

图书基本信息

书名：<<信息与网络安全研究新进展-全国计算机安全学术论文集（第二十五卷）>>

13位ISBN编号：9787312025464

10位ISBN编号：7312025463

出版时间：2010-9

出版时间：中国科学技术大学出版社

作者：中国计算机学会计算机安全专业委员会 编

页数：430

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

前言

一年一度的全国计算机安全学术交流会就要如期召开了，这是中国计算机学会计算机安全专业委员会第25次年会，也是中国计算机学会计算机安全专业委员会每年的头等重要大事，还是全国计算机安全领域中技术、研究、管理人员的盛会。

人们期待着会议的召开，期待着在会议上交流各自的真知灼见，汲取信息安全知识的营养，寻求醍醐灌顶之功效。

因此，计算机安全界人士对会议的召开翘首以待。

当今的时代，年年都不相同，都不重复，每年都有着当年的深刻的烙印。

这样的规律年复一年地重复着。

今年，与往年的不同之处尤为鲜明，中国世纪企盼的世博会，其举办的盛大与祥和重叠在玉树地震与舟曲泥石流的伤痛之上；今年长时间的骄侈的阳光和高温、大范围肆虐的暴雨和洪水、突如其来的塌方和泥石流，这一系列超越以往的天灾重重地冲击着人们所享受着的太平盛世，让人们在身上深深地烙上了“企盼安全”的烙印。

摆在面前的严酷的事实告诉我们，生命的脆弱，不仅仅是表现在老天爷的面前，更重要的也更不应该看到的是表现在缺乏安全防范意识上面。

我们知道，当今的世界，已经分成了两个完整的世界，一个是物理世界，是由原子构成的满足物质不灭定律的真实世界；一个是虚拟世界，是由数字构成的满足幂率模型及小世界模型的网络世界。

但是，所有物理世界的现象在网络世界上都有着相应的投影，安全更不例外。

物理世界的安全教训有着十足的理由来给网络世界以警醒，安全的防范意识及手段必须深深地烙在人们的心底，才能够让网络世界变成太平盛世。

尽管网络世界中没有泥石流、没有暴风骤雨、没有洪水的现实威胁，但却有着僵尸网络、拒绝服务攻击、域名劫持等等破坏程度的威胁；尽管网络世界中没有地震带、不稳定区等现实隐患，但有着物联网、三网融合、云计算等新兴事物，有着在安全方面尚不明确的未知因素。

因此，这一切都需要我们这些信息安全领域的人员为之而付出辛苦。

内容概要

本书为“全国计算机安全学术交流会议”的论文集，由中国计算机学会计算机安全专业委员会编著，本卷为第二十五卷，全书收录了基于遗传算法和LSSVM的网络安全事件发生频率预测、一种跨安全域安全交换平台的实现、一种高效的OLAP最值查询算法等八十余篇论文。

