基于 TrustZone-M 函数级内存地址空间随机化的可信实时系统

项目编号 202309071

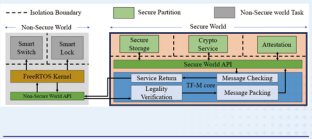
指导教师 凌振（教授,博士生导师）

学生成员

章尊宇(09021318)　　张晗(71121221)　　王罗斌(71121128)
江紫弦(09021235)

项目简介

本项目设计和实现了基于ARM TrustZone-M硬件隔离机制的函数级地址空间随机化技术和受限内存随机内存管理机制，并成功部署到主流实时操作系统FreeRTOS以及可信执行系统TrustedFirmware-M上，有效缓解了低端嵌入式系统面临的内存破坏威胁，提高了物联网系统的安全性。



研究成果

参加第十六届全国大学生信息安全竞赛作品赛，获得我院该项赛事的首个全国一等奖。该作品为低端嵌入式的安全防护提供了新的解决方案。

创新点

1.本作品面向低端嵌入式系统，设计并实现了函数级的动态地址空间布局随机化技术，并针对其性能和内存受限问题设计了相应的受限内存优化机制

2.基于上述技术，我们将该技术部署至目前主流实时操作系统FreeRTOS以及安全区的可信执行系统TrustedFirmware-M上，实现了对上述两个嵌入式主流操作系统的地址空间随机化