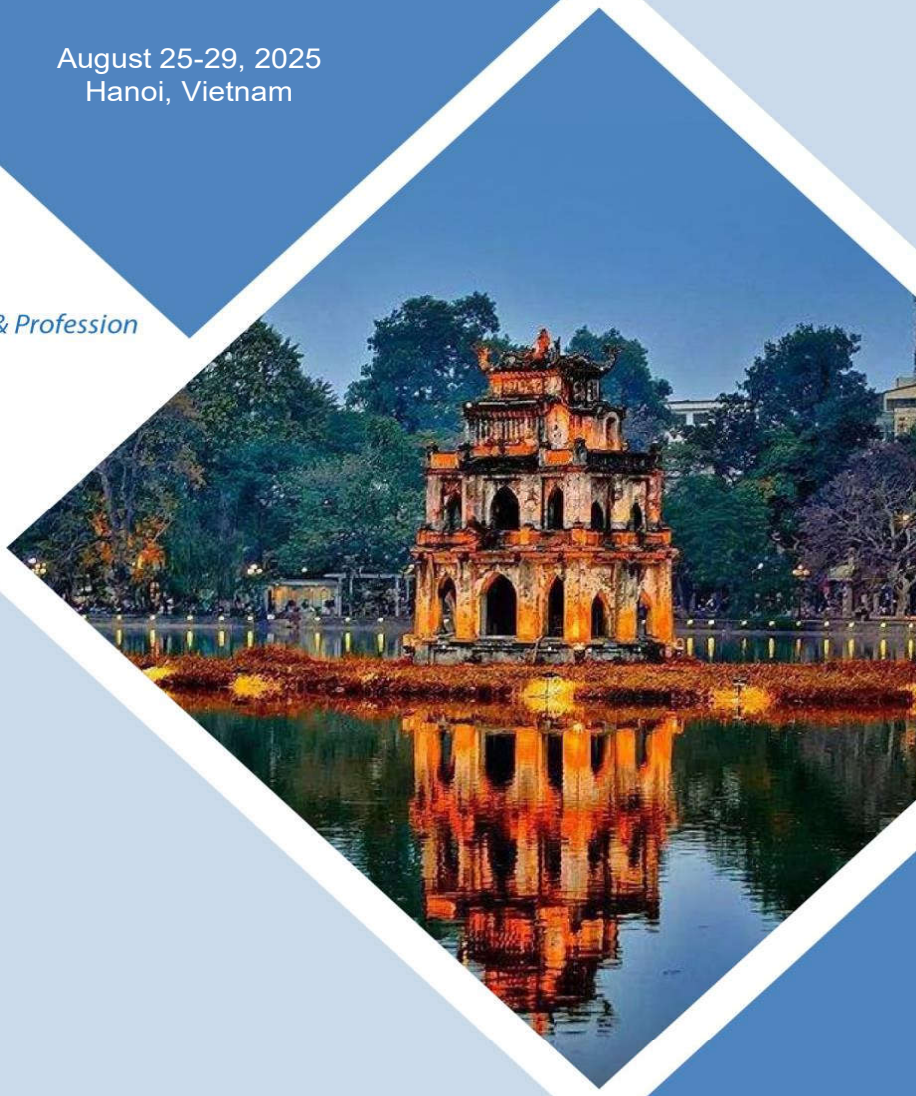
August 25-29, 2025
Hanoi, Vietnam



Association for Computing Machinery

Advancing Computing as a Science & Profession

ACM ASIACCS 2025

Proceedings of the 20th ACM ASIA
Conference on Computer and Communications Security

Sponsored by:
ACM SIGSAC

General Chairs:
Huynh Quyet Thang, HUST, Vietnam
Phan Duong Hieu, Institut Polytechnique de Paris, France

Program Chairs:
Michail Maniatakos, NYU Abu Dhabi, United Arab Emirates
Yinqian Zhang, SUSTech, China

The Association for Computing Machinery
1601 Broadway, 10th Floor
New York, New York 10019, USA

ACM ISBN: 979-8-4007-1410-8/25/08

Message from General Co-Chairs

It is our great pleasure to welcome you to AsiaCCS 2025, the 20th ACM Asia Conference on Computer and Communications Security (AsiaCCS 2025). This year's event will be held at the Meliá Hanoi in Hanoi, Vietnam, from 25 to 29 August 2025.

AsiaCCS 2025 marks a special milestone - its 20th anniversary - and we are proud of how the conference has grown into the premier venue for cybersecurity research in the Asia-Pacific region. To commemorate two decades of development, AsiaCCS 2025 is introducing a Test-of-Time Award and will host a special 20th-birthday celebration. This year also marks the first time Vietnam will host AsiaCCS, and we hope AsiaCCS 2025 will further strengthen Vietnam's cybersecurity community and foster new collaborations across the region.

The main conference features three keynote talks by world-renowned researchers - Prof. Moti Yung (Google / Columbia University), Prof. Wenyuan Xu (Zhejiang University), and Prof. Yier Jin (Huawei) - alongside our full-paper presentations and a vibrant poster session.

As in past years, we offer a rich program of workshops and keynotes. On the first day, eight workshops will explore cutting-edge topics:

- 12th ACM ASIA Public-Key Cryptography Workshop (APKC)
- 7th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI)
- 11th ACM Cyber-Physical System Security Workshop (CPSS)
- Workshop on Privacy in Large Language Models (LLM) and Natural Language Processing
- 2nd Workshop on Security-Centric Strategies for Combating Information Disorder (SCID)
- 3rd ACM Workshop on Secure and Trustworthy Deep Learning Systems (SecTL)
- 4th Workshop on Security Implications of Deepfakes and Cheapfakes
- International Workshop on Secure and Efficient Federated Learning

We would like to express our deep gratitude to our organizing committee, including

- **Program Chairs:** Michail Maniatakos and Yinqian Zhang
- **Local Organizing Chairs:** Huynh Thi Thanh Binh and Tran Quang Duc
- **Workshop Chair:** Khoa Nguyen
- **Poster Chairs:** Pham Van Thuan and Yue Duan
- **Sponsorship Chair:** Le Xuan Thanh
- **Web Chair:** Tran Hai Anh
- **Publicity Chairs:** Vo Quang Viet and Cao Minh Phuong
- **Publication Chairs:** Dinh Tien Tuan Anh and Tong Van Van

In particular, we owe a special debt of gratitude to Tran Quang Duc as a lead coordinator, his tireless efforts behind the scenes have kept every piece of this conference running smoothly - without him, AsiaCCS 2025 simply would not have happened.

We would also like to acknowledge our generous supporters: Calif Global Inc. as Supporting Partner, sponsoring a large portion of local participants, and the Singapore Institute of Technology (SIT) as a sponsor.

We hope you enjoy the program, the city of Hanoi, and that AsiaCCS 2025 provides an inspiring forum for collaboration for all participants.

General Chairs
Huynh Quyet Thang and Phan Duong Hieu

Message from Program Co-Chairs

It has been an exciting journey for us to serve as PC Co-Chairs of AsiaCCS 2025. Selecting the papers to be presented is the ultimate responsibility and the most important part of a conference organization. We would like to express our gratitude to all authors, PC members, the organizing committee, as well as the steering committee for their great support in the past months. This team effort led to the formation of an exciting program!

Submissions were received from researchers worldwide, from both academia and industry. These submissions present novel contributions related to real-world aspects of security, privacy, and cryptography, with real world impact and applications. A total of 558 submissions were received: 289 in the first Cycle and 269 in the second Cycle. The reviewing process for each Cycle consisted of two rounds.

- In the first Cycle, 12 papers were desk rejected for violation of submission policies, 133 papers were early rejected in the first round, and 80 were rejected in the second round. 34 papers were invited for a major revision, 19 were accepted with shepherding, and 11 were accepted straight away. Out of 34 major revision papers, 31 were accepted, for a total of 61 papers accepted in Cycle 1.
- In the second Cycle, 24 papers were desk rejected for violation of submission policies, 109 papers were early rejected in the first round, and 83 were rejected in the second round. There was no Major Revision process in Cycle 2. 39 papers were accepted with shepherding, and 14 were accepted straight away, for a total of 53 papers accepted in Cycle 2.

In total 114/558 submissions were accepted, for an acceptance rate of 20.4%.

The AsiaCCS 2025 technical program consists of 114 talks corresponding to the accepted papers, a poster session, as well as three keynote talks by internationally prominent and active researchers. Also, for the first time in the history of AsiaCCS a Test-of-Time nomination process was initiated with the awards to be given during the conference.

We offer our deepest gratitude to:

- Authors of every submission to AsiaCCS 2025. We thank them for considering AsiaCCS as their preferred venue for demonstrating their research outputs and for their trust in us and the PC to thoroughly and faithfully conduct the reviewing process.
- Local Chairs Tran Quang Duc and Huynh Thi Thanh Binh for being very responsive, answering every query promptly, supporting us and keeping us on track with timely follow ups!

- Publication Chairs Dinh Tien Tuan Anh and Tong Van Van for taking care of the proceedings and handling numerous requests from the authors.
- The Test-Of-Time award committee who joined us, namely Debin Gao, Alvaro Cardenas, Surya Nepal and Gene Tsudik, for their input, nominations, and participation in the award selection process.
- General Chairs Phan Duong Hieu and Huynh Quyet Thang, who demonstrated great leadership and dealt with all the logistical and organizational matters.
- The AsiaCCS Steering Committee for their confidence in selecting us as PC Co-Chairs and their support throughout the process leading to the program and successful conference.
- And last but certainly not least, all PC members who are the main driving force of success and whose hard work yielded the excellent program. Special thanks to the recipients of the “Outstanding PC Members”, William Blair, Kristen Moore, Andreas Kogler, George Stergiopoulos, Nir Drucker, Ding Wang, Sofia Celi, Xianghang Mi, Jianliang Wu, for going the extra mile to provide high-quality reviews and volunteering to shepherd and review more papers.

