

# **2025 IEEE Conference on Dependable and Secure Computing (DSC 2025)**

**Taipei, Taiwan  
18-20 October 2025**



**IEEE Catalog Number: CFP25J65-POD  
ISBN: 979-8-3315-1539-3**

**Copyright © 2025 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:	CFP25J65-POD
ISBN (Print-On-Demand):	979-8-3315-1539-3
ISBN (Online):	979-8-3315-1538-6

**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

# 2025 IEEE Conference on Dependable and Secure Computing (DSC)

<i>HTTP Adversarial Activity in Honeypots</i> Shun-Wen Hsiao (National Chengchi University, Taiwan), Kelvin Io Wai Kuok (National Chengchi University, Taiwan) .....	1
<i>Multi-Authority Attribute-Based Multi-Keyword Searchable Encryption with Dynamic Membership from Lattices</i> Er-Shuo Zhuang (National Sun Yat-Sen University, Taiwan), Chia-Yu Lin (Taiwan), Chun-I Fan (National Sun Yat-sen University, Taiwan), Arijit Karati (National Sun Yat-sen University, Taiwan), Debasis Das (IIT Jodhpur, India) .....	3
<i>Attack Information Spectrum: a Taxonomy of Adversarial Attack Methods for Images</i> Yuanzhe Jin (University of Oxford, United Kingdom (Great Britain)) .....	9
<i>Scalable Kernel Integrity Monitor</i> Jun-Yu Lai (National Yang Ming Chiao Tung University, Taiwan), Jui-An Chang (National Yang Ming Chiao Tung University, Taiwan), Yu-Sung Wu (National Yang Ming Chiao Tung University, Taiwan), Ying-Dar Lin (National Yang Ming Chiao Tung University, Taiwan), Chia-Mu Yu (National Chiao Tung University, Taiwan), Wei-Bin Lee (Feng Chia University, Taiwan) .....	17
<i>Quantum-Resistant Subset Predicate Encryption Supporting Traitor Tracing</i> You-Qian Chen (National Chengchi University, Taiwan), Li-Tien Kung (National Chengchi University, Taiwan), Yi-Fan Tseng (National Chengchi University, Taiwan) .....	19
<i>Adaptive Fuzzing Framework for Embedded Systems Vulnerability Detection Using Reinforcement and Deep Learning</i> Hafiz Muhammad Soban Khan (University of Cyprus KIOS CoE, Cyprus), Costas Pashiourides (University of Cyprus & KIOS Research and Innovation Center of Excellence, Cyprus), Angelos K. Marnerides (University of Cyprus, Cyprus) .....	27
<i>Identity-Based Chameleon Hashing from the SIS Assumption in a Central Authority Model</i> Dai-Rui Lin (National Kaohsiung University of Science, Taiwan) .....	35
<i>HoneyWin: High-Interaction Windows Honeypot in Enterprise Environment</i> Yan Lin Aung (University of Derby, United Kingdom (Great Britain)), Yee Loon Khoo (Singapore Institute of Technology, Singapore), Yang Davis Zheng (Singapore Institute of Technology, Singapore), Bryan Swee Duo (Singapore Institute of Technology, Singapore), Sudipta Chattopadhyay (Singapore University of Technology and Design (SUTD), Singapore), Jianying Zhou (Singapore University of Technology and Design (SUTD), Singapore), Liming Lu (Singapore Institute of Technology, Singapore), Weihai Goh (Singapore Institute of Technology, Singapore) .....	41
<i>Dissecting Privacy-Exposing Identifiers in 5G/4G Networks</i> Munshi Saifuzzaman (Utah State University, USA), Ke Xie (Utah State University, USA), Tian Xie (Utah State University, USA), Xiao Zhang (University of Michigan-Dearborn, USA), Xinyu Lei (Michigan Technological University, USA) .....	47
<i>Vulnerability Assessment of Open-Source Large Language Models Against Prompt Variation Attacks</i> Lu-An Chen (National Institute of Cyber Security, Taiwan), Yu-Chen Dai (National Institute of Cyber Security, Taiwan) .....	56
