基于可信策略语言的主动安全免疫系统

可信华泰-田健生

2023/12/18

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

安全可信既是政策、标准要求，也是技术发展趋势

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，**推广安全可信的网络产品和服务**，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

国家网络空间安全战略

夯实网络安全基础

坚持创新驱动发展，积极创造有利于技术创新的政策环境，统筹资源和力量，以企业为主体，产学研用相结合，协同攻关、以点带面、整体推进，**尽快在核心技术上取得突破。**重视软件安全，**加快安全可信产品推广应用。**

网络安全等级保护制度2.0标准及**关键信息基础设施安全保护条例**要求应当优先采购**全面使用安全可信的产品和服务**来构建关键信息基础设施安全保障体系。

安全操作系统标准（GB/T 20272）要求符合等级保护三级以上的系统“支持硬件可信芯片作为信任根”。

安全可信既是政策、标准要求，也是技术发展趋势

系统要求

系统要求这些是在电脑上安装 Windows 11 的最低系统要求。如果您的设备不满足这些要求，您可能无法在设备上安装 Windows 11，建议您考虑购买一台新电脑。如果您不确定您的电脑是否满足这些要求，可以咨询您的原始设备制造商 (OEM)；如果您的设备已经在运行 Windows 10，您可以使用电脑健康状况检查应用来评估兼容性。请注意，此应用不会检查显卡或显示器，因为大多数的兼容设备都能满足以下列出的要求。

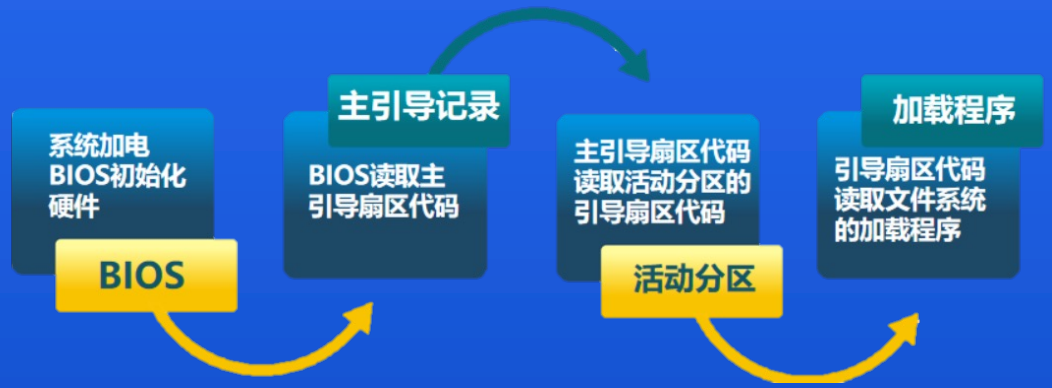
您的设备必须已安装 Windows 10 的 2004 或更高版本，才能升级。可在'设置 > 更新和安全'中的 Windows 更新功能中获取免费更新。

处理器	1 GHz 或更快的支持 64 位的处理器（双核或多核）或系统单芯片 (SoC)。
内存	4 GB。
存储	64 GB 或更大的存储设备，注：有关详细信息，请参见以下"关于保持 Windows 11 最新所需存储空间的更多信息"。
系统固件	支持 UEFI 安全启动。请在此处查看关于如何启用电脑以满足这一要求的说明。
TPM	受信任的平台模块 (TPM) 2.0 版本。请在此处查看关于如何启用电脑以满足这一要求的说明。