In closing, we look forward to the exciting conference days in beautiful Vietnam in August and hope that all attendees enjoy the conference.

PC Co-Chairs
Mihalis Maniatakos and Yinqian Zhang

Table of Contents

Homomorphic Encryption and Zero knowledge

Enhanced CKKS Bootstrapping with Generalized Polynomial Composites Approximation 1

Seonhong Min (Seoul National University, Republic of Korea), Joon-Woo Lee (Chung-Ang University, Republic of Korea), Yongsoo Song (Seoul National University, Republic of Korea)

An Efficient Circuit Synthesis Framework for TFHE via Convex Sub-graph Optimization 13

Animesh Singh (Indian Institute of Technology, Kharagpur), Ayantika Chatterjee (Indian Institute of Technology, Kharagpur), Anupam Chattopadhyay (Nanyang Technological University, Singapore), Debdeep Mukhopadhyay (Indian Institute of Technology, Kharagpur)

A Novel Asymmetric BSGS Polynomial Evaluation Algorithm under Homomorphic Encryption 30

Qingfeng Wang (University of Chinese Academy of Sciences, China), Li-Ping Wang (University of Chinese Academy of Sciences, China)

Efficient Updatable Private Information Retrieval from Simulatable Homomorphic Ciphertexts 45

Yini Lin (Sun Yat-sen University, China and Monash University, Australia), Haibo Tian (Sun Yat-sen University, China)

Key Extension: Multi-Key FHE Utilizing LWR 58

Mansi Goyal (Indian Institute of Technology Roorkee, India), Aditi Kar Gangopadhyay (Indian Institute of Technology Roorkee, India)

DUPLEX: Scalable Zero-Knowledge Lookup Arguments over RSA Group 72

Semin Han (Hanyang University, Republic of Korea), Geonho Yoon (Hanyang University, Republic of Korea), Hyunok Oh (Hanyang University, Republic of Korea and Zkrypto Inc., Republic of Korea), Jihye Kim (Kookmin university, Republic of Korea)

Multi-party Computation

Pay What You Spend! Privacy-Aware Real-Time Pricing with High Precision IEEE 754 Floating Point Division 87

Soumyadyuti Ghosh (Indian Institute of Technology, Kharagpur), Boyapally Harishma (Technological University, Singapore), Ajith Suresh (Technology Innovation Institute, United Arab Emirates), Arpita Patra (Indian Institute of Science, India), Soumyajit Dey (IIT Kharagpur, India), Debdeep Mukhopadhyay (IIT Kharagpur, India)

Efficient Private Set Intersection by Utilizing Oblivious Transfer Extension 104

Mingli Wu (The University of Hong Kong, Hong Kong), Tsz Hon Yuen (Monash University, Australia), Siu-Ming Yiu (The University of Hong Kong, Hong Kong)

SEEC: Memory Safety Meets Efficiency in Secure Two-Party Computation 118

Henri Dohmen (TU Darmstadt), Robin Hundt (TU Darmstadt), Nora Khayata (TU Darmstadt), Thomas Schneider (TU Darmstadt)

Fair Server-Aided Multiparty Private Set Intersection from OKVS and OPRF 136

Fei Xiao (Xidian University, China), Chunyang Lv (Xidian University, China), Jianfeng Wang (Xidian University, China)

Concretely Efficient Private Set Union via Circuit-Based PSI 149

Gowri R Chandran (TU Darmstadt, Germany), Thomas Schneider (TU Darmstadt, Germany), Maximilian Stillger (TU Darmstadt, Germany), Christian Weinert (University of London, United Kingdom)

Prior-Based Label Differential Privacy via Secure Two-Party Computation 163

Amit Agarwal (University of Illinois, USA), Stanislav Peceny (Georgia Institute of Technology, USA), Mariana Raykova (Google, USA), Phillipp Schoppmann (Google, USA), Karn Seth (Google, USA)

Applied Crypto

A Cryptographic Analysis of Google's PSP and Falcon Channel Protocols 180

Marc Fischlin (Technical University of Darmstadt, Germany), Sascha Hoffmann (Technical University of Darmstadt, Germany), Leonhard Ruppel (Technical University of Darmstadt, Germany), Gözde Saçıak (Technical University of Darmstadt, Germany), Tobias Schnitzler (Technical University of Darmstadt, Germany), Christian Schwarz (Technical University of Darmstadt, Germany), Maximilian Stillger (Technical University of Darmstadt, Germany)

Rejection Sampling for Covert Information Channel: Symmetric Power-Of-2-Choices 198

Dominik Bojko (Wroclaw University of Science and Technology, Poland), Jacek Cichoń (Wroclaw University of Science and Technology, Poland), Mirosław Kutyłowski (NASK National Research Institute, Poland), Oliwer Sobolewski (NASK National Research Institute, Poland)

LogaLookup: Efficient Multivariate Lookup Argument for Accelerated Proof Generation 215

Dien H. A. Tran (University of Science, Vietnam), Tam N. B. Nguyen (University of Science, Vietnam), Nhien-An Le-Khac (University College Dublin, Ireland), Thuc D. Nguyen (University of Science, Vietnam)

Post-Compromise Security with Application-Level Key-Controls - with a Comprehensive Study of the 5G AKMA Protocol 231

Ioana Boureanu (Univ. of Surrey, United Kingdom), Cristina Onete (University of Limoges/XLIM/CNRS, France), Stephan Wesemeyer (Univ. of Surrey, United Kingdom), Léo Robert (Université de Picardie Jules, France), Rhys Miller (Univ. of Surrey, United Kingdom), Pascal Lafourcade (Universite Clermont Auvergne, France), Fortunat Rajaona (University of Surrey, United Kingdom)

Post-Quantum

An Optimized Instantiation of Post-Quantum MQTT Protocol on 8-bit AVR Sensor Nodes 248

YoungBeom Kim (Kookmin University, Republic of Korea), Seog Chung Seo (Kookmin University, Republic of Korea)

Quantum-safe Signatureless DNSSEC 267

Aditya Singh Rawat (Ashoka University, India), Mahabir Prasad Jhanwar (Ashoka University, India)

Ring-LWR based Commitments and ZK-PoKs with Application to Verifiable Quantum-Safe Searchable Symmetric Encryption 283

Debadrita Talapatra (Indian Institute of Technology, India), Nimish Mishra (Indian Institute of Technology, India), Debdeep Mukhopadhyay (Indian Institute of Technology, India)

Practical Deniable Post-Quantum X3DH: A Lightweight Split-KEM for K-Waay 298

Guilhem Niot (PQShield SAS, France and Univ Rennes, CNRS, IRISA, France)

A Quantum-Secure Framework for IoD: Strengthening Authentication and Key-Establishment 313

Salman Shamshad (University of Bristol, United Kingdom), Sana Belguith (University of Bristol, United Kingdom), Alma Oracevic (University of Bristol, United Kingdom)

poqeth: Efficient, Post-Quantum Signature Verification on Ethereum 327

Ruslan Kysil (Eötvös Loránd University, Hungary), István András Seres (Eötvös Loránd University, Hungary), Péter Kutas (Eötvös Loránd University, Hungary and University of Birmingham, United Kingdom), Nándor Kelecsényi (Eötvös Loránd University, Hungary)

LLM for Security

Perses: Unlocking Privilege Escalation for Small LLMs via Extensible Heterogeneity 344

Dominik M. Weber (Huawei Munich Research Center, Germany), Ioannis Tzachristas (Huawei Munich Research Center, Germany), Aifen Sui (Huawei Munich Research Center, Germany)

Generalized Adversarial Code-Suggestions: Exploiting Contexts of LLM-based Code-Completion 358

Karl Rubel (Karlsruhe Institute of Technology, Germany), Maximilian Noppel (Karlsruhe Institute of Technology, Germany), Christian Wressnegger (Karlsruhe Institute of Technology, Germany)

PentestAgent: Incorporating LLM Agents to Automated Penetration Testing 375

Xiangmin Shen (Northwestern University, USA), Lingzhi Wang (Northwestern University, USA), Zhenyuan Li (Zhejiang University, China), Yan Chen (Northwestern University, USA), Wencheng Zhao (Ant Group, China), Dawei Sun (Ant Group, China), Jiashui Wang (Zhejiang University, China), Wei Ruan (Zhejiang University)

SAFE: A Novel Approach for Software Vulnerability Detection from Enhancing the Capability of Large Language Models 392

Van Nguyen (Monash University, Australia and CSIRO's Data61, Australia), Surya Nepal (CSIRO's Data61, Australia), Xingliang Yuan (The University of Melbourne, Australia), Tingmin Wu (CSIRO's Data61, Australia), Carsten Rudolph (Monash University, Australia)

Sounds Vishy: Automating Vishing Attacks with AI-Powered Systems 407

João Figueiredo (Universidade de Lisboa, Portugal), Afonso Carvalho (Universidade de Lisboa, Portugal), Daniel Castro (Universidade de Lisboa, Portugal), Daniel Gonçalves (Universidade de Lisboa, Portugal), Nuno Santos (Universidade de Lisboa, Portugal)

SoK: The Privacy Paradox of Large Language Models: Advancements, Privacy Risks, and Mitigation 425

Yashothara Shanmugarasa (CSIRO's Data61, Australia), Ming Ding (CSIRO's Data61, Australia), Chamikara Mahawaga Arachchige (CSIRO's Data61, Australia), Thierry Rakotoarivelo (CSIRO's Data61, Australia)

ML Security

ChainMarks: Securing DNN Watermark with Cryptographic Chain 442

Brian Choi (Johns Hopkins University, USA), Shu Wang (Palo Alto Networks, Inc., USA), Isabelle Choi (University of California, Los Angeles, USA), Kun Sun (George Mason University, USA)

