可信计算

李涛

目录
CONTENTS

01 概述

产生安全事故的技术原因

- PC机软、硬件结构简化，导致资源可任意使用，尤其是执行代码可修改，恶意程序可以被植入
- 病毒程序利用PC操作系统对执行代码不检查一致性弱点，将病毒代码嵌入到执行代码程序，实现病毒传播
- 黑客利用被攻击系统的漏洞窃取超级用户权限，植入攻击程序，肆意进行破坏
- 更为严重的是对合法的用户没有进行严格的访问控制，可以进行越权访问，造成不安全事故

产生安全事故的技术原因

- 为了解决计算机和网络结构上的不安全，从根本上提高其安全性，必须从芯片、硬件结构和操作系统等方面综合采取措施，由此产生出可信计算的基本思想，其目的是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高整体的安全性。

什么是可信?

- 可信是指“一个实体在实现给定目标时其行为总是如同预期一样的结果”。强调行为的结果可预测和可控制。

什么是可信?

- 国际可信组织(TCG)的定义:一个实体是可信的，它的行为总是以一个预期的方式达到预期的目标。
- 国际标准化组织与国际电子技术委员会定义（1990年）：
  如果第2 个 实体完全按照第1 个实体的预期行动时，则第1 个实体认为第2 个实体是可信的。
- 国际标准化组织与国际电子技术委员会定义（1999年）：
  参与计算的组件、操作或过程在任意的条件下是可预测的，并能够抵御病毒和一定程度的物理干扰。

什么是可信?

- 信任是一种二元关系：
  - 一对一 （个体对个体）
  - 一对多（个体对群体）
  - 多对一（群体对个体）
  - 多对多（群体对群体）
- 信任的二重性：主观性和客观性
- 信任不具对称性：A信任B，不一定有B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：在传播过程中可能有损失，而且传递的路径越长，损失可能越大。

什么是可信计算?

- **数据的秘密性**
- **数据的真实性**
- **数据的完整性**

要点：

- 在各种信息安全技术措施中，硬件结构的安全和操作系统的安全是基础，密码、网络安全等技术是关键技术。
- 只有从芯片、主板等硬件结构和BIOS、操作系统等底层软件作起，综合采取措施，才能比较有效的提高微机系统的安全性。
- 解决方法——可信计算

什么是可信计算?

- 可信计算指一个可信的组件，操作或过程的行为在任意操作条件下是可预测的，并能很好地抵抗不良代码和一定的物理干扰造成的破坏。

- 可信计算是安全的基础，从可信根出发，解决PC机结构所引起的安全问题。

什么是可信计算?

具有以下功能：

- 确保用户唯一身份、权限、工作空间的完整性/可用性
- 确保存储、处理、传输的机密性/完整性
- 确保硬件环境配置、操作系统内核、服务及应用程序的完整性
- 确保密钥操作和存储的安全
- 确保系统具有免疫能力，从根本上阻止病毒和黑客等软件的攻击

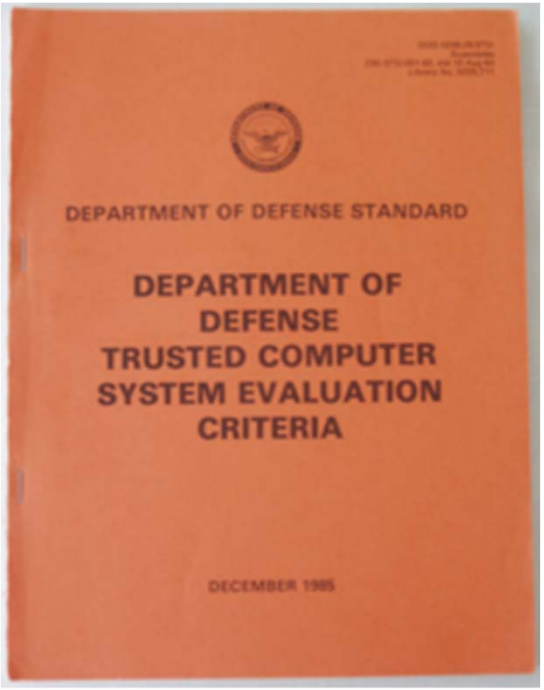
什么是可信计算?

可信计算平台特性：

- 定义了TPM
  - TPM = Trusted Platform Module可信平台模块；
- 定义了访问者与TPM交互机制
  - 通过协议和消息机制来使用TPM的功能；
- 限定了TPM与计算平台之间的关系
  - 必须绑定在固定计算平台上，不能移走；
- TPM应包含
  - 密码算法引擎
  - 受保护的存储区域

什么是可信计算?

- 美国国防部在20世纪80年代提出了《可信计算机安全评估准则》(TCSEC)，即橘皮书
  - 定义系统中实现安全功能的软件和硬件的总和为可信计算基
  - 明确安全机制首先要做到“可信”



什么是可信计算?

- 安全机制自身的安全问题
  - 上世纪八十年代的TCSEC标准将系统中所有安全机制的总和定义为可信计算基（TCB）
  - TCB的要求：
    - 独立的，具有抗篡改性
    - 不可旁路
    - 最小化以便于分析和测试
- 问题：当安全机制分布在系统的各个位置时，如何保证TCB的要求能够满足？

什么是可信计算?

- 信息系统中的“可信”表示可预期性
  - 信息系统会按照人们所预期的方式运行
  - 系统行为可预期 ≠ 系统已经安全
  - 预期到了正常行为和风险，可以未雨绸缪
- 可信 ≠ 安全，可信是安全的前提

什么是可信计算?

- 可信计算安全防护原理类似于人体的免疫系统
  - 按照属主要求部署和运行以完成属主所需要功能的部分当作“自己”
  - 可能干扰属主功能正常执行的部分定义为“非己”
- 在密码机制支持下实施身份识别、状态度量、保密存储，及时识别“自己”和“非己”部分
- 通过破坏和排斥“非己”部分确保信息系统的可信

什么是可信计算?

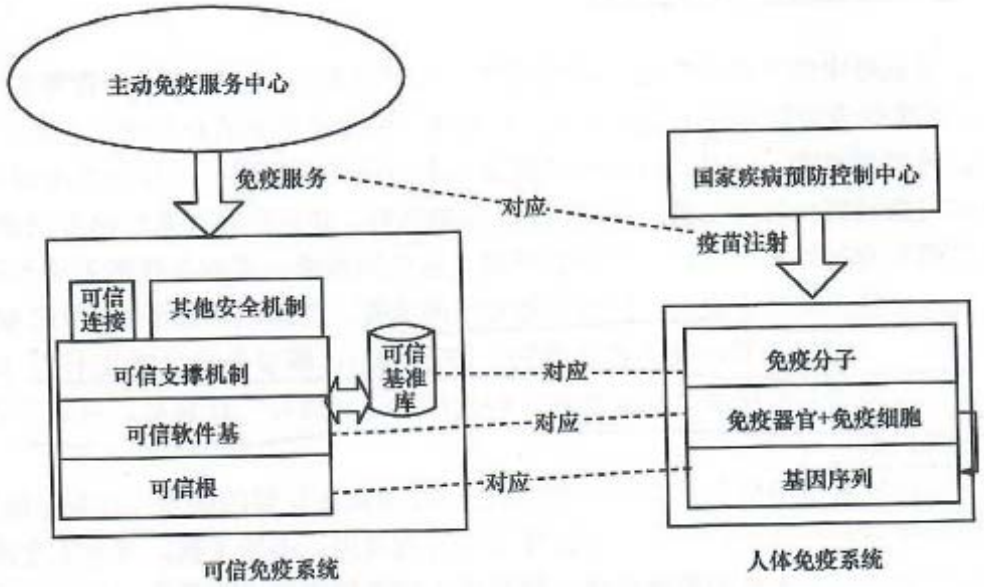
- 可信计算的保障措施是一种主动免疫的方式
- 与当前流行的以防火墙、防病毒、入侵检测等产品为代表的基于特征库进行被动查杀的防护方式有本质区别
- “老三样”工作方式
  - 搜集攻击信息，建立特征库
  - 采取“封堵查杀”的方式，消灭已知的安全威胁
- “老三样”采取的被动查杀的防护方式在新的形势下已经防不胜防
  - 攻击手段越来越系统化、多样化、隐蔽化
  - 往往初次攻发起即致命

什么是可信计算?

- 基于可信计算的主动免疫方式
  - 搜集系统和应用的信息
  - 根据用户的信任需求，确定系统的可信特征并建立起可信策略库
  - 策略库定义了信息系统“自己”部分的特征，不符合可信策略的行为则被标识为“非己”部分
  - 通过物理保护支持的密码学机制确保度量和识别过程的可信
  - 通过灵活应用不同的安全监控措施，识别“自己”和“非己”
  - 保护“自己”部分不受干扰，破坏和排斥“非己”部分
  - 确保信息系统的行为符合预期
- 传统访问控制原理在新型信息系统环境中的发展
- 是逻辑正确验证、计算体系结构、逻辑识别等技术在网络安全方面的创新应用

什么是可信计算?

- 可信计算的技术要素与免疫系统的类比，主动免疫系统和人体免疫机制的对应



什么是可信计算?

