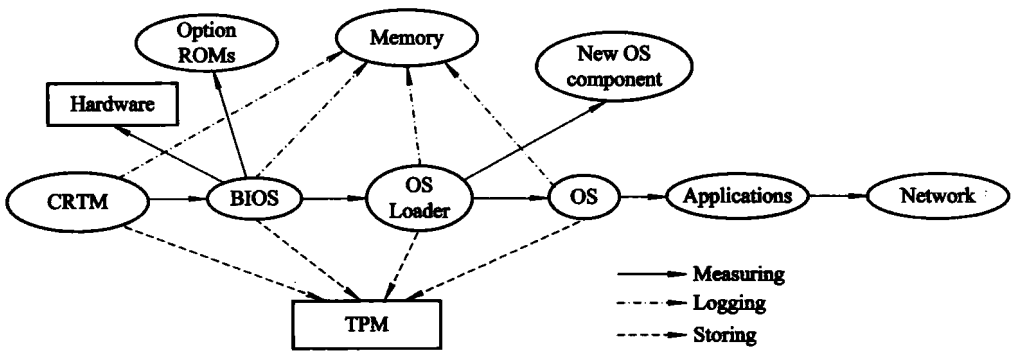


图 1.2 可信链定义

图 1.2 给出了可信链的定义。当系统加电以后，CRTM 首先对 BIOS 的完整性进行度量。通常，这种度量就是把 BIOS 当前代码的哈希摘要计算出来(例如计算 SHA-1)，并把计算结果与预期的哈希值进行比较。如果两者一致，则说明 BIOS 的内容没有被篡改，BIOS 是可信的；如果不一致，则说明 BIOS 被攻击，其完整性遭到了破坏。如果 BIOS 度量可信，那么可信的边界将会从 CRTM 扩大到“CRTM+BIOS”。之后，“CRTM+BIOS”将会进一步对 OS Loader 进行度量。OS Loader 就是操作系统“加载器”，包括主引导扇区(Master Boot Record，MBR)、操作系统引导扇区、内核文件等。如果 OS Loader 也是可信的，则信任的边界将会扩大到“CRTM+BIOS+OS Loader”，同时，系统将会执行操作系统的加载动作，启动操作系统。当操作系统启动以后，由操作系统执行对应用程序 Applications 的完整性度量动作(包括运行前的“静态”度量部分和运行时的“动态”度量部分)。上述过程看起来如同一根链条一样环环相扣，因此称之为“可信链”。

需要指出的是，在度量的过程中，一方面，所有的度量结果会保存到内存的度量日志 ML 中；另一方面，度量结果也会按照 PCR[i] = HASH (PCR[i] ‖ MeaVal)的形式集成到 TPM 的平台配置寄存器 PCR 中(其中 PCR[i]表示第 i 个寄存器；‖ 表示连接操作；MeaVal 表示当前的度量结果)。

## 1.3 可信计算机

作为可信链开发和实验的基础，本节对可信计算机作一个简要说明。其原型是武汉大学和武汉瑞达信息安全股份有限公司联合研制的国内第一代可信计算机[6-7]。

该可信计算机与普通计算机的最大区别是在主板上嵌入了一个称为嵌入式安全模块[9](Embedded Security Module，ESM)的芯片。ESM 芯片和 TPM 的主要技术思想和实现路线是一致的。因此，基于这种一致性，在后文中，如果不加以特别说明，则 ESM 和 TPM 两者是通用的，可以互换。当然，由于 ESM 是在 TCG 规范出来之前独立自主进行开发的，因此两者并不完全一致，ESM 还有自己的创新。不过，这种细微的差别并不影响 ESM 和 TPM 主体技术思路和实现的一致性。

