



信息安全导论

第五章可信计算

黄 珮



温故

- 公钥密码
- 散列函数
- 密码学相关应用
 - 数字签名
 - 公钥基础设施



知新

- 安全需要信任，安全基于信任

如何实现可信计算？



本章内容提要

- 可信计算概述
- 可信计算平台密码方案
- 可信平台控制模块
- 可信平台主板
- 可信基础支撑软件
- 可信网络连接
- 可信计算的应用



可信计算的概念 (1/3)

- 容错计算领域
 - 计算机系统所提供的服务可论证其是可信的
- 可信计算组织 (TCG)
 - 1999年对“可信”的定义
 - An entity can be trusted if it always behaves in the expected manner for the intended purpose.
 - 实体的行为是预期的



可信计算的概念 (2/3)

- IOS/IEC 15408 《信息技术安全评估准则》
 - 参与计算的组件、操作或过程在任意的条件下是可预测的，并能够抵御病毒和物理干扰
- 微软公司
 - 2002年提出可信计算的概念，认为可信计算是一种可以随时获得的可靠安全的计算，使人类信任计算机，就像使用电力系统、电话那样自由和安全



可信计算的概念 (3/3)

- Trusted Computing
- Dependable Computing
- Dependable and Secure Computing



可信计算的发展与现状

中国传媒大学



- Fault Tolerant Computing Seminar
 - 国际容错计算会议
- 首届会议召开于1971
- 关键应用的容错计算
 - 航空
 - 航天
 - 铁路运输
- 纯学术研讨会议



- Trusted Computer System Evaluation Criteria
 - 可信计算机系统评估准则
- 1983年由美国国防部制定
 - 首次提出可信计算基 (TCB) 的概念
 - Trusted Computing Base
 - 强调信息保密和访问控制



- Trusted Computing Platform Alliance (TCPA)
 - 可信计算平台联盟
 - 1999年10月成立
 - Intel、微软、IBM、HP和Compaq共同发起
 - TPM 1.0
 - Trusted Computing Platform
 - 强调数据完整性
- 2003年：TCPA → TCG
 - Trusted Computing Group
 - 可信计算平台
 - TPM 1.1



可信计算的商用 (1/2)

- 2003年, Intel正式推出了支持Palladium的LaGrande技术
 - 保护PC免受基于软件和硬件的攻击
 - 微处理器、芯片组、I/O设备及其相应软件
- 微软将Palladium改名为NGSCB
 - Next-Generation Secure Computing Base
 - 其中包括安全启动和数据存储保护等功能



可信计算的商用 (2/2)

- 虚拟TPM

- 2006年，IBM的Reiner Sailer和Trent Jaeger等人为Xen虚拟机设计
- 一个可信计算硬件能够为多个运行的操作系统提供安全服务

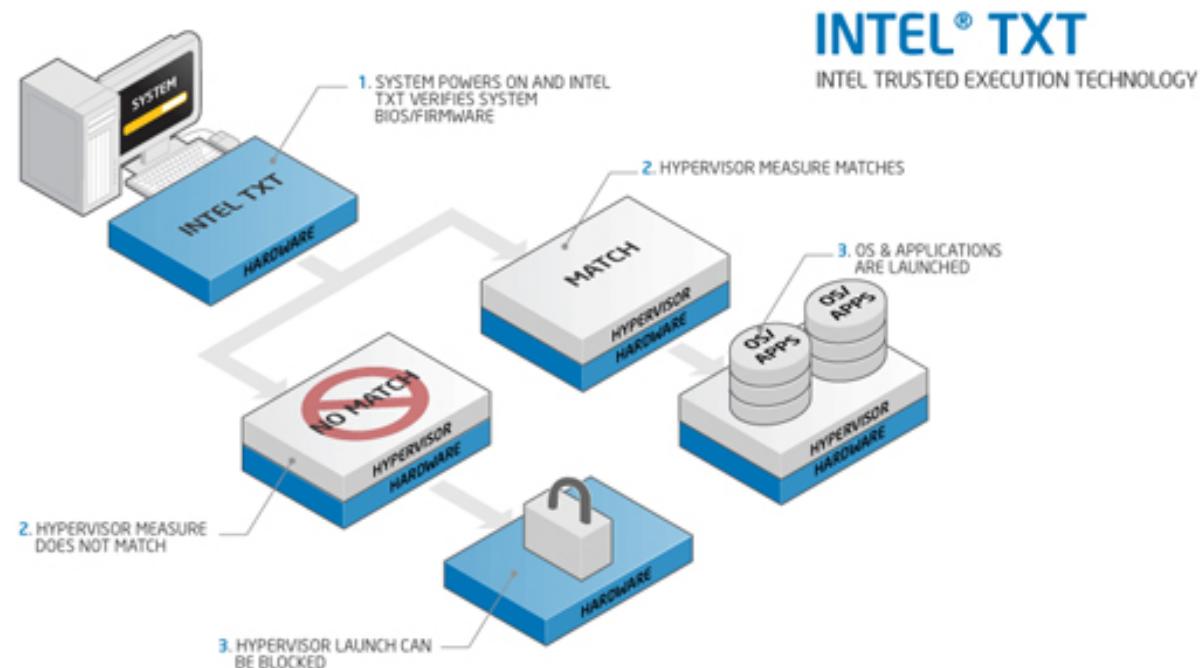
- 可信执行技术

- TXT, Trusted Execution Technology
- 2007年第一代
- 2010年第二代



Intel TXT架构及原理图

- 系统加电后TXT检查BIOS和固件完整性
- 密码学计算通过后允许继续加载可执行组件
—否则，禁止执行





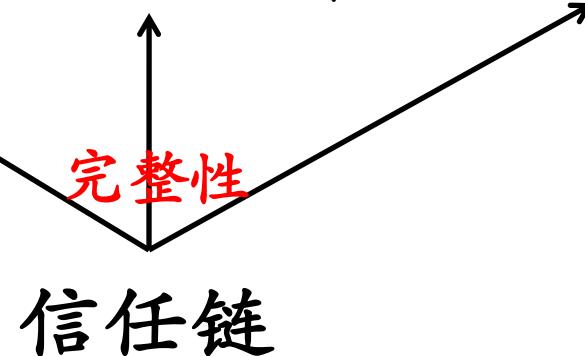
国内可信计算发展

- 2002年的微机保护卡
—基于硬件的防病毒卡
- 2000年开始，武汉瑞达和武汉大学开始合作研究安全计算机
—2004年10月，国内第一款可信计算机通过验收
- 2007年12月，国家密码管理局发布了《可信计算密码支撑平台功能与接口规范》