- 信息系统中必定存在逻辑不全的缺陷
  - 逻辑不全的问题难以根除，封堵查杀的被动防御方式无法彻底解决问题，拥有特权的软件还会引来新的问题
- 可信计算不根除逻辑缺陷，建立主动免疫机制
  - 确保任务运行环境可信，确保完成任务的必要逻辑按照预期执行
- 可信计算并不是独立的解决安全问题，而是为安全提供可信支撑，为系统构建可信的安全保护框架
- 可信是安全的前提
  - 需要与系统的安全机制配合
  - 保障安全机制

可信计算简史

- 可信1.0时代：容错计算
  - 针对大型机时代主机可靠性需求提出的，主要是容错专家提出的Dependable Computing，从软件客体角度出发，强调软件应提供可靠的服务，避免出现严重服务故障
  - 针对计算机部件不稳定的问题，采取冗余备份、故障诊断、容错算法等技术，确保信息系统在局部故障的情况下仍能保持运行符合预期
  - 没有对恶意代码、黑客攻击等威胁提出针对性解决方案

可信计算简史

- 可信2.0时代：被动可信体系
- 以TCG组织的可信计算标准体系以及Microsoft、Intel等公司遵循这一体系设计的可信硬软件系统架构
  - 从物理安全的可信根出发，在计算环境中构筑从可信根到应用的完整可信链条
  - 为系统提供可信度量、可信存储、可信报告等可信支撑功能，支持系统应用的可信运行
  - 明确了物理可信根的基础地位，通过可信链传递将新人扩展到整个系统

可信计算简史

- 可信2.0没有明确的可信计算理论模型，没有从计算机体系结构上入手解决可信问题
  - 应用兼容问题，被动可信机制需要在应用中嵌入可信计算调用函数，需要对现有应用做大量更改
  - 可信管理问题，采取“保护可信”思路，大厂商或联盟审批可信，再通过证书机制发许可，限制了开发者空间
  - 可信开发问题，可信计算开发接口内容过于繁琐，开发门槛高

可信计算简史

- 可信3.0时代：主动免疫体系
  - 提出了全新的可信计算体系框架，在计算节点构建一个“宿主—可信双节点”的可信免疫架构
  - 构建独立的可信计算子系统作为可信节点
  - 通过可信节点对系统实施主动监控，为应用提供支撑

可信计算简史

- 可信3.0简化了宿主系统层面的可信开发，为可信开发者提供了高度的灵活性
  - 可信节点的构建及与系统的互动是可信3.0的关键

02

可信计算基本概念

可信计算的解决思路

- 首先建立一个信任根

  信任根的可信性由物理安全和管理安全确保。

- 再建立一条信任链

  从信任根开始到硬件平台、到BIOS、到操作系统、再到应用，一级测量认证一级，一级信任一级。从而把这种信任扩展到整个计算机系统。

可信计算的解决思路

- 可信计算的核心概念：可信根和可信链
  - 可信环境必须有一个基于密码学和物理保护的可靠的信任源头，这一信任源头就是系统的可信根（TPM/TCM或者TPCM）。
  - 系统中的可信元件（安全机制），其可信性应通过从这一可信根出发，经过一环套一环的可信传递过程来保障其可信性。
  - 系统的可信计算基中所有元件应构成一个完整的可信链条，以确保整个可信计算基的可信性。

信任根的概念

- TCG认为：一个信任根包括三个根：
  - 可信测量根(Root of Trust for Measurement)
  - 可信存储根(Root of Trust for Storage)
  - 可信报告根(Root of Trust for reporting)

信任根技术

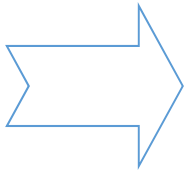
信任根的概念

- TCG**的技术规范**：

可信测量根(RTM): 软件可信测量根核CRTM（BIOS）

可信存储根(RTS)：

可信报告根(RTR)：



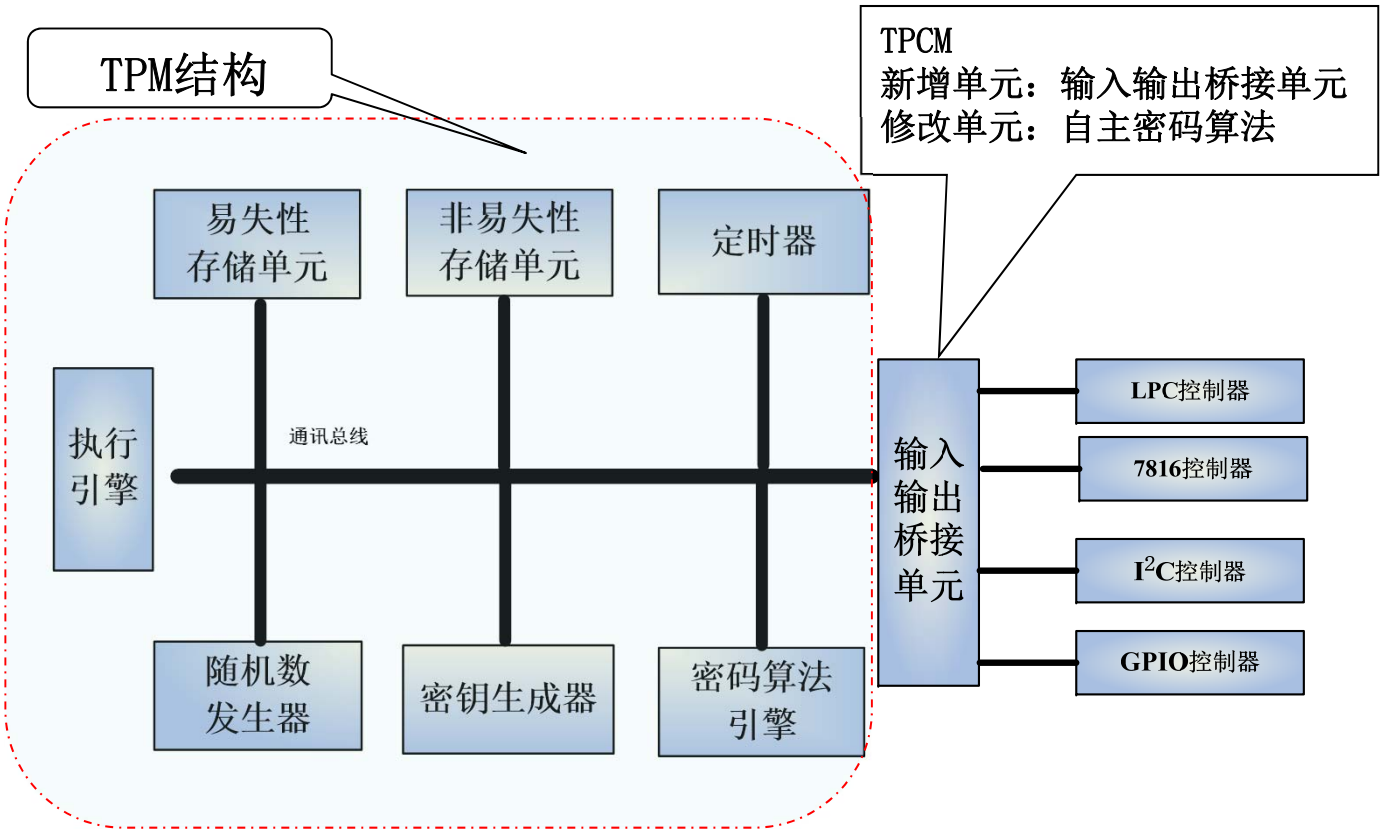
硬件芯片TPM

信任根技术

- 它由CPU、存储器、I/O、密码运算器、随机数产生器和嵌入式操作系统等部件组成。

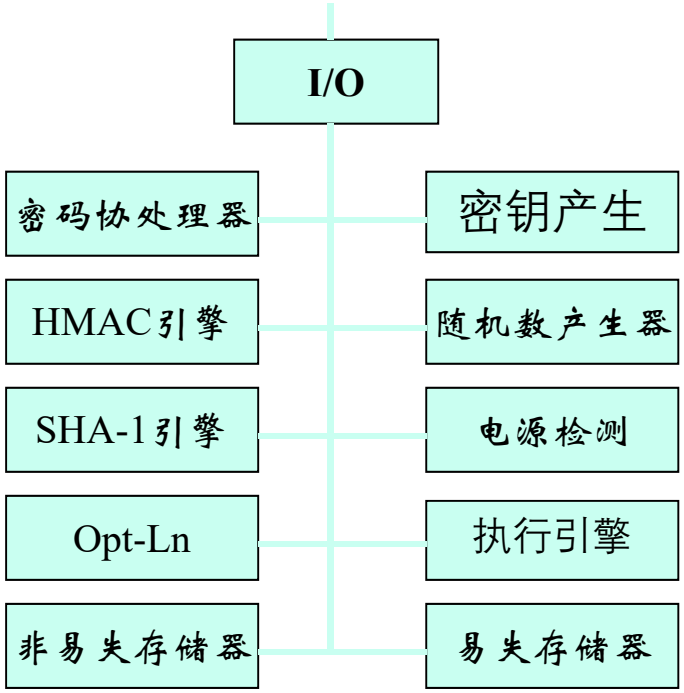
- TPM本身就是一个小的计算机系统，一般是一种片上系统SOC（System on Chip）,而且它应当是物理可信和管理可信的。
- TPM供应厂商：

  Atmel,Broadcom,Infineon, National Semiconductor, STMicroelectronics,国民技术


TPM结构
TPCM
新增单元：输入输出桥接单元
修改单元：自主密码算法
易失性
存储单元
非易失性
存储单元
定时器
执行
引擎
通讯总线
输入
输出
桥接
单元
LPC控制器
7816控制器
I2C控制器
GPIO控制器
随机数
发生器
密钥生成器
密码算法
引擎