<i>LLM-Based Multi-Label Mapping of Snort Rules to ATT&amp;CK</i> Yu Hsun Lee (National Institute of Cyber Security, Taiwan), Chansu Han (National Institute of Information and Communications Technology, Japan), Min-Chun Peng (National Institute of Cyber Security, Taiwan), Takeshi Takahashi (National Institute of Information and Communications Technology, Japan) .....	63
<i>A Scalable Multi-Datasource IDS Dataset with Technique and Lifecycle Labels Based on MITRE ATT&amp;CK</i> Fietyata Yudha (National Yang Ming Chiao Tung University, Taiwan & Universitas Islam Indonesia, Indonesia), Ying-Dar Lin (National Yang Ming Chiao Tung University, Taiwan), Yuan-Cheng Lai (Information Management, NTUST, Taiwan), Ren-Hung Hwang (National Yang Ming Chiao Tung University, Taiwan), Rasul Mankaev (National Yang Ming Chiao Tung University, Taiwan) .....	69
<i>Code as a Weapon: Generating Malware with Large Language Models</i> Yen-Ju Lin (National Taiwan University of Science and Technology, Taiwan), Pohan Chou (National Taiwan University of Science and Technology, Taiwan), Wan-Ying Shen (National Taiwan University of Science and Technology, Taiwan), Ying-Ren Guo (Academia Sinica, Taiwan), Chun Lun Nicoa Wu (National Taiwan University of Science and Technology, Taiwan), Yi-Ting Huang (National Taiwan University of Science and Technology, Taiwan) .....	77
<i>Optimized Lightweight VGG-Based AI Model for Phishing Detection in Cloud Applications</i> Akshat Gaurav (Asia University, Taiwan), Varsha Arya (Hong Kong Metropolitan University (HKMU), Hong Kong), Kwok Tai Chui (Hong Kong Metropolitan University, Hong Kong), Brij Gupta (NIT Kurukshetra, India) .....	85
<i>Research on Hierarchical Model of BERT-CNN-BiLSTM for Long Dialog Classification</i> Renyuan Deng (Harbin Institute of Technology, Weihai, China), Hongri Liu (Harbin Institute of Technology, Weihai, China), Yang Liu Yang (Department of Computer Science & Technology, China), Lingzhi Wang (Harbin Institute of Technology, Weihai, China) .....	92
<i>Privacy-Enhancing LLM-Based Synthetic Dataset Generation by LoRA Fine-Tuning and Prompting</i> Sheng-Chieh Hung (Telecom Technology Center, Taiwan), Chen-Fan Chang (National Taipei University of Technology, Taiwan), Yu-Chi Chen (National Taipei University of Technology, Taiwan), Yu-Ming Chang (National Taipei University of Technology, Taiwan), Yu-Ta Lin (National Taipei University of Technology, Taiwan), Michael Lin (Massachusetts Institute of Technology, USA), Wei-Bin Lee (Feng Chia University, Taiwan) .....	98
<i>Post-Exploitation Unveiled: Analyzing RAT Behaviors in a Realistically Simulated Enterprise Network</i> Shohei Hiruta (National Institute of Information and Communications Technology, Japan), Yuki Umamura (National Institute of Information and Communications Technology, Japan), Masaki Kubo (National Institute of Information and Communications Technology, Japan), Nobuyuki Kanaya (National Institute of Information and Communications Technology, Japan), Takahiro Kasama (National Institute of Information and Communications Technology, Japan) .....	100
<i>SDN-Based Out-of-Band Hash Checking for Secure QKD Basis Exchange</i> Wenjun Fan (University of Washington, USA), Siyuan Wu (University of Virginia, USA) .....	108
<i>Dynamic Decision Support Framework for Smart Home Security</i> Youssef Yamout (Queen's University, Canada), Shahrear Iqbal (National Research Council, Canada), Mohammad Zulkernine (Queen's University, Canada) .....	116

