计算机工程与应用 2008 44 (18): 113-114 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于D-S证据理论的入侵检测模型

龚琼瑶[1], 丁 宏[1], 孔 霆[2]
1.杭州电子科技大学 计算机学院，杭州 310018
2.浙江警察学院 实验中心，杭州 310053

收稿日期 2007-9-20 修回日期 2007-11-30 网络版发布日期 2008-6-16 接受日期

摘要 将数据融合理论引入到入侵检测过程，提出基于数据融合的入侵检测系统模型，并在系统模型的实现过程中应用了多Agent技术，使整个模型具有良好的扩展性。在聚类、合并、关联的数据融合过程中应用了D-S证据理论，在一定程度上解决当前入侵检测系统中存在的告警洪流、误报率高、告警之间的关联性差等问题，提高了分布式入侵检测系统的检测性能。

关键词 入侵检测系统 数据融合 D-S证据理论 Agent
分类号

Intrusion detection model based on D-S evidence theory

GONG Qiong-yao[1],DING Hong[1],KONG Ting[2]

1.School of Computer，Hangzhou Dianzi University，Hangzhou 310018，China
2.Zhejiang Police College，Hangzhou 310053，China

Abstract
This article introduces the data fusion theory into the intrusion detection process，proposes an intrusion detection system model based on the data fusion，and has applied the multi- Agent technology in the system model realization process，enable the entire model having the good extension.In the data fusion process of clustering，merging and associating this article applies the D-S evidence theory，solves the problems of warning onrush，high false reporting rate，inferior question between the warning association which existed in the current intrusion detection system，enhances the detection performance of the distributing intrusion detection system.

Key words intrusion detection system data fusion D-S evidence theory Agent

DOI:

通讯作者 龚琼瑶 gongqy1982@gmail.com