

图书基本信息

书名：<<信息与网络安全研究新进展 (第23卷) >>

13位ISBN编号：9787312022777

10位ISBN编号：7312022774

出版时间：2008-9

出版时间：中国科学技术大学出版社

作者：中国计算机安全专业委员会 组编

页数：452

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

2008年对我们国家来说是极其特殊的一年,既有“1.25”南方凝冻灾害给地方经济带来的灾难,又有“3.14”事件给社会稳定带来的冲击,还有汶川大地震给人民群众带来的创伤;更有北京奥运会给中国带来的历史性的机遇,让中国站在了改革开放的一个新的起点。

在这特殊的一年里,这一系列特殊的事件都紧紧地围绕着这样一个术语:“安全”。

凝冻灾害涉及的是经济安全,“3.14”事件涉及的是政治安全,汶川大地震涉及的是人身安全,北京奥运会涉及的是信息安全。

事实上,所有这些事件,都与我们的学术领域密切相关:凝冻灾害需要的是应急处理与通信安全技术,“3.14”事件需要的是信息内容安全技术,汶川大地震需要的是系统容灾与数据灾备技术,而北京奥运会需要的则是网络安全技术。

在举世瞩目的北京两奥会闭幕之后的一个月,由中国计算机学会计算机安全委员会主办和中国电子学会计算机工程与应用学会计算机安全保密学组协办的第23届全国计算机安全学术交流会将于10月12日至14日在上海松江举行。

我们从征集到的各位同仁一年来辛勤工作的结晶——学术论文中,细心遴选了88篇论文汇编成《全国计算机安全学术交流会论文集(第二十三卷)》呈献给大家。

内容概要

在举世瞩目的北京两奥会闭幕之后的一个月,由中国计算机学会计算机安全委员会主办和中国电子学会计算机工程与应用学会计算机安全保密学组协办的第23届全国计算机安全学术交流会于10月12日至14日在上海松江举行。

