



● ISSN 0254-4164

● CODEN JIXUDT

计算机学报

CHINESE JOURNAL OF COMPUTERS

第38卷 Vol.38

第4期 No.4



2015.4

● 中国计算机学会 中国科学院计算技术研究所 主办

● 科学出版社 出版

CHINESE JOURNAL OF COMPUTERS

Vol.38 No.4 April 2015

CONTENTS

Information Security

- Analyzing Trusted Computing Protocol Based on the Strand Spaces Model FENG Wei et al. (701)
- Survey of Software Vulnerability Detection Techniques LI Zhou-Jun et al. (717)
- Provable Secure Trusted and Anonymous Roaming Protocol for Mobile Internet
..... ZHOU Yan-Wei et al. (733)
- An Improved Quantitative Evaluation Method for Network Security XI Rong-Rong et al. (749)
- A Survey of Key-Insulated Cryptography QIN Zhi-Guang et al. (759)
- An Efficient FIBE Scheme Based on Ideal Lattices WU Li-Qiang et al. (775)
- Differential Frequency Analysis Method Based on Resample WANG Zhe et al. (783)
- A New Message Authentication Code Based on Hash Function and Block Cipher ... XU Jin et al. (793)
- Provably Secure Certificateless Hybrid Signcryption YU Hui-Fang et al. (804)
- Multiple Differential Cryptanalysis Based on Optimal Distinguisher GAO Hai-Ying et al. (814)
- Wireless Key Generation for RFID Systems LU Li (822)
- Website Fingerprinting Attack Based on Hyperlink Relations GU Xiao-Dan et al. (833)
- Parallel Community Detection Based Worm Containment in Online Social Network
..... HE Liang et al. (846)
- Provable Secure Mechanism for BGP Path Protection in the Standard Model LI Dao-Feng et al. (859)
- A Method of OpenFlow-Based Real-Time Conflict Detection and Resolution for SDN Access Control
Policies WANG Juan et al. (872)

Privacy Protection

- Location Privacy Preserving k Nearest Neighbor Query Method on Road Network in Presence of User's
Preference NI Wei-Wei et al. (884)
- Privacy-Preserving and Adaptively-Secure Encryptions with Deterministic Finite Automata Policy and
Their Applications ZHANG Ming-Wu et al. (897)

计 算 机 学 报

(JISUANJI XUEBAO)

第 38 卷 第 4 期 2015 年 4 月

目 次

信息安全

- 基于串空间的可信计算协议分析 冯 伟 冯登国 (701)
- 软件安全漏洞检测技术 李舟军 张俊贤 廖湘科 马金鑫 (717)
- 可证安全的移动互联网可信匿名漫游协议 周彦伟 杨 波 张文政 (733)
- 一种改进的网络安全态势量化评估方法 席荣荣 云晓春 张永铮 郝志宇 (749)
- 密钥隔离密码系统研究现状 秦志光 刘京京 赵 洋 吴松洋 熊 虎 聂旭云 朱国斌 (759)
- 基于理想格的高效模糊身份加密方案 吴立强 杨晓元 韩益亮 (775)
- 基于重采样的差分频域分析方法 王 喆 刘 戩 王飞宇 刘剑峰 (783)
- 一种基于 Hash 函数和分组密码的消息认证码 徐 津 温巧燕 王大印 (793)
- 可证安全的无证书混合签密 俞惠芳 杨 波 (804)
- 基于最优区分器的多差分密码分析方法 高海英 金晨辉 (814)
- RFID 系统密钥无线生成 鲁 力 (822)
- 针对 SSH 匿名流量的网站指纹攻击方法 顾晓丹 杨 明 罗军舟 蒋 平 (833)
- 基于社团并行发现的在线社交网络蠕虫抑制 和 亮 冯登国 苏璞睿 应凌云 杨 轶 (846)
- 标准模型下可证明安全的 BGP 路由属性保护机制
..... 李道丰 王高才 王志伟 钟 诚 李陶深 (859)
- 一种基于 OpenFlow 的 SDN 访问控制策略实时冲突检测与解决方法
..... 王 鹏 王 江 焦虹阳 王 勇 陈诗雅 刘世辉 胡宏新 (872)

隐私保护

- 支持偏好调控的路网隐私保护 k 近邻查询方法 倪巍伟 陈 萧 马中希 (884)
- 隐私保护的推理机策略加密及应用 张明武 杨 波 王春枝 TAKAGI Tsuyoshi (897)