TPM 结构——TCG 标准

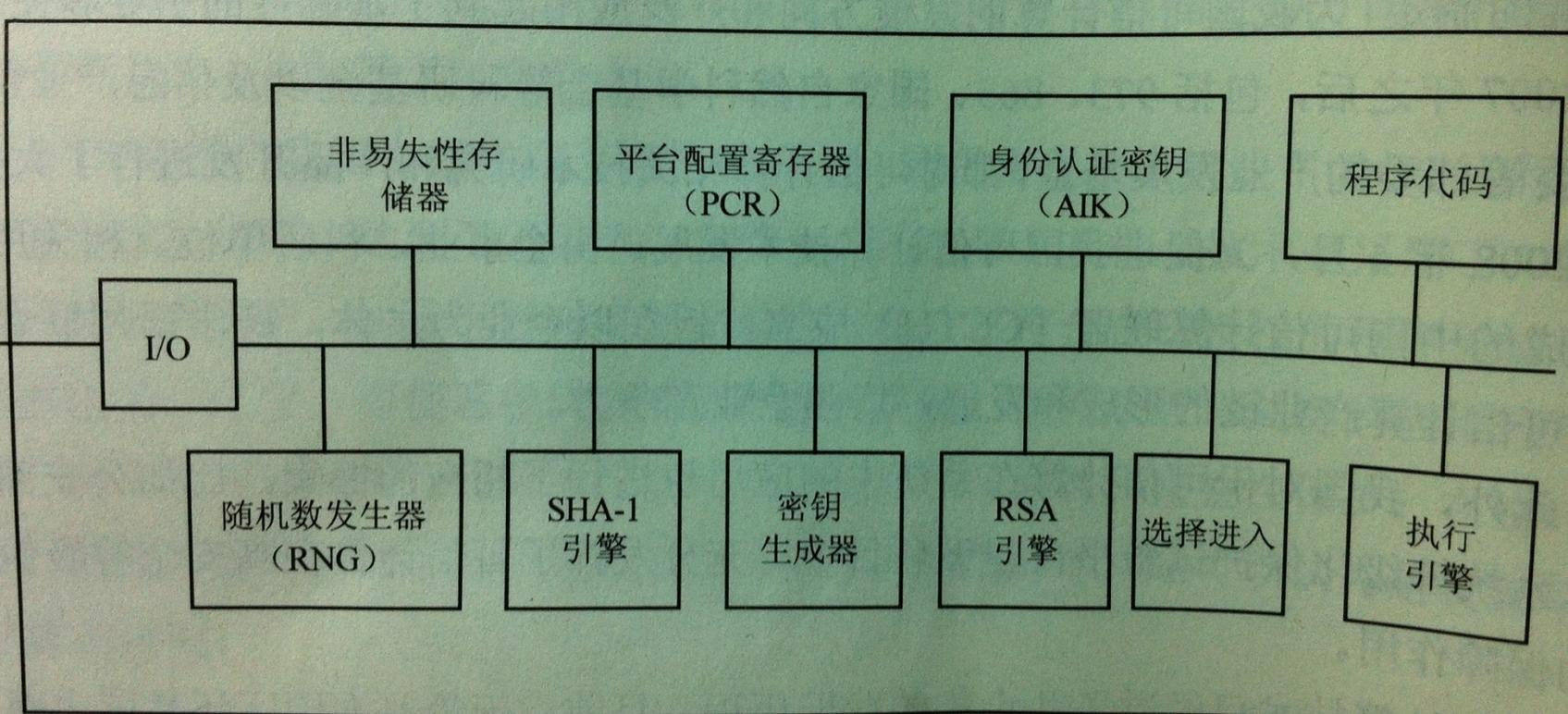
- 信任根 → 硬件平台 → 操作系统 → 应用



- 可信度量根: Root of Trust Measurement
- 可信存储根: Root of Trust for Storage
- 可信报告根: Root of Trust for Reporting



TPM 结构——TCG 标准





TPM中的密钥管理 (1/2)

- 签名密钥
 - 非对称密钥，数据签名
- 存储密钥
 - 非对称密钥，数据或其他密钥加密
- 平台身份认证密钥
 - 非对称密钥
 - 专用于TPM产生的不可迁移数据的签名



TPM中的密钥管理 (2/2)

- 签署密钥
 - 平台不可迁移的解密密钥
 - 从不用做数据加密和签名
- 绑定密钥
 - 加密小规模可迁移数据
- 继承密钥
 - TPM外部生成的可迁移（签名和加密）密钥
- 验证密钥
 - 保护引用TPM完成传输会话的对称密钥