可信模块TPCM结构

信任根技术


I/O
密码协处理器
密钥产生
HMAC引擎
随机数产生器
SHA-1引擎
电源检测
Opt-Ln
执行引擎
非易失存储器
易失存储器

- I/O ： 负责管理通信总线，它的任务包括执行内部总线和外部总线之间进行转换的通信协议，将消息发送到合适的部件，执行对TPM进行操作的安全策略。
- 密钥生成器：负责生成对称密码的密钥和非对称密码运算的密钥对，TPM可以无限制地生成密钥。对于RSA算法而言，它要完成大素数的测试，密钥生成过程会使用到随机数发生器随机产生的数据。
- HMAC引擎：通过确认报文数据是否以正确的方式为TPM提供信息，它可以发现数据和命令发生错误或者被篡改的情况。

- 随机数发生器：负责产生各种运算所需要的随机数，它通过一个内部的状态机和单向散列函数将一个不可预测的输入变成32字节长度的随机数，其输入数据源可以是噪音、时钟等，该数据源对外不可见。随机数发生器在系统掉电时产生RESET操作。
- SHA-1引擎：负责完成一种基本的HASH运算，其HASH接口对外暴露，可以被调用，它的输出是160位二进制位。
- 电源检测：TPM要求能够感应任何电源状态的变化，TPM 电源与可信计算平台电源关联在一起，电源检测帮助TPM在电源状态发生变化的时候采取适当的限制措施。

- 选项控制：提供了对TPM功能开启与关闭的机制，通过改变一些永久性的可变标志位，可以设置TPM的功能选项，但这种设置必须是TPM的所有者或者经所有者授权的情况下才能进行。
- 执行部件：负责执行经过I/O传送给TPM的命令，在执行命令之前应确信命令执行环境是隔离的和安全的。非挥发性的存储器用于存放一些永久性的数据。

信任根技术

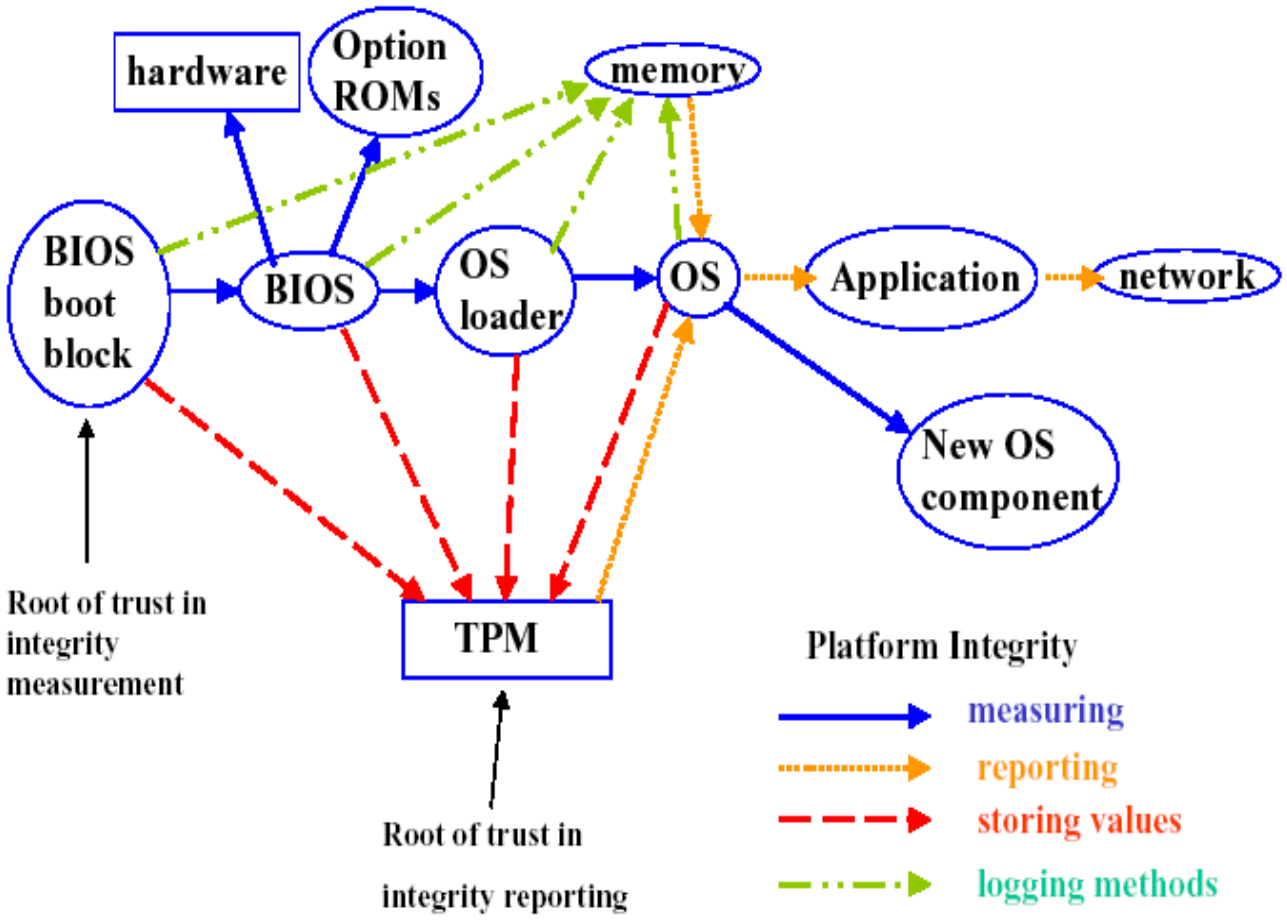
- 可信平台3个信任根
  - 可信度量RT M ：一个软件模块。
  - 可信存储RTS：由可信平台模块TPM芯片和存储根密钥SRK组成。
  - 可信报告RTR：由可信平台模块TPM芯片和根密钥EK组成。
- TPM的不足：
  - TPM被设计成一种被动部件，缺少对平台安全的主动控制作用。
  - 采用LPC总线与系统连接，不适合大数据量的通信。

信任根技术

- 缺少芯片本身物理安全方面的设计.
- 可信测量根RTM是一个软件模块，它存储在TPM之外,易受到恶意攻击。
- 在密码配置方面也存在一些不足。密钥种类繁多、授权协议复杂,存在TPM密钥内外部不同步问题，缺少对称密码。
- 公钥密码采用了RSA ，由于RSA的密钥很长， 因此实现电路规模大、 运算慢。HASH 函数采用的SHA-1很快将被更换，从而使得TPM 的安全使用寿命较短。

信任链的基本思想

- 信任链的目的：测试信任链上各节点的真实性和正确性。
- 硬件的正确性测试比较容易，而软件正确性测试比较困难。
- 对BIOS、OS的数据完整性测试认证是静态的
- 软件数据完整性是信息安全的重要部分
- 但是，软件数据完整性还不能保证动态的安全性
- 因此，还必须进行动态可信性


hardware
Option ROMs
memory
BIOS boot block
BIOS
OS loader
OS
Application
network
New OS component
Root of trust in integrity measurement
TPM
Root of trust in integrity reporting
Platform Integrity
measuring
reporting
storing values
logging methods

信任链的主要技术

完整性测量值的存储

- TCG规范：存入TPM （TPM是信任存储根）
- TPM中设置了平台配置寄存器(PCRs)，作为完整性度量值的安全仓库。
- PCRs在平台启动时用预先确定的数值初始化
- 现值与新值相连，两者的摘要被作为新的完整性度量值存储起来。

  PCRi New=HASH（PCRi Old||New Value）

- 这样，一个160位的累计HASH值就可以表示所有被度量过的组件的完整性状态。并且可以存储无限多个完整性度量值。

信任链的主要技术

可信测量

- 可信的测量：任何想要获得平台控制权的实体，在获得控制权之前都要被测量，判断其是否可信。
- 度量的存储：对实体可信的测量以及该过程的审计信息将被TPM保存，以此向访问实体报告平台或其上运行实体的可信度的依据。
- 度量的报告：需要知道平台可信状态的实体，在获得许可后，可以得到当前TPM中保存的测量值的报告。询问实体据此来衡量当前平台的可信度，并决定是否与该平台建立会话。

密钥和证书机制

- TCG定义了7种密钥类型。每种类型都附加了一些约束条件以限制其应用。TCG的密钥可以粗略的分类为签名密钥和存储密钥。更进一步的分类有：平台、身份认证、绑定、普通和继承密钥。对称密钥被单独分类为验证密钥。

7种密钥类型如下：

1）签名密钥(Signing Key)：非对称密钥，用于对应用数据和信息签名。

2）存储密钥(SK-Storage Key)：非对称密钥，用于对数据或其他密钥进行加密。存储根密钥(SRK-Storage Root Key)是存储密钥的一个特例。

3）平台身份认证密钥(AIK-Attestation Identity Key)：专用于对TPM产生的数据（如TPM功能、PCR寄存器的值等）进行签名的不可迁移的密钥。

密钥和证书机制

4）签署密钥(EK-Endorsement Key)：平台的不可迁移的解密密钥。在确立平台所有者时，用于解密所有者的授权数据和与产生AIK相关的数据。签署密钥从不用作数据加密和签名。