Toward Malicious Clients Detection in Federated Learning 456

Zhihao Dou (Duke University, USA), Jiaqi Wang (Hainan Normal University, China), Wei Sun (Wichita State University, USA), Zhuqing Liu (University of North Texas, USA), Minghong Fang (University of Louisville, USA)

Nosy Layers, Noisy Fixes: Tackling DRAs in Federated Learning Systems using Explainable AI 473

Meghali Nandi (The University of New South Wales (UNSW), Australia and CSIRO's Data61, Australia), Arash Shaghaghi (The University of New South Wales (UNSW), Australia), Nazatul Haque Sultan (CSIRO's Data61, Australia), Gustavo Batista (The University of New South Wales (UNSW), Australia), Raymond K. Zhao (CSIRO's Data61, Australia), Sanjay Jha (The University of New South Wales (UNSW), Australia)

When Better Features Mean Greater Risks: The Performance-Privacy Trade-Off in Contrastive Learning 488

Ruining Sun (Xiangtan University, China), Hongsheng Hu (University of Newcastle, Australia), Wei Luo (Deakin University, Australia), Zhaoxi Zhang (University of Technology Sydney, Australia), Yanjun Zhang (University of Technology Sydney, Australia), Haizhuan Yuan (Xiangtan University, China), Leo Yu Zhang (Griffith University, Australia)

Unraveling Elevated Data Leakage in Split Learning for Fine-Tuning Stable Diffusion Models 501

Fei Wang (University of Toronto, Canada), Yan Zhu (University of California, Berkeley, USA), Baochun Li (University of Toronto, Canada)

Transferable Adversarial Examples with Bayesian Approach 517

Mingyuan Fan (East China Normal University, China), Cen Chen (East China Normal University, China), Wenmeng Zhou (Alibaba Group, China), Yinggui Wang (Ant Group, China)

ML Applications to Security

Glitch in Time: Exploiting Temporal Misalignment of IMU for Eavesdropping 530

Ahmed Najeeb (RIT, USA and LUMS, Pakistan), Abdul Rafay (LUMS, Pakistan), Muhammad Hamad Alizai (LUMS, Pakistan), Naveed Anwar Bhatti (LUMS, Pakistan)

Eradicating the Unseen: Detecting, Exploiting, and Remediating a Path Traversal Vulnerability across GitHub **542**

Jafar Akhoundali (Leiden University, Netherlands), Hamidreza Hamidi (Technical and Vocational University, Iran), Kristian Rietveld (Leiden University, Netherlands), Olga Gadyatskaya (Leiden University, Netherlands)

PITCH: AI-assisted Tagging of Deepfake Audio Calls using Challenge-Response **559**

Govind Mittal (New York University, USA), Arthur Jakobsson (Carnegie Mellon University, USA), Kelly Marshall (NYU, USA), Chinmay Hegde (New York University, USA), Nasir Memon (New York University, USA)

Minerva: A File-Based Ransomware Detector **576**

Dorjan Hitaj (Sapienza University of Rome, Italy), Giulio Pagnotta (Sapienza University of Rome, Italy), Fabio De Gaspari (Sapienza University of Rome, Italy), Lorenzo De Carli (University of Calgary, Canada), Luigi V. Mancini (Sapienza University of Rome, Italy)

Evaluating Robustness of Reference-based Phishing Detectors **591**

Eunjin Roh (Oregon State University, USA), Sungwoo Jeon (KAIST, Republic of Korea), Sooel Son (KAIST, Republic of Korea), Sanghyun Hong (Oregon State University, USA)

Comprehensive Evaluation of Cloaking Backdoor Attacks on Object Detector in Real-World **605**

Hua Ma (CSIRO, Australia), Alsharif Abuadbba (CSIRO, Australia), Yansong Gao (The University of Western Australia, Australia), Hyoungshick Kim (Sungkyunkwan University, Republic of Korea), Surya Nepal (CSIRO, Australia)

Privacy 1

Enhancing Search Privacy on Tor: Advanced Deep Keyword Fingerprinting Attacks and BurstGuard Defense **621**

Chaiwon Hwang, (Ewha Womans University, Republic of Korea), Haeseung Jeon (Ewha Womans University, Republic of Korea), Jiwoo Hong (Ewha Womans University, Republic of Korea), Hosung Kang (Ewha Womans University, Republic of Korea), Nate Mathews (Rochester Institute of Technology, USA), Goun Kim (Ewha Womans University, Republic of Korea), Se Eun Oh (Ewha Womans University, Republic of Korea)

Robust Locally Differentially Private Graph Analysis **635**

Amrita Roy Chowdhury (University of Michigan, Ann Arbor, USA), Jacob Imola (University of Copenhagen, Denmark), Kamalika Chaudhuri (UCSD, USA)

PSP: A Privacy-Preserving Self-certify Pseudonym Protocol for V2X **651**

Xuyuan Cai (The Hong Kong Polytechnic University, Hong Kong), Rui Song (The Hong Kong Polytechnic University, Hong Kong), Bin Xie (The Hong Kong Polytechnic University, Hong Kong), Qingjun Xiao (Southeast University of China, China), Bin Xiao (The Hong Kong Polytechnic University, Hong Kong)

Unveiling Privacy Risks in Quantum Optimization Services 665

Mateusz Leśniak (National Research Institute, Poland), Michał Wroński (National Research Institute, Poland), Ewa Syta (Trinity College, USA), Mirosław Kutyłowski (National Research Institute, Poland)

QUIC-Exfil: Exploiting QUIC's Server Preferred Address Feature to Perform Data Exfiltration Attacks 682

Thomas Grübl (University of Zürich UZH, Switzerland), Weijie Niu (University of Zürich UZH, Switzerland), Jan von der Assen (University of Zürich UZH, Switzerland), Burkhard Stiller (University of Zürich UZH, Switzerland)

ClearMask: Noise-Free and Naturalness-Preserving Protection Against Voice Deepfake Attacks 696

Yuanda Wang (Michigan State University, USA), Bocheng Chen (Michigan State University, USA), Hanqing Guo (University of Hawaii at Manoa, USA), Guangjing Wang (University of South Florida, USA), Weikang Ding (Michigan State University, USA), Qiben Yan (Michigan State University, USA)

Privacy 2

Slice it up: Unmasking User Identities in Smartwatch Health Data 710

Lucas Lange (Leipzig University & ScaDS.AI Dresden/Leipzig, Germany), Tobias Schreieder (Leipzig University & ScaDS.AI Dresden/Leipzig, Germany), Victor Christen (Leipzig University & ScaDS.AI Dresden/Leipzig, Germany), Erhard Rahm (Leipzig University & ScaDS.AI Dresden/Leipzig, Germany)

Secure Steganography Based on Chaos-Aided Quantization Index Modulation 727

Shanxiang Lyu (Jinan University, China), Xinquan Xu (Jinan university, China), Ling Liu (Xidian University, China), Lip Yee Por (Universiti Malaya, Malaysia)

App-solutely Modded: Surveying Modded App Market Operators and Original App Developers 739

Luis A. Saavedra (University of Cambridge, United Kingdom), Hridoy S. Dutta (University of Cambridge, United Kingdom), Alastair R. Beresford (University of Cambridge, United Kingdom), Alice Hutchings (University of Cambridge, United Kingdom)

Proxies as Sensors: Measuring Censorship of Refraction Networking in Iran 759

Abdulrahman Alaraj (University of Colorado Boulder, USA and Prince Sattam Bin Abdulaziz University, Saudi Arabia), Eric Wustrow (University of Colorado Boulder, USA)

Virtual End-to-End Encryption: Analysis of the Doctolib Protocol 773

Dennis Dayanikli (University of Potsdam, Germany), Laura Holz (University of Potsdam, Germany), Anja Lehmann (University of Potsdam, Germany)

Towards Usability of Data with Privacy: A Unified Framework for Privacy-Preserving Data Sharing with High Utility 790

M.A.P. Chamikara (CSIRO's Data61, Australia), Seung Ick Jang (CSIRO's Data61, Australia), Ian Oppermann (University of Technology Sydney, Australia), Dongxi Liu (CSIRO's Data61, Australia), Musotto Roberto (D'Angelo Legal, Australia), Sushmita Ruj (University of New South Wales, Australia), Arindam Pal (TechSoftX, Australia), Meisam Mohammady (Iowa State University, USA), Seyit Camtepe (CSIRO's Data61, Australia), Sylvia Young (Department of Health, Australia), Chris Dorrian (Department of Health, Australia), Nasir David (Department of Health, Australia)

Blockchain 1

Fast SNARK-based Non-Interactive Distributed Verifiable Random Function with Ethereum Compatibility 807

Jia Liu (Enya Labs, USA), Mark Manulis (Universität der Bundeswehr München, Germany)

VeRange: Verification-efficient Zero-knowledge Range Arguments with Transparent Setup for Blockchain Applications and More 823

Yue Zhou (Australian National University, Australia), Sid Chi-Kin Chau (CSIRO, Australia)

Scalable Time-Lock Puzzle 839

Aydin Abadi (Newcastle University, USA), Dan Ristea (University College London, United Kingdom), Artem Grigor (University of Oxford, United Kingdom), Steven Murdoch (University College London, United Kingdom)

BIP32-Compatible Threshold Wallets 856

Poulami Das (Least Authority, Germany), Andreas Erwig (Technische Universität Darmstadt, Germany), Sebastian Faust (Technische Universität Darmstadt, Germany), Philipp-Florens Lehwalder (Technische Universität Darmstadt, Germany), Julian Loss (CISPA Helmholtz Center for Information Security, Germany), Ziyan Qu (Technische Universität Darmstadt, Germany), Siavash Riahi (Technische Universität Darmstadt, Germany)

Blockchain 2

FIRST: FrontrunnIng Resistant Smart ConTracts 873

Emrah Sariboz (New Mexico State University, USA), Gaurav Panwar (New Mexico State University, USA), Roopa Vishwanathan (New Mexico State University, USA), Satyajayant Misra (New Mexico State University, USA)

