

# 信息安全学报

Journal of Cyber Security

第 7 卷

第 6 期

2022 年 11 月

## 目 次

机器学习中成员推理攻击和防御研究综述 .....	1
牛 俊, 马骁骥, 陈 颖, 张 歌, 何志鹏, 侯哲贤, 朱笑岩, 伍高飞, 陈 恺, 张玉清	
远程办公系统安全综述 .....	31
杨泽霖, 王基策, 徐 斐, 黄宇航, 艾铭超, 马 慧, 王 鹤, 张玉清	
基于自定义后门的触发器样本检测方案 .....	48
王 尚, 李 昕, 宋永立, 苏 铨, 付安民	
面向 Java 的高对抗内存型 Webshell 检测技术 .....	62
张金莉, 陈星辰, 王晓蕾, 陈庆旺, 代 峰, 李香龙, 冯 云, 崔 翔	
基于 Reed-Solomon 编码的抗边信道攻击云数据安全去重方法 .....	80
刘小梅, 唐 鑫, 杨舒婷, 陈 雄, 高语灿	
一种基于局部扰动的图像对抗样本生成方法 .....	94
王辛晨, 苏秋旸, 杨邓奇, 陈本辉, 李晓伟	
基于标志网络的深度学习多模型水印方案 .....	105
刘伟发, 张光华, 杨 婷, 王 鹤	
面向物联网设备安全的多层次内核访问控制方法 .....	116
詹东阳, 俞兆丰, 叶 麟, 张宏莉	
开源软件缺陷报告自动摘要研究综述 .....	126
刘翠兰, 张嘉元, 曹旭栋, 伍高飞, 朱笑岩, 任家东, 冯 涛	

# Journal of Cyber Security

Volume 7      Issue 6      November, 2022

## Contents

A survey on Membership Inference Attacks and Defenses in Machine Learning .....	1
<i>NIU Jun, MA Xiaoji, CHEN Ying, ZHANG Ge, HE Zhipeng, HOU Zhexian, ZHU Xiaoyan, WU Gaofei, CHEN Kai, ZHANG Yuqing</i>	
Survey of Telecommuting System Security .....	31
<i>YANG Zelin, WANG Jice, XU Fei, HUANG Yuhang, AI Mingchao, MA Hui, WANG He, ZHANG Yuqing</i>	
A Trigger Sample Detection Scheme Based on Custom Backdoor Behaviors .....	48
<i>WANG Shang, LI Xin, SONG Yongli, SU Mang, FU Anmin</i>	
Java-oriented High-adversarial Memory Webshell Detection Technology .....	62
<i>Zhang Jinli, Chen Xingchen, Wang Xiaolei, Chen Qingwang, Dai Feng, Li Xianglong, Feng Yun, Cui Xiang</i>	
Reed-Solomon Coding Based Secure Deduplication for Cloud Storage with Resistance Against Side Channel Attack .....	80
<i>LIU Xiaomei, TANG Xin, YANG Shuting, CHEN Xiong, GAO Yucan</i>	
A Method of Image Adversarial Sample Based on Local Disturbance .....	94
<i>WANG Xinchen, SU Qiuyang, YANG Dengqi, CHEN Benhui, LI Xiaowei</i>	
Logo Network based Deep Learning Multi-model Watermarking Scheme .....	105
<i>LIU Weifa, ZHANG Guanghua, YANG Ting, WANG He</i>	
Multi-layer Kernel Access Control Method for Internet of Things Device Security .....	116
<i>ZHAN Dongyang, YU Zhaofeng, YE Lin, ZHANG Hongli</i>	
A survey of Automatic Summarization of Open Source Software Bug Reports .....	126
<i>LIU Cuilan, ZHANG Jiayuan, CAO Xudong, WU Gaofei, ZHU Xiaoyan, REN Jiadong, FENG Tao</i>	