5）绑定密钥(Binding Key)：用于加密小规模数据（如对称密钥），这些数据将在另一个TPM平台上进行解密。

6）继承密钥：在TPM外部生成，在用于签名和加密的时候输入到TPM中，继承密钥是可以迁移的。

7）验证密钥：用于保护引用TPM完成的传输会话的对称密钥。

密钥和证书机制

- TCG定义了五类证书，每类都被用于为特定操作提供必要的信息。

证书的种类包括：

1）签署证书(Endorsement Credential)

2）符合性证书(Conformance Credential)

3）平台证书(Platform Credential)

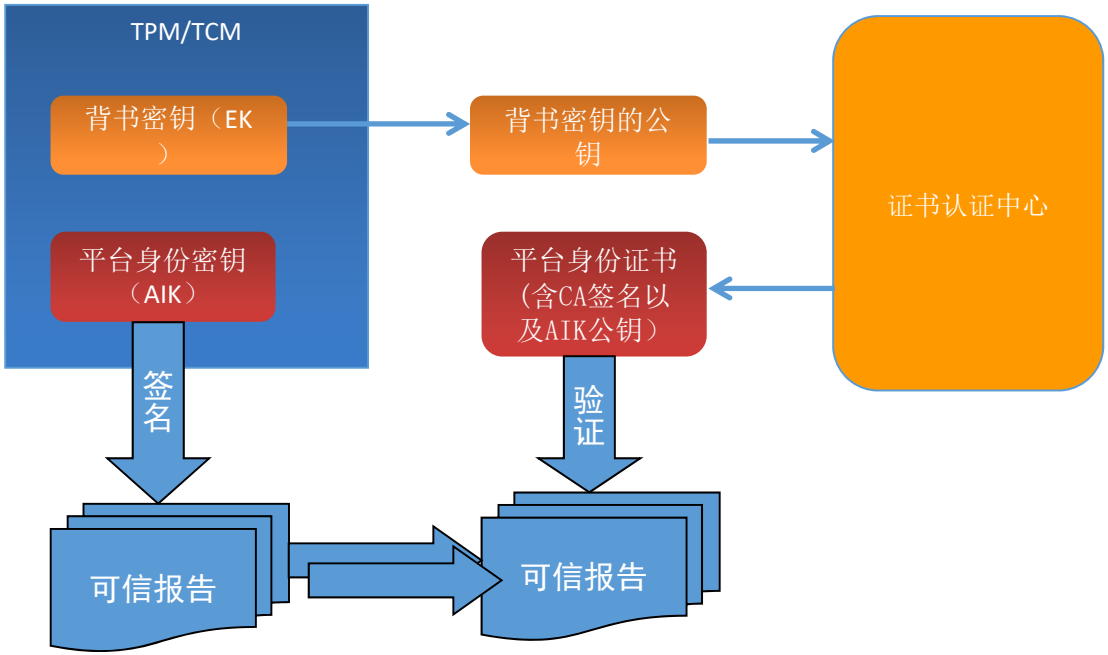
4）认证证书(Validation Credential)

5）身份认证证书(Identity or AIK Credential)