TPM中的证书管理

- 签署证书
- 符合性证书
- 平台证书
- 认证证书
- 身份认证证书



可信计算平台体系结构

一个基础：密码技术

三大功能

四大组成

纽带：可信网络连接

核心：可信基础支撑软件

平台：可信平台主板

信任根：可信平台控制模块（TPCM）

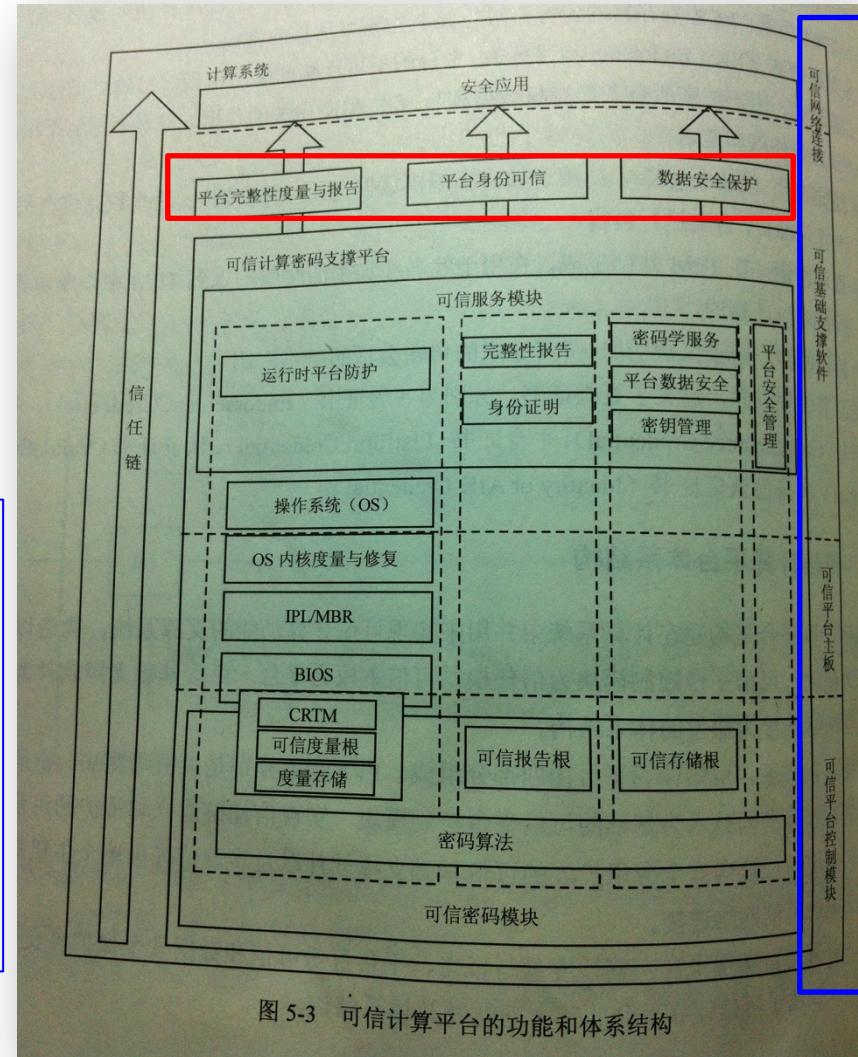


图 5-3 可信计算平台的功能和体系结构



本章内容提要

- 可信计算概述
- 可信计算平台密码方案
- 可信平台控制模块
- 可信平台主板
- 可信基础支撑软件
- 可信网络连接
- 可信计算的应用



TCG的TPM 1.1标准的缺陷

- 复杂性太高
 - 密钥和证书种类繁多
- 安全缺陷
 - 密码和授权协议存在缺陷
- 隐私泄漏风险
 - 唯一的身份认证根标志，在网络上发生的任何访问动作都能准确定位动作发起者的身份



密码与可信计算平台之间的关系

平台完整性度量报告

平台身份可信

平台数据安全保护

密码算法

SM3

SM2

SMS4

随机数生成器



密码算法配置

- 密码算法包括
 - 随机数产生算法
 - 散列算法
 - 我国自主研制的SCH算法（512bit消息分组，256bit定长输出）
 - 消息验证码算法（HMAC）
 - 对称密钥算法
 - 我国自主研制的SMS4算法（128bit密钥长度、128bit明文和密文分组）
 - 公钥算法
 - F_p 上的ECC国家标准算法
系统参数、密钥对产生、签名/验证算法、加密解密算法和密钥协商

