首届高校ICT产教融合创新大赛企业命题

命题编号：27

|  |  |  |
| --- | --- | --- |
| 命题企业 | 华为 | |
| 命题题目 | 面向计算机容器可信启动的远程证明方法 | |
| 命题方向 | （请填写命题应用的场景领域）  网络虚拟化与可信网络技术，适用于对系统安全、数据完整性和可信度有高度要求的场景，例如：云环境、金融和医疗、嵌入式和物联网设备等 | |
| （请填写命题涉及的技术方向）  虚拟化，计算机容器，远程证明 | |
| 命题内容 | 命题背景 | 网络基础设施云化和虚拟化是5G/6G网络的基础，云网分属不同的厂商是未来网络的演进趋势之一， 虚拟机和容器技术是主要的网络虚拟化技术，远程证明技术是构建可信网络基础实施的基石, 如何通过远程证明技术保证虚拟机和容器可信是运营商面临的重大挑战。  可信计算在解决云环境的安全性问题中发挥了重要作用。TCG(Trusted Computing Group)提出的解决方案是以TPM(trusted platform module)为可信根，作为外挂部件被动调用无法进行主动度量。TCG标准组织制定基于TPM和远程证明的可信启动方法，为了解决虚拟机的远程证明挑战，TCG正在研究虚拟机远程证明方案。  然而，有时候，对TPM的依赖可能会引入一些限制，如依赖硬件支持、复杂的部署和管理等。因此，需要一种对底层的硬件TPM的依赖性低的远程证明方案，可以通过软件和增硬件抽象层等方式。  同时，由于虚拟机需要占用更多的系统资源，轻量级的容器正在成为虚拟化网元部署的载体，但是容器的远程证明方法还有待进一步研究。 |
| 研究目标 | 1. 比较虚拟机与容器在可信启动方面的差异 2. 根据TCG标准组织制定的虚拟机远程证明规范，研究并设计容器的远程证明方案，并支持容器的迁移 3. 可信启动方案对底层的硬件TPM的依赖性低 |
| 输出成果 | 1. 研究报告：容器与虚拟机在可信启动方面的差异 2. 方案：支持容器可信启动，参考TCG/IETF rats 协议，设计面向容器的可信启动远程证明协议 3. 原型：基于Linux平台，实现上述方案 |
| 评价指标 | （请详细阐述项目评价的核心指标或验收标准）   1. 研究报告全面对比虚拟机和容器在可信启动方面的差异，语言清晰，逻辑良好 2. 方案能够为容器的可信启动提供远程证明，支持迁移，协议与IETF RATS协议兼容 3. 原型完整，包括虚拟机平台，容器+证明方（attester），可信启动协议，验证方（verifier），信任方（relying party） | |
| 提交材料 | （请详细阐述团队最终提交的对策方案中需展示的核心内容，如技术手段、创新点、基于场景的实物功能展示等）   1. 研究报告 2. 设计报告 3. 演示原型系统：硬件平台（Linux），容器，信任方（虚拟机），验证方（虚拟机） | |
| 答题所需软硬件资源 | （请写明团队完成命题必要的软硬件资源）  硬件： PC机  软件：Linux系统 | |
| 配套支持 | （企业为参赛团队提供的技术支持、软硬件资源配套，包括线上命题宣讲、赛题辅导、线下活动等）  可提供技术咨询 | |
| 政策支持 | （企业在优秀项目成果知识产权转化、优秀学生技术认证、实习和就业等方面能够提供的支持）  如果设计良好或者优秀，可以为优秀学生提供推荐信 | |
| 其他 | （比赛相关的未尽事宜） | |