Mining Attack with Zero Knowledge in the Blockchain 890

Yu Jiaping (Ocean University of China, China and The Hong Kong Polytechnic University, Hong Kong), Gao Shang (The Hong Kong Polytechnic University, Hong Kong), Song Rui (The Hong Kong Polytechnic University, Hong Kong), Zhiping Cai (National University of Defense Technology, China), Xiao Bin (The Hong Kong Polytechnic University, Hong Kong)

Infiltrated Selfish Mining: Think Win-Win to Escape Dilemmas..... 906

Xuelian Cao (Southwest University, China), Zheng Yang (Southwest University, China), Tao Xiang (Chongqing University, China), Jianting Ning (Wuhan University, China), Yuhan Liu (Southwest University, China), Zhiming Liu (Southwest University, China), Jianying Zhou (Singapore University of Technology and Design, Singapore)

BRC20 Snipping Attack..... 923

Minfeng Qi (City University of Macau, China), Qin Wang (CSIRO Data61, Australia), Ningran Li (The University of Adelaide, Australia), Shiping Chen (CSIRO Data61, Australia), Tianqing Zhu (City University of Macau, China)

Blockchain 3

An Empirical Study on Cross-chain Transactions: Costs, Inconsistencies, and Activities..... 939

Kailun Yan (Shandong University, China and George Mason University, USA), Bo Lu (George Mason University, USA), Pranav Agrawal (George Mason University, USA), Jiasun Li (George Mason University, USA), Wenrui Diao (Shandong University, China), Xiaokuan Zhang (George Mason University, USA)

AWOSE: Probabilistic State Model for Consensus Algorithms Fuzzing Frameworks 955

Tannishtha Devgun (University of Padua, Italy and University of Camerino, Italy), Gulshan Kumar (University of Padua, Italy and Lovely Professional University, India), Rahul Saha (University of Padua, Italy and Lovely Professional University, India), Alessandro Brighente (University of Padua, Italy), Mauro Conti (University of Padua, Italy and Örebro University, Sweden)

DTL: Data Tumbling Layer A Composable Unlinkability for Smart Contracts..... 971

Mohsen Minaei (Visa Research, USA), Pedro Moreno-Sanchez (IMDEA Software Institute, Spain and Visa Research, USA and MPI-SP, Germany), Zhiyong Fang (Texas A&M University, USA), Srinivasan Raghuraman (Visa Research, USA and MIT, USA), Navid Alamati (VISA Research, USA), Panagiotis Chatzigiannis (Visa Research, USA), Ranjit Kumaresan (Visa Research, USA), Duc V. Le (Visa Research, USA)

Pace: Privacy-Preserving and Atomic Cross-Chain Swaps for Cryptocurrency Exchanges..... 985

Jianhuan Wang (The Hong Kong Polytechnic University, Hong Kong), Bin Xiao (The Hong Kong Polytechnic University, Hong Kong)

IoT Security

NoBU: An Effective and Viable Cyber-Physical Solution to Thwart BadUSB Attacks..... 1003

Andrea Ciccotelli (King Abdullah University of Science and Technology (KAUST), Saudi Arabia), Maurantonio Caprolu (King Abdullah University of Science and Technology (KAUST), Saudi Arabia), Roberto Di Pietro (King Abdullah University of Science and Technology (KAUST), Saudi Arabia)

Your Control Host Intrusion Left Some Physical Breadcrumbs: Physical Evidence-Guided Post-Mortem Triage of SCADA Attacks 1016

Moses Ike (Sandia National Laboratories, USA), Keaton Sadoski (Sandia National Laboratories, USA), Romuald Valme (Sandia National Laboratories, USA), Burak Sahin (Georgia Institute of Technology, USA), Saman Zonouz (Georgia Institute of Technology, USA), Wenke Lee (Georgia Institute of Technology, USA)

Bits and Pieces: Piecing Together Factors of IoT Vulnerability Exploitation..... 1032

Arwa Abdulkarim Al Alsadi (Delft University of Technology, Netherlands), Mathew Vermeer (Delft University of Technology, Netherlands), Takayuki Sasaki (Yokohama National University, Japan), Katsunari Yoshioka (Yokohama National University, Japan), Michel Van Eeten (Delft University of Technology, Netherlands), Carlos Gañán (Delft University of Technology, Netherlands)

AuthentiSafe: Lightweight and Future-Proof Device-to-Device Authentication for IoT 1050

Lukas Petzi (University of Würzburg, Germany), Torsten Krauß (University of Würzburg, Germany), Alexandra Dmitrienko (University of Würzburg, Germany), Gene Tsudik (UC Irvine, USA)

CPS Security

Runtime Stealthy Perception Attacks against DNN-based Adaptive Cruise Control Systems..... 1065

Xugui Zhou (Louisiana State University, USA), Anqi Chen (Northeastern University, USA), Maxfield Kouzel (University of Virginia, USA), Haotian Ren (University of Virginia, USA), Morgan McCarty (Northeastern University, USA), Cristina Nita-Rotaru (Northeastern University, USA), Homa Alemzadeh (University of Virginia, USA)

Adversarial Fog: Exploiting the Vulnerabilities of LiDAR Point Cloud Preprocessing Filters..... 1083

Yuna Tanaka (Waseda University, Japan and Deloitte Tohmatsu Cyber LLC, Japan), Kazuki Nomoto (Waseda University, Japan and Deloitte Tohmatsu Cyber LLC, Japan), Ryunosuke Kobayashi (Waseda University, Japan), Go Tsuruoka (Waseda University, Japan), Tatsuya Mori (Waseda University/NICT/RIKEN, Japan)

From Transients to Flips: Hardware-level Bit Manipulation of In-Vehicle Serial Communication 1101

Abdullah Zubair Mohammed (Virginia Tech, USA), Ryan Gerdes (Virginia Tech, USA)

Preventing Radio Fingerprinting through Low-Power Jamming 1114

Muhammad Irfan (Hamad Bin Khalifa University, Qatar), Savio Sciancalepore (Eindhoven University of Technology, Netherlands), Gabriele Oligeri (Hamad Bin Khalifa University, Qatar)

Hardware Security

N-Tracer: A Trace Driven Attack on NoC-Based MPSoC Architecture 1127

Dipesh (Indian Institute of Technology Kanpur, India), Urbi Chatterjee (Indian Institute of Technology Kanpur, India)

FP-Rowhammer: DRAM-Based Device Fingerprinting 1141

Hari Venugopalan (University of California, Davis, USA), Kaustav Goswami (University of California, Davis, USA), Zainul Abi Din (Independent Researcher, USA), Jason Lowe-Power (University of California, Davis, USA), Samuel T. King (University of California, Davis, USA), Zubair Shafiq (University of California, Davis, USA)

ProbeShooter: A New Practical Approach for Probe Aiming 1158

Daehyeon Bae (Korea University, Republic of Korea), Sujin Park (Korea University, Republic of Korea), Minsig Choi (Korea University, Republic of Korea), Young-Giu Jung (YM-NaeulTech., Republic of Korea), Changmin Jeong (Agency for Defense Development, Republic of Korea), Heeseok Kim (Korea University, Republic of Korea), Seokhie Hong (Korea University, Republic of Korea)

GAE4HT: Detecting Hardware Trojans with Graph Autoencoder-Trained on Golden Model Data Flow Graphs 1175

Daehyeon Lee (Korea University Seoul, Republic of Korea), Junghee Lee (Korea University Seoul, Republic of Korea)

Monocle: Transient Execution Proof Memory Views for Runtime Compiled Code..... 1188

Matteo Oldani (ETH Zurich, Switzerland and Oracle Labs, Switzerland), William Blair (Oracle Labs, USA), Shweta Shinde (ETH Zurich, Switzerland), Matthias Neugschwandtner (Oracle Labs, Austria)

Okapi: Efficiently Safeguarding Speculative Data Accesses in Sandboxed Environments 1203

Philipp Schmitz (RPTU Kaiserslautern-Landau, Germany), Tobias Jauch (RPTU Kaiserslautern-Landau, Germany), Alex Wezel (RPTU Kaiserslautern-Landau, Germany), Mohammad Rahmani Fadiheh (Stanford University, USA), Thore Tiemann (University of Lübeck, Germany), Jonah Heller (University of Lübeck, Germany), Thomas Eisenbarth (University of Lübeck, Germany), Dominik Stoffel (RPTU Kaiserslautern-Landau, Germany), Wolfgang Kunz (RPTU Kaiserslautern-Landau, Germany)

Fault Injection and Side Channels

FAULT+PROBE: A Generic Rowhammer-based Bit Recovery Attack..... 1219

Kemal Derya (Worcester Polytechnic Institute, USA), M. Caner Tol (Worcester Polytechnic Institute, USA), Berk Sunar (Worcester Polytechnic Institute, USA)

Three Glitches to Rule One Car: Fault Injection Attacks on a Connected EV..... 1235

Niclas Kühnapfel (TU Berlin, Germany), Christian Werling (TU Berlin, Germany), Hans Niklas Jacob (TU Berlin, Germany), Jean-Pierre Seifert (TU Berlin, Germany)

AVXProbe: Enhancing Website Fingerprinting with Side-Channel-Assisted Kernel-Level Traces 1250

Suryeon Kim (KAIST, Republic of Korea), Seung Ho Na (KAIST, Republic of Korea), Jaehan Kim (KAIST, Republic of Korea), Seungwon Shin (KAIST, Republic of Korea), Hyunwoo Choi (Sungshin Women's University, Republic of Korea)

BranchGauge: Modeling and Quantifying Side-Channel Leakage in Randomization-Based Secure Branch Predictors..... 1265

Quancheng Wang (Wuhan University, China), Ming Tang (Wuhan University, China), Ke Xu (Wuhan University, China), Han Wang (Wuhan University, China)

