

网络、通信与安全

大规模网络安全事件预警可视化算法研究

孙艺峻, 张宏莉, 何 慧

哈尔滨工业大学 国家计算机信息内容安全重点实验室, 哈尔滨 150001

收稿日期 修回日期 网络版发布日期 2007-7-9 接受日期

摘要 安全事件的可视化是大规模网络安全宏观预警的重要组成部分。根据大规模网络拓扑的结构特点, 结合空间信息可视化领域中H3算法, 提出了对大规模网络安全事件的宏观分布特征和局部细节进行空间可视化的处理办法。最后有效应用于教育网网络安全数据的宏观显示, 实验证明为网络管理员提供了直观的显示效果并为其了解网络安全事件整体态势和从全局角度制定行之有效的控制策略提供了有力依据。

关键词 [入侵检测](#) [大规模网络安全预警](#) [安全事件](#) [可视化](#) [H3算法](#)

分类号

Study on visualization algorithm in large-scale network security precaution

SUN Yi-jun, ZHANG Hong-li, HE Hui

National Computer Information Content Security Key Laboratory, Harbin Institute of Technology, Harbin 150001, China

Abstract

Visualization of security events is an important component of large-scale network security warning. The research includes combining structural characteristic of large-scale network topology with the H3 algorithm in the field of information visualization, providing methods for visualizing the overall distribution and local details of large-scale network security events, and applying it effectively to the visualization of network security data on CERNET. Experiment results show that the methods present a sound visual effect to the network administrator to help him/her grasp the global security situation, and then work out an effective control plan in an overall perspective.

Key words [intrusion detection](#) [large-scale network security warning](#) [security events](#) [visualization](#) [H3 algorithm](#)

DOI:

通讯作者 孙艺峻 [E-mail: sunyijun@psvy518.hit.edu.cn](mailto:sunyijun@psvy518.hit.edu.cn)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(946KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“入侵检测”的相关文章](#)
- ▶ 本文作者相关文章

- [孙艺峻](#)
- [张宏莉](#)
- [何 慧](#)