

# **2022 IEEE Conference on Dependable and Secure Computing (DSC 2022)**

**Edinburgh, United Kingdom  
22-24 June 2022**



**IEEE Catalog Number: CFP22J65-POD  
ISBN: 978-1-6654-2142-3**

**Copyright © 2022 by the Institute of Electrical and Electronics Engineers, Inc.  
All Rights Reserved**

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\* This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP22J65-POD
ISBN (Print-On-Demand):	978-1-6654-2142-3
ISBN (Online):	978-1-6654-2141-6

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: (845) 758-0400  
Fax: (845) 758-2633  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# TABLE OF CONTENTS

Show Me Your Attach Request and I'll Tell You Who You Are: Practical Fingerprinting Attacks in 4G and 5G Mobile Networks .....	1
<i>Daniel Fraunholz, Richard Schörghofer-Vrinssen, Hartmut König, Richard Zahoransky</i>	
High Speed Encrypted Computing: Stochastic Confusion and Lies in a Secret Computer .....	9
<i>Peter T. Breuer</i>	
A Scary Peek into the Future: Advanced Persistent Threats in Emerging Computing Environments.....	17
<i>Talal Halabi, Aawista Chaudhry, Sarra Alqahtani, Mohammad Zulkernine</i>	
Reliability Models and Analysis for Triple-Model with Triple-Input Machine Learning Systems.....	25
<i>Qiang Wen, Fumio Machida</i>	
Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots.....	33
<i>Upendra Bartwal, Subhasis Mukhopadhyay, Rohit Negi, Sandeep Shukla</i>	
FREED: An Efficient Privacy-Preserving Solution for Person Re-IDentification .....	41
<i>Bowen Zhao, Yingjiu Li, Ximeng Liu, Hwee Hua Pang, Robert H. Deng</i>	
A Co-Evolutionary Algorithm-Based Malware Adversarial Sample Generation Method .....	49
<i>Fangwei Wang, Yuanyuan Lu, Qingru Li, Changguang Wang, Yonglei Bai</i>	
Securing Password Authentication for Web-Based Applications.....	57
<i>Teik Guan Tan, Pawel Szalachowski, Jianying Zhou</i>	
Graph Neural Network-Based Android Malware Classification with Jumping Knowledge .....	67
<i>Wai Weng Lo, Siamak Layeghy, Mohanad Sarhan, Marcus Gallagher, Marius Portmann</i>	
Multi-Task Learning Model Based on Multiple Characteristics and Multiple Interests for CTR Prediction .....	76
<i>Yufeng Xie, Mingchu Li, Kun Lu, Syed Bilal Hussain Shah, Xiao Zheng</i>	
IoT Botnet Detection Based on the Behaviors of DNS Queries .....	83
<i>Chun-I Fan, Cheng-Han Shie, Che-Ming Hsu, Tao Ban, Tomohiro Morikawa, Takeshi Takahashi</i>	
Clustering-Based Network Intrusion Detection System.....	90
<i>Chun-I Fan, Yen-Lin Lai, Cheng-Han Shie</i>	
Device-To-Device Task Offloading in a Stochastic Invalid-Device Scenario with Social Awareness .....	98
<i>Mingchu Li, Linlin Yang, Kun Lu, Syed Bilal Hussain Shah, Xiao Zheng</i>	
A Novel Approach for Providing Client-Verifiable and Efficient Access to Private Smart Contracts .....	105
<i>Alexander Köberl, Holger Bock, Christian Steger</i>	
A Hybrid Graph Neural Network Approach for Detecting PHP Vulnerabilities.....	113
<i>Rishi Rabheru, Hazim Hanif, Sergio Maffei</i>	
Symbolon: Enabling Flexible Multi-Device-Based User Authentication.....	122
<i>Thalia Laing, Eduard Marin, Mark D. Ryan, Joshua Schiffman, Gaëtan Wattiau</i>	

