

信息安全学报

Journal of Cyber Security

第 7 卷

第 4 期

2022 年 7 月

目 次

| | |
|-------------------------------------|-----|
| 机器学习中差分隐私的数据共享及发布:技术、应用和挑战 | 1 |
| 胡奥婷, 胡爱群, 胡 韵, 李古月, 韩金广 | |
| 处理器微体系结构安全研究综述 | 17 |
| 尹嘉伟, 李孟豪, 霍 玮 | |
| 基于深度加权特征学习的网络安全态势评估 | 32 |
| 杨宏宇, 张梓铎, 张 良 | |
| 基于异常利用的安卓应用重打包对抗技术 | 44 |
| 周立博, 梁 彬, 游 伟, 黄建军, 石文昌 | |
| SiCsFuzzer: 基于稀疏插桩的闭源软件模糊测试方法 | 55 |
| 刘丽艳, 李 丰, 邹燕燕, 周建华, 朴爱花, 刘 峰, 霍 玮 | |
| 基于数据结构特征发现的脚本引擎内置对象别名关系识别 | 71 |
| 张昇伟, 游 伟, 梁 彬, 万欣宇, 郭苏越 | |
| 基于不定长卷积神经网络的恶意流量分类算法 | 90 |
| 杨 璇, 邬江兴, 赵 博 | |
| 源代码漏洞静态分析技术 | 100 |
| 刘嘉勇, 韩家璇, 黄 诚 | |
| 编译支持的多变体融合执行设计与实现 | 114 |
| 李秉政, 张 铮, 马博林, 邢福康, 邬江兴 | |
| 基于自适应滤波算法的有线网卡指纹提取方法 | 124 |
| 胡园园, 胡爱群, 李 晟, 刘佳琪 李 冰 | |

Journal of Cyber Security

Volume 7 Issue 4 July, 2022

Contents

| | |
|--|-----|
| Differentially Private Data Sharing and Publishing in Machine Learning: Techniques, Applications, and Challenges | 1 |
| <i>HU Aoting, HU Aiqun, HU Yun, LI Guyue, HAN Jinguang</i> | |
| Survey on Security Researches of Processor's Microarchitecture | 17 |
| <i>YIN Jiawei, LI Menghao, HUO Wei</i> | |
| Network Security Situation Assessment Based on Deep Weighted Feature Learning | 32 |
| <i>YANG Hongyu, ZHANG Zixin, ZHANG Liang</i> | |
| Countering Android Application Repackaging Attacks via Exception Exploitation | 44 |
| <i>ZHOU Libo, LIANG Bin, YOU Wei, HUANG Jianjun, SHI Wenchang</i> | |
| SiCsFuzzer: A Sparse-instrumentation-based Fuzzing Platform for Closed Source Software | 55 |
| <i>LIU Liyan, LI Feng, ZOU Yanyan, ZHOU Jianhua, PIAO Aihua, LIU Feng, HUO Wei</i> | |
| Identifying Alias Relationship between Built-in Objects of Script Engine Based on the Discovery of Data Structure Signatures | 71 |
| <i>ZHANG Yiwei, YOU Wei, LIANG Bin, WAN Xinyu, GUO Suyue</i> | |
| Malicious Traffic Classification Based on Indefinite Length Convolutional Neural Network | 90 |
| <i>YANG Xuan, WU Jiangxing, ZHAO Bo</i> | |
| Vulnerability Detection In Source Code Using Static Analysis | 100 |
| <i>LIU Jiayong, HAN Jiaxuan, HUANG Cheng</i> | |
| Design and Implementation of Integrated Multi-Variant Execution Supported by Compiler | 114 |
| <i>LI Bingzheng, ZHANG Zheng, MA Bolin, XING Fukang, WU Jiangxing</i> | |
| Fingerprint Extraction of Ethernet Card Based on Adaptive Filtering Algorithm | 124 |
| <i>HU Yuanyuan, HU Aiqun, LI Sheng, LIU Jiaqi, LI Bing</i> | |