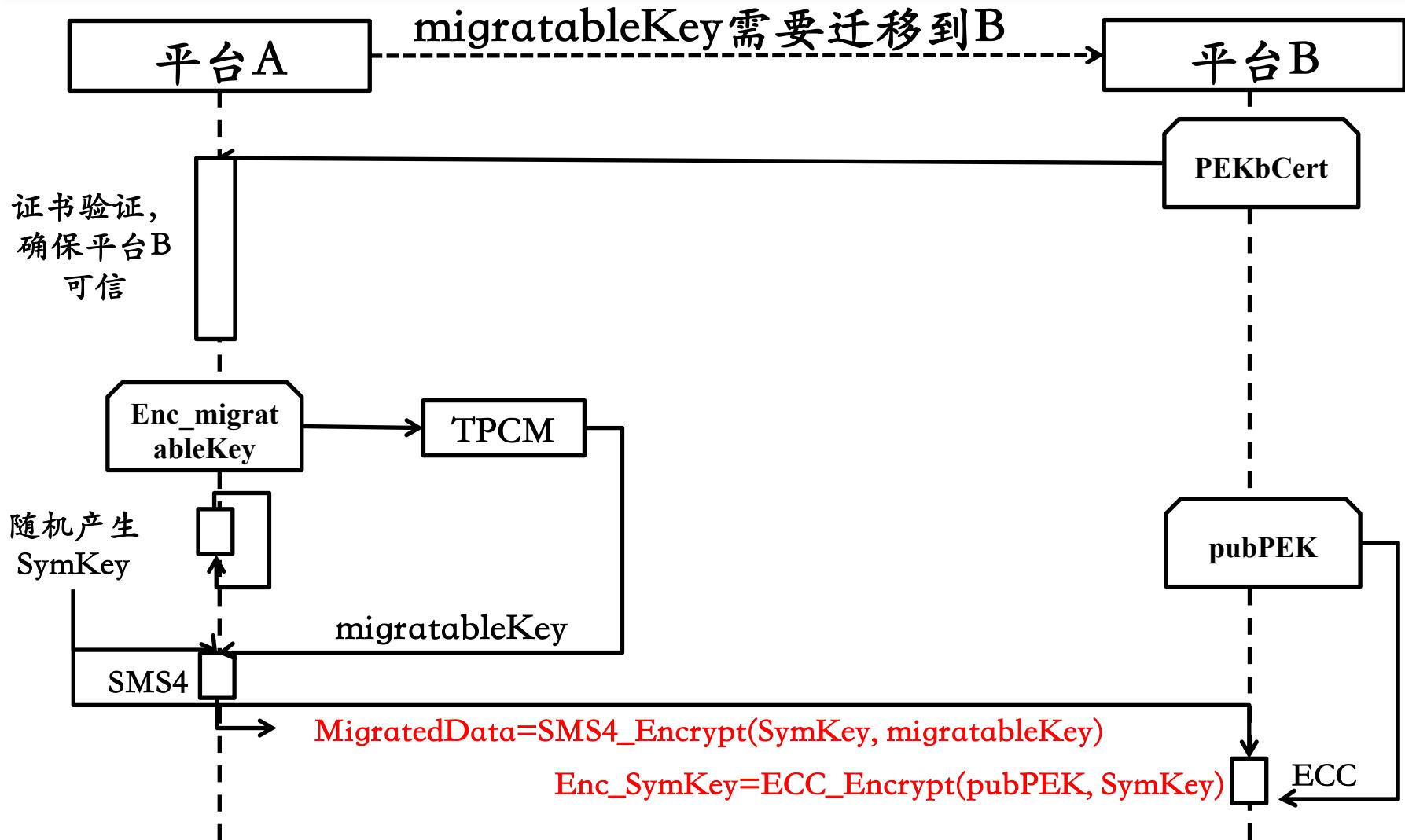


密码使用

- 需求
 - 灾备
 - 更换硬件
 - 密钥的机密性和完整性保护
- 解决方案
 - 密钥迁移
 - 授权协议
 - DAA数字签名

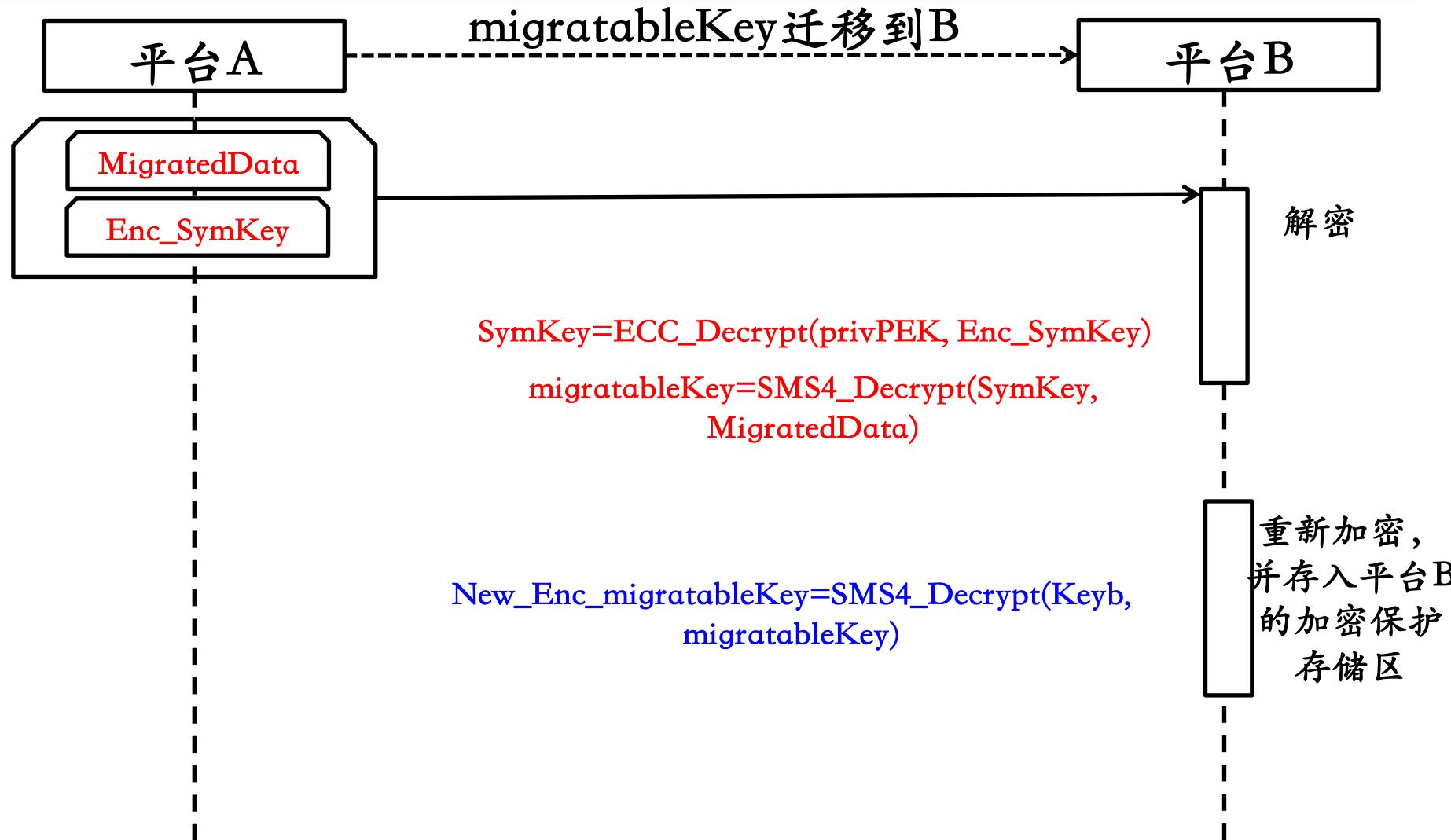


密钥迁移 (1/2)





密钥迁移 (2/2)





授权协议 (Authorization Protocol)

- 外部实体与TPCM之间的访问协议
- 实现
 - 外部实体与TPCM之间的授权认证
 - 信息完整性验证
 - 敏感数据的机密性保护



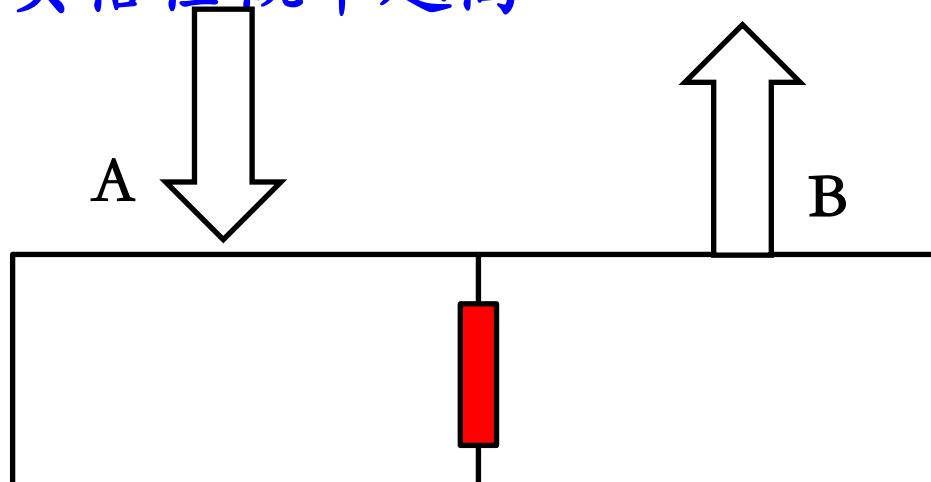
DAA数字签名

- 基于零知识证明理论的签名方案
 - 签名者为TPM
 - 验证者为外部实体
 - TPM v1.2支持DAA协议
- DAA的含义
 - Direct proof 不借助可信第三方
 - Anonymous 不暴露TPM的身份
 - Attestation 表明来自某个TPM



关于零知识证明

- 张三向李四证明自己有开启山洞内门的钥匙
 - 声称者：张三
 - 验证者：李四
 - 证明方法：李四要求张三不断变换从A入，B出，或B入，A出，张三成功次数越多，李四对张三声称的事实信任概率越高





密钥管理

• 种类和用途

平台身份类密钥	密码模块密钥 (EK)
	平台身份密钥 (PIK)
	平台加密密钥 (PEK)
平台存储类密钥	存储主密钥 (SMK)
用户类密钥	用户密钥 (UK)



密钥管理流程

- 密钥生成和登记
- 密钥分配和协商
- 密钥保护
- 密钥撤销和销毁
- 密钥备份



密钥生命周期

- 制造
 - 可信密码模块生产、集成和计算机系统的制造
- 初始化
 - 取得平台所有者权限的过程
- 部署
 - 平台所有者将平台部署到应用系统的过程
- 应用
 - 平台用户使用平台完成平台完整性度量、平台身份证明和数据安全保护的过程
- 撤销
 - 平台的销毁过程



证书管理

- 数字证书
 - 密码模块证书
 - 平台证书（双证书机制）
 - 平台身份证件证书：平台身份的证明
 - 平台加密证书：平台间密钥迁移和其他敏感数据的交换保护



密码模块证书

- 签发
 - 平台的生产阶段由可信方颁发，也可在平台部署阶段由用户委托可信方颁发
- 使用
 - 平台所有者授权外部实体后可访问
- 撤销
 - 正常情况下无证书更新需求
 - 例外情况，如：平台弃用或丢失，重新生成密码模块密钥等
- 内容
 - X.509 V3标准