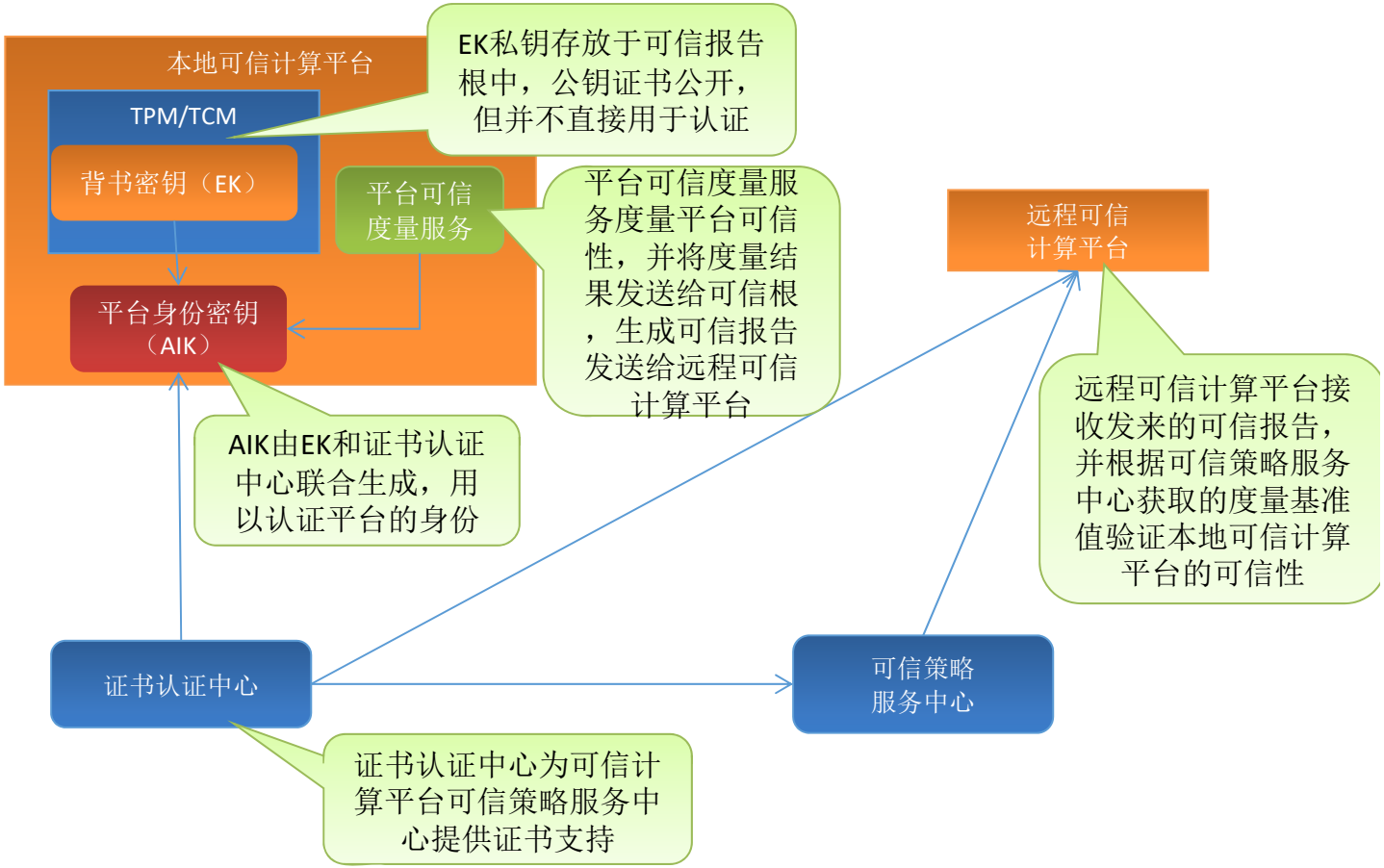
可信计算的关键技术

- 可信报告
- 可信存储
- 可信度量

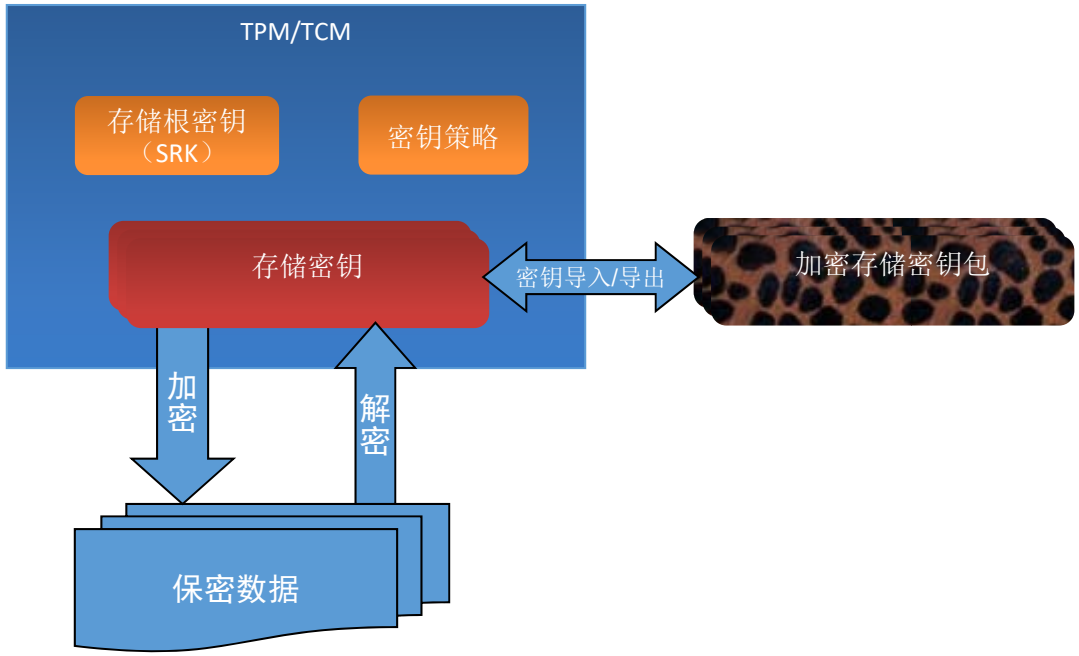
可信报告基本原理


TPM/TCM
背书密钥（EK）
平台身份密钥（AIK）
背书密钥的公钥
证书认证中心
平台身份证书（含CA签名以及AIK公钥）
签名
验证
可信报告
可信报告

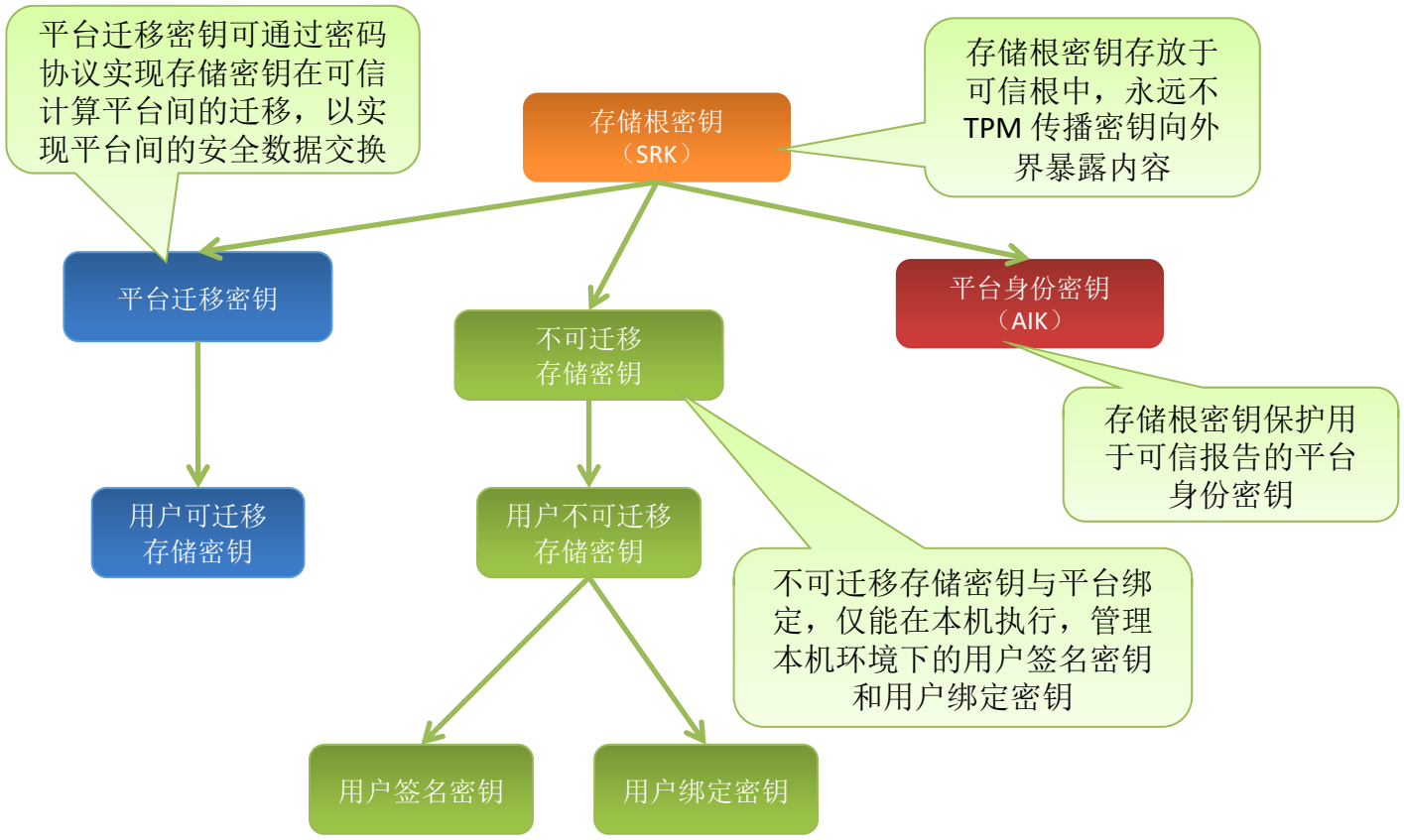
可信报告实施方式


本地可信计算平台
TPM/TCM
背书密钥（EK）
平台可信
度量服务
平台身份密钥
（AIK）
EK私钥存放于可信报告根中，公钥证书公开，但并不直接用于认证
平台可信度量服务度量平台可信性，并将度量结果发送给可信根，生成可信报告发送给远程可信计算平台
AIK由EK和证书认证中心联合生成，用以认证平台的身份
远程可信
计算平台
远程可信计算平台接收发来的可信报告，并根据可信策略服务中心获取的度量基准值验证本地可信计算平台的可信性
证书认证中心
可信策略
服务中心
证书认证中心为可信计算平台可信策略服务中心提供证书支持

