

ISSN 2096-1146

信息安全学报

Journal of Cyber Security



ISSN 2096-1146



9 772096 114213



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

万方数据

目 次

智能家居攻击与防御方法综述.....	1
严 寒, 彭国军, 罗 元, 刘思德	
面向安卓恶意软件检测的对抗攻击技术综述.....	28
李佳琳, 王雅哲, 罗吕根, 王 瑜	
网络弹性与恢复机制的研究综述.....	44
刘青霞, 王 邦	
一种基于知识蒸馏的神经网络鲁棒性迁移方法.....	60
张 维, 易 平	
一种面向工控系统的 PU 学习入侵检测方法.....	72
吕思才, 张 格, 张耀方, 刘红日, 王子博, 王佰玲	
基于格的高效通用累加器与被累加值的零知识证明.....	90
谭子欣, 邓 燚, 马 丽	
差分隐私保护约束下集成分类算法的研究.....	106
贾俊杰, 邱万勇, 马慧芳	
子树类型敏感的 JavaScript 引擎灰盒测试技术.....	119
王聪冲, 甘水滔, 王晓锋	
基于区块链的智慧城市边缘设备可信管理方法研究.....	132
石鹏展, 戴 欢, 陈 洁, 陈儒玉	
信号人工智能对抗攻击综合分析平台.....	141
宣 琦, 周 晴, 崔 慧, 顾淳涛, 徐东伟, 朱佳伟, 王 巍, 杨小牛	

Contents

Survey on Smart Home Attack and Defense Methods.....	1
<i>YAN Han, PENG Guojun, LUO Yuan, LIU Side</i>	
A Survey of Adversarial Attack Techniques for Android Malware Detection	28
<i>LI Jialin, WANG Yazhe, LUO Lvgen, WANG Yu</i>	
Network Resilience and Recovery Mechanism: A Review.....	44
<i>LIU Qingxia, WANG Bang</i>	
A Robust Transfer Method of Neural Network based on Knowledge Distillation	60
<i>ZHANG Wei, YI Ping</i>	
A PU learning intrusion detection method for industrial control system.....	72
<i>LV Sicai, ZHANG Ge, ZHANG Yaofang, LIU Hongri, WANG Zibo, WANG Bailing</i>	
Lattice-Based Efficient Universal Accumulator and Zero-Knowledge Proofs of an Accumulated Value.....	90
<i>Tan Zixin, Deng Yi, Ma Li</i>	
Research on an Ensemble Classification Algorithm under Differential Privacy	106
<i>JIA Junjie, QIU Wanyong, MA Huifang</i>	
Subtree Type Sensitive Greybox Testing Technique of JavaScript Engines	119
<i>WANG Congchong, GAN Shuitao, WANG Xiaofeng</i>	
Blockchain-based Approach for Trustworthy Management of Edge Device in Smart City.....	132
<i>SHI Pengzhan, DAI Huan, CHEN Jie, CHEN Ruyu</i>	
A Comprehensive Evaluation Platform of Adversarial Attacks on Artificial Intelligence for Signal.....	141
<i>XUAN Qi, ZHOU Qing, CUI Hui, GU Chuntao, XU Dongwei, ZHU Jiawei, WANG Wei, YANG Xiaoniu</i>	