同济大学学报自然科学版

基于k循环随机序列的动态缓冲区溢出防御

Dynamic Buffer Overflow Prevention Based on k Circular Rar

投稿时间：2009-8-7　最后修改时间：2010-4-1

DOI:10.3969/j.issn.0253-374x.2010.06.024　稿件编号:0253-374X(2010)06-0917-08　中

中文关键词:缓冲区溢出　栈溢出　软件漏洞　动态检测　容侵

英文关键词:buffer overflow　stack overflow　software vulnerability　dynamic prevention　intrusior

作者	单位
江建慧	同济大学 计算机科学与技术系,上海 201804
章力源	同济大学 计算机科学与技术系,上海 201804
金涛	上海轨道交通信息管理中心,上海 201103
陈川	上海轨道交通信息管理中心,上海 201103

中文摘要

面向Intel 80×86体系结构和C/C++语言,介绍了栈缓冲区溢出攻击的基本原理及攻击模式,分析了现有的动态防御典型方案的优
思想,提出了一种基于k循环随机序列的动态缓冲区溢出防御方案.该方案能够在极大概率下防御多种模式的缓冲区溢出攻击,解决了“

英文摘要

The paper presents an analysis of the principle of stack buffer overflow attacks and basic attack patterns for
merits and drawbacks of the existing dynamic buffer overflow prevention methods are discussed.On the basis of the ad
paper presents a new dynamic buffer overflow prevention method based on k circular random sequence.This improved pre
patterns with high probability and enhance the intrusion-tolerance capability of the vulnerable software.