### 1.3.1 可信计算机体系结构

从体系结构上来说，第一代可信计算机(以下简称可信计算机)有如下特点：

(1) 主板上有嵌入式安全模块 ESM。

(2) 以 ESM 为基础的信任链机制。

(3) 智能卡子系统。

(4) 安全增强的 BIOS。

(5) 安全增强的国产 Linux 操作系统。

图 1.3 例示了可信计算机的硬件结构[6]。

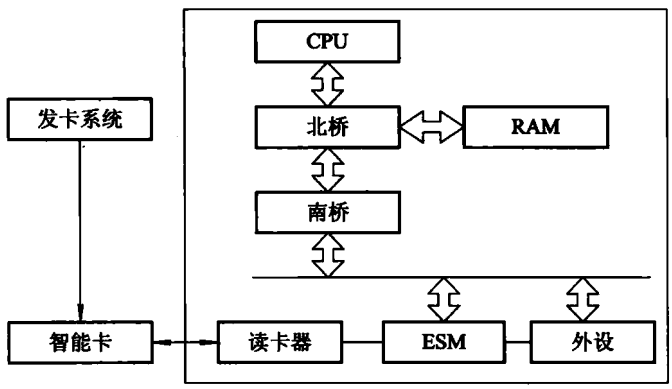


图 1.3 可信计算机的硬件结构

基于这种体系结构，可信计算机系统实现了如下的安全/可信功能：

(1) 基于智能卡和口令的用户身份认证。在智能卡当中包含了用户的身份和特权等信息。通过智能卡，能够实现身份认证、特权管理、系统锁定、系统登录等一系列安全增强。

需要说明的是：在后续的可信计算机研制过程中，已经去除了智能卡系统。在这里仍然将其列出来，是为了和最初的研发环境保持一致。不过，对本书的可信链研究而言，是否存在智能卡系统对我们的研究方法和研究结果是没有影响的。

(2) 安全增强的访问控制。

(3) 安全增强的两级日志。为了增强日志系统的安全，可信计算机采用了两级日志结构。一部分重要的日志内容记录在 ESM 的日志文件中；另外一部分记录在 Linux 的日志文件中。由于 ESM 的安全性高于微机硬盘，因此可以增强整个日志系统的安全。

(4) 可控制所有 I/O 口的开放与关断。在不影响用户正常使用的情况下，根据需要关闭或者开放 I/O 端口，可以大大增强系统的安全性。例如：当用户暂时离开的时候，可以拔出智能卡，这时系统自动关闭所有的 I/O 端口；当用户返回，重新插入智能卡的时候，

系统恢复原来的工作现场。通过 ESM 对南、北桥芯片的控制，系统可以实现上述功能。

(5) 具有唯一标号，签名与 ESM 绑定。该唯一标号确保了 ESM 与它所嵌入主板所在主机系统之间一一对应的关系，攻击者不能把其他平台的 ESM 嵌入到本平台使用。

(6) 屏蔽对 BIOS 的攻击(例如 CIH 病毒)。由于 ESM 可以控制 Flash Memory 的写操作，因此可以杜绝 CIH 类病毒对主板 BIOS 的攻击。同时，系统的信任链在启动的时候也会对 BIOS 进行度量，从而发现对 BIOS 的攻击。

(7) 数据加密和解密。

(8) 数字签名。

包括数据加密和解密、数字签名、真随机数发生器等在内的安全服务都包含在 ESM 当中，构成了整个平台的安全基础。

### 1.3.2 嵌入式安全模块 ESM

前面提到了，可信计算机与普通计算机最大的物理差别之一，就是可信计算机在主板上嵌入了一个可信平台模块 TPM。在我们的可信计算机中，嵌入式安全模块 ESM 就担当了 TPM 的功能。从本质上来说，ESM 本身是一个小的计算机系统，它是一种片上系统(System on Chip，SOC)，是物理可信的。

ESM 紧密嵌入在主板上，并将重要的数据信号线和重要的存储区严格保护起来，用人为的物理探头或一般的光探测技术就很难窥探到 ESM 内部存储的数据。除了对内部数据进行保护以外，ESM 自身也具有防止物理攻击的保护措施。在 ESM 封装的时候使用信号探测的方式防止拔除。如果有人将 ESM 从主板上拔除，则会触动一根预先埋好的信号线，该信号线上的信号将会发生变化，从而激发一个硬中断。之后，系统将会执行自毁程序，清除内部的所有数据，并导致整个可信计算平台无法使用。图 1.4 给出了 ESM 的硬件体系结构[9]。

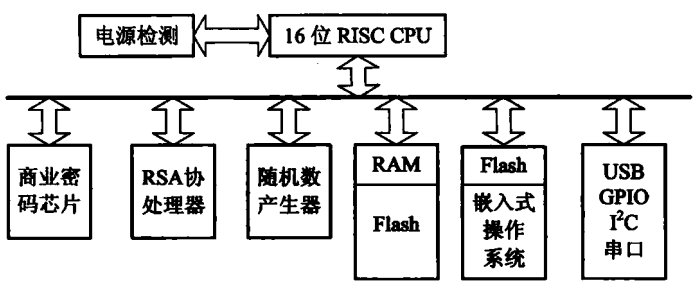


图 1.4 ESM 的硬件体系结构

ESM 所使用的 CPU 是 16 位的 RISC CPU，具有速度快、程序精简的特点，其指令系统与 Intel 80186 兼容。ESM 使用 RSA 协处理器来加快签名速度，利用商业密码芯片实现数据的加/解密操作。ESM 中的随机数产生器是基于半导体物理热噪声的真随机数产生器。同时可以看到，ESM 的 Flash 分为了两个部分：一部分用来固化嵌入式操作系统 JetOS，JetOS 是 ESM 的资源管理者，同时也兼起可信度量根核 CRTM 的作用；另一部分 Flash 用来做安全存储，存储密钥、证书、日志等重要信息。安全存储也是 ESM 的一个重要功能。最后，ESM 也支持多种协议，用来实现不同的功能，如 I/O 端口控制、智能卡读卡器控制等。

