计算机应用 2006 26 (10): 2310-2314 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

基于危险模型的三级模块式入侵检测系统

赵林惠[1]; 戴亚平[2]; 付东梅[2]; 董芳艳[2];[2]

北京理工大学，信息科学与技术学院[1]

收稿日期 2006-4-3 修回日期 2006-5-30 网络版发布日期 2006-11-14 接受日期

摘要 利用危险理论和数据融合技术，提出一种基于危险模型的三级模块式入侵检测系统，并在第三级模块中提出了一种自适应决策模板算法，实现了检测模板的在线自动修正。系统的优点在于：对于利用现有知识难以给出检测结果的情况，系统将根据是否有危险信号做出判断，不但可减少误报还能改善对未知攻击的识别能力；利用自适应决策模板算法，系统的检测模板能够在线调整，不需要定期更新，使系统能适应行为经常改变的环境，也因此提高了检测未知攻击的能力。基于KDD-CUP-99数据库的实验验证了系统的有效性。

关键词 危险理论 危险模型 入侵检测 数据融合

分类号

DOI:

对应的英文版文章：6041770

通讯作者:
赵林惠 dtree_zhao@bit.edu.cn;accept_yin@hotmail.com
作者个人主页: 赵林惠 戴亚平 付东梅 董芳艳