	《计算机学报》文章摘要　　全文下载
文章题目	基于粗糙集理论的入侵检测新方法
作者	蔡忠闽 管晓宏 邵 萍 彭勤科 孙国基
作者单位	(西安交通大学系统工程研究所网络化系统与信息安全研究中心 西安 710049)
发表年份	2003
发表月份	3期 （页码：361—366）
文章摘要	摘要 提出了一种高效低负荷的异常检测方法，用于监控进程的非正常行为.该方法借助于粗糙集理论从进程正常运行情况下产生的系统调用序列中提取出一个简单的预测规则模型，能有效地检测出进程的异常运行状态.同其它方法相比，用粗糙集建立正常模型要求的训练数据获取简单，而且得到的模型更适用于在线检测.实验结果表明，该方法的检测效果优于同类的其它方法. 关键词 入侵检测； 异常检测； 网络安全； 粗糙集理论； 系统调用中图法分类号 TP309