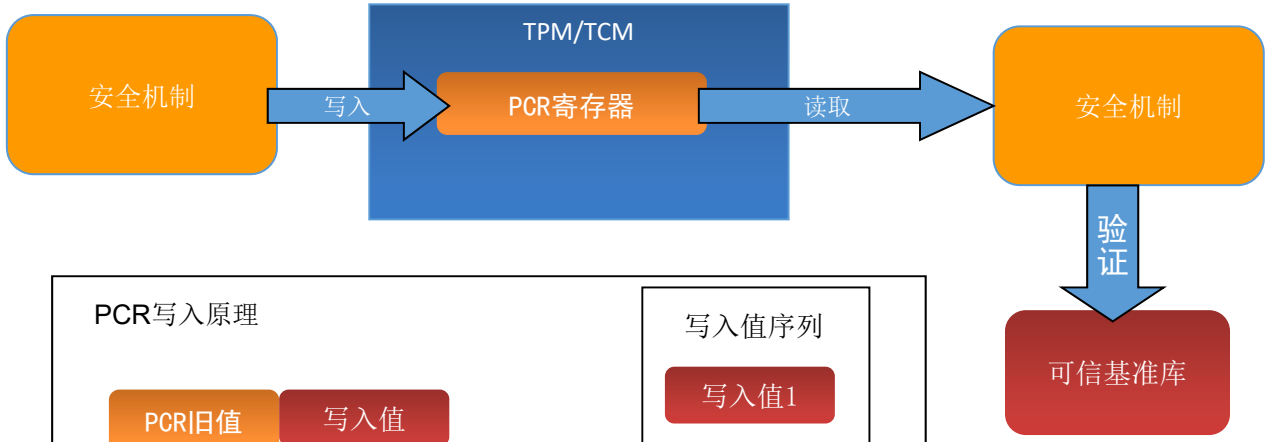
可信存储基本原理

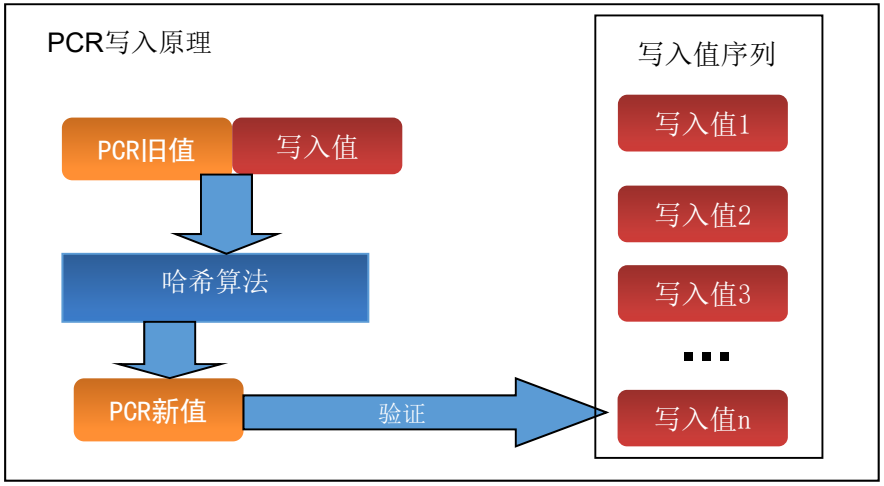


可信存储实施方式

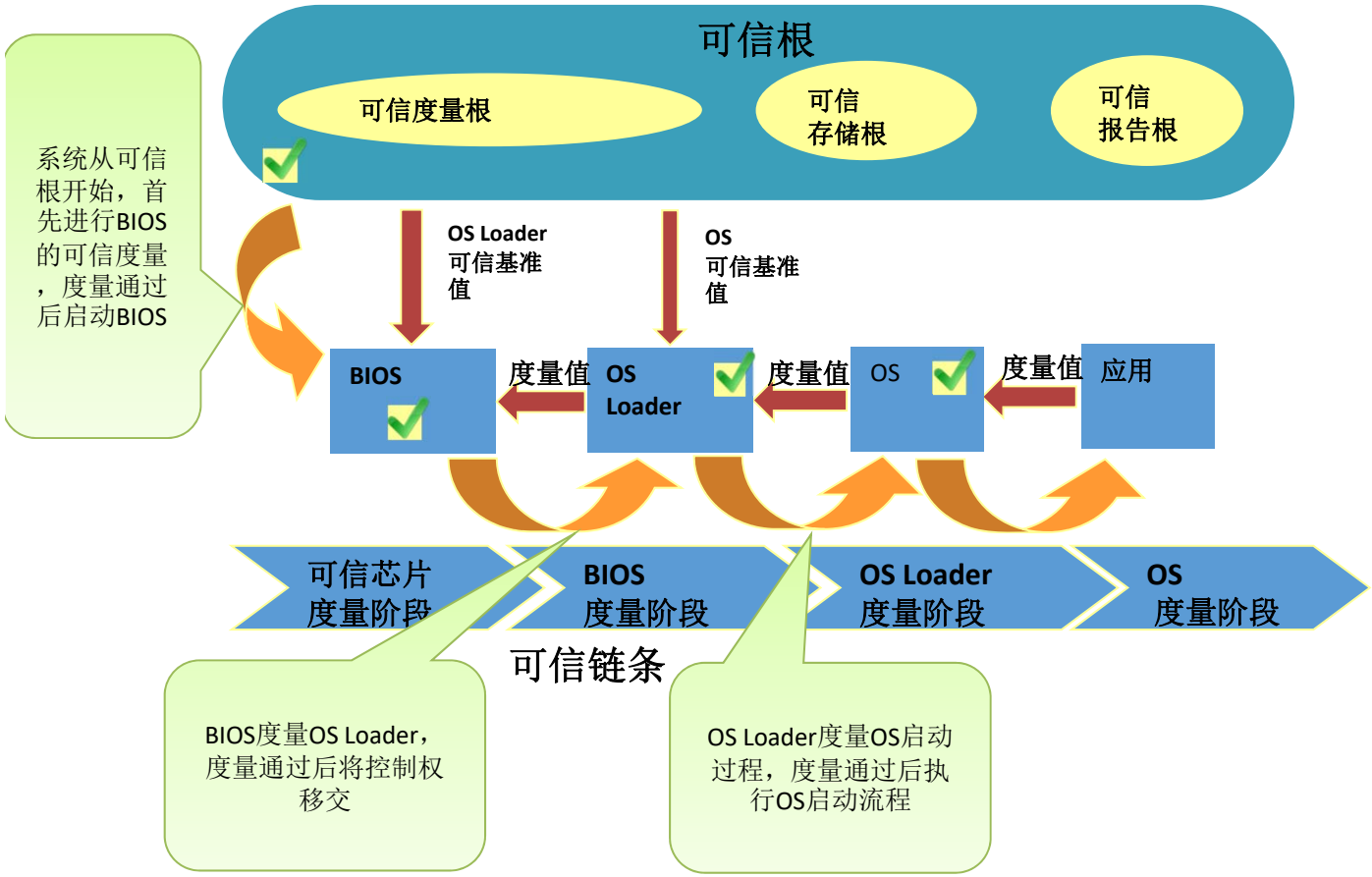

平台迁移密钥可通过密码协议实现存储密钥在可信计算平台间的迁移，以实现平台间的安全数据交换
存储根密钥（SRK）
存储根密钥存放于可信根中，永远不TPM 传播密钥向外界暴露内容
平台迁移密钥
不可迁移存储密钥
平台身份密钥（AIK）
存储根密钥保护用于可信报告的平台身份密钥
用户可迁移存储密钥
用户不可迁移存储密钥
不可迁移存储密钥与平台绑定，仅能在本机执行，管理本机环境下的用户签名密钥和用户绑定密钥
用户签名密钥
用户绑定密钥

可信度量基本原理


安全机制
写入
TPM/TCM
PCR寄存器
读取
安全机制
验证
可信基准库


PCR写入原理
PCR旧值
写入值
哈希算法
PCR新值
验证
写入值序列
写入值1
写入值2
写入值3
...
写入值n

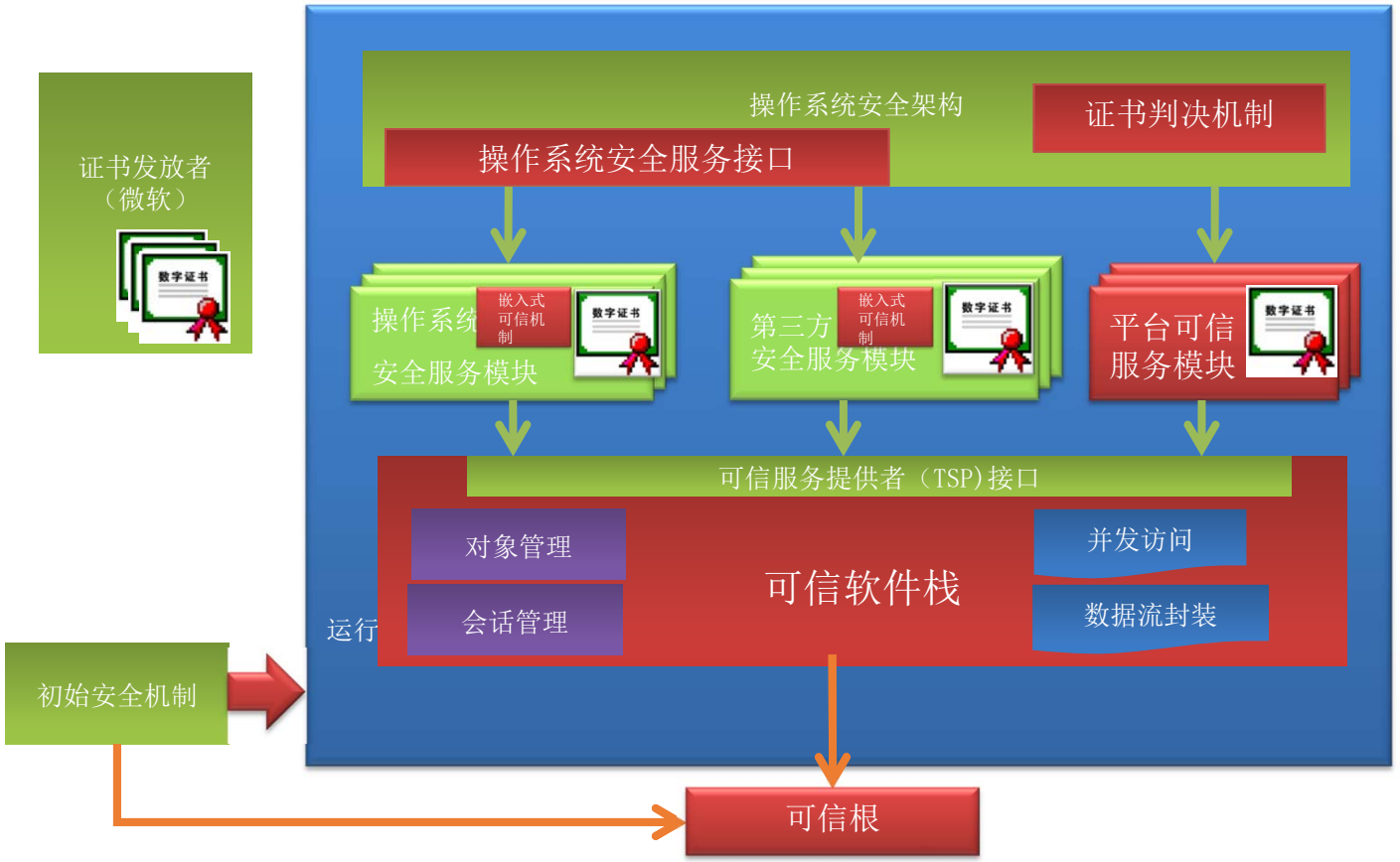
可信度量实施方式


可信根
可信度量根
可信
存储根
可信
报告根
系统从可信根开始，首先进行BIOS的可信度量，度量通过后启动BIOS
OS Loader
可信基准值
OS
可信基准值
BIOS
度量值
OS
Loader
度量值
OS
度量值
应用
可信芯片
度量阶段
BIOS
度量阶段
OS Loader
度量阶段
OS
度量阶段
可信链条
BIOS度量OS Loader，度量通过后将控制权移交
OS Loader度量OS启动过程，度量通过后执行OS启动流程

两种可信计算体系

- 被动可信计算体系：TCG可信
  - 可信机制由安全机制调用，被动地提供服务
  - 所有经可信认证的系统元件构成一个生态圈，排除所有未经认证的元件和修改件
- 主动可信计算体系：我国的可信计算标准体系
  - 可信机制自成系统，主动监控系统并提供可信服务
  - 可信的标准由安全管理者自行制定，可信机制验证系统是否符合安全管理者所制定的标准

