



ISSN 1000-1239
CODEN JYYFEY

Journal of Computer Research and Development

计算机研究与发展

第52卷 第10期 2015年10月

Vol.52 No.10 Oct. 2015

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

JOURNAL OF COMPUTER RESEARCH AND DEVELOPMENT

Vol. 52 No. 10 October 2015

CONTENTS

Preface Cao Zhenfu, et al. (2163)

System Security

Survey of Android Vulnerability Detection Zhang Yuqing, et al. (2167)

A Cloud Model Based Trust Evaluation Model for Defense Agent Yu Yang, et al. (2178)

An Auditing Protocol for Data Storage in Cloud Computing with Data Dynamics
..... Qin Zhiguang, et al. (2192)

SPFPA: A Format Parsing Approach for Unknown Security Protocols Zhu Yuna, et al. (2200)

pTrace: A Counter Technology of DDoS Attack Source for Controllable Cloud Computing
..... Li Baohui, et al. (2212)

A Trustzone-Based Trusted Code Execution with Strong Security Requirements
..... Zhang Yingjun, et al. (2224)

Multi-Criteria Mathematical Programming Based Method on Network Intrusion Detection
..... Wang Bo, et al. (2239)

Cryptographic Security

Advances in Key Techniques of Practical Secure Multi-Party Computation ... Jiang Han, et al. (2247)

A Strongly Secure Lattice-Based Key Exchange Protocol Wen Weiqiang, et al. (2258)

Adaptively Secure Outsourcing Ciphertext-Policy Attribute-Based Encryption
..... Wang Hao, et al. (2270)

A Privacy Preserving Attribute-Based Encryption Scheme with User Revocation
..... Li Jiguo, et al. (2281)

Accountable Attribute-Based Encryption Scheme Without Key Escrow Zhang Xing, et al. (2293)

A Trustee-Based and Efficient Divisible E-Cash Scheme Yu Yulei, et al. (2304)

A Discretionary Searchable Encryption Scheme in Multi-User Settings Li Zhen, et al. (2313)

A Universally Composable Secure Group Ownership Transfer Protocol for RFID Tags
..... Yuan Bianqing, et al. (2323)

Rational Secret Sharing Scheme Based on Reconstruction Order Adjustment Mechanism
..... Liu Hai, et al. (2332)

Privacy Protection

Advances of Privacy Preservation in Internet of Things Dong Xiaolei (2341)

Privacy-Preserving Public Auditing for Multiple Managers Shared Data in the Cloud
..... Fu Anmin, et al. (2353)

A Community Detecting Method Based on the Node Intimacy and Degree in Social Network
..... Liu Yao, et al. (2363)

Towards Measuring Unobservability in Anonymous Communication Systems
..... Tan Qingfeng, et al. (2373)

Study on Semi-Homogenous Algorithm Based on Ring Generalization He Xianmang, et al. (2382)

Privacy Requirement Modeling and Consistency Checking in Cloud Computing
..... Wang Jin, et al. (2395)

Collaboration Supported Mandatory Access Control Model Fan Yanfang, et al. (2411)

