



QK1902922

主管：中华人民共和国公安部

主办：公安部第三研究所

中国计算机学会（计算机安全专业委员会）

ISSN1671-1122

CN31-1859/TN

中文核心期刊

中国科技核心期刊

中国科学引文数据库来源期刊

信息安全

NETINFO SECURITY

等级保护

一种基于随机探测算法和信息聚合的漏洞检测方法

技术研究

基于改进DGHV算法的云存储密文全文检索研究

对三个无双线性对的密钥协商协议分析

一种改进的基于认证测试的形式化分析方法

理论研究

新时代下网络安全服务能力体系建设思路

ISSN 1671-1122



9 771671 112194

2019年 第1期

总第217期

□ 等级保护

- 1 一种基于随机探测算法和信息聚合的漏洞检测方法 文伟平, 李经纬, 焦英楠, 李海林

□ 技术研究

- 8 基于改进 DGHV 算法的云存储密文全文检索研究 秦中元, 韩尹, 朱雪金
- 16 对三个无双线性对的密钥协商协议分析 程庆丰, 阮展靖, 张瑞杰
- 27 一种改进的基于认证测试的形式化分析方法 姚萌萌, 朱正超, 刘明达
- 34 基于格的身份基矩阵加密方案 李明祥, 王洪涛
- 42 可证安全的高效无证书聚合签名方案 曹素珍, 郎晓丽, 刘祥震, 王斐
- 51 基于区块链的社区分布式电能安全交易平台方案 田秀霞, 陈希, 田福粮
- 59 一种基于信任的组播路由协议 李本霞, 夏辉, 张三顺
- 68 大数据平台下应用程序保护机制的研究与实现 吴天雄, 陈兴蜀, 罗永刚
- 76 基于国产密码算法的印章防伪技术研究 邹翔, 陈兵

□ 理论研究

- 83 新时代下网络安全服务能力体系建设思路 曲洁, 范春玲, 陈广勇, 赵劲涛

□ 权威分析

- 88 2018 年 11 月计算机病毒疫情分析 张超, 肖姝瑶
- 89 2018 年 11 月违法有害恶意 APP 情况报告 陈建民, 刘彦
- 90 2018 年 11 月十大重要安全漏洞分析 中国科学院大学国家计算机网络入侵防范中心
- 92 2018 年 11 月网络安全监测数据发布 郭晶, 张腾

□ 网域动态

- 94 “第九届中国信息安全法律大会”在北京顺利举行
- 95 “等级保护新标准培训班”在京举办
- 96 江南大学“物联网技术应用教育部工程研究中心 2018 年学术年会”召开
- 97 湖北省网络空间安全学会正式成立

CONTENTS

- 1 A Vulnerability Detection Method Based on Random Detection Algorithm
and Information Aggregation WEN Weiping, LI Jingwei, JIAO Yingnan, LI Hailin
- 8 Research on Ciphertext Full-text Retrieval of Cloud Storage Based
on Improved DGHV Algorithm.....QIN Zhongyuan, HAN Yin, ZHU Xuejin
- 16 Analysis of Three Pairing-free Authenticated Key
Agreement Protocols.....CHENG Qingfeng, RUAN Zhanjing, ZHANG Ruijie
- 27 An Improved Formal Analysis Method Based on
Authentication Tests..... YAO Mengmeng, ZHU Zhengchao, LIU Mingda
- 34 Identity-based Matrix Encryption Scheme Based on LatticesLI Mingxiang, WANG Hongtao
- 42 Probably Secure and Efficient Certificateless Aggregate
Signature Scheme.....CAO Suzhen, LANG Xiaoli, LIU Xiangzhen, WANG Fei
- 51 Community Distributed Power Security Transaction Scheme Based
on Blockchain TIAN Xiuxia, CHEN Xi, TIAN Fuliang
- 59 A Trust-based Multicast Routing Protocol..... LI Benxia, XIA Hui, ZHANG Sanshun
- 68 Research and Implementation of Application Program Protection Mechanism
under Big Data Platform..... WU Tianxiong, CHEN Xingshu, LUO Yonggang
- 76 Research on Anti-counterfeiting Technology of Seal Based
on Domestic Cryptography Algorithm ZOU Xiang, CHEN Bing
- 83 Research on Establishment of Network Security Service Ability System
for A New Era..... QU Jie, FAN Chunling, CHEN Guangyong, ZHAO Jintao

敬告

本期所有文字和图片未经本刊书面许可,不得转载。

本刊已被中国科技核心期刊、中国科学引文数据库来源期刊、中国学术期刊全文数据库、中文科技期刊数据库(全文版)等数据库收录,如果作者不同意文章被收录,请在来稿时向本刊声明,本刊将做适当处理。

深信服科技股份有限公司



深信服官方微信
sangfor.com.cn

深信服智安全 业务图谱



内容安全

- 上网行为管理AC
- 行为感知系统BA



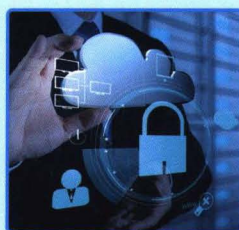
边界安全

- 下一代防火墙NGAF
- 一体化网关MIG



移动安全

- SSL VPN
- 企业移动管理EMM



云安全

- 云安全资源池
- 云端安全服务
- 云安全代理CASB



传输安全

- 硬件VPN
- 广域网优化WOC



网络空间安全

- 全网安全感知平台
- 潜伏威胁探针



深信服智安全
SANGFOR SECURITY

专注做实用的安全
让每个组织的安全建设更有效、更简单