目前，瑞达公司的芯片已经升级到J3210[10]，如图1.5所示。J3210芯片的特点是：既支持TCG规范，也支持国内的可信计算规范。

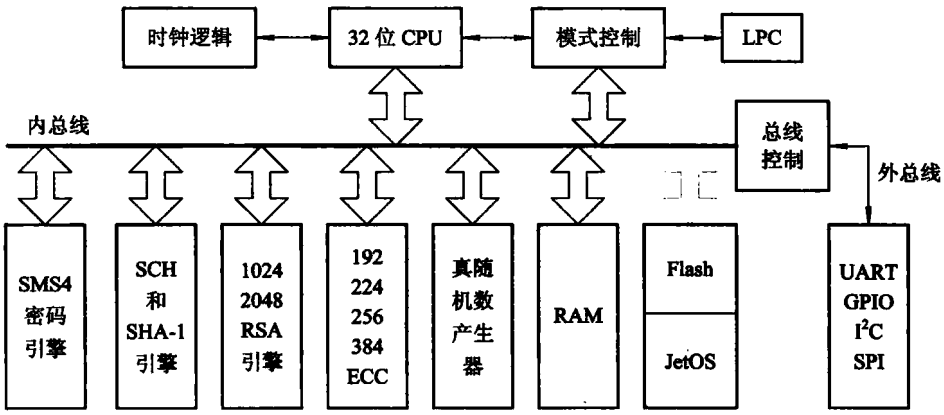


图1.5 J3210芯片结构

## 1.4 本章小结

近年来，可信计算成为了国际信息安全领域的新热点。我国在可信计算领域起步不晚，水平不低，成果可喜，已经站在国际可信计算领域的前列[1]。

本章的1.1节首先对可信计算的基本概念、国内外可信计算的研究进展做了基本说明。根据TCG规范，可信计算具有完整性度量、完整性存储和完整性报告三大基本功能。其中，完整性度量功能又是另外两大功能的基础，能否实现安全、完备的完整性度量功能，关系到整个可信计算平台是否能够正常运行。为了实现完整性度量功能，TCG定义了可信链技术。那么，究竟什么是可信链，以及可信链的本质含义是什么呢？针对这个问题，在1.2节中进行了详细说明。对可信链进行理论研究和具体实现，离不开可信计算平台硬/软件的支持，为此，1.3节对我们最初开展研究工作的硬件平台——国内第一代可信计算机进行了介绍，阐述了可信计算机的基本体系结构，以及ESM(对应于可信平台模块TPM)的构成和实现。至此，进行可信链研究的基本知识都已经具备。在此基础上，在后续的章节中，我们将对可信链的度量以及安全测评问题展开研究。

可信链实现是一项复杂的工作，它涉及可信度量根核、相关证书、TPM/TCM驱动、完整性度量、完整性度量结果存储与集成、可信链恢复、可信链安全性测评等多方面的工作。鉴于完整性度量和安全测评在可信链实现中的重要地位，本书重点展开对可信链完整性度量和安全测评问题的研究。但是，这并不意味着其他方面的工作不重要。事实上，任何一个信息系统(包括可信链在内)的安全性都是一项系统性的工作，只有从信息系统整体入手考虑问题，并从信息系统的硬件和软件底层进行安全增强，才能比较有效地确保信息系统的安全性[1]。因此，除完整性度量和安全测评问题之外，对可信链的其他方面也应该展开深入研究，但这不是本书讨论的重点。

根据可信链的定义：CRTM→BIOS→OS Loader→OS→Applications，可信链可以人为分为两部分：第一段是CRTM→BIOS→OS Loader→OS段，第二段是OS→Applications段。其中，第一段是与操作系统的启动相关的，我们称为可信启动段，对于这一段的研究将在第二章中进行说明；第二段是与应用程序相关的，我们称为应用程序段，对于这一段的研究将在第三章中进行说明。第四章对整个可信链的测评工作进行了说明。在第五章中对可信链的研究进行了总结和展望。

# 参考文献


[1] 沈昌祥，张焕国，王怀民，等. 可信计算的研究与发展[J]. 中国科学：信息科学，2010，40(2)：139－166.