Provable Data Possession by Partial Delegation Zhong Ting, et al. (2422)

~~~~~  
Editorial Columns ..... (2312)

Reader's Columns ..... (2223,2269,2292,2303,back cover)



# 计算机研究与发展

(Jisuanji Yanjiu Yu Fazhan)

第 52 卷 第 10 期 2015 年 10 月

## 目 次

|                                                  |                                    |
|--------------------------------------------------|------------------------------------|
| 前 言 .....                                        | 曹珍富 徐秋亮 张玉清 董晓蕾 (2163)             |
| <b>系统安全</b>                                      |                                    |
| Android 安全漏洞挖掘技术综述 .....                         |                                    |
| ..... 张玉清 方喆君 王 凯 王志强 乐洪舟 刘奇旭 何 远 李晓琦 杨 刚 (2167) |                                    |
| 基于云模型的防御代理信任评估模型 .....                           | 余 洋 夏春和 王星河 (2178)                 |
| 云存储服务的动态数据完整性审计方案 .....                          | 秦志光 王士雨 赵 洋 熊 虎 吴松洋 (2192)         |
| SPFPA: 一种面向未知安全协议的格式解析方法 .....                   | 朱玉娜 韩继红 袁霖 陈韩托 范钰丹 (2200)          |
| pTrace: 一种面向可控云计算的 DDoS 攻击源控制技术 .....            | 李保琿 徐克付 张 鹏 郭 莉 (2212)             |
| 基于 Trustzone 的强安全需求环境下可信代码执行方案 .....             | 张英骏 冯登国 秦 宇 杨 波 (2224)             |
| 基于多目标数学规划的网络入侵检测方法 .....                         | 汪 波 聂晓伟 (2239)                     |
| <b>密码安全</b>                                      |                                    |
| 实用安全多方计算协议关键技术研究进展 .....                         | 蒋 瀚 徐秋亮 (2247)                     |
| 基于格问题的强安全密钥交换协议 .....                            | 温伟强 王立斌 (2258)                     |
| 自适应安全的外包 CP-ABE 方案研究 .....                       | 王 皓 郑志华 吴 磊 王伊蕾 (2270)             |
| 隐私保护且支持用户撤销的属性基加密方案 .....                        | 李继国 石岳蓉 张亦辰 (2281)                 |
| 可追责并解决密钥托管问题的属性基加密方案 .....                       | 张 星 文子龙 沈晴霓 方跃坚 吴中海 (2293)         |
| 基于可信第三方的高效可分电子现金方案 .....                         | 虞郁磊 董晓蕾 曹珍富 (2304)                 |
| 一个自主授权的多用户可搜索加密方案 .....                          | 李 真 蒋 瀚 赵明昊 (2313)                 |
| 通用可组合安全的 RFID 标签组所有权转移协议 .....                   | 原变青 刘吉强 (2323)                     |
| 基于重构顺序调整机制的理性秘密共享方案 .....                        | 刘 海 李兴华 马建峰 (2332)                 |
| <b>隐私保护</b>                                      |                                    |
| 物联网隐私保护研究进展 .....                                | 董晓蕾 (2341)                         |
| 云端多管理者群组共享数据中具有隐私保护的公开审计方案 .....                 | 付安民 秦宁元 宋建业 苏 铨 (2353)             |
| 基于节点亲密度和度的社会网络社团发现方法 .....                       | 刘 瑶 康晓慧 高 红 刘 峤 吴祖峰 秦志光 (2363)     |
| 匿名通信系统不可观测性度量方法 .....                            | 谭庆丰 时金桥 方滨兴 郭 莉 张文涛 王学宾 卫冰洁 (2373) |
| 基于环概化的半同构泛化算法研究 .....                            | 何贤芒 陈银冬 李 东 郝艳妮 (2382)             |
| 云计算中隐私需求的建模与一致性检测 .....                          | 王 进 黄志球 (2395)                     |
| 支持协作的强制访问控制模型 .....                              | 范艳芳 蔡 英 (2411)                     |
| 基于部分授权的可证明数据持有性验证 .....                          | 钟 婷 韩 校 赵宇龙 (2422)                 |

### 编者专栏

|                                   |        |
|-----------------------------------|--------|
| 2013 年《计算机研究与发展》高被引论文 TOP10 ..... | (2312) |
|-----------------------------------|--------|

### 读者专栏

|                                  |        |
|----------------------------------|--------|
| 2016 年《计算机研究与发展》专题(正刊)征文通知 ..... | (2223) |
| 2015 年起《计算机研究与发展》双月将固定领域专题 ..... | (2269) |
| 《信息安全研究》期刊简介 .....               | (2292) |
| 《计算机研究与发展》征订启事 .....             | (2303) |
| 《计算机研究与发展》编委会 .....              | (封底)   |

责任编辑: 齐 蓉

万方数据

## 《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  | 中国科学院重庆绿色智能<br>技术研究院 |
| 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.52 No.10 Oct.2015

**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