Design and Analysis of Novel Bit-Flip Attacks and Defense Strategies for DNNs .....	134
<i>Yash Khare, Kumud Lakara, Maruthi S. Inukonda, Sparsh Mittal, Mahesh Chandra, Arvind Kaushik</i>	
Discovering Exfiltration Paths using Reinforcement Learning with Attack Graphs .....	142
<i>Tyler Cody, Abdul Rahman, Christopher Redino, Lanxiao Huang, Ryan Clark, Akshay Kakkar, Deepak Kushwaha, Paul Park, Peter Beling, Edward Bowen</i>	
A Call for a New Privacy & Security Regime for IoT Smart Toys .....	150
<i>Joshua Streiff, Naheem Noah, Sanchari Das</i>	
Malicious and Benign URL Dataset Generation using Character-Level LSTM Models .....	158
<i>Spencer Vecile, Kyle Lacroix, Katarina Grolinger, Jagath Samarabandu</i>	
Protecting White-Box Block Ciphers with Galois/Counter Mode.....	166
<i>Nanjiang Xie, Zheng Gong, Yufeng Tang, Lei Wang, Yamin Wen</i>	
A Node-Embedding Features Based Machine Learning Technique for Dynamic Malware Detection .....	173
<i>Sudhir Kumar Rai, Ashish Mittal, Sparsh Mittal</i>	
Curse of System Complexity and Virtue of Operational Invariants: Machine Learning Based System Modeling and Attack Detection in CPS.....	181
<i>Muhammad Omer Shahid, Chuadhry Mujeeb Ahmed, Venkata Reddy Palleti, Jianying Zhou</i>	
Linux Kernel Module Development with Rust.....	189
<i>Shao-Fu Chen, Yu-Sung Wu</i>	
How National CSIRTs Operate: Personal Observations and Opinions from MyCERT .....	191
<i>Sharifah Roziah Binti Mohd Kassim, Solahuddin Bin Shamsuddin, Shujun Li, Budi Arief</i>	
Capturing Malware Behaviour with Ontology-Based Knowledge Graphs.....	193
<i>Ipshita Roy Chowdhury, Deepayan Bhowmik</i>	
A Survey on Explainable Anomaly Detection for Industrial Internet of Things .....	200
<i>Zijie Huang, Yulei Wu</i>	
Cyber Security Risks of Net Zero Technologies .....	209
<i>Haiyue Yuan, Shujun Li</i>	
Towards Secure Multi-Agent Deep Reinforcement Learning: Adversarial Attacks and Countermeasures .....	220
<i>Changgang Zheng, Chen Zhen, Haiyong Xie, Shufan Yang</i>	
Using Poisson Distribution to Enhance CNN-Based NB-IoT LDoS Attack Detection.....	228
<i>Jiang-Yi Zeng, Li-En Chang, Hsin-Hung Cho, Chi-Yuan Chen, Han-Chieh Chao, Kuo-Hui Yeh</i>	
LAEG: Leak-Based AEG using Dynamic Binary Analysis to Defeat ASLR .....	235
<i>Wei-Loon Mow, Shih-Kun Huang, Hsu-Chun Hsiao</i>	
Shodan Indicators Used to Detect Standard Conpot Implementations and Their Improvement Through Sophisticated Customization.....	243
<i>Warren Z. Cabral, Leslie F. Sikos, Craig Valli</i>	
Optimising User Security Recommendations for AI-Powered Smart-Homes.....	250
<i>Emma Scott, Sakshyam Panda, George Loukas, Emmanouil Panaousis</i>	

Enabling Device Trustworthiness for SDN-Enabled Internet-of-Battlefield Things.....	258
<i>Abel O. Gomez Rivera, Evan M. White, Jaime C. Acosta, Deepak Tosh</i>	
Cache Locking and Encryption to Prevent Memory Snooping in Embedded Systems .....	265
<i>Jason Dejesus, John A. Chandy</i>	
An Engineering Process Framework for Cybersecurity Incident Response Assessment .....	273
<i>Robert L. Freas, Heather F. Adair, Eman Hammad</i>	
Network Intrusion Detection in Encrypted Traffic.....	281
<i>Eva Papadogiannaki, Giorgos Tsirantonakis, Sotiris Ioannidis</i>	
Defending OC-SVM Based IDS from Poisoning Attacks .....	289
<i>Lu Zhang, Reginald Cushing, Paola Grosso</i>	
A Low Cost Blockchain-Based Framework for Preserving Critical Data in Health-Care IoT Systems using Classification .....	297
<i>Heba Takruri Tamemi, Manar Rabayah, Kareem Abu Raad, Mai Kanaan, Ahmed Awad</i>	
ELSA: Edge Lightweight Searchable Attribute-Based Encryption Multi-Keyword Scalability .....	305
<i>Jawhara Aljabri, Anna Lito Michala, Jeremy Singer</i>	
Automated Anomaly Detection Tool for Industrial Control System.....	309
<i>Mariam Varkey, Jacob John, Umadevi K. S.</i>	
A Digital Forensics Live Suspicious Activity Toolkit to Assist Investigators with Sexual Harm Prevention Order Monitoring .....	315
<i>Andrew Scholey, Pooneh Bagheri Zadeh</i>	
A Novel Chaos-Based Light-Weight Image Encryption Scheme for Multi-Modal Hearing Aids .....	321
<i>Awais Aziz Shah, Ahsan Adeel, Jawad Ahmad, Ahmed Al-Dubai, Mandar Gogate, Abhijeet Bishnu, Muhammad Diyan, Tassadaq Hussain, Kia Dashtipour, Tharm Ratnarajah, Amir Hussain</i>	
Facilitating Deep Learning for Edge Computing: A Case Study on Data Classification .....	327
<i>Abdullah Alsalemi, Abbas Amira, Hossein Malekmohamadi, Kegong Diao</i>	
A Generative Neural Network for Enhancing Android Metamorphic Malware Detection Based on Behaviour Profiling .....	331
<i>Leigh Turnbull, Zhiyuan Tan, Kehinde O. Babaagba</i>	

## **Author Index**