安全技术

入侵检测系统的数据标准化应用研究

叶和平1,2，尚 敏1，范路桥1,2

（1. 广东科学技术职业学院软件工程系，广州 510640；2. 华南理工大学计算机学院，广州 510640）

收稿日期 修回日期 网络版发布日期 2007-4-27 接受日期

摘要 在分析入侵检测系统原理及通用入侵检测框架（CIDF）的基础上，按照CIDF的结构要求，设计了基于CIDF的入侵检测系统原型。在系统实现的内部机制上，采用链表的形式保存各类事件的完整信息并按CIDF的要求进行检测数据的标准化，为系统构件共享信息提供高效、准确的保证。结合实践，指出了用语义标识符SID扩充以适应异常检测方面的问题。

关键词 入侵检测 通用入侵检测对象 通用入侵检测框架 数据标准化

分类号 TP393.08

DOI:

通讯作者:

作者个人主页: 叶和平1;2;尚 敏1;范路桥1;2