西安电子科技大学学报　2007 34 (6): 887-894　ISSN: 1001-2400　CN: 61-1076/TN

# 利用多线程技术改造Snort系统

林国庆, 王新梅

(西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

收稿日期　修回日期　网络版发布日期 2007-11-19　接受日期

摘要　Snort是一个基于规则的轻量级网络入侵检测系统．为提高Snort系统的性能，针对其工作流程是单线程的特征，用处理模块间设置缓冲队列、各个协议解码器和链表节点设置忙闲标识等方法实现了对其的多线程改造，并详细描述了改造后系统的工作流程，最后结合简化模型模拟实验结果，分析了改造前后的系统各性能的变化．改造后的系统在检测速度和漏检率等性能方面有所提高，但也增加了CPU的工作量和内存的使用量．

关键词　网络安全 Snort 网络入侵检测系统 多线程 Snort工作流程

分类号 TP393

## Reform of the Snort system by the multithreading technique

LIN Guo-qing,WANG Xin-mei

(State Key Lab. of Integrated Service Networks, Xidian Univ., Xi′an 710071，　China)

**Abstract**

The Snort system is a lightweight network intrusion detection system based on rules. In this paper, the principle, the basic structure and the workflow of this system are analyzed. Aiming at the Snort system working in a single thread, a reform scheme based on the multithreading technique for developing its performance is put forward, including a queue between two function modules and a busy sign flag in every decoder and chain node. The workflow of the reformed system is described then. Finally, the performance of the reformed system is analyzed theoretically associating with the result of a simulated experiment with a simplified model, which shows the detection efficiency is increased and the rate of miss-detection is decreased, but the workloads of CPU and the computer memory are increased. <BR>

**Key words** network safety Snort network intrusion detection system multithreading Snort workflow

DOI:

通讯作者

扩展功能

本文信息

- Supporting info
- PDF(864KB)
- [HTML全文](0KB)
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 复制索引
- Email Alert
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“网络安全”的相关文章
- 本文作者相关文章
  - 林国庆
  - 王新梅