Telescope: Top-Down Hierarchical Pre-silicon Side-channel Leakage Assessment in System-on-Chip Design 1280

Zhenyuan Liu (Worcester Polytechnic Institute, USA), Andrew Malnicof (Worcester Polytechnic Institute, USA), Arna Roy (Worcester Polytechnic Institute, USA), Patrick Schaumont (Worcester Polytechnic Institute, USA)

EXAM: Exploiting Exclusive System-Level Cache in Apple M-Series SoCs for Enhanced Cache Occupancy Attacks 1294

Tianhong Xu (Northeastern University, USA), Aidong Adam Ding (Northeastern University, USA), Yunsi Fei (Northeastern University, USA)

Web Security

Open Access Alert: Studying the Privacy Risks in Android WebView's Web Permission Enforcement 1309

Trung Tin Nguyen (CISPA Helmholtz Center for Information Security, Germany), Ben Stock (CISPA Helmholtz Center for Information Security, Germany)

TrustyMon: Practical Detection of DOM-based Cross-Site Scripting Attacks Using Trusted Types 1323

Sunnyeo Park (KAIST, Republic of Korea), Jihwan Kim (KAIST, Republic of Korea), Seongho Keum (KAIST, Republic of Korea), Hyunjoon Lee (KAIST, Republic of Korea), Sooel Son (KAIST, Republic of Korea)

ProwseBox: A Framework for the Analysis of the Web at Scale 1338

Dolière Francis Somé (CISPA Helmholtz Center for Information Security, Germany)

BISON: Blind Identification with Stateless scOped pseudoNyms 1355

Jakob Heher (Graz University of Technology, Austria and Secure Information Technology Center Austria (A-SIT), Austria), Stefan More (Graz University of Technology, Austria and Secure Information Technology Center Austria (A-SIT), Austria), Lena Heimberger (Graz University of Technology, Austria)

Protocols and Formal Models for Delegated Authorisation with Server-Side Secrecy 1372

Jean Snyman (University of Surrey, United Kingdom and Hewlett Packard Enterprise, United Kingdom), Chris Culnane (Castellate Consulting Ltd London, United Kingdom and University of Melbourne, Australia), Ioana Boureanu (University of Surrey, United Kingdom), Gerault David (Technology Innovation Institute (TII), United Arab Emirates)

OblivCDN: A Practical Privacy-preserving CDN with Oblivious Content Access 1394

Viet Vo (Swinburne University of Technology, Australia), Shangqi Lai (CSIRO's Data61, Australia), Xingliang Yuan (The University of Melbourne, Australia), Surya Nepal (CSIRO's Data61 Australia, Australia), Qi Li (Tsinghua University, China)

Network Security

OMAD5G: Online Malware Detection in 5G Networks using Compound Paths 1411

Zhixin Wen (Binghamton University, USA), Guanhua Yan (Binghamton University, USA)

Ruling the Unruly: Designing Effective, Low-Noise Network Intrusion Detection Rules for Security Operations Centers 1428

Koen T. W. Teuwen (Eindhoven University of Technology, Netherlands), Tom Mulders (Eindhoven University of Technology, Netherlands), Emmanuele Zambon (Eindhoven University of Technology, Netherlands), Luca Allodi (Eindhoven University of Technology, Netherlands)

SigN: SIMBox Activity Detection Through Latency Anomalies at the Cellular Edge 1442

Anne Josiane Kouam (TU Berlin, Germany), Aline Carneiro Viana (INRIA, France), Philippe Martins (Telecom Paris, France), Cédric Adjih (INRIA, France), Alain Tchana (Grenoble INP, France)

An Automated Blackbox Noncompliance Checker for QUIC Server Implementations 1459

Kian Kai Ang (The University of Adelaide, Australia), Guy Farrelly (The University of Adelaide, Australia), Cheryl Pope (The University of Adelaide, Australia), Damith C. Ranasinghe (The University of Adelaide, Australia)

Formal Analysis of SDNsec: Attacks and Corrections for Payload, Route Integrity and Accountability 1476

Ayoub Ben Hassen (École Supérieure des Communications, Tunisia), Pascal Lafourcade (Université Clermont Auvergne, CNRS, Clermont, France), Dhekra Mahmoud (Université Clermont Auvergne, CNRS, Clermont, France), Maxime Puys (Université Clermont Auvergne, CNRS, Clermont, France)

Learning to Identify Conflicts in RPKI 1490

Haya Schulmann (Goethe-Universität Frankfurt and National Research, Germany), Shujie Zhao (Fraunhofer SIT, ATHENE, Germany)

Usable Security and Privacy

NailKey: Mutable Biometric Using Fingernails 1506

Yihong Hang (ShanghaiTech University, China), Zhice Yang (ShanghaiTech University, China)

Different Seas, Different Phishes – Large-Scale Analysis of Phishing Simulations Across Different Industries 1520

Oskar Braun (AWARE7 GmbH, Germany and Rhine-Waal University of Applied Sciences, Germany), Jan Hörnemann (AWARE7 GmbH, Germany and Westphalian University of Applied Sciences, Germany), Norbert Pohlmann (Westphalian University of Applied Sciences, Germany), Tobias Urban (Westphalian University of Applied Sciences, Germany), Matteo Grosse-Kampmann (Rhine-Waal University of Applied Sciences, Germany)

Can Small-scale Evaluation Reflect Real Ability? A Performance Study of Emerging Biometric Authentication..... 1535

Hangcheng Cao (University of Electronic Science and Technology of China, China), Guowen Xu (University of Electronic Science and Technology of China, China), Wenbin Huang (Nanjing University of Information Science and Technology, China), Hongwei Li (University of Electronic Science and Technology of China, China)

The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails against Organizations..... 1550

Marie Weinz (University of Liechtenstein, Liechtenstein), Nicola Zannone (Eindhoven University of Technology, Netherlands), Luca Allodi (Eindhoven University of Technology, Netherlands), Giovanni Apruzzese (University of Liechtenstein, Liechtenstein)

PRISM: To Fortify Widget Based User-App Data Exchanges Using Android Virtualization Framework..... 1567

YingTat Ng (Singapore Management University, Singapore), Zhe Chen (Singapore Management University, Singapore), Haiqing Qiu (Singapore Management University, Singapore), Xuhua Ding (Singapore Management University, Singapore)

On the Account Security Risks Posed by Password Strength Meters..... 1582

Ming Xu (Fudan University, China and National University of Singapore, Singapore), Weili Han (Fudan University, China), Jitao Yu (Fudan University, China), Jing Liu (UC Irvine & MPI-SP, USA), Xinyi Zhang (Meta, USA), Yun Lin (Shanghai Jiao Tong University, China), Jin Song Dong (National University of Singapore, Singapore)

Software and OS Security

Can You Run My Code? A Close Look at Process Injection in Windows Malware..... 1600

Giorgia Di Pietro (Sapienza University of Rome, Italy), Daniele Cono D'Elia (Sapienza University of Rome, Italy), Leonardo Querzoni (Sapienza University of Rome, Italy)

CryptoGuard: Lightweight Hybrid Detection and Response to Host-based Cryptojackers in Linux Cloud Environments..... 1617

Gyeonghoon Park (UC Irvine, USA), Jaehan Kim (KAIST, Republic of Korea), Jinu Choi (Kwangwoon University, Republic of Korea), Jinwoo Kim (Kwangwoon University, Republic of Korea)

Vulnerable Intel GPU Context: Prohibit Complete Context Restore by Modifying Kernel Driver..... 1632

Wonseok Choi (Korea University, Republic of Korea), Youngjoo Shin (Korea University, Republic of Korea)

Sigy: Breaking Intel SGX Enclaves with Malicious Exceptions & Signals..... 1643

Supraja Sridhara (ETH Zurich, Switzerland), Andrin Bertschi (ETH Zurich, Switzerland), Benedict Schlüter (ETH Zurich, Switzerland), Shweta Shinde (ETH Zurich, Switzerland)

SoK: A Literature and Engineering Review of Regular Expression Denial of Service (ReDoS)..... 1659

Masudul Hasan Masud Bhuiyan (CISPA Helmholtz Center for Information Security, Germany), Berk Çakar (Purdue University, USA), Ethan H. Burmane (Purdue University, USA), James C. Davis (Purdue University, USA), Cristian-Alexandru Staicu (CISPA Helmholtz Center for Information Security, Germany)

Systematic Analysis of Kernel Security Performance and Energy Costs 1676

Fabian Rauscher (Graz University of Technology, Austria), Benedict Herzog (Ruhr-Universität Bochum, Germany), Timo Hönig (Ruhr-Universität Bochum, Germany), Daniel Gruss (Graz University of Technology, Austria)

Binary Security

Breaking Bad: How Compilers Break Constant-Time Implementations 1690

Moritz Schneider (ETH Zurich, Switzerland), Daniele Lain (ETH Zurich, Switzerland), Ivan Puddu (ETH Zurich, Switzerland), Nicolas Dutly (ETH Zurich, Switzerland), Srdjan Capkun (ETH Zurich, Switzerland)

An Empirical Study of C Decompilers: Performance Metrics and Error Taxonomy 1707

Melih Sirlanci (The Ohio State University, USA), Carter Yagemann (The Ohio State University, USA), Zhiqiang Lin (The Ohio State University, USA)

Enhancing Binary Code Similarity Analysis for Software Updates: A Contextual Diffing Framework 1724

August See (Universität Hamburg, Germany), Moritz Mönnich (Universität Hamburg, Germany), Mathias Fischer (Universität Hamburg, Germany)

Evaluating Disassembly Errors with only Binaries 1741

Lambang Akbar Wijayadi (National University of Singapore, Singapore), Yuancheng Jiang (National University of Singapore, Singapore), Roland H.C. Yap (National University of Singapore, Singapore), Zhenkai Liang (National University of Singapore, Singapore), Zhuohao Liu (National University of Singapore, Singapore)

