信息安全研究 第5卷 第1期 2019年1月
Journal of Information Security Research Vol.5 No.1 Jan. 2019

密钥安全研究进展

林璟锵 郑昉昱 王跃武
(中国科学院数据与通信保护研究教育中心 北京 100093)
(信息安全国家重点实验室(中国科学院信息工程研究所) 北京 100093)
(中国科学院大学网络空间安全学院 北京 100049)
(linjingqiang@iie.ac.cn)

Advances in Cryptographic Key Protection

Lin Jingqiang, Zheng Fangyu, and Wang Yuewu
(*Data Assurance and Communications Security Research Center, Chinese Academy of Sciences, Beijing* 100093)
(*State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing* 100093)
(*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049)

Abstract In order to achieve the security functionality of cryptographic algorithms, we need to ensure the security of cryptographic keys, i.e., no attacker can access the cryptographic keys. However, there are various attacks access the cryptographic keys on computers that implement cryptographic algorithms and perform cryptographic operations, including system attacks and physical attacks. This paper surveys the attacks that steal cryptographic keys and other sensitive data on computers. We analyze the cryptographic key protections including various solutions based on registers, caches, CPU features, and online central servers and data security techniques on top of protected cryptographic keys, in terms of security, performance and applicability. Finally, we discuss and prospect the research direction of cryptographic key protection in the future.

Key words cryptographic key protection; applied cryptography; memory attack; system security; physical attack

摘 要 密码算法提供安全功能的前提是密钥数据的安全性,要求攻击者不能获得密钥.然而,在计算机系统中实现密码算法、执行密码计算,面临着各种非授权读取密钥数据的攻击,包括系统攻击和物理攻击.先大致总结了计算机系统中各种窃取密钥以及其他敏感数据的攻击方法;然后重点分析了当前各种典型的密钥安全技术方案,分别包括基于寄存器、基于Cache、基于处理器增强特性、结合中心服务器的解决方案,以及基于密钥安全解决方案的数据安全系统技术,并从安全性、计算性能、适用性等方面对各种方案进行了全面的对比;最后,展望了将来的密钥安全技术研究方向.

关键词 密钥安全;应用密码学;内存攻击;系统安全;物理攻击

中图法分类号 TP309

收稿日期:2018-09-28
基金项目:国家自然科学基金项目(61772518);国家重点研发计划网络空间安全重点专项(2017YFB0802100)