

# 信息安全学报

Journal of Cyber Security

第 10 卷      第 2 期      2025 年 3 月

## 目 次

基于定义可达性分析的固件漏洞发现技术研究 .....	1
梅润元, 王衍豪, 李子川, 彭国军	
基于响应相似性判定的 Web 越权漏洞测试方法 .....	17
宋 虹, 马俊龙, 王伟平, 诸亿郎, 王建新	
基于联邦学习的动态信任评估身份认证方法 .....	30
石瑞生, 付 彤, 林子丁, 兰丽娜, 姜 宁	
二进制比对技术: 场景、方法与挑战 .....	48
胡梦莹, 王笑克, 赵 磊	
国家网络与运营商网络的一致性分析 .....	67
朱金玉, 张 宇, 王宇楠, 张宏莉, 方滨兴	
基于增强灰度共生矩阵的深度恶意代码可视化分类方法 .....	84
王金伟, 陈正嘉, 谢 雪, 罗向阳, 马 宾	
BGP 异常事件影响风险区域快速识别方法 .....	103
刘自勉, 邱 菡, 王 瑞, 朱俊虎, 王清贤	
多阶 GMM-ResNet 融合在语音伪造检测中的研究 .....	116
曹明明, 雷震春, 杨印根, 周 勇	
引入全局语义增强的人脸欺诈特征提取研究 .....	127
蔡体健, 陈 均, 罗词勇, 刘遵雄, 陈子涵	
基于杀伤链模型的 PLC 安全分析 .....	139
孙 越, 游建舟, 宋站威, 黄文军, 陈 曦, 孙利民	
DNTrans: 基于 Transformer 的黑产域名变换生成方法 .....	163
王 博, 施 凡	
基于网络空间欺骗的移动目标防御技术研究 .....	180
张雅勤, 马多贺, Xiaoyan Sun, 周 川, 刘 峰	
云虚拟网络安全研究 .....	196
涂碧波, 孙瑞娜, 游瑞邦, 程 杰, 陶小结, 张 坤	
联邦学习中隐私攻击与防御综述 .....	219
王恺楠, 张玉会, 侯 锐	

# Journal of Cyber Security

Volume 10 Issue 2 March, 2025

## Contents

Research on Firmware Vulnerability Discovery Technology Based on Reaching Definition Analysis.....	1
<i>MEI Runyuan, WANG Yanhao, LI Zichuan, PENG Guojun</i>	
Black-box Testing Method for Web Authentication Bypass Vulnerability Based on Response Similarity Determination.....	17
<i>SONG Hong, MA Junlong, WANG Weiping, ZHU Yilang, WANG Jianxing</i>	
Research on Dynamic Trust Evaluation Method Based on Federated Learning.....	30
<i>SHI Ruisheng, FU Tong, LIN Ziding, LAN Lina, JIANG Ning</i>	
Binary Comparison Techniques: Applications, Approaches, and Challenges.....	48
<i>HU Mengying, WANG Xiaoke, ZHAO Lei</i>	
Similarity Analysis of National Network and Operator's Network.....	67
<i>ZHU Jinyu, ZHANG Yu, WANG Yunan, ZHANG Hongli, FANG Binxing</i>	
A Deep Learning Visualization Classification Method for Malicious Code Based on Enhanced Gray Level Co-occurrence Matrix.....	84
<i>WANG Jinwei, CHEN Zhengjia, XIE Xue, LUO Xiangyang, MA Bin</i>	
A Rapid Identification Method for Risk Areas Affected by BGP Anomalies.....	103
<i>LIU Zimian, QIU Han, WANG Rui, ZHU Junhu, WANG Qingxian</i>	
Research on Multi-order GMM-ResNet Fusion for Speech Deepfake Detection.....	116
<i>CAO Mingming, LEI Zhenchun, YANG Yingen, ZHOU Yong</i>	
Research on Introducing Global Semantic Enhancement for Face Fraud Feature Extraction.....	127
<i>CAI Tijian, CHEN Jun, LUO Ciyong, LIU Zunxiong, CHEN Zihan</i>	
A Cyber Kill Chain Based Analysis of PLC Security.....	139
<i>SUN Yue, YOU Jianzhou, SONG Zhanwei, HUANG Wenjun, CHEN Xi, SUN Limin</i>	
DNTrans: Illicit Domain Name Transformation Generation Method Based on Transformer.....	163
<i>WANG Bo, SHI Fan</i>	
A Study on Cyber Deception-Based Moving Target Defense.....	180
<i>ZHANG Yaqin, MA Duohe, SUN Xiaoyan, ZHOU Chuan, LIU Feng</i>	
Research on Cloud Virtual Network Security.....	196
<i>TU Bibo, SUN Ruina, YOU Ruibang, CHENG Jie, TAO Xiaojie, ZHANG Kun</i>	
Survey of privacy attack and defense in federated learning.....	219
<i>WANG Kainan, ZHANG Yuhui, HOU Rui</i>	