



ISSN 1000-1239
CODEN JYYFEY

Journal of Computer Research and Development

计算机研究与发展

第51卷 第7期 2014年7月

Vol.51 No.7 July 2014

主办 中国科学院计算技术研究所 中国计算机学会 出版 科学出版社



中国计算机学会会刊

万方数据



计算机研究与发展

(Jisuanji Yanjiu Yu Fazhan)

第 51 卷 第 7 期 2014 年 7 月

目次

专辑:网络与信息安全

前 言	(1383)
综 述	

Android 安全综述	张玉清 王 凯 杨 欢 方喆君 王志强 曹 琛 (1385)
公共云存储服务数据安全及隐私保护技术综述	李 晖 孙文海 李凤华 王博洋 (1397)

云计算与物联网安全

面向云存储的多副本文件完整性验证方案	付艳艳 张 敏 陈开渠 冯登国 (1410)
云计算中一种安全的电子文档自毁方案	姚志强 熊金波 马建峰 李 琦 刘西蒙 (1417)
CACDP:适用于云存储动态策略的密文访问控制方法	张 浩 赵 磊 冯 博 余荣威 刘维杰 (1424)

移动互联网

基于可信移动平台的直接匿名证明方案研究	杨 波 冯登国 秦 宇 张倩颖 奚 璩 郑昌文 (1436)
一种抗混淆的大规模 Android 应用相似性检测方法	焦四辈 应凌云 杨 轶 程 瑶 苏璞睿 冯登国 (1446)
基于 Dalvik 指令的 Android 恶意代码特征描述及验证	李 挺 董 航 袁春阳 杜跃进 徐国爱 (1458)

信息安全算法与协议

基于空域失真模型的修正矩阵编码及其改进	韩 涛 祝跃飞 林斯思 吴 杨 (1467)
混合偏好模型下的分布式理性秘密共享方案	彭长根 刘 海 田有亮 吕 桢 刘荣飞 (1476)
MWNs 中基于跨层动态信誉机制的安全路由协议	林 晖 马建峰 许 力 (1486)
标准模型下高效安全的基于证书密钥封装机制	陆 阳 李继国 (1497)
基于 PRF 的 RFID 轻量级认证协议研究	金永明 吴棋滢 石志强 芦 翔 孙利民 (1506)
具有一致秘密和错误的 LWE 问题及其应用	孙小超 李 宝 路献辉 (1515)
LBlock 算法的相关密钥不可能差分分析	卫宏儒 殷广丽 (1520)

新型网络与计算技术安全

满足可计算序贯均衡的理性公平计算	王伊蕾 郑志华 王 皓 徐秋亮 (1527)
一种安全性增强的 Tor 匿名通信系统	周彦伟 杨启良 杨 波 吴振强 (1538)
基于内存依赖关系度量的解密数据提取方法	魏 强 武泽慧 王清贤 (1547)
匿名网络 I2P 路径选择的安全性分析	刘培朋 王丽宏 时金桥 谭庆丰 (1555)
面向内部威胁的最优安全策略算法研究	陈小军 时金桥 徐 菲 蒲以国 郭 莉 (1565)
一种基于 UML 的网络安全体系建模分析方法	布 宁 刘玉岭 连一峰 黄 亮 (1578)

网络攻击与防御技术

IPv6 与隧道多地址性的 DoS 攻击放大问题研究	崔 宇 张宏莉 田志宏 方滨兴 (1594)
基于行为的多级访问控制模型	苏 锐 李凤华 史国振 (1604)
Kad 网络中 Sybil 攻击团体检测技术研究	李 强 李舟军 周长斌 余 杰 (1614)
Flash 跨站脚本漏洞挖掘技术研究	刘奇旭 温 涛 闻观行 (1624)
一种应对 APT 攻击的安全架构:异常发现	杜跃进 翟立东 李 跃 贾召鹏 (1633)

研发动态

研究开发动态	(1646)
--------------	--------

读者专栏

《计算机研究与发展》征订启事	(1514)
《智能系统学报》2014 年征订启事	(1603)
《计算机研究与发展》编委会	(封底)

责任编辑:齐 蓉

JOURNAL OF COMPUTER RESEARCH AND DEVELOPMENT

Vol. 51 No. 7 July 2014

CONTENTS

Network and Information Security

Preface (1383)

