物联网环境下嵌入式操作系统的安全性设计

杨朋霖，陶利民，王海涛
(北京卫星信息工程研究所，北京 100194)

摘要：本文通过结合可信计算技术，并根据未来物联网网络环境下操作系统应用程序相对固定、内核状态相对稳定的特点，设计具有函数标签检测和地址空间检测功能的安全操作系统.该安全检测机制通过在内核函数首尾两端设置检查点标签和在时钟中断处理历程中设置地址检查来判断操作系统的运行时状况.同时，可信计算芯片在提供系统启动校验等功能的同时，还能够提供相关数据的校验和保密存储功能，提高了系统性能和可信性.经过试验，该操作系统安全检测机制能够实时监控系统状态以发现系统的异常，为未来物联网网络环境下操作系统安全提供有力保障.
关键词： 嵌入式操作系统安全; 函数标签检测；地址空间检测；可信计算

Security Design of Embedded System in the Environment of Internet of Things

YANG Peng-lin, TAO Li-min, WANG Hai-tao
(Beijing Institute of Satellite Information Engineering, Beijing 100194，China)

Abstract： In this paper we combine these features and trusted computing technique to design a security operating system with function signature check and address space check. By setting up head and tail signatures in kernel functions and address check in clock interrupt, we are able to monitor operating system′s runtime status. Meanwhile, trusted computing chip could not only provide booting verification, data verification, but also encryption storage. These functions could promote operating system′s performance and trustworthy. Experiments show that this security check mechanism is able to monitor operating system in real time and find out abnormal behaviors.
Key words： embedded operating system security; function signature check; address space check; TPM

作者简介：
杨朋霖男，（1991-），博士研究生.研究方向为可信计算、嵌入式操作系统安全的研究工作.
E-mail: yangpl_ht@163.com.
陶利民男，（1976-），硕士，高级工程师.研究方向为星载操作系统、嵌入式系统、信息安全相关研究.
王海涛男，（1970-），博士，研究员.研究方向为星上电子信息系统、信息安全、系统工程的研究工作.