计算机工程　2010 36 (7): 139-141　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

基于动态染色的内存漏洞定位技术

房 陈，茅 兵，谢 立

(南京大学计算机科学与技术系软件新技术国家重点实验室，南京 210093)

收稿日期　修回日期　网络版发布日期　接受日期

摘要　针对程序漏洞，提出利用基于二进制的程序染色和程序分析技术来检测恶意攻击并有效定位程序漏洞，采用数据依赖关系分析和动态染色的方法，记录起传播作用的写指令及目的内存地址，当检测到漏洞攻击时，通过内存地址找到恶意写指令并定位漏洞。实验结果证明，该方法能成功定位常见内存漏洞的位置，并能定位到有漏洞的库函数的调用点。

关键词　程序漏洞；攻击检测；程序染色；缓冲区溢出；格式化字符串

分类号　TP393.08

DOI:

通讯作者:

作者个人主页: 房 陈;茅 兵;谢 立