本书编者从征集到的各位同仁一年来辛勤工作的结晶——学术论文中,细心遴选了88篇论文汇编成《全国计算机安全学术交流会论文集(第二十三卷)》呈献给大家。

本书涉及物理安全、网络安全(系统安全、计算机安全)、数据安全(保密)、内容安全等各领域的内

容。

书籍目录

2008年上半年网络安全形势分析报告
2008年中国计算机病毒疫情调查技术分析
2007~2008年度信息安全产品检测概况
跨系统可信互联安全体系研究
一个基于TPM芯片的可信网络接入模型
一种新的匿名路由器问题解决方案
基于多层次多角度分析的网络安全态势感知
基于随机掩码的AES算法抗DPA攻击硬件实现
OO登录协议安全性研究与分析
基于组合对称密钥的机密数据存储和传输研究
涉及P2P软件案件调查取证方法的研究
欧美电子监听技术标准研究
浅探电子商务领域的黑客犯罪
涉密移动存储介质在检察机关应用的防护策略
我国网络实名制立法方向和实现模式
初探网络模拟工具在网络安全试验中的应用
基于主动探测技术的P2P网络监控
一种软件实现的瞬时故障检测方法
基于可信分布式系统的可信认证技术研究
可信计算技术及管理策略比较研究
一种被动式监测信息攻击的新实现方式
利用色彩一致性的数字伪造图像取证方法
基于故障注入的信息系统安全漏洞检测技术研究
文件过滤驱动技术监控系统的设计与实现
基于藏文网页的网络舆情监控系统研究
在J2EE框架下基于LDAP实现RBAC模型面向服务软件架构中的软件测试
数字水印技术的研究
基于M-gent的数字水印检测研究
支持互操作和隐私保护的统一用户认证平台
DRM系统密钥两地存储封装策略研究
一种基于复倒谱变换的自同步音频水印算法
一种MPEG-4视频半脆弱水印认证方案
基于Multi-SVM的网络入侵检测技术研究
一种基于SIM卡的Windows mobile双因素用户认证技术
基于内容的Internet信息过滤方法研究
综述基于NDIS中间层驱动的模拟分布式网络设备测试平台
检察机关专线网络安全分析
对检察机关网络安全架构若干问题的简要分析
浅析如何做好检察机关网络信息安全工作
浅谈借助于计算机病毒危害军队信息安全及其防范
校园网安全探析
浅析检察专线的网络安全
加强内部网络安全的几点思考
SSL协议及其在网络访问中的应用
IPv6过渡期拒绝服务攻击防护
基于文件系统过滤驱动的文件访问控制技术
研究基于身份验证的无线网络网络安全
研究网络协同攻击检测方法
研究无线传感器网络路由协议安全及简化方案
校园网资源管理系统网格体系设计
一个基于NS2的拒绝服务攻击与防御模拟系统
云计算与计算机安全
一种恶意网页检测系统的研究与设计
恶意代码检测技术的研究
打击计算机犯罪
几点思考
移动Agent交易实体间的信任和声誉研究
生物特征加密技术现状与发展趋势
电子证据的证明力研究
Win32环境下恶意代码行为分析技术研究
及实验测试床系统在信息安全领域中的应用与分析
基于主机与网络协同的僵尸网络事件验证技术
基于流量穿越的防火墙在线安全测试系统
基于智能卡和一次性口令技术的身份认证方案
研究信息系统集成中安全级别集成方法
研究涉密网络布线工程设计与施工
一种基于USBLKey的流媒体安全传输方案
电子政务系统中基于策略的访问控制研究
面向移动环境的加密认证系统模型设计
二进制代码隐秘功能的安全性验证
FreeGate软件的逆向分析
计算机网络信息安全保密体系架构研究
浅析检察机关涉密移动存储介质的管理对策
检察门户网站的安全防护措施
剖析构建电子信息系统安全保密防护体系
基于依赖图的入侵检测研究
计算机取证分析工具测试方法研究
信息安全与信息法学预防和打击计算机犯罪
网络诈骗犯罪的特点及其打防对策
计算机黑客行为的罪与罚
预防和惩治网络犯罪机制探索
电子证据的可采性研究
职务犯罪侦查数字化队伍建设构想
浅析利用网络传播有害信息
违法犯罪证据收集固定与处罚依据
计算机取证中的数据恢复技术研究
电子地图安全显示算法设计与实现
一种基于手机拍照和Hash函数的真随机数产生器

章节摘录

插图：1 可信分布式系统的概念目前，业界虽然对可信分布式系统有不同理解，有的认为是基于认证的可信、有的认为是基于现有安全技术的整合、有的认为是分布式系统的内容可信、有的认为是分布式系统本身的可信、有的认为是分布式系统上提供服务的可信。

我们认为一个可信的分布式系统应该是分布式系统和用户的行为及其结果总是可预期与可管理的，能够做到行为状态可监测、行为结果可评估、异常行为可管理。

具体而言，分布式系统的可信性应该包括一组属性，从用户的角度需要保障服务的安全性和可生存性，从设计的角度则需要提供分布式系统的可管理性。

不同于安全性、可生存性和可控可管性在传统意义上分散、孤立的概念内涵，可信分布式系统将在分布式系统可信的目标下融合这3个基本属性，围绕分布式系统组件问信任的维护和行为管理形成一个有机整体。

实现可信分布式系统的可信性，要解决以下四个问题： 远程用户的可信性：用户可信是分布式系统安全的前提，用户可信需要落实用户身份以及用户登陆的终端系统，以便分布式系统能够根据不同的终端和用户进行不同的控制。

远程平台的可信性：平台可信性泛指平台身份可信和平台计算环境可信。

只有平台可信，分布式应用才是安全的，否则说明远程接入端要么是一个伪装的节点，要么可能被木马所控制。

远程任务的可信性：分布式应用的执行体不可能是一个整体，一定在物理上被分割为几个相对独立的模块。

这些独立的模块在执行协作任务时，需要能够验证相互问身份和行为的可信性。

只有这样，任务发起方才能明确任务是否正确无误地完成。

远程行为的可控性，解决可信分布式系统的监管问题。

与任务的可信性相对，远程行为的可控性则要求杜绝某些行为的发生，限制远程用户的使用行为。

远程行为的可控性实际还是一个权限分发和控制的问题，不过这种控制是在限制终端权限的前提下来实现整个系统安全策略的。

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23卷)》由中国科学技术大学出版社出版。

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>