Survey

Survey of Android OS Security *Zhang Yuqing et al.* (1385)

Secure and Privacy-Preserving Data Storage Service in Public Cloud *Li Hui et al.* (1397)

Security of Cloud Computing and Internet of Things

Proofs of Data Possession of Multiple Copies *Fu Yanyan et al.* (1410)

A Secure Electronic Document Self-Destructing Scheme in Cloud Computing
..... *Yao Zhiqiang et al.* (1417)

CACDP: A Cryptographic Access Control for Dynamic Policy in Cloud Storage
..... *Zhang Hao et al.* (1424)

Mobile Internet Security

Research on Direct Anonymous Attestation Scheme Based on Trusted Mobile Platform
..... *Yang Bo et al.* (1436)

An Anti-Obfuscation Method for Detecting Similarity Among Android Applications in Large Scale
..... *Jiao Sibe et al.* (1446)

Description of Android Malware Feature Based on Dalvik Instructions *Li Ting et al.* (1458)

Information Security Algorithms and Protocols

Modified Matrix Encoding Based on the Spatial Distortion Model and Its Improvement
..... *Han Tao et al.* (1467)

A Distributed Rational Secret Sharing Scheme with Hybrid Preference Model
..... *Peng Changgen et al.* (1476)

A Secure Routing Protocol for MWNs Based on Cross-Layer Dynamic Reputation Mechanism ...
..... *Lin Hui et al.* (1486)

Efficient and Provably-Secure Certificate-Based Key Encapsulation Mechanism in the Standard
Model *Lu Yang et al.* (1497)

RFID Lightweight Authentication Protocol Based on PRF *Jin Yongming et al.* (1506)

LWE Problem with Uniform Secret and Errors and Its Application *Sun Xiaochao et al.* (1515)

Related-Key Impossible Differential Cryptanalysis on LBlock *Wei Hongru et al.* (1520)

Security of Novel Network and Computing Technology

Rational Fair Computation with Computational Sequential Equilibrium *Wang Yilei et al.* (1527)

A Tor Anonymous Communication System with Security Enhancements *Zhou Yanwei et al.* (1538)

Plaintext Recovery Based on Memory Dependence Measurement *Wei Qiang et al.* (1547)

Towards Analysis of Security in I2P's Path Selection *Liu Peipeng et al.* (1555)

Algorithm of Optimal Security Hardening Measures Against Insider Threat
..... *Chen Xiaojun et al.* (1565)

UML-Based Modeling Method of Network Security Infrastructure *Bu Ning et al.* (1578)

Network Attack and Defense Technology

Multi-Addresses Amplification DoS Attacks by Native IPv6 and IPv6Tunnels *Cui Yu et al.* (1594)

Action-Based Multi-level Access Control Model *Su Mang et al.* (1604)

Sybil Group Attack Detection in Kad Network *Li Qiang et al.* (1614)

Detection of XSS Vulnerabilities in Online Flash *Liu Qixu et al.* (1624)

