

<<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

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>

## <<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IEEE Nanjing Section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。

## &lt;&lt;信息和通信安全&gt;&gt;

## 书籍目录

第一部分 网络与通信安全 一种基于形式化描述的测试案例生成方法 微内核操作系统中虚存管理系统的设计 对Diameter基于EAP认证的性能分析 一种终端状态评估模型的安全机制 Formal Analysis of Robust E-mail Protocol Based on Authentication Tests 基于扩展串空间模型对802.11i四步握手协议的分析 可信的捐赠监督方案 基于身份的有向签名 基于多重分组的并行认证模式 面向认证认可的信息安全产品分类方法研究 一种计算网络告警因果关联置信度的新方法 基于声誉激励的Ad Hoc网络协同安全路由协议 一个基于全局信任值和局部信任值的P2P信任模型 两种形式化模型的安全性分析 结构化对等网中平均可用容量的分析 A Survey: Polynomial-Based Key: Pre-distribution Schemes in Wireless Sensor Networks 一种基于活动目录的Web认证与授权机制 无线传感器网络的PKI体系设计 一种适用于Ad Hoc空间网络的IPSKC密钥管理方案 基于智能代理的远程控制技术研究 ECDSA可公开验证广播签密 一种基于ElGamal密码体制的重加密方案的改进 一类椭圆曲线密码强指定验证者签名方案 正规性和代数免疫 面向蜜场环境的网络攻击流重定向机制的研究与实现 一个高效的无证书盲签名方案 WiMAX设备中密码算法工程实现的研究 基于可信分布式系统的可信认证技术研究 无线传感器网络中具有撤销功能的自愈组密钥管理方案 AES列混合变换的研究 MICKEY流密码算法的能量攻击 Strong Designated Verifier Signature Scheme with Non-delegatability 一种基于TOR的MANET强匿名路由协议 G-Hordes: 一种安全的匿名通信系统 实现位置及时间绑定的密钥分发——防御传感器网络节点复制攻击的新方法 基于二次剩余问题的部分盲签名协议可证安全 基于GSM网络端到端加密通信的认证密钥交换协议设计 面向CDMA2000网络的信息监管平台前置机设计与实现 基于MSA协议的WLAN Mesh网络的安全体系研究 MMS协议分析系统的设计与实现 Cluste Algorithm for Wireless Sensor Networks Based on Residual Energy and Position MESH型网络组网试验研究 P2P中一种基于数字认证的匿名信誉机制 无线传感器网络中的追踪组播密钥管理机制研究 An Improved Self-healing Key Distribution in Wireless Sensor Network 匿名通信时间攻击的时延规范化防御方法 LTE与UTRAN的切换安全研究 动态密钥托管方案研究 一个基于Ham(r, q)的动态群秘密共享方案 -LFSR序列的圈结构 一种半诚实环境中的多方安全距离比较协议 基于交叉耦合映像格子的单向Hlhash函数构造

第二部分 内容安全 基于FPGA的3G流媒体监控技术 利用分形维数对计算机生成图像的鉴定 基于SIFT的图像复制遮盖篡改检测技术 抗攻击的增强安全路由协议ESRP研究 控制流监控在程序漏洞定位中的应用 射频指纹的产生机理与唯一性 视频镜头的底层特征以及语义分析 基于聚类的Ad Hoc网络入侵检测研究 融合韵律特征的汉语方言辨识 基于小波变换和PDE插值的图像超分辨率重建 一种局部线性嵌入降维的图像隐密检测 服务发现安全问题的研究与进展 利用异常边缘进行图像锐化篡改取证 一种基于DCT域QIM的音频信息伪装算法 一种抵抗插值误差的数字水印方法 基于网格环境的隐私信息保护机制研究 基于报文间隔抖动的网络隐蔽通道信息传递速率估算 基于概念网的文本特征网络图分析 一种基于Bi-gram和HMM的中文未登录词辨识方法 基于非负矩阵分解的数字图像水印算法 移动互联网审计过滤机制分析与测试 一种面向主题重叠情况的文本特征辅助选择模型 动态页面采集关键技术研究 一种IP可追踪性的网络流量异常检测方法 OFDM-based Secure Data Communications over GSM Voice Channel 基于边缘CFA内插特征一致性的图像拼接检测 一种网页防篡改系统中的关键技术 DCT域实现篡改定位的半脆弱水印算法 一种基于SD接口加密的移动通信端到端安全方案及其实现 一种基于无监督学习的MB1隐写分析方法 基于新颖直方图特性的音频水印算法研究 基于局部保持映射的音频数字签名算法 基于协议特征的数据恢复算法 基于粒子群算法和改进PM1的JPEG图像中的安全密写方法 分布式信源编码码率损失的新上界 一种基于对称加密和隐写术的反取证方法 共享加密文件系统的安全机制 基于像素能量分布的自适应差分能量水印算法 基于可变窗的镜头边界检测算法 基于视觉和音频特征的恐怖暴力场景识别算法 一种基于安全标签的网络访问控制系统设计与实现 图像垃圾邮件中文本区域的自动提取方法

第三部分 系统安全及软件安全 基于发送功率的无线网络可靠性分析 基于17PM的安全启动设计 3GPP LTE区间安全切换技术研究 无线网状网络的安全问题 Synthetic Security Assessment Based on Variable Precision Rough Set 信息安全系统软件开发的工程化研究 程序静态分析工具的分类研究 基于频繁模式挖掘的网络流量监测 慢速DoS攻击检测与防御机制研究 VoIP网络

## &lt;&lt;信息和通信安全&gt;&gt;

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 Hoc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。

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>