平台证书

- 签发
 - 可信方签发
 - 平台身份数字证书的ECC密钥对在可信密码模块内部生成
 - 平台加密证书的ECC密钥对由密钥管理中心（KMC）生成，用安全方式传递到平台
 - 平台解密得到平台身份数字证书和平台加密证书，以及平台加密密钥的私钥
- 使用
 - 签名验证身份和平台间密钥迁移以及其他机密数据的交换
- 撤销
- 内容
 - X.509 V3标准

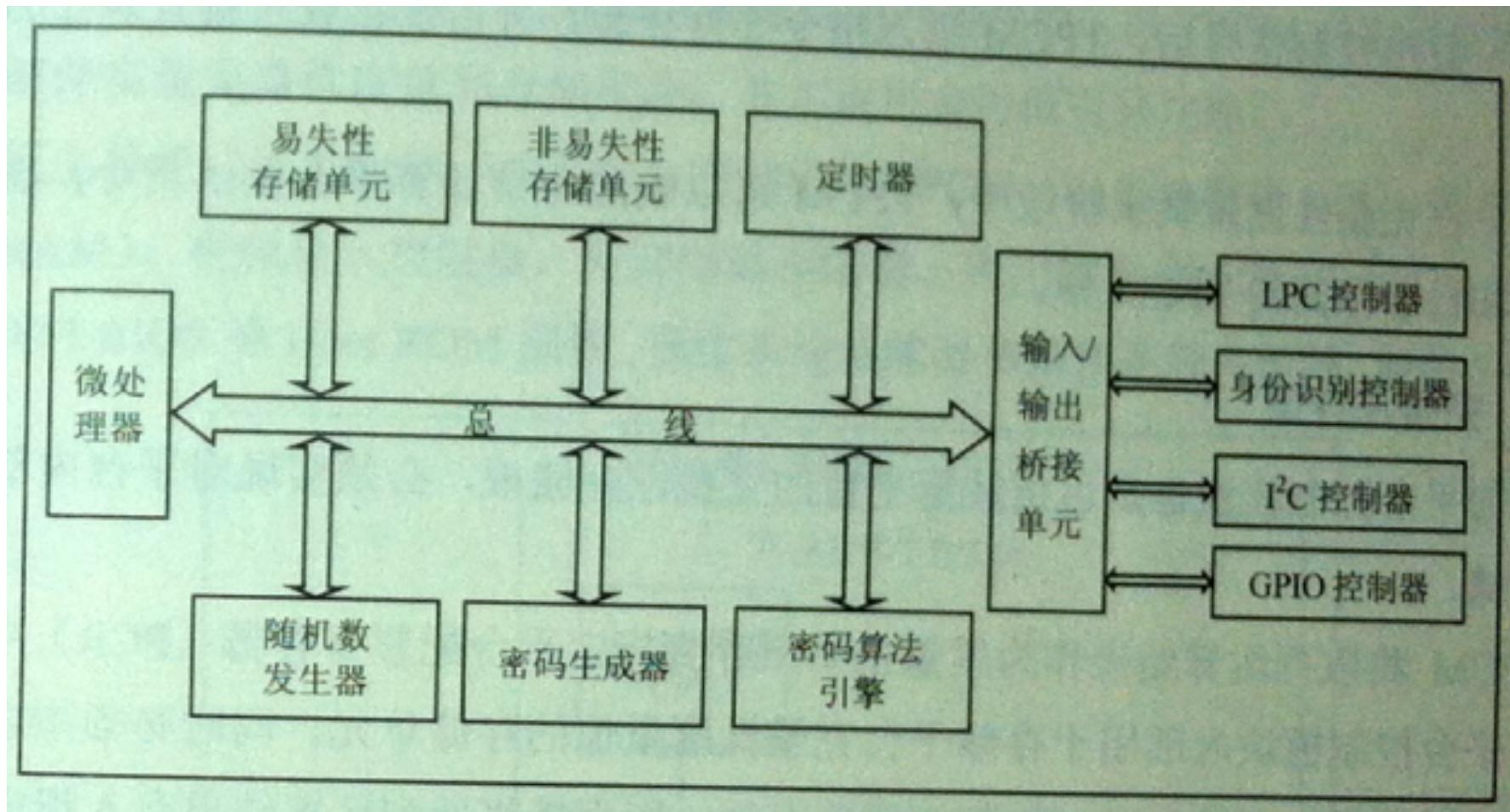


本章内容提要

- 可信计算概述
- 可信计算平台密码方案
- 可信平台控制模块
- 可信平台主板
- 可信基础支撑软件
- 可信网络连接
- 可信计算的应用



TPCM体系结构





TPCM的主要功能

- 三大基本功能（完整性保证）
 - 可信度量
 - 可信存储
 - 可信报告
- 三大辅助功能
 - 可信平台用户管理
 - 可信平台控制模块内部固件
 - 可信平台控制模块内部维护管理