Enabling Microarchitectural Agility: Taking ML-KEM & ML-DSA from Cortex-M4 to M7 with SLOTHY 1756

Amin Abdulrahman (Max Planck Institute for Security and Privacy (MPI-SP), Germany), Matthias J. Kannwischer (Chelpis Quantum Corp, Taiwan), Thing-Han Lim (Chelpis Quantum Corp, Taiwan)

REFLECTA: Reflection-based Scalable and Semantic Scripting Language Fuzzing 1772

Chibin Zhang (EPFL, Switzerland), Gwangmu Lee (EPFL, Switzerland), Qiang Liu (EPFL, Switzerland), Mathias Payer (EPFL, Switzerland)

Poster

POSTER: Stealthy SWAP-Based Side-Channel Attack on Multi-Tenant Quantum Cloud Systems..... 1788

Wei Jie Bryan Lee (Nanyang Technological University, Singapore), Siyi Wang (Nanyang Technological University, Singapore), Suman Dutta (Nanyang Technological University, Singapore), Walid El Maouaki (Hassan II University of Casablanca, Morocco), Anupam Chattopadhyay (Nanyang Technological University, Singapore)

Poster: Typosquatting Attacks on the Rust Ecosystem..... 1791

Minh-Khanh Vu (Birmingham City University, Vietnam), Thanh-Cong Nguyen (University of Information Technology, Vietnam), Duc-Ly Vu (Easter International University, Vietnam)

POSTER: Disappearing Ink: How Partial Model Extraction Erases Watermarks..... 1794

Venkata Sai Pranav Bachina (International Institute of Information Technology, India), Ankit Gangwal (International Institute of Information Technology, India)

POSTER: Transparent Temporally-Specialized System Call Filters..... 1797

Matthew Rossi (Università degli Studi di Bergamo, Italy), Michele Beretta (Università degli Studi di Bergamo, Italy), Dario Facchinetti (Università degli Studi di Bergamo, Italy), Stefano Paraboschi (Università degli Studi di Bergamo, Italy)

POSTER: Policy-Driven Security-Aware Scheduling in Kubernetes 1800

Matthew Rossi (Università degli Studi di Bergamo, Italy), Michele Beretta (Università degli Studi di Bergamo, Italy), Dario Facchinetti (Università degli Studi di Bergamo, Italy), Stefano Paraboschi (Università degli Studi di Bergamo, Italy)

POSTER: An Empirical Study of Smart Contract Patching Practices in the Wild..... 1803

Taeyoung Kim (Sungkyunkwan University, Republic of Korea), Gilhee Lee (Sungkyunkwan University, Republic of Korea), Hyoungshick Kim (Sungkyunkwan University, Republic of Korea)

POSTER: Automating ICS Malware Analysis with MITRE ATT&CK..... 1806

Fatih Kurt (Cardiff University, United Kingdom), Neetesh Saxena (Cardiff University, United Kingdom), Vijay Kumar (Cardiff University, United Kingdom), George Theodorakopoulos (Cardiff University, United Kingdom)

POSTER: When Models Speak Too Much: Privacy Leakage on Large Language Models..... 1809

MingJun Zhang (ANU, Australia), Mahrokh Abdollahi (CSIRO, Australia), Thilina Ranbaduge (CSIRO, Australia), Ming Ding (CSIRO, Australia)

POSTER: Investigating Transferability of Adversarial Examples in Model Merging..... 1812

Ankit Gangwal (International Institute of Information Technology, India), Aaryan Ajay Sharma (International Institute of Information Technology, India)

POSTER: Multimodal Graph Networks for Systematic Generalization in Code Clone Detection..... 1815

Cuong Dao (Hanoi University of Civil Engineering, Vietnam), Van Tong (University of Science and Technology, Vietnam), Hai Anh Tran (University of Science and Technology, Vietnam), Duc Tran (University of Science and Technology, Vietnam), Giang Nguyen (University of Science and Technology, Vietnam)

POSTER: SuriCap - A Measurement Platform to Study and Evaluate Intrusion Detection Rule Engineering..... 1818

Koen T. W. Teuwen (Eindhoven University of Technology, Netherlands), Emmanuele Zambon (Eindhoven University of Technology, Netherlands), Luca Allodi (Eindhoven University of Technology, Netherlands)

ASIA CCS'25 Organisation

General Chairs	Huynh Quyet Thang (Hanoi University of Science and Technology, Vietnam) Phan Duong Hieu (Institut Polytechnique de Paris, France)
Program Chairs	Michail Maniatakos (New York University Abu Dhabi, UAE) Yinqian Zhang (Southern University of Science and Technology, China)
Local Organising Chairs	Huynh Thi Thanh Binh (Hanoi University of Science and Technology, Vietnam) Tran Quang Duc (Hanoi University of Science and Technology, Vietnam)
Workshop Chair	Khoa Nguyen (University of Wollongong, Australia)
Poster Chairs	Pham Van Thuan (University of Melbourne, Australia) Yue Duan (Singapore Management University, Singapore)
Sponsorship Chair	Le Xuan Thanh (Hanoi University of Science and Technology, Vietnam)
Web Chair	Tran Hai Anh (Hanoi University of Science and Technology, Vietnam)
Publicity Chairs	Vo Quang Viet (Swinburne University of Technology, Australia) Cao Minh Phuong (University of Illinois at Urbana-Champaign, USA)
Publication Chairs	Dinh Tien Tuan Anh (Deakin University, Australia) Tong Van Van (Hanoi University of Science and Technology, Vietnam)
Steering Committee	Gail-Joon Ahn (Arizona State University, USA) Robert Deng (Singapore Management University, Singapore) Adrian Perrig (ETH Zürich, Switzerland) Kui Ren (Zhejiang University, China) Shiuhpyng Shieh (National Chiao Tung University, Taiwan) Xiaofeng Wang (Indiana University Bloomington, USA) Jianying Zhou (Singapore University of Technology and Design, Singapore)
Program Committee	Abdelrahaman Aly, Technology Innovation Institute, UAE Abhishek Bichhawat, IIT Gandhinagar Adithya Vadapalli, IIT Kanpur Alejandro Cuevas, Carnegie Mellon University Alessandro Brighente, University of Padova Alptekin Küpçü, Koç University Andreas Kogler, Graz University of Technology Anjia Yang, Jinan University Annabelle McIver, Macquarie University Awais Rashid, University of Bristol, UK Bo Chen, Michigan Technological University Carlos Rubio-Medrano, Texas A&M University- Corpus Christi Changhai Ou, Wuhan University Charalambos Konstantinou, KAUST Chenglu Jin, CWI Amsterdam

	Chia-Mu Yu, National Yang Ming Chiao Tung University Coby Wang, Visa Research Daisuke Mashima, Singapore University of Technology and Design Debin Gao, Singapore Management University Ding Wang, Nankai University Duc Le, Visa Research (Cycle 1 only) Fabio De Gaspari, Sapienza University of Rome Fan Zhang, Zhejiang University Fei Zuo, University of Central Oklahoma Gabriele Oligeri, Hamad bin Khalifa University George Stergiopoulos, University of the Aegean Ghada Almashaqbeh, University of Connecticut Guoxing Chen, Shanghai Jiao Tong University Gustavo Banegas, INRIA Haifeng Yu, National University of Singapore Hao Zhou, The Hong Kong Polytechnic University Haoyu Ma, Zhejiang Lab Haoyu Wang, Huazhong University of Science and Technology Hervé Debar, Télécom SudParis Huawei Huang, Sun Yat-sen University Hung Nguyen, The University of Adelaide Hyoungshick Kim, Sungkyunkwan University Ioannis Demertzis, UCSC Jianliang Wu, Simon Fraser University Jianyu Niu, Southern University of Science and Technology Jin-Hee Cho, Virginia Tech Joaquin GARCIA ALFARO, Institut Polytechnique de Paris Juanru Li, Shanghai Jiao Tong University Jun Sakuma, Tokyo Institute of Technology Kan Yang, University of Memphis Kasper Rasmussen, University of Oxford Katerina Mitrokotsa, University of St. Gallen, Switzerland Katsunari Yoshioka, Yokohama National University Kehuan Zhang, The Chinese University of Hong Kong Kevin Leach, Vanderbilt University Kristen Moore, CSIRO's Data61 Kun Sun, George Mason University Kwok-Yan Lam, Nanyang Technological University, Singapore Lei Xu, Nanjing University of Science and Technology Lei Yu, Rensselaer Polytechnic Institute Leo Zhang, Griffith University Lilas Alrahis, Khalifa University Man Ho Au, The Hong Kong Polytechnic University (Cycle 1 only) Manaar Alam, New York University Abu Dhabi Marcus Botacin, Texas A&M University Mengyuan Li, USC

	Michele Carminati, Politecnico di Milano Min Chen, CISPA Helmholtz Center for Information Security (Cycle 1 only) Minghong Fang, University of Louisville Minghui Xu, Shandong University Mohammad Ashiqur Rahman, Florida International University Nalin Arachchilage, RMIT University, Australia Natalia Stakhanova, University of Saskatchewan, Canada Neetesh Saxena, Cardiff University Nektarios Tsoutsos, University of Delaware Ning Wang, University of South Florida Ning Zhang, Washington University in St. Louis Ningyu He, The Hong Kong Polytechnic University Nir Drucker, IBM Research – Israel Olga Gadyatskaya, Leiden University Peng Gao, Virginia Tech Pengfei Hu, Shandong University Prabhu Karthikeyan Rajasekaran, Google Prashant Hari Narayan Rajput, InterSystems Qingyang Wang, Louisiana State University Rakesh Bobba, Oregon State University Roberto Guanciale, KTH Roopa Vishwanathan, New Mexico State University Rui Ning, Old Dominion University (Cycle 1 only) Runchao Han, Babylon Labs Salil Kanhere, University of New South Wales Sandra Rueda, Universidad de los Andes, Colombia Sanghyun Hong, Oregon State University (Cycle 1 only) Satoshi Obana, Hosei University Seetal Potluri, University at Albany, SUNY Seunghoon Woo, Korea University Shalabh Jain, Bosch Research Sherman S. M. Chow, The Chinese University of Hong Kong Shih-Wei Li, National Taiwan University Shuo Wang, Shanghai Jiao Tong University Siqi Ma, The University of New South Wales Sofia Celi, Brave Song Fang, University of Oklahoma Soteris Demetriou, Imperial College London Steve Granda, National Renewable Energy Laboratory Sven Dietrich, City University of New York Sze Yiu Chau, The Chinese University of Hong Kong Tingmin Wu, CSIRO's Data61 Viet Vo, Swinburne University of Technology Weijia Wang, Shandong University William Blair, SpaceX

