信息安全学报

Journal of Cyber Security

第8卷 第4期 2023年7月

目 次

王大宇,殷婷婷,李 赟,秦嗣量,任 歆,罗夏朴,王浩宇,尹 霞,张 超 基于条件可逆网络的生成式图像隐写算法	1
刘 婷, 任延珍, 王丽娜 基于主机事件的攻击发现技术研究综述 3	
基于主机事件的攻击发现技术研究综述 冯 云, 刘宝旭, 张金莉, 张 越, 刘奇旭 基于马尔可夫过程的 5G 网络功能信任预测机制 张奕鸣, 刘彩霞, 刘树新, 潘 菲 可编辑区块链的研究现状与挑战 罗 彬, 温金明, 吴永东, 陈 洁 基于全系统模拟的 OP-TEE 内核模糊测试方法 王丽娜, 谢辉华, 余荣威, 张 桐, 赵敬昌 支持批量审计的解密外包 Twin-SM9 密钥封装机制 刘 宽, 宁建廷, 伍 玮, 陈海霞 基于 Tsallis 熵的近似差分隐私 K-means 算法 杨舒丹, 李 男, 郑文娟, 杜启明	7
冯 云, 刘宝旭, 张金莉, 张 越, 刘奇旭 基于马尔可夫过程的 5G 网络功能信任预测机制 4 张奕鸣, 刘彩霞, 刘树新, 潘 菲 可编辑区块链的研究现状与挑战 6 罗 彬, 温金明, 吴永东, 陈 洁 基于全系统模拟的 OP-TEE 内核模糊测试方法 8 王丽娜, 谢辉华, 余荣威, 张 桐, 赵敬昌 支持批量审计的解密外包 Twin-SM9 密钥封装机制 9 刘 宽, 宁建廷, 伍 玮, 陈海霞 基于 Tsallis 熵的近似差分隐私 K-means 算法 1/1 杨舒丹, 李 男, 郑文娟, 杜启明	
基于马尔可夫过程的 5G 网络功能信任预测机制	1
张奕鸣, 刘彩霞, 刘树新, 潘 菲 可编辑区块链的研究现状与挑战 6 罗 彬, 温金明, 吴永东, 陈 洁 基于全系统模拟的 OP-TEE 内核模糊测试方法 6 王丽娜, 谢辉华, 余荣威, 张 桐, 赵敬昌 支持批量审计的解密外包 Twin-SM9 密钥封装机制 9 刘 宽, 宁建廷, 伍 玮, 陈海霞 基于 Tsallis 熵的近似差分隐私 K-means 算法 17 杨舒丹, 李 男, 郑文娟, 杜启明 17	
可编辑区块链的研究现状与挑战	6
罗 彬, 温金明, 吴永东, 陈 洁 基于全系统模拟的 OP-TEE 内核模糊测试方法 — — — — — — — — — — — — — — — — — — —	
基于全系统模拟的 OP-TEE 内核模糊测试方法	2
王丽娜, 谢辉华, 余荣威, 张 桐, 赵敬昌 支持批量审计的解密外包 Twin-SM9 密钥封装机制 9 刘 宽, 宁建廷, 伍 玮, 陈海霞 基于 Tsallis 熵的近似差分隐私 K-means 算法 11 杨舒丹, 李 男, 郑文娟, 杜启明	
王丽娜, 谢辉华, 余荣威, 张 桐, 赵敬昌 支持批量审计的解密外包 Twin-SM9 密钥封装机制 9 刘 宽, 宁建廷, 伍 玮, 陈海霞 基于 Tsallis 熵的近似差分隐私 K-means 算法 11 杨舒丹, 李 男, 郑文娟, 杜启明	5
刘 宽, 宁建廷, 伍 玮, 陈海霞 基于 Tsallis 熵的近似差分隐私 K-means 算法 杨舒丹, 李 男, 郑文娟, 杜启明	
刘 宽, 宁建廷, 伍 玮, 陈海霞 基于 Tsallis 熵的近似差分隐私 K-means 算法 杨舒丹, 李 男, 郑文娟, 杜启明	9
基于 Tsallis 熵的近似差分隐私 K-means 算法 杨舒丹, 李 男, 郑文娟, 杜启明	
杨舒丹,李 男,郑文娟,杜启明	3
1/2 A/1 1/1 5% 1/1 1 /2 TP 1/2 1/2 5/2 All U1/1 1 5/2 1 1 2/2 III 2/2 III 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	6
邓慧娜、叶阿勇、刘燕妮、孙明辉	Ū
RTL 级硬件木马问题研究 ····································	G
赵剑锋、史 岗	_
一种针对 TomcatFilter 型的 MemShell 检测技术研究····································	: 2
蔡国宝,张 昆,曲 博,李 俊,袁 方,李振宇,丁 勇	J

Journal of Cyber Security

Volume 8 Issue 4 July, 2023

Contents

BATscope: Demystifying Malicious Addresses and Mixing Transactions in Bitcoin	1
WONG Taiyu, YIN Tingting, LI Yun, QIN Siliang, REN Xin, LUO Xiapu, WANG Haoyu, YIN Xia, 2	
Generative Image Steganography Via Conditional Invertible Neural Network	17
LIU Ting, REN Yanzhen, WANG Lina	
A Survey of Attack Discovery Technology Based on Host Events	31
Feng Yun, Liu Baoxu, Zhang Jinli, Zhang Yue, Liu Qixu	
5G network function trust prediction mechanism based on Markov process	46
ZHANG Yiming, LIU Caixia, LIU Shuxin, PAN Fei	
State of the Art and Challenges of Redactable Blockchain	62
LUO Bin, WEN Jinming, WU Yongdong, CHEN Jie	
OP-TEE Kernel Fuzzy Testing Method Based on Whole System Emulation	85
WANG Lina, XIE Huihua, YU Rongwei, ZHANG Tong, ZHAO Jingchang	
Multi-Ciphertext Batch Auditable Outsourced Twin-SM9 Key Encapsulation Mechanism ·····	99
LIU Kuan, NING Jianting, WU Wei, CHEN Haixia	
An approximate differential privacy K-means algorithm based on Tsallis entropy	113
YANG Shudan, LI Nan, ZHENG WenJuan, DU Qiming	
Privacy-aware online task offloading mechanism in mobile edge computing	126
DENG Huina, YE Ayong, LIU Yanni,SUN Minghui	
Research on RTL level hardware Trojan	139
Zhao Jianfeng, Shi Gang	
Research on MemShell Detection Technology for Tomcat Filter	153
CAI Guobao, Zhang Kun, Qu Bo, Li Jun, Yuan Fang, Li Zhenyu, Ding Yong	

[©]Copyright 2023, Institute of Information Engineering, the Chinese Academy of Sciences. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form without the prior written permission of the Institute of Information Engineering, the Chinese Academy of Sciences.