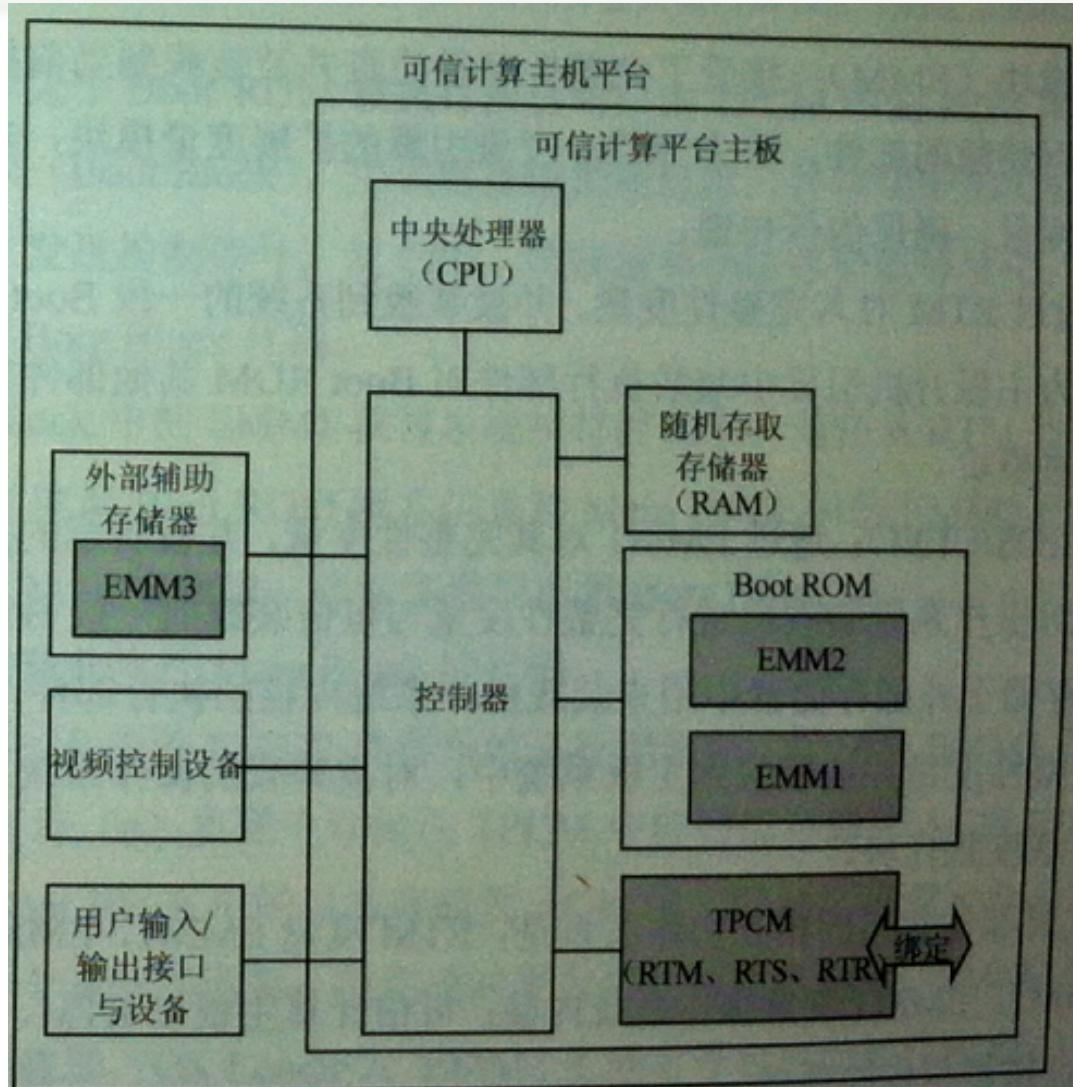


本章内容提要

- 可信计算概述
- 可信计算平台密码方案
- 可信平台控制模块
- 可信平台主板
- 可信基础支撑软件
- 可信网络连接
- 可信计算的应用



可信主板的体系结构





可信主板的主要功能

- 信任链建立
- 完整性度量

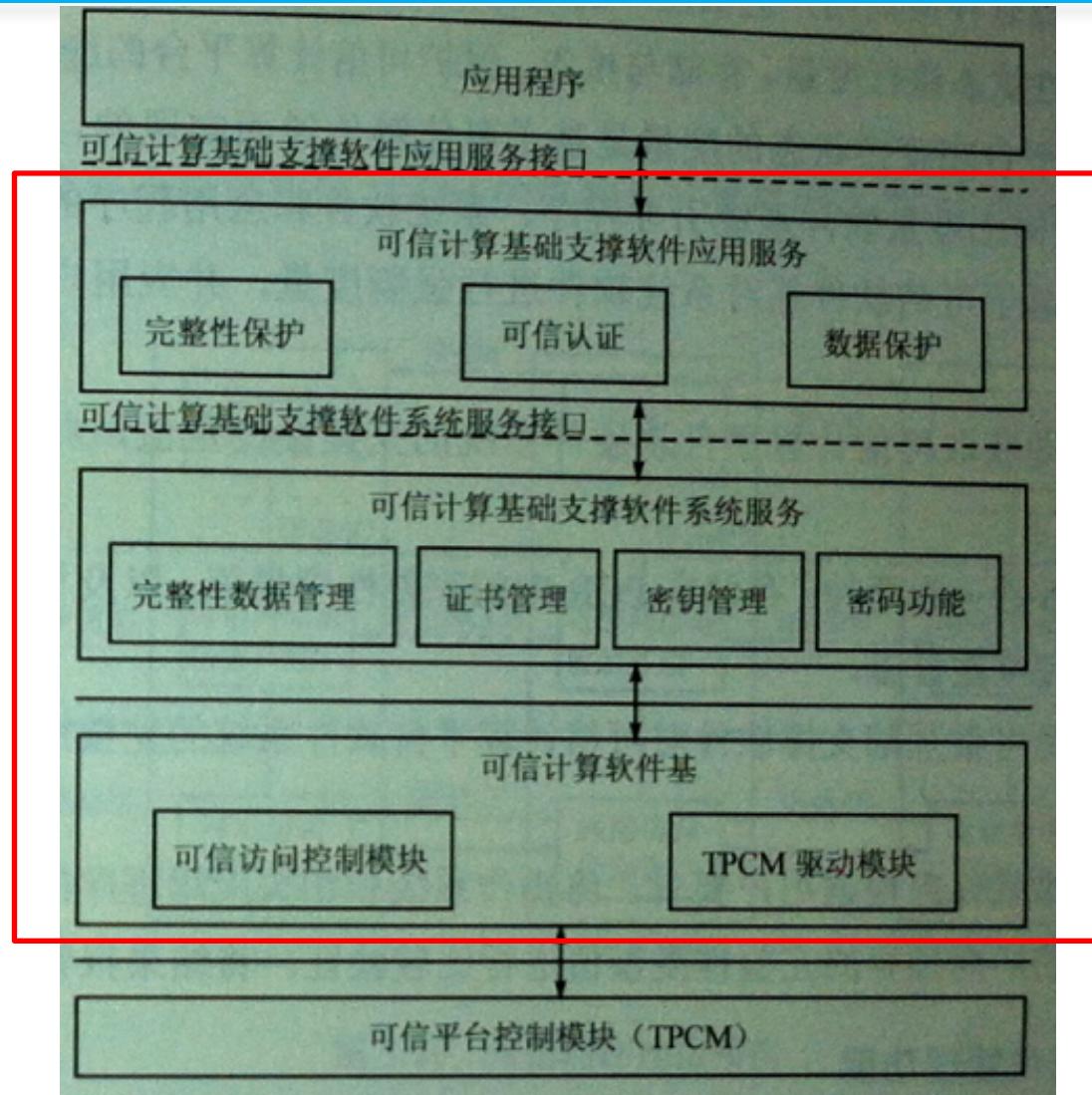


本章内容提要

- 可信计算概述
- 可信计算平台密码方案
- 可信平台控制模块
- 可信平台主板
- 可信基础支撑软件
- 可信网络连接
- 可信计算的应用



可信基础支撑软件体系结构





可信基础支撑软件主要功能

- 完整性管理功能
 - 可信链传递和软硬件系统的完整性度量
 - 完整性状态数据的存储
 - 存储在PCR中的完整性度量值
 - 可信计算平台的软硬件系统完整性日志
- 数据保密性管理功能
- 身份认证管理功能

