计算机工程 2007 33 (10): 144-146 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于系统调用的入侵检测系统研究

戴小鹏1，喻 飞1,2，张林峰1，沈 岳1

(1. 湖南农业大学计算机与通信学院，长沙 410128；2. 浙江大学人工智能研究所，杭州 310027)

收稿日期 修回日期 网络版发布日期 2007-7-19 接受日期

摘要 入侵检测是网络安全研究的热点技术之一，是新一代安全保障方案。该文实现了一种基于系统调用的异常入侵检测方法，使用系统调用作为输入，构建程序中函数的有限状态自动机，利用该自动机检测进程流程是否发生异常来确定是否发生了入侵。实验结果表明，该技术不仅能有效地检测出入侵行为，而且可以发现程序漏洞的位置，便于修改代码。

关键词 入侵检测 异常检测 系统调用 有限状态自动机

分类号 TP301.6

DOI:

通讯作者:

作者个人主页: 戴小鹏1;喻 飞1;2;张林峰1;沈 岳1