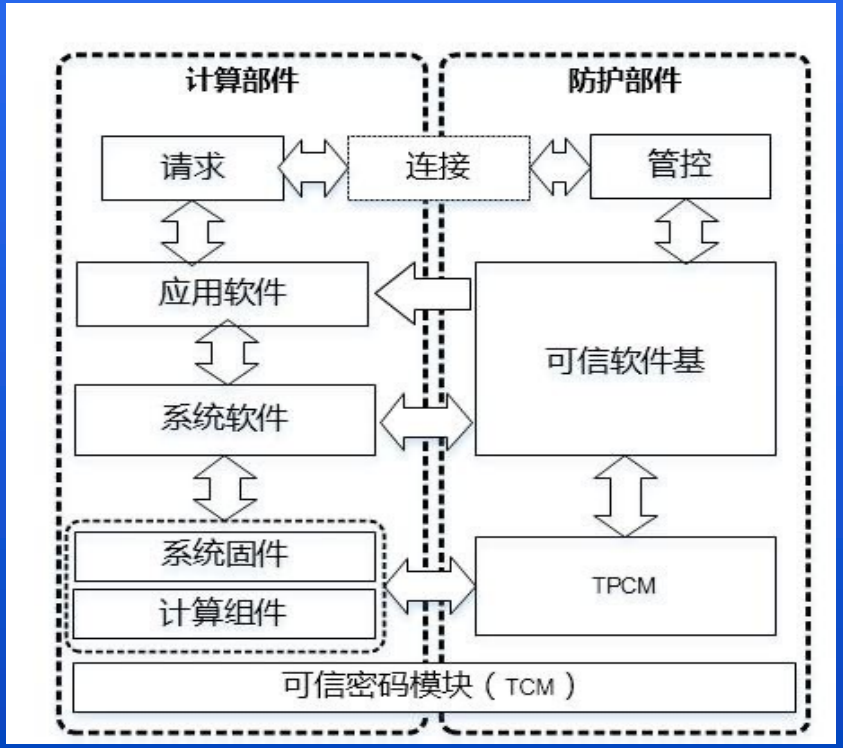
可信计算技术特征

防护部件作用于保护对象和攻击者启动之前或运行层级之下。

- 场景1：可信（安全）引导——检查机制在被检查对象运行前执行



- 场景2：主动免疫——防护部件在被检查对象特权层级之下，主动执行（可信计算3.0框架）



基于可信策略语言的主动安全免疫系统防护思路

构建可信根

- 构建一个对业务系统具有访问和管理特权的、基于硬件可信执行环境；

构建可信软件基

- 在可信执行环境中，部署具备可信策略存储和解析执行的可信软件基；

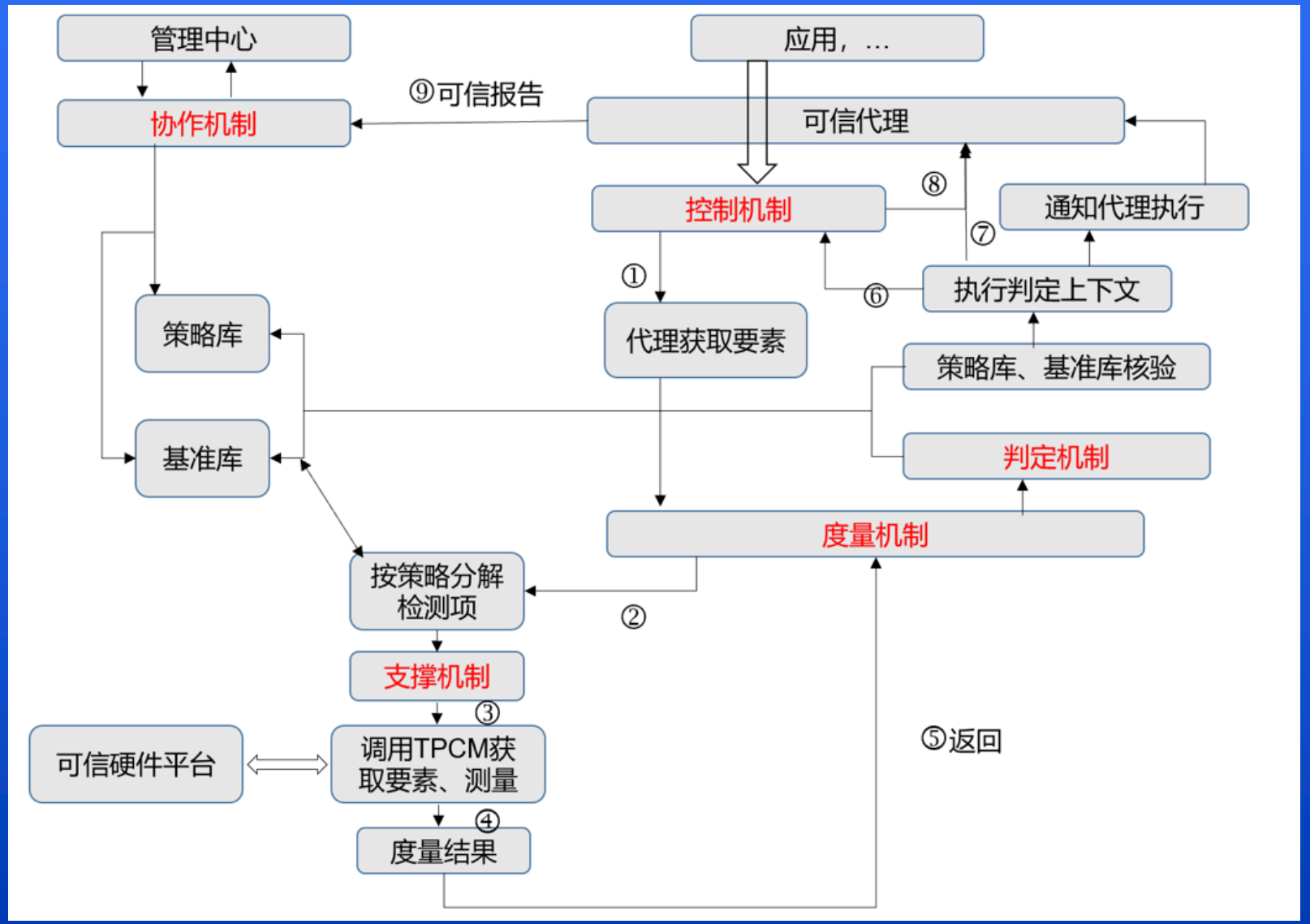
配置可信安全策略