Security Architecture to Deal with APT Attacks: Abnormal Discovery *Du Yuejin et al.* (1633)

~~~~~  
Research & Development News ..... (1646)

Reader's Columns ..... (1514,1603,back cover)

## 《计算机研究与发展》编委会

主 编 徐志伟 中国科学院计算技术研究所  
副 主 编 石纯一 清华大学  
赵沁平 北京航空航天大学  
史忠植 中国科学院计算技术研究所  
郑纬民 清华大学  
吕 建 南京大学

领域编委 刘志勇(体系结构) 中国科学院计算技术研究所  
林 闯(网络技术) 清华大学  
孟小峰(软件技术) 中国人民大学  
曹珍富(信息安全) 上海交通大学  
郑庆华(应用技术) 西安交通大学  
周志华(人工智能) 南京大学

### 编 委

|                   |                        |
|-------------------|------------------------|
| 安 虹 中国科学技术大学      | 欧阳丹彤 吉林大学              |
| 曹军威 清华大学          | 彭宇新 北京大学               |
| 曹子宁 南京航空航天大学      | 钱德沛 北京航空航天大学           |
| 陈恩红 中国科学技术大学      | 秦志光 电子科技大学             |
| 陈国良 中国科学技术大学      | 任丰原 清华大学               |
| 陈左宁 江南计算技术研究所     | 山世光 中国科学院计算技术研究所       |
| 崔 莉 中国科学院计算技术研究所  | 舒继武 清华大学               |
| 窦 勇 国防科学技术大学      | 苏开乐 北京大学               |
| 方滨兴 北京邮电大学        | 孙茂松 清华大学               |
| 冯 丹 华中科技大学        | 孙晓明 中国科学院计算技术研究所       |
| 冯志勇 天津大学          | 王晓阳 复旦大学               |
| 过敏意 上海交通大学        | 王意洁 国防科学技术大学           |
| 何炎祥 武汉大学          | 王永吉 中国科学院软件研究所         |
| 何永强 Dropbox       | 吴 威 北京航空航天大学           |
| 侯丽珊 中国科学院计算技术研究所  | 薛 锐 中国科学院信息工程研究所       |
| 黄河燕 北京理工大学        | 薛向阳 复旦大学               |
| 黄刘生 中国科学技术大学苏州研究院 | 杨学军 国防科学技术大学           |
| 金 海 华中科技大学        | 尹宝林 北京航空航天大学           |
| 李华伟 中国科学院计算技术研究所  | 于 戈 东北大学               |
| 李建中 哈尔滨工业大学       | 于 剑 北京交通大学             |
| 李仁发 湖南大学          | 于 炯 新疆大学               |
| 李晓明 北京大学          | 詹乃军 中国科学院软件研究所         |
| 李宣东 南京大学          | 战晓苏 军事科学院运筹分析研究所       |
| 梁吉业 山西大学          | 张 路 北京大学               |
| 廖士中 天津大学          | 张 伟 烟台大学               |
| 林东岱 中国科学院信息工程研究所  | 张悠慧 清华大学               |
| 刘国华 东华大学          | 张玉清 中国科学院大学            |
| 罗军舟 东南大学          | 章 毅 四川大学               |
| 马华东 北京邮电大学        | 周傲英 华东师范大学             |
| 梅 宏 上海交通大学        | 周 昆 浙江大学               |
| 孟祥旭 山东大学          | 周 曦 中科院重庆绿色智能技术研<br>究院 |
| 苗夺谦 同济大学          |                        |

主 管 中国科学院  
主 办 中国科学院计算技术研究所  
中国计算机学会  
编 辑 《计算机研究与发展》编辑部  
中国科学院计算技术研究所  
地址: 北京中关村科学院南路6号  
邮政编码: 100190  
电话: +86 (10) 62620696(兼传真)  
+86 (10) 62600350  
E-mail: crad@ict.ac.cn  
http://crad.ict.ac.cn  
主 编 徐志伟  
出 版 科学出版社  
地址: 北京东黄城根北街16号  
邮政编码: 100717

印刷装订 北京佳艺恒彩印刷有限公司  
国内总发行 北京报刊发行局  
订 购 处 全国各邮电局  
国外总发行 中国国际图书贸易总公司  
北京399信箱  
邮政编码: 100044

Journal of Computer  
Research and Development  
(Monthly, Started in 1958)  
Vol.51 No.7 July 2014

Supervised by Chinese Academy of Sciences  
Sponsored by Institute of Computing Technology,  
Chinese Academy of Sciences  
China Computer Federation  
Edited by Editorial Office of *Journal of  
Computer Research and Development*  
Institute of Computing Technology,  
Chinese Academy of Sciences  
Add: 6 Kexueyuan South Road,  
Zhongguancun, Beijing  
100190, China  
Tel: +86(10) 62620696 (also Fax)  
+86(10) 62600350  
E-mail: crad@ict.ac.cn  
http://crad.ict.ac.cn  
Editor-in-Chief Xu Zhiwei  
Published by Science Press  
Add: 16 Donghuangchenggen North  
Street, Beijing 100717, China  
Printed by Beijing Jiayi Hengcai Printing Co.Ltd  
Distributed by Beijing Bureau for Distribution of  
Newspapers and Journals  
Domestic All Local Post Offices in China  
Foreign China International Book  
Trading Corporation  
P.O.Box 399, Beijing 100044, China