TCG被动可信机制示例



TCG可信要素

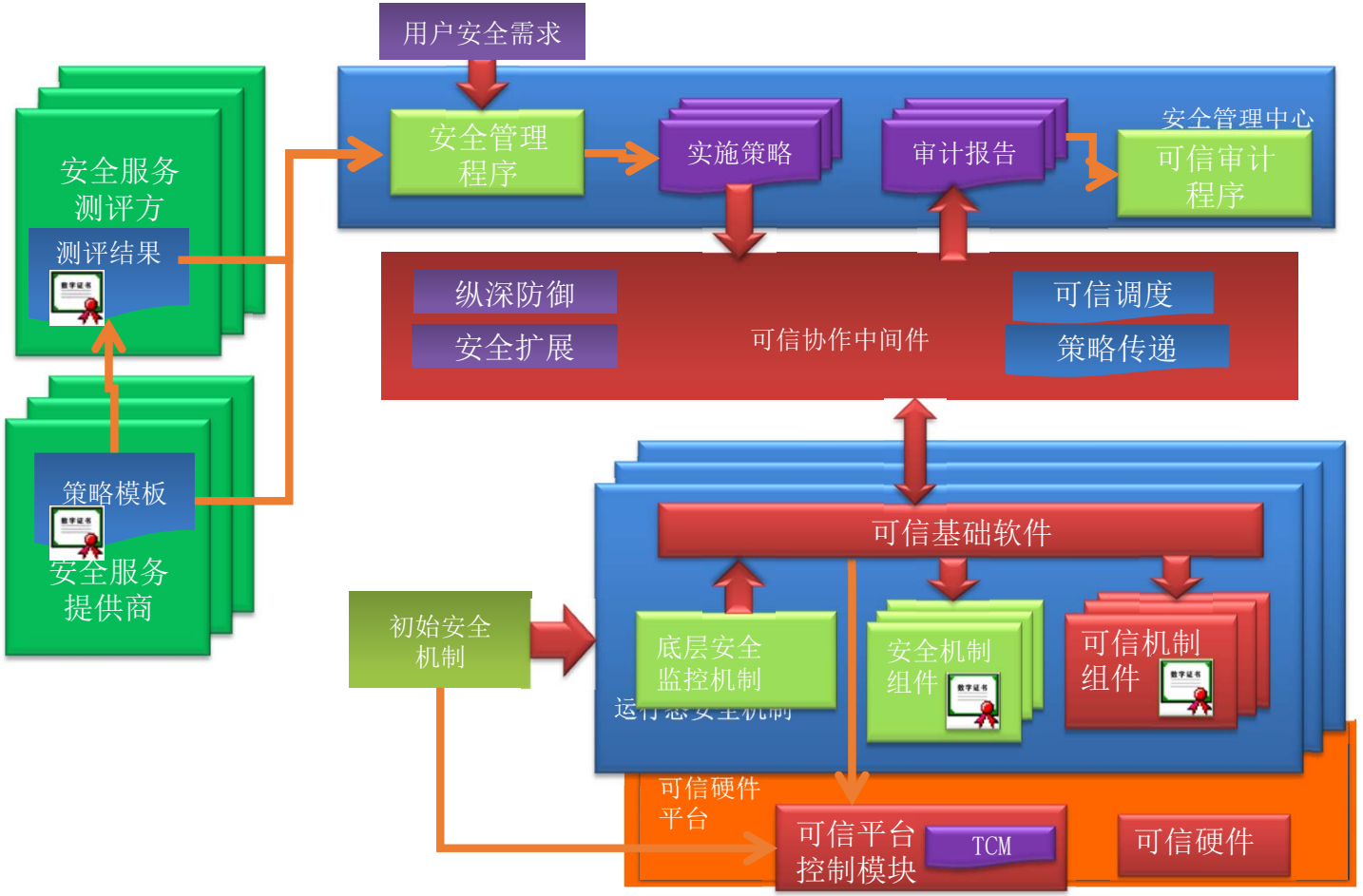
- TCG的可信是“保证可信”
- 通过一个信任领域的“上帝”来保证共同的可信观。
- 可信与不可信的界限之间泾渭分明。
- 用户被动接收可信的结论，没有自主选择权。
- “内鬼”会污染整个可信体系

为什么TCG不适应现代信息系统?

- TCG可信二元化的可信认证方式，不能处理现代信息系统的复杂信任关系

- TCG可信被动式的可信调用模式，无法现代信息系统灵活多变的应用运行模式。

主动可信机制示例


用户安全需求
安全服务
测评方
测评结果
安全管理
程序
实施策略
审计报告
安全管理中心
可信审计
程序
纵深防御
安全扩展
可信协作中间件
可信调度
策略传递
策略模板
安全服务
提供商
可信基础软件
初始安全
机制
底层安全
监控机制
安全机制
组件
可信机制
组件
可信硬件
平台
可信平台
控制模块
TCM
可信硬件

主动可信机制适用于现代信息系统

- 主动可信机制可以实现多元化的复杂可信管理与协作，能适应复杂信任模型的需求
- 主动可信机制能够实现安全机制的按需调度配置，能适应多种软件定义的应用运行模式
- 主动可信机制可以独立于已有架构实现，既可保证系统的兼容性，又便于实现安全的自主自控

小结

- 在信息系统中，不需要，也不应该有一个信任上的“上帝”
- 电子空间的信任体系，应当是现实信任关系在信息系统中的映射。
- 通过主动可信机制，可以逼近这种映射，让用户能掌控自己的信任。
- 电子空间的信任体系，应该通过用户之间的多角度，多层次的协商，以自组织方式实现。
- 从信任入手重组安全，将让信息安全真正走向体系化，带来信息安全领域的一场革命
- 信任机制的实现和信任服务领域，蕴藏着巨大的商机

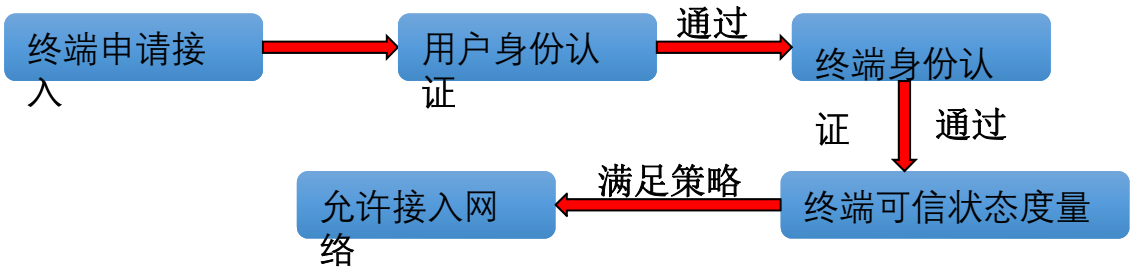
03

可信网络连接

可信网络连接与远程证明

▶可信网络连接(TNC)

将可信计算机制延伸到网络的一种技术。



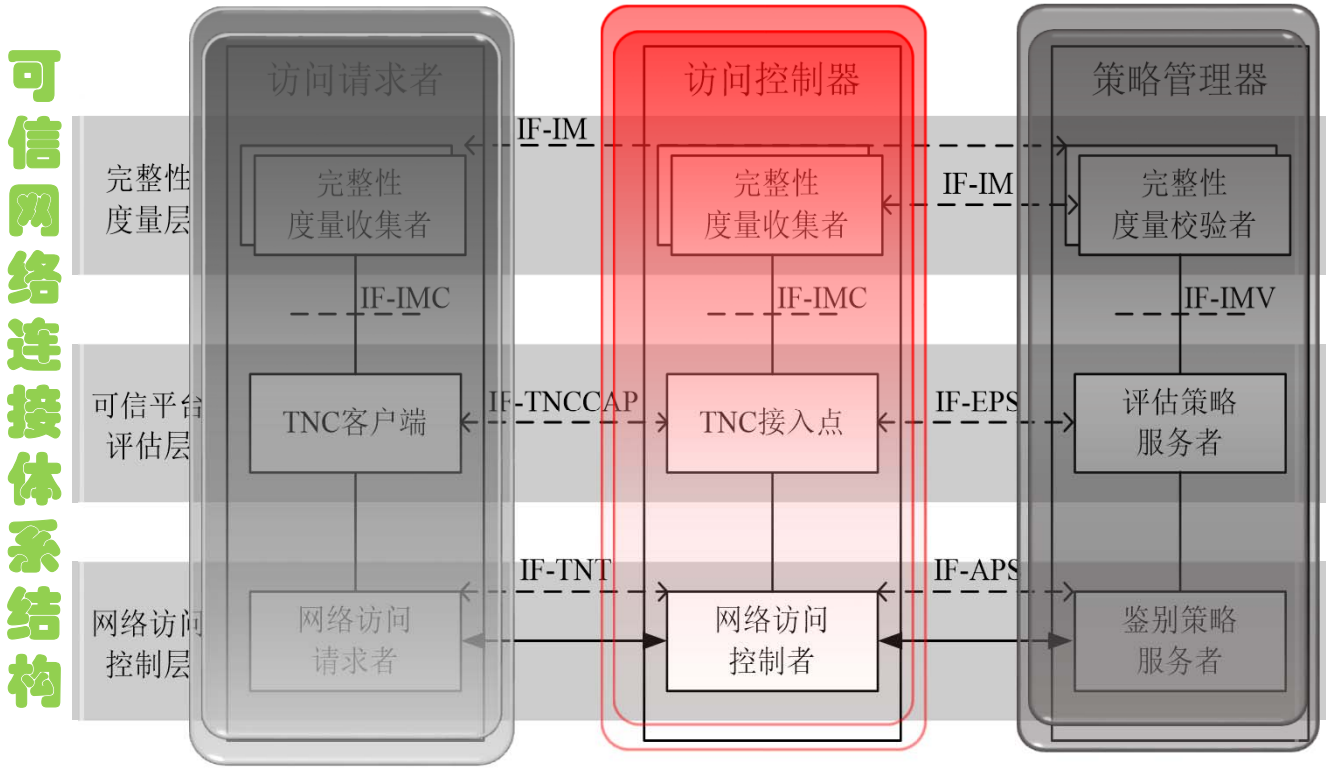
优点与缺点

优点：考虑架构的安全性与现有标准和技术的兼容性。

缺点：

- 限于完整性。 TNC对终端的可信验证基于完整性。 只能确保软件的静态可信，不能确保软件的动态可信。
- 单向可信评估。TNC的出发点是保证网络的安全性，没有考虑如何保护终端的安全.
- 缺乏安全协议支持。TNC架构中,多个实体需要进行信息交互，但是TNC架构本身并没有给出相应的安全协议.
- 缺乏网络接入后的安全保护。
- 应用范围具有局限性。TNC应用目前局限在企业内部网络，难以提供分布式、多层次、电信级、跨网络域的网络访问控制架构。