- 在管理中心，通过可信策略语言描述业务系统/业务应用的完整性、正常资源访问需求、正常调用状态、异常处置方式等安全策略；

提供可信免疫服务

- 系统运行中，由可信软件基通过代理主动获取系统运行状态，依据上述安全策略进行要素获取、度量、判定和处置。

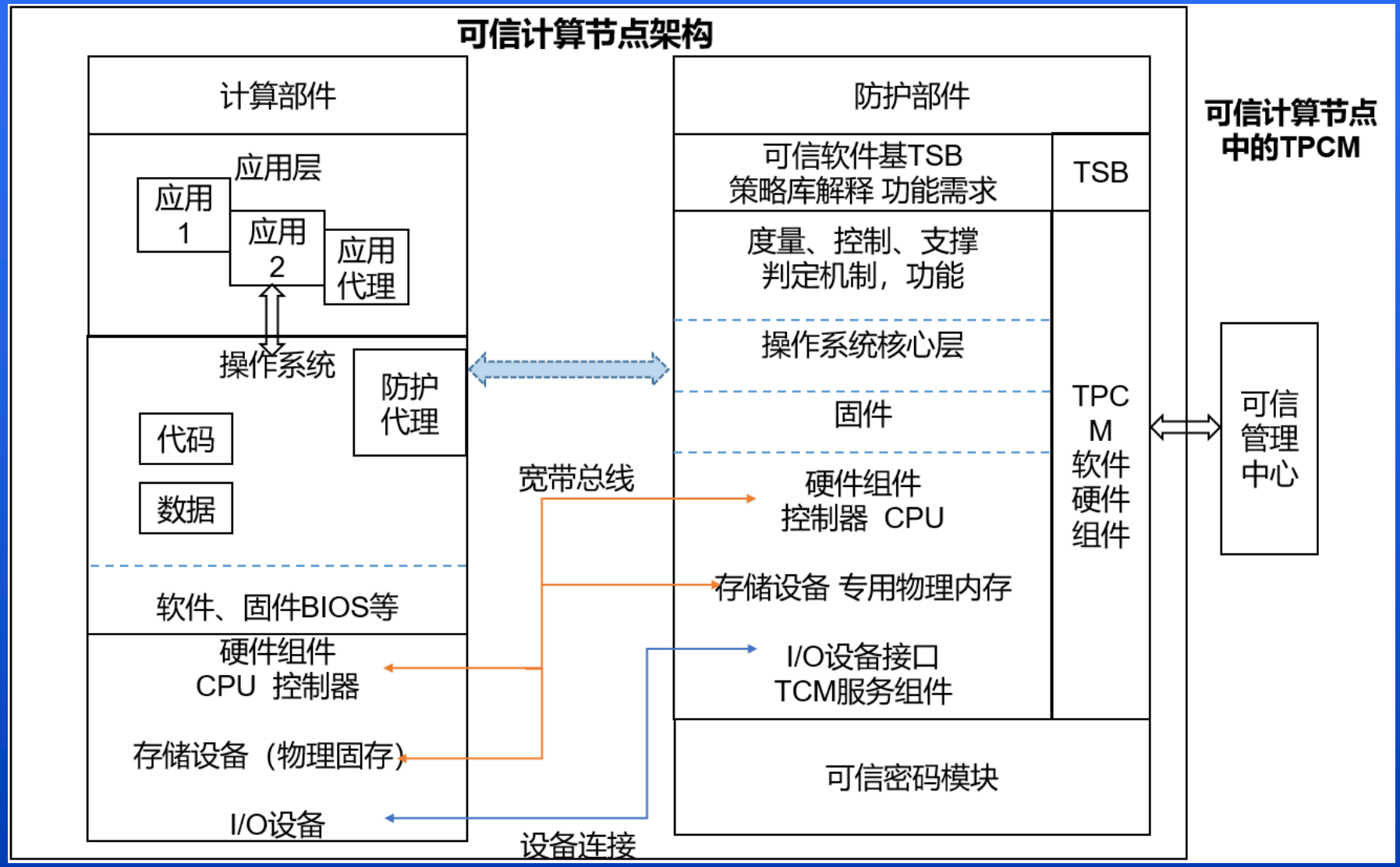
可信策略下发、加载和执行流程



主动可信根——可信平台控制模块（TPCM）

防护部件	
可信软件基TSB 策略库解释 功能需求	TSB
度量、控制、支撑 判定机制，功能	TPCM 软件 硬件 组件
操作系统核心层	
固件	
硬件组件 控制器 CPU 存储设备 专用物理内存 I/O设备接口 TCM服务组件	
可信密码模块	

OS与可信根组成的可信计算节点架构



THANKS

THANKS

THANKS