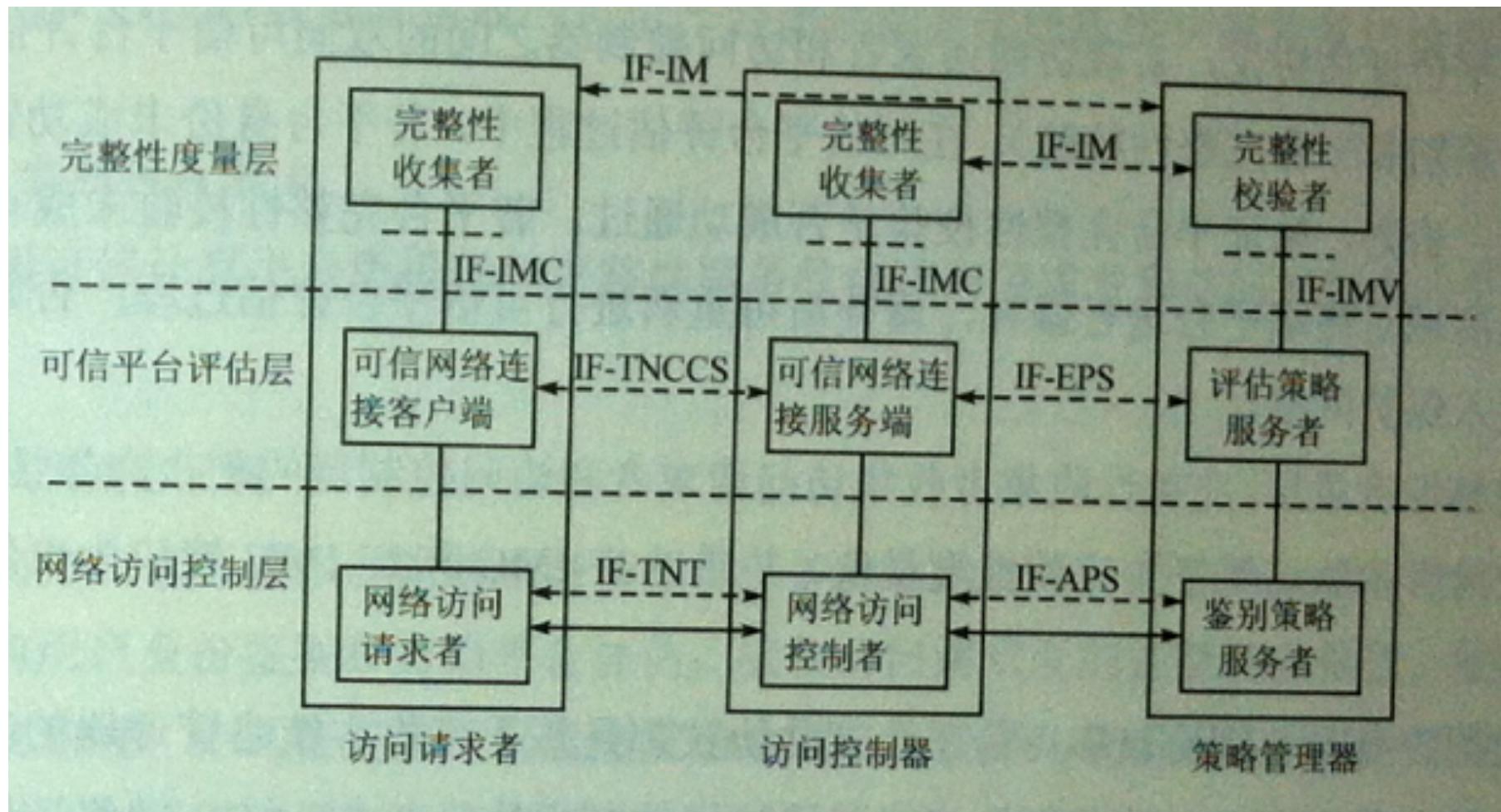


本章内容提要

- 可信计算概述
- 可信计算平台密码方案
- 可信平台控制模块
- 可信平台主板
- 可信基础支撑软件
- 可信网络连接
- 可信计算的应用



可信网络连接架构





可信网络连接主要功能

- 访问请求者
- 访问控制器
- 策略管理器



远程证明

- 传统网络应用根据远程访问者的身份实施访问控制
 - 不考虑远程操作平台运行环境的可信性
- 引入可信的度量代理对指定的状态进行度量
 - 度量结果提交给TPM
 - TPM通过由硬件保护的私钥（AIK, Attestation Identity Key）对度量结果加以签名
 - 向第三方证明度量结果的来源真实性和完整性



本章内容提要

- 可信计算概述
- 可信计算平台密码方案
- 可信平台控制模块
- 可信平台主板
- 可信基础支撑软件
- 可信网络连接
- 可信计算的应用



可信计算平台应用领域广阔

- 政府信息系统领域
- 金融信息系统领域
- 企业信息系统领域
- 军队信息系统领域



可信网络连接应用领域广阔

- 政府信息系统领域
- 企业信息系统领域
- 电子商务领域
- 网上银行
- 军事信息系统领域



个人笔记本也玩可信计算



BIOS设置里的TPM设置

Aptio Setup Utility - Copyright (C) 2005-2007 American Megatrends, Inc.

Main Advanced Security Server Management Boot Options ►

Administrator Password	Not Installed	[No Operation] - No changes to current state.
User Password Status	Not Installed	[Turn On] - Enables and activates TPM.
Set Administrator Password		[Turn Off] - Disables and deactivates TPM.
Set User Password		[Clear Ownership] - Removes the TPM ownership authentication
TPM State	Disabled & Deactivated	>< Select Screen
TPM Administrative Co	[No Operation]	↑↓ Select Item
		+/- Change Value
		Enter Select Field
		F1 General Help
		F9 Optimized Defaults
		F10 Save and Exit
		ESC Exit

Version 1.20.1093 Copyright (C) 2005-2007 American Megatrends, Inc.



ThinkPad笔记本中的TPM安全芯片 (1/2)

- ThinkPad笔记本中的TPM安全芯片可以与指纹识别模块一起使用
 - 普通笔记本中的指纹识别技术一般是把指纹验证信息储存在硬盘中，而ThinkPad中的TPM安全芯片则是直接将指纹识别信息置于安全芯片中
 - 一旦遭到暴力破解，安全芯片就启动自毁功能，这样保证了您的个人信息资料不会泄密。
 - 安全芯片通过LPC总线下的系统管理总线来与处理器进行通信，安全芯片的密码数据只能输入而不能输出。
 - 即关键的密码加密与解密的运算将在安全芯片内完成，而只将结果输出到上层。
 - TPM安全芯片和笔记本上的指纹识别模块搭配能达到最高的安全级别，即便是在无尘实验室对磁盘进行暴力拆解，也无法获得有效信息。



ThinkPad笔记本中的TPM安全芯片 (2/2)

- 个人电脑的口令加密存储管理
 - 口令加密存储在TPM芯片
 - 口令解密过程在TPM芯片内完成
 - 在Windows操作系统中提供客户端软件CSS管理TPM芯片内数据
 - Client Security Solution



设置TPM芯片保存密码 (1/7)

