<<信息和通信安全>>

图书基本信息

书名：<<信息和通信安全>>

13位ISBN编号：9787030245144

10位ISBN编号：7030245148

出版时间：2009-6

出版时间：科学出版社

作者：胡爱群　主编

页数：884

<<信息和通信安全>>

前言

第六届中国信息和通信安全学术会议（CCICS ’2009）由东南大学、南京大学、南京邮电大学、解放军理工大学、江苏省网络与信息安全重点实验室共同主办，本次会议共收到论文投稿200篇，每篇论文经过初审、修改和终审三个环节，共录用论文150篇。
本论文集内容涉及密码技术、网络（包括互联网、通信网、无线网络等）安全技术、内容安全技术、系统安全及软件安全技术、电磁辐射与涉密信息检查保护技术、电子对抗技术、安全应用技术等方面的研究课题。
这些论文集中反映了我国当前在信息和通信安全理论与应用方面的研究动态与创新成果，对从事信息和通信安全方面的研究具有重要的参考作用。
我们衷心感谢所有支持本次会议的论文作者，感谢曾庆凯、吴蒙、齐望东、罗军舟等程序委员会委员及论文评审专家为评审论文付出的艰辛劳动，感谢东南大学信息科学与工程学院的大力支持，感谢罗德与施瓦茨、思博伦、安捷伦、TILERA等公司的友情赞助，感谢东南大学信息安全研究中心的老师们和同学们为组织本次会议及处理会议事务所付出的努力.感谢本次会议主席冯登国教授以及IEEENanjingSection主席何振亚先生对本次会议各项工作的指导，感谢本次会议的共同主办单位东南大学、南京大学、南京邮电大学、解放军理工大学、江苏省网络与信息安全重点实验室为筹办本次会议所做的很多工作。
感谢江苏省电子学会的大力支持。
正是由于各方面的努力，才使得本次会议可以顺利进行。

<<信息和通信安全>>

内容概要

本书为第六届中国信息和通信安全学术会议论文集，收录论文150篇，涉及信息和通信安全技术的各个领域，内容包括：密码技术、网络(包括互联网、通信网、无线网络等)安全技术、内容安全技术、系统安全及软件安全技术、电磁辐射与涉密信息检查保护技术、电子对抗技术以及信息安全应用技术等。

本书可供从事网络、通信与信息安全方面研究的科技人员和高等院校相关专业的师生参考。

<<信息和通信安全>>

书籍目录

安全性增强技术研究　基于状态转换的SIP代理服务器容侵技术研究　连续数据保护研究　恶意代码自动分析技术研究　Win32环境下恶意代码行为分析实验及思考　基于嵌入式系统的移动视频监控终端及平台安全性　基于扩展的不干扰模型的系统完整保护研究　基于语义抽象的内存访问错误检测　基于虚拟机监控的系统完整性保护　利用流量矩阵识别DDoS攻击源　可信移动Agent的研究及在分布式网络管理中的应用　基于云安全的入侵检测模型　基于粗糙集的最小风险贝叶斯垃圾邮件过滤算法　基于DNS日志分析的网络异常检测系统的设计与实现　基于滑动窗口技术计算网络节点对可靠性　移动Ad Hoe网络的可靠性评估方法研究　基于MHC的恶意代码检测方法　基于暗网的蠕虫检测系统的性能　多源流量特征分析方法及其在异常检测中的应用　ESR：一种能量有效的安全的传感器网络路由协议　用于大规模暗网监测的蠕虫诱捕蜜罐　僵尸网络生存性研究　基于SDIO接口的智能移动安全终端系统设计　实用安全WMN的设计与构建　NP防火墙中异常策略检测的研究与实现　P2P僵尸网络的跟踪与测量：Storm Worm实例研究　面向安全态势的权限有效性定量评估方法研究　基于Hurst参数的网络异常流量动态自适应实时检测　基于安全服务的移动网络统一安全防护体系　一种p元扩域上的快速乘法第四部分 安全应用技术　基于FPGA的3G网络数据分流系统　TD-SCDMA中基于分布式系统负载均衡的内容监管方式　一种有利于消除阴影的监控视频对象提取方法　一种更安全的RKE系统设计与实现　基于Qt的无线网络监测系统的界面　短距离高精度无线定位方法的研究及实现　继电保护定值远程安全配置系统的设计与研究　基于报文转发时延的传感器网络拓扑发现算法　基于攻击树模型的信息系统脆弱性分析　电力系统网络监管技术的研究与实现　一种基于miniSI)接口的信息安全模块　基于IP网的煤矿井下无线语音通信系统及协议　与SPIN相关的模型检测研究　基于移动终端的VPN安全访问控制　面向蓝牙病毒采集的移动蜜罐研究与设计　基于灰色关联决策算法的信息安全风险评估方法　异常检测在报警关联分析中的应用

章节摘录

插图：一、引目Ad Hoc网络由于不需要固定的基础设施，可以快速架设、布置，因此在一些特殊的应用环境中发挥至关重要的作用.路由协议作为Ad Hoc的重要核心问题，其安全性在整个网络的安全中更是有着极其重要的地位。
现有的Ad Hoc网络的路由协议大都建立在节点之间相互协同的假设之上，节点之间具有完全的信任关系，自愿为其他节点转发分组，然而现实情况并非如此，一方面，一些节点为了节约自身有限的资源，表现出一定的自私行为，另一方面，一些恶意节点为了破坏网络的正常运行，通过发布错误的路由更新和路由信息来实现其恶意攻击的目的。
因此，安全路由协议必须能有效应对这两种不合作节点，对保证节点的协同性有更多考虑。
本文第二节对Ad Hoc网络现有的一些经典安全路由协议进行了分析，总结出各种方案的优点和缺陷；第三节提出了一种基于声誉机制的协同安全路由协议CE-AODV，并对该协议进行一定的性能评价；最后对全文进行总结，提出进一步的研究方向和工作展望。
二、Ad Hoc网络传统安全路由算法的比较及存在的问题表工对现有传统安全路由协议从安全技术、基本路由协议、优缺点等几个方面进行了比较，发现它们共同存在以下几个方面的问题：1）传统安全路由算法计算量和处理强度太大，消耗能量过多，不符合Ad Hoc网络资源和处理能力有限的特点.2）传统安全路由协议缺乏对节点协同激励和惩罚机制的考虑，对不安全因素缺乏强有力的全面的抵制，对节点不良行为的应对措施还不够。
3）传统安全路由协议无法鉴定源节点的IP地址，恶意节点可通过更改其MAC地址或IP地址轻松达到恶意攻击的目的。

<<信息和通信安全>>

编辑推荐

《信息和通信安全:CCICS'2009第六届中国信息和通信安全学术会议论文集》是胡爱群编写的，由科学出版社出版的。

<<信息和通信安全>>

版权说明