书籍目录

1 基于遗传算法和LSSVM的网络安全事件发生频率预测2 一种跨安全域安全交换平台的实现3 一种高效的OLAP最值查询算法4 单元环上的多方并发签名5 基于Windows内核的服务器安全检测系统6 LT码的性能分析与研究7 基于模糊层次法的网络态势量化评估方法8 逆向工程之软件破解与注册机编写9 基于语义的违法上网行为旁路阻断系统的设计与实现10 B/S环境下反网络钓鱼双向身份鉴别系统的设计与实现11 基于RFID的物联网安全需求研究12 基于YAFFS文件系统的数据恢复13 高速网络数据包新捕获方法研究14 基于CVFDT入侵检测技术的研究15 基于状态的Fuzz测试模型设计与实现16 基于vSphere的安全管理套件17 一种改进的确定有限自动机入侵检测算法研究18 对IMS的DoS攻击检测和防御机制19 基于Windows的现代木马技术研究和分析20 Web应用风险扫描的研究与应用21 基于资源的集中式P2P网络节点测量研究22 基于UIMAAS的文本挖掘系统的性能分析与评估23 在线Web挖掘中的计算资源动态平衡24 基于Hadoop的并行化命名实体识别技术研究与实现25 漏洞库发展现状的研究及启示26 基于PKI的跨域边界信任计算方法27 基于ActiveX漏洞模拟机制的网页木马检测方法28 基于CAAR算法的文本倾向性分析技术29 一种动态细粒度跨域访问控制模型30 基于小波子带EM矩特征的隐写分析方法31 基于数据流管理系统的网络安全事件多维分析32 网页木马场景展示与辅助分析技术研究33 一种基于动态指令流的恶意程序检测方法34 一种恶意代码评估和预测方法的研究35 无密钥托管的基于身份加密36 浅谈基于海量样本的恶意程序自动鉴别技术37 云安全的信任管理研究38 基于朴素贝叶斯方法的邮件样本预筛选39 电子商务中基于相似信任度的信任协商机制研究40 基于推理机的网络安全事件关联分析及实现41 计算机取证中数据恢复的特点、难点和解决方法42 计算机取证中的数据恢复技术研究43 电子证据监督链可视化平台研究44 计算机动态取证技术的挑战45 视频监控安全接入系统研究实现46 模糊综合评判法在网络安全控制效能评估中的应用研究47 网络安全事件关联规则的自动化生成方法研究与实践48 基于Hadoop的网络安全日志分析系统的设计与实现49 一种电子商务环境下面向服务的信任机制50 恶意软件防治产品检测技术和标准的研究51 对突破网络审查之技术及软件的总结与思考52 垃圾邮件与反垃圾邮件新技术追踪53 信息安全事件在安全评估中的定性与定量作用分析54 构建OA系统安全评估及保障体系55 浅析可信计算在商用平台下的应用56 网络舆情现状分析与引导机制研究57 Fast-flux服务网络可用性研究58 NFC手机支付技术安全性浅析59 “智慧地球”的战略影响与安全问题60 网络安全指标体系合理性评估研究61 等级测评中主机安全配置检查方法研究62 对行业部门中移动数据业务安全问题的思考63 浅析CDP技术与CDP应用价值64 可信计算定义初探65 一种高信度计算平台的设计与实现66 科研信息化安全保障体系建设方案67 Xen虚拟显卡共享帧缓冲区安全漏洞分析68 浅谈计算机内存数据获取及分析69 一种简单实用的移动通信终端监管新实现方法70 浅谈检察机关自侦工作中的计算机取证71 我国政务终端安全桌面核心配置标准研究72 电子文件鉴定综述73 需要关注在网络空间中的“军备竞赛”74 Botnet网络组织机制研究75 透视美国《国家网络安全综合计划(CNCI)》76 关于我国为保护青少年对手机网络内容监管的思考77 上海车牌拍卖系统被攻击案的证据审查和启示78 美国网络入侵信息披露制度简介79 网络服务提供商的社会责任研究80 实行网络实名制,规范“虚拟社会”81 论打击网络虚拟财产盗窃82 网络实名制有利于现阶段中国互联网发展83 网络实名制势在必行

章节摘录

插图：随着网络技术和网络规模的不断发展，网络遭到入侵的风险性越来越高，网络安全已经成为一个全球化的重要课题。

在网络安全问题日益突出的今天，如何迅速、有效地发现各种入侵行为，对于保障系统和网络资源的安全显得十分重要。

随着模式匹配技术的发展，自动机已经在入侵检测技术中得到广泛应用。

自动机具有灵活、高效等特点，在模式匹配时比字符串表现得更加优异。

但是在实际应用网络中，一个典型的模式集合往往需要上百个自动机和数以万计的状态组成。

传统的基于自动机的入侵检测算法为了达到最佳的匹配速度，将整个模式集合构造成一个自动机，以至于需要数百兆，甚至上千兆字节的运算空间支持。

这就极大地影响了检测算法的效率，在现实应用中是很难被接受的。

针对这种情况，本文提出了一种改进的基于确定有限自动机的入侵检测算法，并且通过实验数据验证了本文提出的算法能在不增加入侵检测算法的运算时间的前提下，极大地减少算法所需的运算空间。

2入侵检测与确定型有穷自动机入侵检测（Intrusion Detection）是用于检测任何损害或企图损害系统的保密性、完整性或可用性行为的一种网络安全技术。

入侵检测提供了用于发现入侵攻击与合法用户滥用特权的一种方法。

入侵检测按照其检测方法来看，可以分为三类：基于行为的入侵检测、基于模型推理的入侵检测和采用两者混合的入侵检测。

基于行为的检测指根据使用者的行为或资源使用状况来判断是否有入侵，而不依赖于具体行为是否出现来检测。

基于模型推理的入侵检测根据入侵者在进行入侵时所执行的某些行为程序的特征，建立一种入侵行为模型，根据这种行为模型所代表的入侵意图的行为特征来判断用户执行的操作是否是属于入侵行为。

当然这种方法也是建立在对当前已知的入侵行为程序的基础之上的。

目前，基于模型推理的入侵检测是应用最广泛的。

编辑推荐

《信息与网络安全研究新进展·全国计算机安全学术交流会论文集(第25卷)》是由中国科学技术大学出版社出版的。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>