	Xiang Li, Nankai University Xianghang Mi, USTC Xiangkun Jia, Institute of Software Chinese Academy of Sciences Xiaokuan Zhang, George Mason University Xiaoli ZHANG, University of Science and Technology Beijing Xiaoning Liu, RMIT University, Australia Xiapu Luo, The Hong Kong Polytechnic University Xinda Wang, University of Texas at Dallas Xingliang Yuan, University of Melbourne Xinlei He, Hong Kong University of Science and Technology (Guangzhou) Xueqiang Wang, University of Central Florida Xuhua Ding, SMU Yan Lin, Jinan University Yanjiao Chen, Zhejiang University Yansong Gao, Data61, CSIRO Yifeng Zheng, The Hong Kong Polytechnic University Yinzhi Cao, Johns Hopkins University Yuanchao Xu, University of California Santa Cruz Zhe Wang, ICT, CAS Zhenyu Ning, Hunan University Zhi Zhang, The University of Western Australia Zhibo Wang, Zhejiang University Ziming Zhao, Northeastern University Zubair Baig, Deakin University
Poster Reviewers	Amirmohammad Pasdar (The University of Melbourne, Australia) Soohyeon Choi (Singapore Management University, Singapore) Pham Van Thuan (University of Melbourne, Australia) Yue Duan (Singapore Management University, Singapore)

ASIA CCS'25 Sponsor and Supporters

Main Sponsors

Supporter

Supporting Partner

Bronze Sponsor

POSTER

POSTER: Policy-driven security-aware scheduling in Kubernetes

MATTHEW ROSSI, University of Bergamo, Bergamo, BG, Italy

MICHELE BERETTA, University of Bergamo, Bergamo, BG, Italy

DARIO FACCHINETTI, University of Bergamo, Bergamo, BG, Italy

STEFANO PARABOSCHI, University of Bergamo, Bergamo, BG, Italy

Published: 25 August 2025

Citation in BibTeX format

ASIA CCS '25: 20th ACM Asia Conference on Computer and Communications Security
August 25 - 29, 2025
Hanoi, Vietnam

Conference Sponsors:
SIGSAC

https://doi.org/10.1145/3708821.3735343
ISBN: 9798400714108

POSTER: Policy-driven security-aware scheduling in Kubernetes

Matthew Rossi
Università degli Studi di Bergamo
Bergamo, Italy
matthew.rossi@unibg.it

Michele Beretta
Università degli Studi di Bergamo
Bergamo, Italy
michele.beretta@unibg.it

Dario Facchinetti
Università degli Studi di Bergamo
Bergamo, Italy
dario.facchinetti@unibg.it

Stefano Paraboschi
Università degli Studi di Bergamo
Bergamo, Italy
stefano.paraboschi@unibg.it

Abstract

Nowadays, Kubernetes is the leading platform for managing containerized application workloads. These are built of numerous *pods*, groups of one or more containers that are always co-located and co-scheduled on the same node. Given a pod, the *scheduler* performs a critical task, i.e., it finds the best possible node for its execution. This process is affected by several factors, including resource availability, hardware requirements, data processing restrictions (e.g., GDPR and CCPA), workload sensitivity, and the presence of other workloads. Developers can control the scheduling process through several methods, such as node selectors, affinity, anti-affinity, and topology spread constraints. However, this activity is cumbersome, error prone, and can easily lead to security incidents.

In this paper we propose an approach to constrain and validate pod scheduling decisions without relying on complex, handwritten node selection policies. The idea is to combine the node filtering capabilities of Kubernetes with the use of OPA Gatekeeper for automated policy enforcement. We discuss how this approach overcomes the limitation associated with existing solutions, and then describe how it is used to support corporate governance policies in common scenarios. Preliminary experiments confirm the applicability of our proposal.

CCS Concepts

• **Security and privacy → Software and application security**; **Access control**.

Keywords

Kubernetes, Security, Scheduling, Multi-tenancy, Data sovereignty, Workload isolation

ACM Reference Format:
Matthew Rossi, Michele Beretta, Dario Facchinetti, and Stefano Paraboschi. 2025. POSTER: Policy-driven security-aware scheduling in Kubernetes. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '25), August 25–29, 2025, Hanoi, Vietnam.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3708821.3735343

ASIA CCS '25, Hanoi, Vietnam

ACM ISBN 979-8-4007-1410-8/25/08
https://doi.org/10.1145/3708821.3735343

1 Introduction

Since its announcement in 2014, Kubernetes has become the industry leading solution for the orchestration of containerized workloads. According to a 2023 Cloud Native Computing Foundation's survey [1], 71% of respondents are using Kubernetes in production, and another 18% are evaluating its adoption. The reason of this success is Kubernetes' ability to automatically deploy, scale, and manage applications in a declarative way, independently of the size and complexity of the underlying cluster of nodes. To do so, it leverages the concept of *pod*, a group of containers that are tightly coupled, always co-located and co-scheduled, and share the same execution context and resources (e.g., storage, network).

However, companies that rely on Kubernetes also face some challenges. Indeed, as reported by Red Hat in the 2024 State of Kubernetes security report [2], nearly 9 in 10 organizations experienced security incidents, causing delays in application development to approximately 67% of companies, and even revenue or customer loss to 46% of all respondents. Indeed, when a vulnerable container is compromised the damage easily spreads to the entire pod due to the shared execution context, and when the vulnerability is severe and compromises the security of the node, it undermines all the co-located workloads.

Given this scenario, it is critical to provide developers and organizations with tools to improve the isolation between workloads. In particular, there are three common situations that can benefit from this: (i) *multi-tenancy*, where multiple tenants (e.g., customers or teams) run applications on the same cluster and need strong access control guarantees; (ii) *data sovereignty*, where several regulations (e.g., GDPR in Europe, and CCPA in California) require to control the geographical area where data is either stored and/or processed; and (iii) *incompatible sensitivity levels* for different workloads, as some may process personal data, implement critical services such as authentication and identity management, while others are exposed to untrusted input and/or depend on third-party code. In all these cases, it is crucial to select the execution node appropriately. While Kubernetes allows customizing the decision of the execution node during *scheduling*, this is done using verbose handwritten node selectors, affinity, anti-affinity, and topology spread constraints in the pod specification. Therefore, this process is tedious, error prone, and depends entirely on the developer.

In this paper we address this limitation by proposing the use of policies that are defined at cluster level, and are evaluated automatically every time pod creation requests are submitted to Kubernetes.

These policies are tailored on the previously mentioned use cases (i.e., multi-tenancy, data sovereignty, incompatible security levels), and mutate each pod creation request to ensure the selection of a policy-compliant execution node. In the following sections, we will first look at the native Kubernetes capabilities for limiting pod assignment, and then provide a detailed explanation of our solution. Finally, we will illustrate the experimental evaluation, showing the limited overhead associated with our approach.[1]

2 Native node filtering capabilities

As mentioned in Section 1, Kubernetes assigns pods to nodes based on many factors like the availability of resources in the cluster, the pod's resource requirements, and the distribution of the workloads. It also provides native methods to customize this process. We briefly explain the advantages and drawbacks associated with each of them.

Node labels and selectors. Node labels [4] are key-value pairs attached to nodes. When paired with the definition of node selectors in the pod specification, they allow to restrict the group of nodes eligible for execution to the ones matching all required node labels. While this is a viable solution, it has limited flexibility, hence it is only suitable for simple use cases.

Node affinity. Node affinity [3] complements node selectors creating a set of additional rules. These rules can express requirements (i.e., `requiredDuringSchedulingIgnoredDuringExecution`) and preferences (i.e., `preferredDuringSchedulingIgnoredDuringExecution`), allowing the scheduler to assign a pod even when it cannot find a node that satisfies all the constraints. Node affinity rules can quickly become complex to write and hard to validate, especially when using multiple `matchExpressions` clauses (e.g., `In`, `NotIn`, `Exists`, `DoesNotExist`, `Gt`, `Lt`).

Taints and tolerations. While node selection and affinity attract pods to a set of nodes, taints [7] allow nodes to repel pods that do not specify the corresponding taint tolerations. This capability is useful when a hardware feature is present only on few nodes in the cluster, and needs to be reserved for a specific set of pods that benefit from it. Taints are represented with simple key-value pairs and their resulting effect (e.g., `NoSchedule`). Therefore, they lack flexibility and do not allow the definition of complex expressions.

Although these features offer a solid starting point, it is essential to acknowledge their limitations. Indeed, they require all developers operating on the cluster to manually introduce a compliant and effective set of constraints. Moreover, since this activity is cumbersome and error prone, it can easily lead to security incidents due to lack of training, unclear company guidelines, or misconfigurations.

3 Our approach

The primary goal of this work is to improve workload isolation by automatically enforcing governance guidelines at the cluster level, without relying solely on handwritten policy constraints. In the following we clarify the threat model and illustrate our approach.

