计算机工程 2006 32 (16): 125-126,162 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

入侵检测中的归纳学习方法

刘培顺1,王学芳2

1. 中国海洋大学计算机科学系，青岛 266071； 2. 中国海洋大学数学系，青岛 266071

收稿日期 修回日期 网络版发布日期 2006-8-14 接受日期

摘要 结合使用着色Petri网和EDL语言描述攻击模型，该文给出了使用归纳学习对攻击模型进行泛化和特化操作，泛化后的模型可以检测出与已知攻击实例类似的未知攻击行为，实现了攻击知识库进行自动更新和扩展的方法。攻击实例首先使用EDL语言表述为一个攻击实例模型，对实例模型进行泛化得到攻击实例的3层概念空间，进而转化为着色Petri网模型，利用着色Petri网的运行机制对攻击行为进行检测。实验结果表明该方法对于具有相似攻击行为的未知攻击的检测非常有效。

关键词 入侵检测 归纳学习 着色Petri网 泛化 特化

分类号

DOI:

通讯作者:

作者个人主页: 刘培顺1;王学芳2