

信息安全学报

Journal of Cyber Security



中国计算机学会会刊
计算机学会计算领域高质量期刊T2类
通信学会信息通信领域高质量科技期刊T2级
Scopus收录期刊
CSCD收录期刊
中国科技核心期刊



主办



中国科学院 信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING, CAS



SKLOIS
信息安全国家重点实验室



科学出版社
Science Press

信息安全学报

Journal of Cyber Security

第 9 卷

第 1 期

2024 年 1 月

目次

隐私保护的网约出行的研究综述	1
于海宁, 张宏莉, 余翔湛, 曲家兴	
基于区块链共识激励机制的新型联邦学习系统	15
米波, 翁渊, 黄大荣, 刘洋	
面向深度学习模型的可靠性测试综述	33
陈若曦, 金海波, 陈晋音, 郑海斌, 李晓豪	
基于可截取签名的药品管理隐私保护方案	56
胡荣磊, 丁安邦, 李莉, 段晓毅	
基于噪声破坏和波形重建的声纹对抗样本防御方法	71
魏春雨, 孙蒙, 张雄伟, 邹霞, 印杰	
基于 Stacking 融合模型的 Web 攻击检测方法	84
万巍, 石鑫, 魏金侠, 李畅, 龙春	
一种基于联盟管理的高效分布式域名系统	95
邓锦禧, 韩毅, 苏申, 郭泽宇, 李爽, 田志宏	
基于安全风险的 RTL 级硬件木马验证研究	111
赵剑锋, 史岗	
DataCon: 面向安全研究的多领域大规模竞赛开放数据	123
郑晓峰, 段海新, 陈震宇, 应凌云, 何直泽, 汤舒俊, 郑恩南, 刘保君, 陆超逸, 沈凯文, 张甲, 陈卓, 林子翔	
基于集成学习技术的恶意软件检测方法	137
李芳, 朱子元, 闫超, 孟丹	

Journal of Cyber Security

Volume 9 Issue 1 January, 2024

Contents

A Survey on Privacy-Preserving Ridesharing for Online Ride Hailing Services	1
<i>YU Haining, ZHANG Hongli, YU Xiangzhan, QU Jiaying</i>	
A Novel FL System Based on Consensus Motivated Blockchain	15
<i>MI Bo, WENG Yuan, HUANG Darong, LIU Yang</i>	
Deep Learning Testing for Reliability: A Survey	33
<i>CHEN Ruoxi, JIN Haibo, CHEN Jinyin, ZHENG Haibin, LI Xiaohao</i>	
A Privacy Protection Scheme for Drug Management Based on Content Extraction Signature	56
<i>HU Ronglei, DING Anbang, LI Li, DUAN Xiaoyi</i>	
Defense of Speaker Recognition Against Adversarial Examples Based on Noise Destruction and Waveform Reconstruction	71
<i>WEI Chunyu, SUN Meng, ZHANG Xiongwei, ZOU Xia, YIN Jie</i>	
Web Attack Detection Method Based on Stacking Fusion Model	84
<i>WAN Wei, SHI Xin, WEI Jinxia, LI Chang, LONG Chun</i>	
An Efficient Decentralized Domain Name System Based on Consortium Management	95
<i>DENG Jinxi, HAN Yi, SU Shen, GUO Zeyu, LI Shuang, TIAN Zhihong</i>	
Research on RTL Level Hardware Trojan Verification Based on Security Risk	111
<i>Zhao Jianfeng, Shi Gang</i>	
DataCon: Open Dataset for Large-scale Multiple Fields Security Research and Competitions	123
<i>ZHENG Xiaofeng, DUAN Haixin, CHEN Zhenyu, YING Lingyun, HE Zhize, TANG Shujun, ZHENG Ennan, LIU Baojun, LU Chaoyi, SHEN Kaiwen, ZHANG Jia, CHEN Zhuo, LIN Zixiang</i>	
Malware Detection Method Based on Ensemble Learning Technology	137
<i>LI Fang, ZHU Ziyuan, YAN Chao, MENG Dan</i>	

信息安全学报

Xinxi Anquan Xuebao
(双月刊, 2016年创刊)
第9卷 第1期 2024年1月

Journal of Cyber Security

(Bimonthly)
(Started in 2016)
Vol.9 No.1 January 2024

编辑 《信息安全学报》编辑部
(北京海淀区树村路19号,
邮编 100085)
电话: 010-82345198 010-82345199
E-mail: jcs@iie.ac.cn

主编 方滨兴

主办单位 中国科学院信息工程研究所
中国科技出版传媒股份有限公司

主管单位 中国科学院

出版 中国科技出版传媒股份有限公司

印刷装订 北京科信印刷有限公司

总发行 中国科技出版传媒股份有限公司
地址: 北京东黄城根北街16号
邮政编码: 100717
电话: 010-64017032
E-mail: journal@mail.sciencep.com

Edited by Editorial Board of Journal of Cyber Security
(No.19 Shucun Road, Haidian District, Beijing
100085, China)
E-mail: jcs@iie.ac.cn
Editor-in-Chief: Binxing Fang
Sponsored by Institute of Information Engineering,
Chinese Academy of Sciences(IIECAS);
China Science Publishing & Media LTD
Published by China Science Publishing & Media LTD
Printed by Beijing Kexin Printing Limited Company
Distributed by Science Press
No.16 Donghuangchenggen North Street
Beijing 100717,China
Telephone:010-64017032
E-mail:journal@mail.sciencep.com