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

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、域名劫持等同等破坏程度的威胁；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

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