



计算机研究与发展

(Jisuanji Yanjiu Yu Fazhan)

第 54 卷 第 10 期 2017 年 10 月

目 次

应用驱动的网络空间安全研究进展专题

前 言 曹珍富 徐秋亮 张玉清 董晓蕾 (2103)

综 述

可搜索加密研究进展 董晓蕾 周 俊 曹珍富 (2107)

格密码技术近期研究进展 张平原 蒋 瀚 蔡 杰 王晨光 郑志华 徐秋亮 (2121)

物联网安全综述 张玉清 周 威 彭安妮 (2130)

可修订数字签名研究综述 马金花 刘江华 伍 玮 黄欣沂 (2144)

隐私保护集合交集计算技术研究综述 申立艳 陈小军 时金桥 胡兰兰 (2153)

区块链隐私保护研究综述 祝烈煌 高 峰 沈 蒙 李艳东 郑宝昆 毛洪亮 吴 震 (2170)

密码安全

RAKA:一种新的基于 Ring-LWE 的认证密钥协商协议 杨亚涛 张亚泽 李子臣 张峰娟 刘博雅 (2187)

基于 LWE 的高效身份分级加密方案 叶 青 胡明星 汤永利 刘 琨 闫玺玺 (2193)

物联网环境中 LED 轻量级密码算法的统计故障分析研究 李 玮 葛晨雨 谷大武 廖林峰 高志勇 郭 箐 刘 亚 刘志强 石秀金 (2205)

一个单服务器辅助的高效 n 取 k 茫然传输协议 赵圣楠 蒋 瀚 魏晓超 柯俊明 赵明昊 (2215)

轻量级分组密码算法 ESF 的安全性分析 尹 军 马楚焱 宋 健 曾 光 马传贵 (2224)

云计算中基于身份的双服务器密文等值判定协议 吴黎兵 张宇波 何德彪 (2232)

基于强变色龙 Hash 函数的紧致安全签名通用构造 李 飞 高 伟 王贵林 谢冬青 唐春明 (2244)

系统安全

基于半监督学习和信息增益率的入侵检测方案 许勤璠 李兴华 刘 海 钟 成 马建峰 (2255)

基于 TrustZone 的开放环境中敏感应用防护方案 张英俊 冯登国 秦 宇 杨 波 (2268)

一种可信虚拟机迁移模型构建方法 石 源 张焕国 吴福生 (2284)

基于漏洞类型的漏洞可利用性量化评估系统 雷柯楠 张玉清 吴晨思 马 华 (2296)

基于 VMFUNC 的虚拟机自省触发机制 刘维杰 王丽娜 谈 诚 徐 来 (2310)

MNOS:拟态网络操作系统设计与实现 王祺鹏 扈红超 程国振 (2321)

高级持续性威胁中隐蔽可疑 DNS 行为的检测 王晓琪 李 强 闫广华 玄光哲 郭 东 (2334)

基于专家系统的高级持续性威胁云端检测博弈 胡 晴 吕世超 石志强 孙利民 肖 亮 (2344)

基于网络资源管理技术的 SDN DoS 攻击动态防御机制 王 涛 陈鸿昶 程国振 (2356)

应用密码与隐私保护

适合移动云存储的基于属性的关键词搜索加密方案 苏 航 朱智强 孙 磊 (2369)

一种安全的多帧遥感图像的外包融合去噪方案 黄冬梅 戴 亮 魏立斐 魏泉苗 吴国健 (2378)

比特币区块链扩容技术研究 喻 辉 张宗洋 刘建伟 (2390)

业务流程授权约束依从性分析 薄 阳 夏春和 (2404)

编者专栏

《信息安全研究》期刊简介 (2243)

《计算机研究与发展》征订启事 (2389)

2015 年《计算机研究与发展》高被引论文 TOP10 (2418)

《计算机研究与发展》编委会 (封底)

CONTENTS

Applications-Driven Research Advances in Cyber Security

Preface Cao Zhenfu, et al. (2103)

Surveys

Research Advances on Secure Searchable Encryption Dong Xiaolei, et al. (2107)

Recent Advances in Lattice-Based Cryptography Zhang Pingyuan, et al. (2121)

Survey of Internet of Things Security Zhang Yuqing, et al. (2130)

Survey on Redactable Signatures Ma Jinhua, et al. (2144)

Survey on Private Preserving Set Intersection Technology Shen Liyan, et al. (2153)

Survey on Privacy Preserving Techniques for Blockchain Technology Zhu Liehuang, et al. (2170)

Cryptographic Security

RAKA: New Authenticated Key Agreement Protocol Based on Ring-LWE
..... Yang Yatao, et al. (2187)

Efficient Hierarchical Identity-Based Encryption Scheme from Learning with Errors
..... Ye Qing, et al. (2193)

Research on the LED Lightweight Cipher Against the Statistical Fault Analysis in Internet of
Things Li Wei, et al. (2205)

An Efficient Single Server-Aided k -out-of- n Oblivious Transfer Protocol
..... Zhao Shengnan, et al. (2215)

Security Analysis of Lightweight Block Cipher ESF Yin Jun, et al. (2224)

Dual Server Identity-Based Encryption with Equality Test for Cloud Computing
..... Wu Libing, et al. (2232)

Generic Tightly Secure Signature Schemes from Strong Chameleon Hash Functions
..... Li Fei, et al. (2244)

System Security

An Intrusion Detection Scheme Based on Semi-Supervised Learning and Information Gain Ratio
..... Xu Mengfan, et al. (2255)

A TrustZone Based Application Protection Scheme in Highly Open Scenarios
..... Zhang Yingjun, et al. (2268)

A Method of Constructing the Model of Trusted Virtual Machine Migration ... Shi Yuan, et al. (2284)

A System for Scoring the Exploitability of Vulnerability Based Types Lei Kenan, et al. (2296)

A Virtual Machine Introspection Triggering Mechanism Based on VMFUNC
..... Liu Weijie, et al. (2310)

Design and Implementation of Mimic Network Operating System Wang Zhenpeng, et al. (2321)

Detection of Covert and Suspicious DNS Behavior in Advanced Persistent Threats
..... Wang Xiaoqi, et al. (2334)

Advanced Persistent Threats Detection Game with Expert System for Cloud ... Hu Qing, et al. (2344)

A Dynamic Defense Mechanism for SDN DoS Attacks Based on Network Resource Management
Technology Wang Tao, et al. (2356)

Application Security and Privacy Preserving

Attribute-Based Encryption with Keyword Search in Mobile Cloud Storage Su Hang, et al. (2369)

A Secure Outsourced Fusion Denoising Scheme in Multiple Encrypted Remote Sensing Images
..... Huang Dongmei, et al. (2378)

Research on Scaling Technology of Bitcoin Blockchain Yu Hui, et al. (2390)

Compliance Analysis of Authorization Constraints in Business Process Bo Yang, et al. (2404)

~~~~~  
Editorial Columns ..... (2243,2389,2418,back cover)