[2] 沈昌祥，张焕国，冯登国，等. 信息安全综述[J]. 中国科学：信息科学，2007，37(2)：129—150.

[3] Microsoft Next-Generation Secure Computing Base-Technical FAQ[EB/OL]. 2011－05－31. http://technet.microsoft.com/en-us/library/cc723472.aspx.

[4] Intel. White Paper：Intel Trusted Execution Technology[EB/OL]. 2011－05－31. http://www.intel.com/technology/security/downloads/arch-overview.pdf.

[5] Open Trusted Computing [EB/OL]. 2011－05－31. http://www.opentc.net.

[6] 张焕国，毋国庆，覃中平. 一种新型安全计算机[J]. 武汉大学学报：理学版，2004，50(A01)：1－6.

[7] 余发江，张焕国. 可信安全计算平台的一种实现[J]. 武汉大学学报：理学版，2004，50(1)：69－73.

[8] 可信计算规范(TCG Specification Architecture Overview，Revision 1.4，2007) [EB/OL]. 2011－05－31.
http://www.trustedcomputinggroup.org/files/resouce_files/AC652DE1－1D09－3519－ADA026A0C05CFAC2/TCG_1_4_Architecture_Overview.pdf.

[9] 张焕国，刘玉珍，余发江，等. 一种新型嵌入式安全模块[J]. 武汉大学学报：理学版，2004，50(S1)：7－11.

[10] Zhang H G，Qin Z P，Yang Q. Design and Implementation of the TPM Chip J3210 [C]. Proceedings of the 3rd Asia-Pasic Trusted Infrastructure Technologies Conference，2008：72－78.

# 第二章 可信启动完整性度量

完整性度量功能是可信计算平台的三大核心功能(完整性度量、完整性存储和完整性报告)之一，并且位于最基础的地位——完整性存储的数据来自于完整性度量的结果，而完整性报告的数据又来自于完整性存储的结果。因此，对完整性度量功能展开研究，具有重要的意义。

可信计算组织 TCG 对完整性度量的要求比较简单：对于任何一个实体，先计算该实体的当前哈希值，然后将计算所得的当前哈希值与预期哈希值相比较，如果两者一致，则认为该实体是可信的；否则是不可信的。显然，完整性度量的要求并不复杂，但是，这个要求是否完备，以及如何基于这个要求实现实际可用的完整性度量系统，仍然有不少问题需要深入研究。

在第一章中已经指出，可信链可以人为分为两个部分：可信启动段(即 CRTM→BIOS→OS Loader→OS)和应用程序段(即 OS→Applications)。在本章中，我们将对可信启动段的完整性度量工作展开研究，而应用程序段的完整性度量工作将在第三章中进行研究。

## 2.1 可信启动完整性度量分析

为了解决可信启动完整性度量问题，本章提出了一个基于 PMBR(Pre-MBR)的安全启动架构(Secure Bootstrap Architecture，SBA)，该架构的基本思想是：在 BIOS 和主引导扇区 MBR 之间插入一个名为 PMBR 的组件，利用 PMBR 作为完整性度量代理，实现对操作系统启动流程的完整性度量。与已有的工作相比[2-6]，SBA 具有以下特点：

(1) SBA 能够度量从 BIOS 自检结束开始到操作系统启动完毕的整个流程上所有关键扇区、代码、文件和数据的完整性，达到“全程覆盖”。已有的部分工作如文献[4]等所给出的，并不能做到对启动流程的全程覆盖。

(2) 虽然 SBA 最初是为可信计算平台所开发的，但是本质上，SBA 的唯一硬/软件要求是 BIOS 的可信性。只要 BIOS 是完整的，则 SBA 一定能够确保整个操作系统启动流程的完整性。这就降低了对可信硬/软件(如 AEGIS ROMs[2]、智能卡[3]、U-Key[4]、TPM[5-6]等)的依赖。因此，SBA 不但能应用在可信计算机上，也能够应用到普通计算机上，这就增强了 SBA 的现实意义。

(3) SBA 引入了一个新的组件 PMBR。为了保证 PMBR 的可信性，防止 PMBR 引入新的安全缺陷，我们对 PMBR 的安全性和形式化开发问题做了研究。

SBA 架构具有通用性，适用于不同的操作系统，如 Windows、Linux、Unix 等。实际