	《计算机学报》文章摘要　　全文下载
文章题目	基于可执行文件静态分析的入侵检测模型
作者	苏璞睿 杨轶
作者单位	(中国科学院软件研究所信息安全国家重点实验室 北京 100039)
发表年份	2006
发表月份	9期(1570—1576)
文章摘要	摘要 基于进程行为的入侵检测技术是主机防范入侵和检测恶意代码的重要技术手段之一.该文提出了一种基于可执行文件静态分析的入侵检测模型，该模型通过对应用程序可执行文件的静态分析，建立应用程序所有可能执行的定长系统调用集合，通过实时监控进程执行的系统调用序列是否在该集合中实施检测.该模型不需要源文件、大规模训练数据，通用性和易用性好；在应用程序可执行文件完整的情况下，误报率为0，抵抗模仿攻击的能力更强，漏报率更低. 关键词 入侵检测；系统调用；静态分析 中图法分类号 TP309