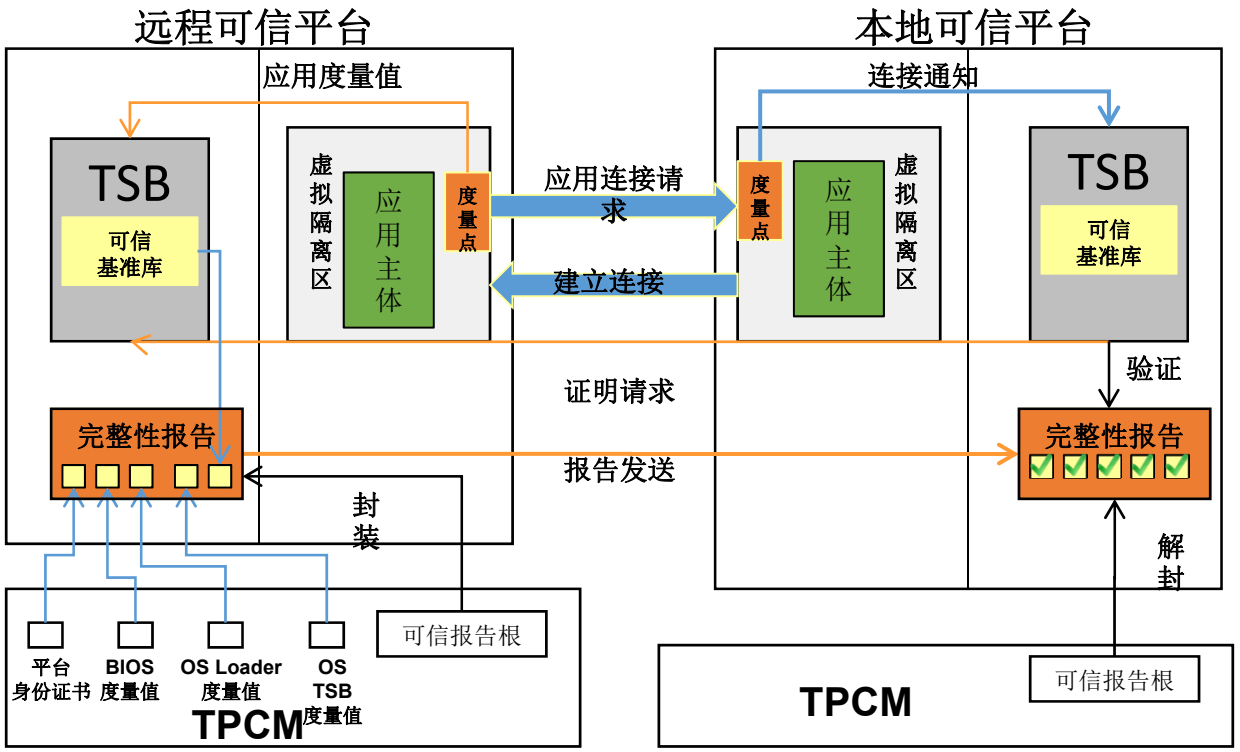
可信网络连接架构


可信网络连接体系结构
访问请求者
访问控制器
策略管理器
完整性度量层
可信平台评估层
网络访问控制层
IF-IM
IF-IMC
IF-IMV
IF-TNCCAP
IF-EPS
IF-TNT
IF-APS
完整性度量收集者
完整性度量校验者
TNC客户端
TNC接入点
评估策略服务者
网络访问请求者
网络访问控制者
鉴别策略服务者

远程证明

远程证明是指网络中的两个节点,一个节点将自己平台的某些信息使用约定的格式和协议向另一个节点报告，使得另一节点能够获得这些信息，并判定该平台的可信状态。远程证明是TNC架构中可信评估层与可信验证层功能的结合。

可信网络连接与远程证明



中国的可信网络连接研究

采用了一种三元、三层、 对等、集中管理的结构. 通过引入一个策略管理器作为可信第三方，对访问请求者和访问控制器进行集中管理，网络访问控制层、可信平台评估层、执行基于策略管理器为可信第三方的三元对等鉴别协议，实现访问请求者和访问控制器之间的双向用户身份认证和双向平台可信性评估.

优点：采用国家自主知识产权的鉴别协议，将访问请求者和访问控制器作为对等实体，以策略管理器为可信第三方，既简化了身份管理、策略管理和证书管理机制，又保证了终端与网络的双向认证，具有很大的创新性。

04

可信3.0

可信3.0的应用模式

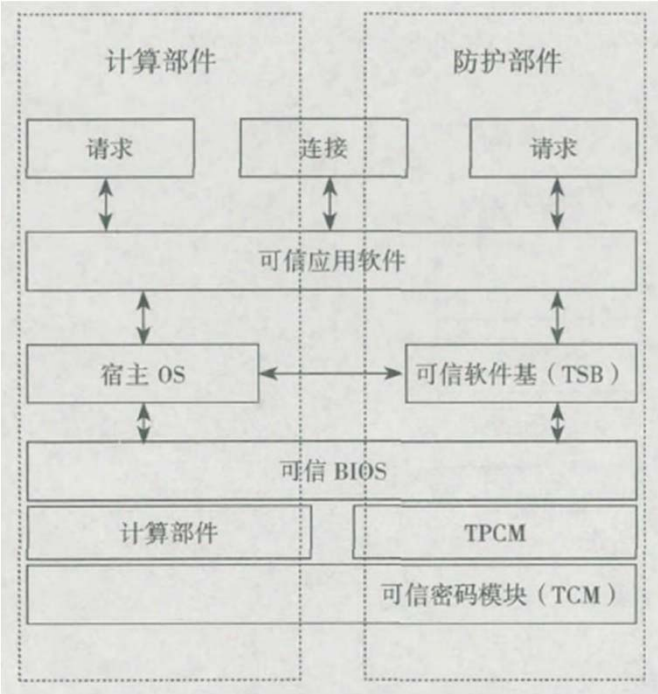
- 计算的同时进行安全防护
- 构建了基本的可信免疫机制后，由管理员参与，为不同的计算任务定制可信策略
- 通过可信策略驱动可信免疫机制识别“自己”和“非己”，保障计算任务运行环境的可信
- 应用模式包含
  - 可信机制
  - 可信策略
  - 可信保障

可信机制

- 以双系统体系架构的模式实现可信机制，为各种安全机制提供了一个统一的、通用性的可信平台
  - 为系统中的安全机制提供了一个共同的基础
  - 给安全机制提供统一的可信保障
  - 为各安全机制动态连接、构成纵深防御安全体系提供了支持

可信机制

- 可信支持的双体系结构



可信机制

- 宿主系统中运行的应用是传统的应用程序，接收并响应用户的请求，完成预设的应用流程
- 可信子系统提供可信管理应用，由管理员操作，执行对系统的可信管理控制
- 宿主系统和可信子系统均通过网络与其他宿主系统和可信子系统进行连接，形成同构的分布式网络系统

可信机制

- 安全机制遵循引用监视器模型，运行过程包括：
  - 接收安全策略
  - 执行监控行为
  - 返回审计信息
- 在可信3.0下，安全机制可以看作是一个或一组监控点，与可信软件基对接，通过可信软件基接收安全策略，并将审计信息反馈给可信软件基

可信策略

- 可信策略根据用户信任情况、系统部署情况和计算任务的流程定制，在计算任务执行前部署，定义可信机制的具体行为方式
- 信息系统中所有的行为都可以用四元组（主体、客体、操作、环境）来描述
  - 主体：代表用户执行主动操作的实体
  - 客体：数据的容器
  - 操作：主体对客体执行的访问行为，一般与监控点绑定
  - 环境：主体对客体执行操作时所处环境的状态

可信策略

- 可信策略包含
  - 识别策略：确定信息系统行为四元组的可信属性
  - 策略控制：在明确主体、客体、操作和环境后，确定操作是否可信并根据不同的可信状况确定系统的应对策略
  - 报警策略：在系统发现异常时，搜集审计信息进行初步判断，将判断结果和相关数据组成报警

可信保障

- 可信节点的可信保障主要从可信根出发，依托密码学技术和可信扩展技术实现贯穿系统的可信链
- 可信根是一个物理保护的可信运行环境，可保证内部计算数据的保密、计算过程不受外界干扰
- 可信根是可信计算平台信任的源头

可信保障

- 可信链从信任根出发，先后扩展到系统，并通过可信连接与其他可信平台上的可信节点建立协作关系，通过可信策略的管理控制，将这些可信节点整合成可信体系
- 可信链并不验证应用自身的可信，它只是为应用提供可信的计算环境，确保应用的执行符合预期，不受病毒、黑客和内部人员越权攻击等威胁

可信保障

- 可信节点的可信保障主要从可信根出发，依托密码学技术和可信扩展技术实现贯穿系统的可信链
- 可信根是一个物理保护的可信运行环境，可保证内部计算数据的保密、计算过程不受外界干扰
- 可信根是可信计算平台信任的源头
  - 识别策略：确定信息系统行为四元组的可信属性
  - 策略控制：在明确主体、客体、操作和环境后，确定操作是否可信并根据不同的可信状况确定系统的应对策略
  - 报警策略：在系统发现异常时，搜集审计信息进行初步判断，将判断结果和相关数据组成报警