计算机工程与应用　2005下 (35期):　ISSN: 1002-8331　CN: 11-2127/TP

网络、通信与安全

（50元）（1000元）GECISM中沙盒主机的“非我”检测与分类

李珍, 王凤先, 余晓雅

河北大学数学与计算机学院

收稿日期 2005-1-20　修回日期　网络版发布日期　接受日期

摘要　对仿生免疫系统GECISM(General Computer Immune System Model)，沙盒主机是其中的一个主要代理。详细介绍了沙盒主机中对“非我”检测与分类的结构。通过定义安全相关调用，对采集形成的安全相关调用短序列进行训练，生成序列库和规则库，从而对 “非我”进行检测和分类，同时对测试程序“非我”类型的分布进行了讨论。实验证明了用此方法进行“非我”检测和分类的可行性和高效性。

关键词　计算机免疫系统,系统调用序列,“非我”,检测,分类,分布

分类号

Detection and Classification of “Non-self” in Sand Box of GECISM

,,

河北大学数学与计算机学院

Abstract

Sand box is a main component of agents in GECISM. The structure of detection and classification of “non-self” in sand box is introduced in detail. The concept of system call related to security is defined, and sequence library and rule library are built by training short sequences of system call related to security. Then “non-self” can be detected and classified, and the distributing of different types of “non-self” in testing program is discussed. The experiment verifies the feasibility and effectiveness of this method.

Key words computer immune system　sequence of system call　“non-self”　detection　classification　distributing

DOI:

通讯作者　李珍　livf livflivf@126.com

扩展功能

本文信息

- Supporting info
- PDF(0KB)
- [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“计算机免疫系统,系统调用序列,“非我”,检测,分类,分布”的 相关文章
- 本文作者相关文章
  - 李珍
  - 王凤先
  - 余晓雅