Threat model. In a Kubernetes cluster there is a risk of security incidents when workloads with incompatible security requirements and/or sensitivity levels are deployed on the same nodes. Indeed, workloads that process untrusted input can be compromised by an attacker, potentially gaining code execution at node level. When this happens, all workloads running on the node are exposed to the attacker, hence applications can suffer disruptions and failures, user data can be lost or leaked, and the company can be held liable and suffer financial and reputational damage.

[1]The code is available at https://github.com/matthewrossi/k8s-secure-scheduling

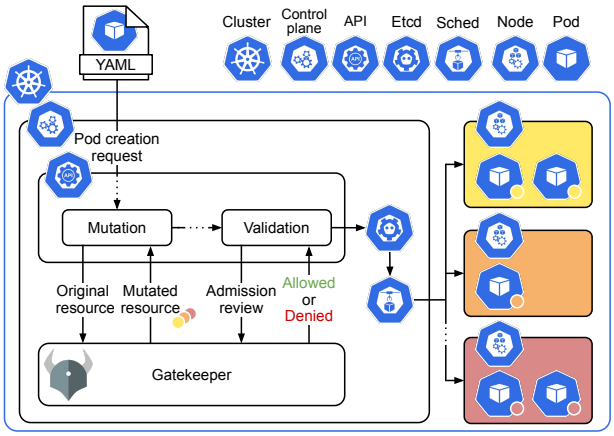


Figure 1: The architecture of our solution: Kubernetes scheduling capabilities are enhanced by OPA Gatekeeper, which automatically mutates and validates pod creation requests to enforce cluster-defined policies

Our solution. We propose to strengthen Kubernetes scheduling decisions using OPA Gatekeeper [6], an open source policy and governance framework for Kubernetes built on the Open Policy Agent (OPA) engine. In detail, Kubernetes delegates runtime policy decisions to the Gatekeeper admission controller. Gatekeeper acts as a bridge between the Kubernetes API server and OPA, fetching the relevant information associated with the pod resource definition, and invoking OPA to evaluate a set of cluster policies. Policies operate at the cluster level, and implement the use cases presented in Section 1. OPA Gatekeeper employs them in two stages: mutation and validation. During mutation Gatekeeper modifies the pod resource definition to include elements from a policy template, supporting the developer in the correct definition of pod scheduling constraints. During validation instead, OPA ensures pod creation requests comply with the cluster policy guidelines, allowing to admit (or reject) pod creation requests at runtime.

This approach does not require to modify extensively the architecture of an existing cluster (Figure 1). We only assume that (i) nodes in the cluster have already been labelled meaningfully (e.g., with information about tenant, geographical location, and sensitivity level), and (ii) the developer can leverage a comprehensive set of labels to classify pods based on their security needs (e.g., a pod processes sensitive data, it must be deployed in given region).

Our solution brings several advantages: (i) policy enforcement is automated by Gatekeeper, this avoids manually replicating error-prone node filtering definitions; (ii) policies are decoupled from the pod specification, simplifying pod definition and improving developer productivity; and most importantly, (iii) Gatekeeper ensures policies are applied consistently over the cluster, independently of the tenant that implements or deploys the workload.

Table 1: 90th percentiles for the evaluation of policies regarding data sovereignty (DS), multi-tenancy (MT), and incompatible security levels (ISL) scenarios. Mutation does not introduce scheduling changes in unconstrained use cases

Scenario	Latency [μs]		
	Mutation	Validation	Scheduling
DS (EEA)	900.09	900.73	942.77
DS (US)	900.12	900.57	982.35
DS (unconstrained)	900.17	900.76	925.56
MT (tenant-A)	900.23	900.32	951.11
MT (tenant-B)	900.21	900.41	944.19
MT (unconstrained)	900.07	900.14	926.24
ISL (sensitive)	900.12	900.50	942.34
ISL (unhardened)	900.30	900.54	936.39
ISL (unconstrained)	900.21	900.24	916.22

4 Evaluation

We performed a set of experiments to measure the time associated with the mutation and validation stages of pod creation requests, along with their subsequent pod scheduling latency.

The experiments have been performed on a server with Ubuntu 24.04 with kernel 6.8.0, a 128 cores AMD 7985WX CPU, 256 GiB of DDR5 RAM, and 2 TB SSD. To setup the Kubernetes cluster we used `kind` 0.27.0, Docker 28.0.1 for control plane nodes, the `containerd` 1.7.25 container runtime, KWOK[2] v0.6.1 to simulate worker nodes, and ClusterLoader2[3] to run performance tests. OPA Gatekeeper 3.18.2 was used to mutate and validate scheduling requests, and Prometheus 2.25.0 to gather the test metrics.

To assess the accuracy of our test environment in measuring the impact of our solution on control plane components, we initially run a small-scale test with 3 control plane nodes, comparing the performance associated with the use of 10 real versus 10 simulated worker nodes. As expected, simulating workers still provides accurate control plane performance measures. So, we proceeded with the creation of 3 control plane nodes, on which our solution is run, and a total of 1k simulated worker nodes for the creation of 30k pods (with 500 qps). Table 1 shows the results for each use case. The measures report the 90th percentile of the latency introduced to mutate and validate pod creation requests, as well as the pod scheduling time. In all use cases these steps are completed within 1 *ms*. Finally, we monitored the API availability and confirmed that our solution does not affect the normal functioning of the cluster, as availability always remains at 100% even under heavy load.

5 Related Work

Several approaches improve the isolation in a Kubernetes cluster.

Kubernetes namespaces. Namespaces [5] provide a mechanism for isolating groups of API resources within a single cluster. They are useful to avoid name clashes and play a significant role in the definition of resource quotas (e.g., memory, CPU). However, namespaces are not meant to influence scheduling decisions, so a privileged pod or a container breakout can affect workloads in other namespaces on the same node.

Sandboxing. In Kubernetes, workloads can benefit from the isolation provided by sandboxed runtimes, such as gVisor [16] and Firecracker [11], as well as take advantage of common kernel-based sandboxing solutions [8–10, 13, 14]. While all these techniques offer strong security guarantees, they also increase complexity, and inevitably introduce higher overhead and resource utilization.

Node isolation. With node isolation, a set of nodes is dedicated to running pods having a particular security profile. In Workload Security Rings [12], a proposal by Google, this technique is used to mitigate the risk of lateral movement, as sensitive workloads are never co-located with the ones that process untrusted data. However, their approach is only available in Borg [15], while our solution can replicate this behavior on Kubernetes.

6 Conclusions and future work

The results achieved by our approach are promising: not only it permits to automatically apply cluster-level policies during pod creation without significant architectural changes, but it is also associated with a negligible performance impact. Future work includes the exploration of real-time threat-informed policy adaptation and the extension of our solution to multi-cluster deployments.

Acknowledgments

This work was supported in part by the EC under project GLACIATION (01070141), by the Italian MUR under PRIN project POLAR (2022LA8XBH), and by projects SERICS (PE00000014) and GRINS (PE00000018) in the NRRP MUR program funded by the EU–NGEU.

References

[1] 2023. *CNCF Annual Survey.* https://cncf.io/reports/cncf-annual-survey-2023/
[2] 2024. *Kubernetes adoption, security, and market trends report.* https://www.redhat.com/en/resources/kubernetes-adoption-security-market-trends-overview
[3] 2025. *Assign Pods to Nodes using Affinity.* https://kubernetes.io/docs/tasks/configure-pod-container/assign-pods-nodes-using-node-affinity/
[4] 2025. *Assign Pods to Nodes with Node labels.* https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/#built-in-node-labels
[5] 2025. *Namespaces | Kubernetes.* https://kubernetes.io/docs/concepts/overview/working-with-objects/namespaces/
[6] 2025. *OPA Gatekeeper.* https://open-policy-agent.github.io/gatekeeper/website/
[7] 2025. *Taints and Tolerations – Kubernetes.* https://kubernetes.io/docs/concepts/scheduling-eviction/taint-and-toleration/
[8] M. Abbadini, M. Beretta, D. Facchinetti, G. Oldani, M. Rossi, and S. Paraboschi. 2023. Lightweight Cloud Application Sandboxing. In *CLOUDCOM.*
[9] M. Abbadini, M. Beretta, D. Facchinetti, G. Oldani, M. Rossi, and S. Paraboschi. 2023. POSTER: Leveraging eBPF to enhance sandboxing of WebAssembly runtimes. In *ASIACCS.*
[10] M. Abbadini, D. Facchinetti, G. Oldani, M. Rossi, and S. Paraboschi. 2023. NatiSand: Native Code Sandboxing for JavaScript Runtimes. In *RAID.*
[11] A. Agache, M. Brooker, A. Iordache, A. Liguori, R. Neugebauer, P. Piwonka, and D. Popa. 2020. Firecracker: Lightweight Virtualization for Serverless Applications. In *NSDI.*
[12] M. Czapiński and R. Wolafka. 2023. Workload Security Rings. https://www.usenix.org/publications/loginonline/workload-security-rings
[13] M. Rossi, M. Beretta, D. Facchinetti, and S. Paraboschi. 2025. POSTER: Transparent Temporally-Specialized System Call Filters. In *ASIACCS.*
[14] Y. Sun, D. Safford, M. Zohar, D. Pendarakis, Z. G., and T. Jaeger. 2018. Security Namespace: Making Linux Security Frameworks Available to Containers. In *USENIX Security.*
[15] A. Verma, L. Pedrosa, M. R. Korupolu, D. Oppenheimer, E. Tune, and J. Wilkes. 2015. Large-scale cluster management at Google with Borg. In *EuroSys.*
[16] E. G. Young, P. Zhu, T. Caraza-Harter, A. C. Arpaci-Dusseau, and R. H. Arpaci-Dusseau. 2019. The true cost of containing: a gVisor case study. In *HotCloud.*

[2] https://github.com/kubernetes-sigs/kwok
[3] https://github.com/kubernetes/perf-tests/tree/master/clusterloader2