《计算机学报》编辑委员会

The Editorial Board of Chinese Journal of Computers

主 编 Editor-in-Chief 孙凝晖 SUN Ning-Hui

副主编 Associate Editors-in-Chief

陈熙霖 CHEN Xi-Lin 冯登国 FENG Deng-Guo 金 芝 JIN Zhi

林 闯 LIN Chuang 周傲英 ZHOU Ao-Ying

委 员 Members

陈贵海 CHEN Gui-Hai	陈克非 CHEN Ke-Fei	程学旗 CHENG Xue-Qi	范玉顺 FAN Yu-Shun
方滨兴 FANG Bin-Xing	傅育熙 FU Yu-Xi	高 文 GAO Wen	韩燕波 HAN Yan-Bo
何新贵 HE Xin-Gui	胡事民 HU Shi-Min	华庆一 HUA Qing-Yi	怀进鹏 HUAI Jin-Peng
黄继武 HUANG Ji-Wu	蒋昌俊 JIANG Chang-Jun	蒋焱川 JIANG Yi-Chuan	焦李成 JIAO Li-Cheng
金 海 JIN Hai	李德毅 LI De-Yi	李 刚 LI Gang	李国杰 LI Guo-Jie
李建中 LI Jian-Zhong	李克秋 LI Ke-Qiu	李 未 LI Wei	李晓明 LI Xiao-Ming
李忠诚 LI Zhong-Cheng	林惠民 LIN Hui-Min	刘大有 LIU Da-You	刘云浩 LIU Yun-Hao
刘志勇 LIU Zhi-Yong	卢汉清 LU Han-Qing	卢锡城 LU Xi-Cheng	陆汝钤 LU Ru-Qian
吕 建 LU Jian	罗军舟 LUO Jun-Zhou	马建峰 MA Jian-Feng	梅 宏 MEI Hong
孟 丹 MENG Dan	孟祥旭 MENG Xiang-Xu	闵革勇 MIN Ge-Yong	钮心忻 NIU Xin-Xin
欧阳丹彤 OUYANG Dan-Tong	潘启敬 PAN Qi-Jing	潘云鹤 PAN Yun-He	潘志庚 PAN Zhi-Geng
彭群生 PENG Qun-Sheng	钱德沛 QIAN De-Pei	瞿裕忠 QU Yu-Zhong	沈向洋 SHEN Xiang-Yang
沈绪榜 SHEN Xu-Bang	史忠植 SHI Zhong-Zhi	舒继武 SHU Ji-Wu	苏金树 SU Jin-Shu
谭铁牛 TAN Tie-Niu	唐志敏 TANG Zhi-Min	田 捷 TIAN Jie	王国胤 WANG Guo-Yin
王怀民 WANG Huai-Min	王 戟 WANG Ji	王 珊 WANG Shan	王兴伟 WANG Xing-Wei
吴建平 WU Jian-Ping	肖建国 XIAO Jian-Guo	许 进 XU Jin	杨学军 YANG Xue-Jun
杨义先 YANG Yi-Xian	于 戈 YU Ge	于 剑 YU Jian	查红彬 ZHA Hong-Bin
张 钹 ZHANG Bo	张长水 ZHANG Chang-Shui	张大鹏 ZHANG Da-Peng	张 健 ZHANG Jian
张尧学 ZHANG Yao-Xue	赵沁平 ZHAO Qin-Ping	周立柱 ZHOU Li-Zhu	周兴社 ZHOU Xing-She
朱传琪 ZHU Chuan-Qi	祝跃飞 ZHU Yue-Fei		

计算机学报
(月刊, 1978年创刊)

Chinese Journal of Computers
(Monthly, Started in 1978)

第38卷 第4期 总第388期 2015年4月

Vol. 38 No. 4 Series No. 388 April 2015

主 管	中国科学院	Supervised by Chinese Academy of Sciences
主 办	中国计算机学会 中国科学院计算技术研究所	Sponsored by China Computer Federation, Institute of Computing Technology, CAS
主 编	孙凝晖	Editor-in-Chief: SUN Ning-Hui
编 辑	《计算机学报》编辑委员会 中国科学院计算技术研究所 邮政编码 100190, 北京 2704 信箱 E-mail: cjc@ict.ac.cn http://cjc.ict.ac.cn	Edited by Editorial Board of Chinese Journal of Computers P. O. Box 2704, Beijing 100190, China
编辑部主任	李 刚	Director: LI Gang
出 版	科 学 出 版 社	Published by Science Press
印刷装订	北京中科印刷有限公司	Printed by Beijing Zhongke Printing Limited Company
总发行处	科 学 出 版 社 北京东黄城根北街16号 邮政编码 100717	Distributed by Science Press 16 Donghuangchenggen North Street, Beijing 100717, China
国外总发行	中国国际图书贸易总公司 (中国国际书店) 北京 399 信箱	Foreign: Guoji Shudian P. O. Box 399, Beijing 100044, China
数字出版	CNKI http://www.cnki.net	Online Published by CNKI http://www.cnki.net

国内统一连续出版物号: CN 11-1826/TP

ISSN 0254-4164

订 购 处: 全国各邮电局

国内邮发代号: 2-833

定 价: 58.00 元

国外发行代号: M 206

国内外公开发行