- 在开机时按F1，进入Security安全栏选中Security Chip,使得在启动状态，如下图所示





设置TPM芯片保存密码（2/7）

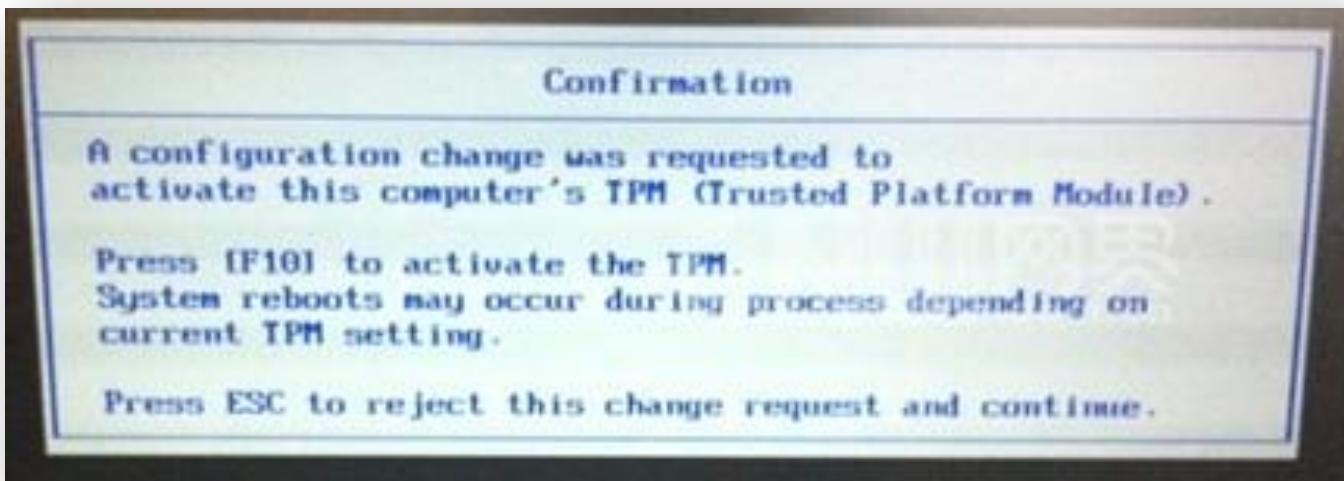
- 当你在BIOS中设置好启动安全芯片时，这时系统提示“是否立即激活安全设备”，选中是以后，系统会提示需要重启。





设置TPM芯片保存密码 (3/7)

- 当再次启动时，首先系统会提示配置TPM平台，只需要按F10即可激活TPM





设置TPM芯片保存密码 (4/7)

- 这时进入Windows系统就会看到安全设备已激活的信息。点击确定以设置Client Security Solution：





设置TPM芯片保存密码 (5/7)

- 首次进入CSS会有几秒钟时间系统初始化设置



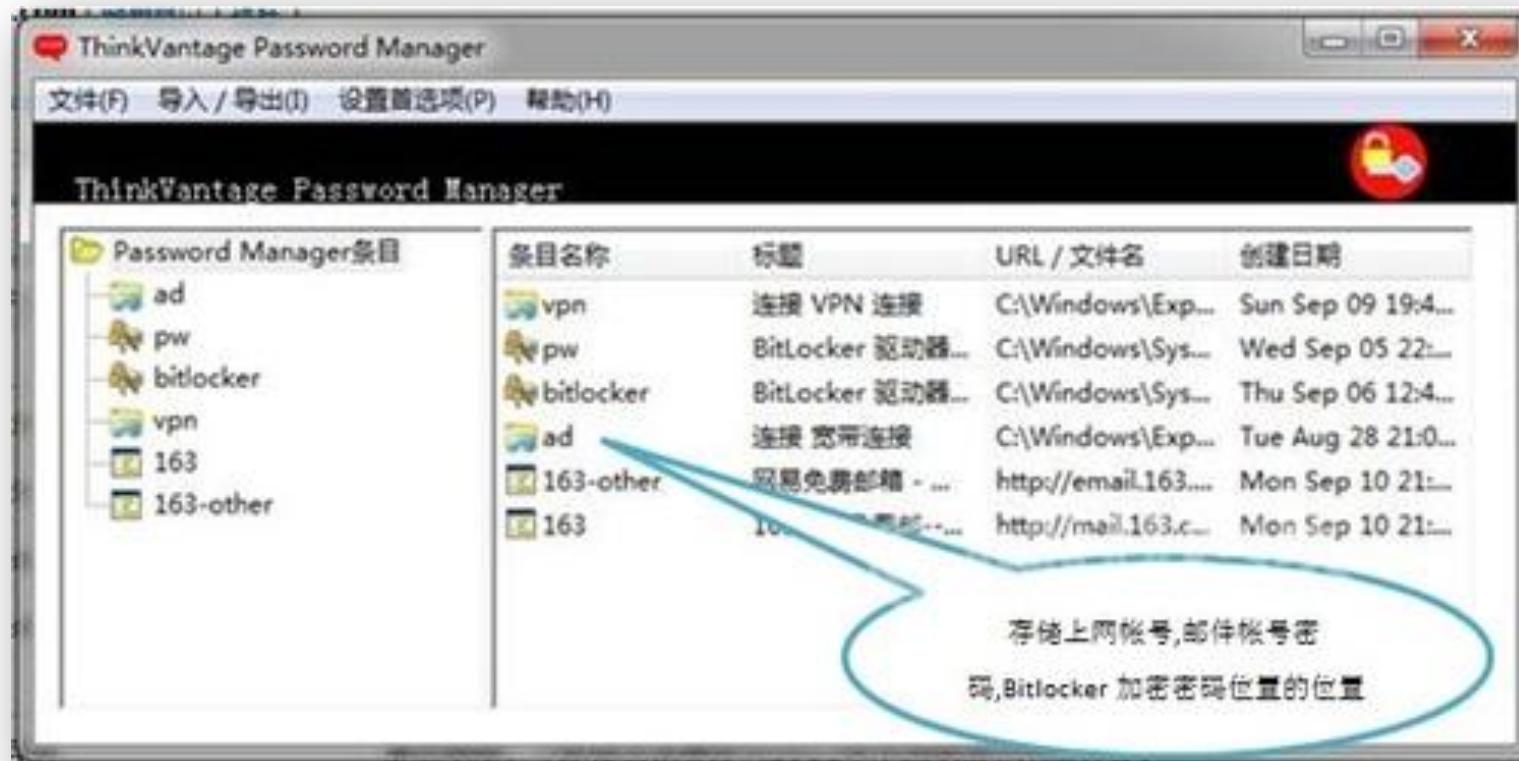


设置TPM芯片保存密码 (6/7)





设置TPM芯片保存密码 (7/7)





参考文献

- ① [Intel® Trusted Execution Technology: A Primer](#)
- ② [揭秘TPM安全芯片及加密应用](#)



课后思考题

- 如何理解可信计算的概念？