第一图书网, tushu007.com

<<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：9787030193124

10位ISBN编号：7030193121

出版时间：2007-7

出版时间：科学出版社

作者：谢冬青等

页数：404

字数：610000

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

第五届中国信息和通信安全学术会议由湖南大学主办，国防科技大学协办，于2007年7月在长沙召开。
本书收集了在这次会议上报告的63篇论文，内容涉及密码学、网络安全、信息隐藏与数字水印、电子商务安全等研究课题。
这些论文反映了我国当前在信息安全领域的研究动态，也展现出我国信息安全研究与应用的学术水平。
本次会议共收到投稿论文212篇，每篇论文至少由两位专家审评，录用论文63篇。
我们衷心感谢所有向本次会议投稿的作者对会议的关心与支持。
由于受文集篇幅所限，向论文未能被收录的作者表示歉意；感谢程序委员会的所有成员，他们为从众多的稿件中选出更具代表性的论文参加会议交流而做了大量的工作。
我们还要感谢会议的主办单位——湖南大学，感谢协办单位——国防科技大学，他们在本次会议的筹备和组织中做了很多工作。
正是由于各方的共同努力，本次会议才得以顺利进行。
最后还要感谢科学出版社责任编辑鞠丽娜女士为会议论文集的出版做了大量细致而繁琐的工作。
本论文集的出版得到了科学出版社的大力支持，在此向他们表示衷心的感谢。

第一图书网, tushu007.com

内容概要

本书为第五届信息和通信安全学术会议论文集，收录论文63篇，内容涉及信息和通信安全的各个领域，包括密码学、网络安全、信息隐藏与数字水印、电子商务安全等。

本书可供从事信息安全、密码学、计算机、通信、数学等专业的科技人员和高等院校相关专业的师生参考。

书籍目录

密码学　序列密码的局部线性复杂度　F4上n元n-1阶相关免疫逻辑函数的等价条件　基于规划系统的密码协议安全性验证机制研究　Correlation Attack on Stop／Go Clocked Combiners with Memory Based on Posterior Probability　A New Type of Group Blind Signature Scheme Based on Bilinear Pairings　Efficient Countermeasures Against Side-channel Attacks on Elliptic Curve Cryptosystems　WAPI认证和密钥交换协议的安全性分析　动态对等群中基于身份及口令认证的密钥协商方案　广义正形置换的Chrenstenson谱特征和自相关函数特征　关于布尔向量函数的非线性度　On 9 Absolute Fixed Points of RSA　基于EPR纠缠态的量子签名方案　基于离散对数问题的分散式组密钥管理方案　基于身份的多用户密钥协商协议　基于植物叶脉特征提取的流密码产生方法　模2n剩余类环上加法运算的差分性质　具有高非线性度的弹性函数的构造　模差分与异或差分的性质及其应用　一个安全的基于广播加密的会话密钥分配新方案　一类偶数元代数免疫最优布尔函数的构造　一种基于H.264的多安全级视频加密方案　一种新的基于身份的门限代理签名方案　一种新的双环形OCDMA-PON无源光接入方案　有理分式公钥密码体制　环乙上圆锥曲线RSA型公钥密码体系的小私钥指数攻击　An Improved Three-party Password-based Key Exchange Protocol Using Weil Pairing。
Blind Quadruple Watermarking Scheme Robust to Geometric Distortions　A Trusted Cluster-based Algorithm Based on LEACH for Wireless Sensor Networks　一个基于身份的认证群密钥协商协议的安全性分析　确定周期为p-的二元周期序列的差错序列的一个算法　基于H.264的信源选择加密方案研究　一种基于陷门置换的多重签密模型　基于Groebner基的改进XL算法　协同环境下基于委托的动态信任模型　IPSec与NAT协同工作的研究及改进　基于L-模糊集的网格信任模型的研究　基于可信计算的汽车电子控制系统维护认证方案　拟Bent函数的构造网络安全　一个基于DTE和平台证明的网络强制访问控制形式模型　A Practical Algorithm for Modeling Computer Based Attacks Using Network Entropy　一种可生存性增强的网络信息系统体系结构设计　航电分布式管理软件中的密钥管理与认证方案　拒绝服务攻击源端快速检测方法　一种通用Shellcode变形引擎框架的设计与实现　安全操作系统测评系统的研究与实现　基于NiosII的安全通道的应用研究　基于查找的分散式角色激活管理　基于粗糙集和行为分析的计算机病毒检测　基于海明神经网络的未知多态病毒检测　基于可信计算的一个内网身份认证方案　计算机生态系统安全宏观进化思考　下一代网络信令流量正常行为混沌模型研究　一个可信文件系统TrustedFS的设计与实现　机载综合核心处理系统安全技术研究　一种基于端址跳变的DoS主动防御策略　一种基于算法优化的桌面数据备份系统　一种检测恶意软件的统计方法　用基于规则的贝叶斯算法实现网络钓鱼的过滤　Face Recognition Based on Discrete Cosine Transform and Support Vector Machines信息隐藏与数字水印　一种新的半脆弱图像认证水印算法　基于SVR和HVS的自适应图像数字水印算法　基于边缘检测的脆弱水印电子印章系统电子商务　指定验证人签名及其在电子商务中的应用

章节摘录

插图：三、安全测评系统的设计原理3.1 测评原理及流程评估测试的发起源于用户的申请，控制端用该请求激发核心数据驱动引擎，使引擎根据驱动表集中的测试驱动表格依次从知识体系库中取出测试数据、从组件库和系统支持库中取出测试脚本和通用例程，从而形成符合用户需求的一个自动化测试套件，该套件通过测试端完成对操作系统的测试，测试完成后将测试结果放回知识体系库，由评估测评器根据知识体系库中的预期结果，与测试结果进行比较，并依据测评标准通过评估算法生成测评报告以提交给用户。
3.1.1 组件库与系统支持库组件库用来存放各种测试脚本和程序，并且各种脚本和程序的层次相对独立，利于组件库的配置和管理。
系统支持库用于存放各种通用的标准和通用的例程以及通用安全测试工具程序（例如漏洞扫描工具、隐蔽通道工具、渗透测试工具等）。
步进驱动表格指导测试脚本的测试过程，而测试目的由测试数据决定和实现。
脚本通过步进驱动表格来取得所需的测试数据、预期结果、测试结果文件名。
脚本测试从数据文件中读取测试数据记录然后执行以数据记录内容为基础的动作。
在测试脚本中，可能会出现同一测试场景的不同测试输人，因此需要循环驱动表格读取每个测试数据记录，测试将继续进行直到没有数据记录要处理。

编辑推荐

《信息和通信安全-CCICS'2007第五届中国信息和通信安全学术会议论》：第五届中国信息和通信安全学术会议由湖南大学主办，国防科技大学协办，于2007年7月在长沙召开。
《信息和通信安全-CCICS'2007第五届中国信息和通信安全学术会议论》收集了在这次会议上报告的63篇论文，内容涉及密码学、网络安全、信息隐藏与数字水印、电子商务安全等研究课题。
这些论文反映了我国当前在信息安全领域的研究动态，也展现出我国信息安全研究与应用的学术水平。
本次会议共收到投稿论文212篇，每篇论文至少由两位专家审评，录用论文63篇。

第一图书网, tushu007.com

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