<i>Watchers Compromised: The Stealthy and Persistent Strategies of IoT Botnet</i>	
Yuki Umemura (National Institute of Information and Communications Technology, Japan), Masaki Kubo (National Institute of Information and Communications Technology, Japan), Yoshiaki Mori (National Institute of Information and Communications Technology, Japan), Hideyuki Furukawa (National Institute of Information and Communications Technology, Japan), Kanta Okugawa (National Institute of Information and Communications Technology, Japan), Takahiro Kasama (National Institute of Information and Communications Technology, Japan) .....	122
<i>Can AI Outsmart Firewall Errors? a Study on LLMs for Anomaly Generation and Detection</i>	
Chang-Sheng Lee (Academia Sinica, Taiwan), Ling-Jyh Chen (Academia Sinica, Taiwan) .....	130
<i>Securing Enterprise Wi-Fi Data Plane with off-the-Shelf Wi-Fi 6 Controllers</i>	
Tai Tan Phan (National Yang Ming Chiao Tung University, Taiwan), Liang-Shu Hsu (ZCOM, Hsinchu, Taiwan), Chi-Yu Li (National Yang Ming Chiao Tung University, Taiwan) .....	132
<i>6G-DTAuth: Distributed Token-Based Authentication for Resilient 6G Networks with LEO Satellites</i>	
Jeng-Shin Huang (National Yang Ming Chiao Tung University, Taiwan), Kuan-Hsien Tu (ITRI, Taiwan), Jie-Yu Luo (National Yang Ming Chiao Tung University, Taiwan), Min-Chih Hsu (National Yang Ming Chiao Tung University, Taiwan), Chi-Yu Li (National Yang Ming Chiao Tung University, Taiwan) .....	134
<i>An Automated Detection Platform Against TLS Vulnerabilities for Wi-Fi IoT Devices</i>	
Yen-Chia Chen (National Yang Ming Chiao Tung University, Taiwan), Tzu-Chi Yu (National Yang Ming Chiao Tung University, Taiwan), Chi-Yu Li (National Yang Ming Chiao Tung University, Taiwan) .....	143
<i>Failure Rate Analysis by PFC Function of 3-Phase Vienna Converter Using Fault-Tree Analysis</i>	
Yun Sik Jang (Gyeongsang National University, Korea (South)), Sung-Geun Song (Korea Electronics Technology Institute, Korea (South)), Sang-Hyeok Lee (Electronics Technology Institute, Korea (South)), Feelsoon Kang (Geyongsng National University, Korea (South)) .....	N/A
<i>Comparison of Volume, Price, and Reliability by the DC-Link Capacitor Structure of the Vienna Converter</i>	
Seong Jin Im (Gyeongsang National University, Korea (South)), Sang-Hyeok Lee (Electronics Technology Institute, Korea (South)), Sung-Geun Song (Korea Electronics Technology Institute, Korea (South)), Feelsoon Kang (Geyongsng National University, Korea (South)) .....	N/A
<i>PrivCCA: Protection of Credentials Using ARM CCA from Privilege Escalation Attack</i>	
Yuki Komori (Kobe University, Japan), Hiroki Kuzuno (Kobe University, Japan), Masaya Sato (Okayama Prefectural University, Japan), Makoto Takita (Kobe University, Japan), Yoshiaki Shiraiishi (Kobe University, Japan) .....	149
<i>AutoCut-2D: Enhancing Secure AI for Telegram Financial Fraud Detection via Elbow-Based Feature Selection</i>	
Chunlan Gao (Georgia State University, USA), Yubao Wu (Georgia State University, USA) .....	157
<i>Boosting Network Protocol Fuzzing Efficiency with Modern Techniques</i>	
Kai-Jung Chen (National Yang Ming Chiao Tung University, Taiwan), Yu-Cheng Yang (National Yang Ming Chiao Tung University, Taiwan), Meng-Yan Luo (National Yang Ming Chiao Tung University, Taiwan), Jun-Hong Cheng (National Yang Ming Chiao Tung University, Taiwan), Chun-Ying Huang (National Yang Ming Chiao Tung University, Taiwan) .....	165
<i>Securing Fine Timing Measurement Protocol in Wi-Fi Networks</i>	
Yu-Hung Chou (National Yang Ming Chiao Tung University, Taiwan), Yu-An Chen (Michigan State University, USA), Yu-Xun Tang (National Yang Ming Chiao Tung University, Taiwan), Chi-Yu Li (National Yang Ming Chiao Tung University, Taiwan), Guan-Hua Tu (Michigan State University, USA) .....	173
<i>Adversarial Agents: LLM-Powered Attacks and Defenses for Android Malware Detectors</i>	
Tianwei Lan (Université Paris Cité, France), Farid Nait-Abdesselam (Université Paris Cité, France) .....	181
<i>CCFDP: Co-Frequency Co-Time Full Duplex Protocol</i>	
Jheng-Jia Huang (National Taiwan University of Science and Technology, Taiwan), Wei-Hsueh Wang (National Taiwan University of Science and Technology, Taiwan), Yi-Fan Tseng (National Chengchi University, Taiwan), Nai-Wei Lo (National Taiwan University of Science and Technology, Taiwan) .....	N/A