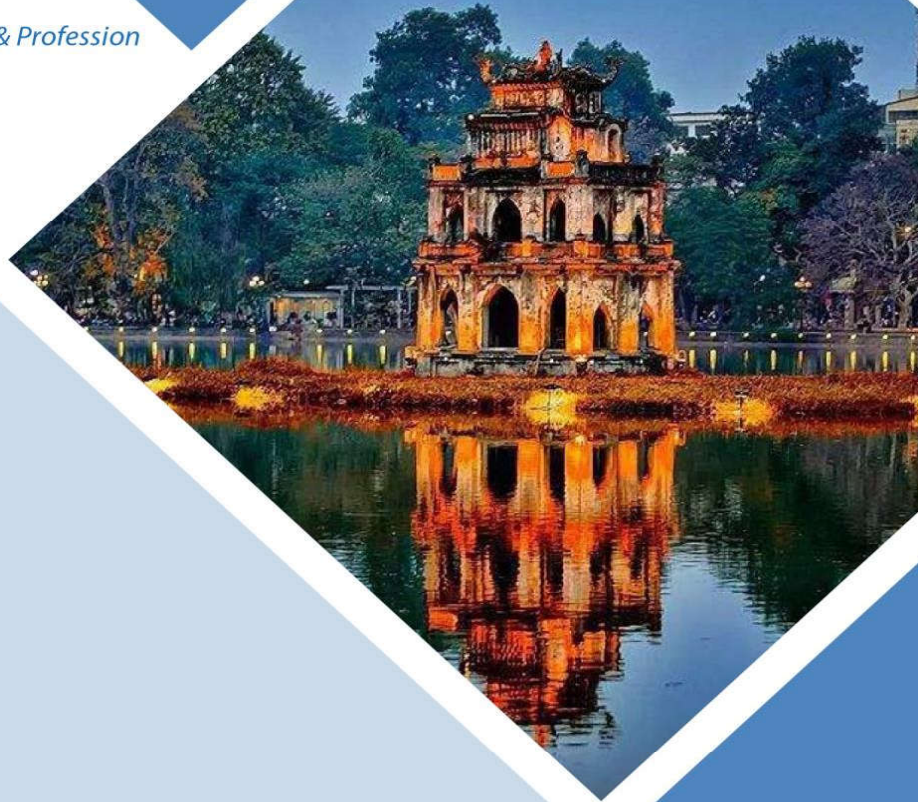


August 25-29, 2025  
Hanoi, Vietnam



**Association for  
Computing Machinery**

*Advancing Computing as a Science & Profession*



# ACM ASIACCS 2025

**Proceedings of the 20<sup>th</sup> 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, 10<sup>th</sup> Floor  
New York, New York 10019, USA**

**ACM COPYRIGHT NOTICE. Copyright © 2025 by the Association for Computing Machinery, Inc. Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Publications Dept., ACM, Inc., fax +1 (212) 869-0481, or [permissions@acm.org](mailto:permissions@acm.org).**

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, +1-978-750-8400, +1-978-750-4470 (fax).

**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

<b>Enhanced CKKS Bootstrapping with Generalized Polynomial Composites Approximation.....</b>	<b>1</b>
<i>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)</i>	
<b>An Efficient Circuit Synthesis Framework for TFHE via Convex Sub-graph Optimization .....</b>	<b>13</b>
<i>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)</i>	
<b>A Novel Asymmetric BSGS Polynomial Evaluation Algorithm under Homomorphic Encryption.....</b>	<b>30</b>
<i>Qingfeng Wang (University of Chinese Academy of Sciences, China), Li-Ping Wang (University of Chinese Academy of Sciences, China)</i>	
<b>Efficient Updatable Private Information Retrieval from Simulatable Homomorphic Ciphertexts.....</b>	<b>45</b>
<i>Yini Lin (Sun Yat-sen University, China and Monash University, Australia), Haibo Tian (Sun Yat-sen University, China)</i>	
<b>Key Extension: Multi-Key FHE Utilizing LWR.....</b>	<b>58</b>
<i>Mansi Goyal (Indian Institute of Technology Roorkee, India), Aditi Kar Gangopadhyay (Indian Institute of Technology Roorkee, India)</i>	
<b>DUPLEX: Scalable Zero-Knowledge Lookup Arguments over RSA Group .....</b>	<b>72</b>
<i>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)</i>	

## Multi-party Computation

<b>Pay What You Spend! Privacy-Aware Real-Time Pricing with High Precision IEEE 754 Floating Point Division .....</b>	<b>87</b>
<i>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)</i>	
<b>Efficient Private Set Intersection by Utilizing Oblivious Transfer Extension.....</b>	<b>104</b>
<i>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)</i>	
<b>SEEC: Memory Safety Meets Efficiency in Secure Two-Party Computation .....</b>	<b>118</b>
<i>Henri Dohmen (TU Darmstadt), Robin Hundt (TU Darmstadt), Nora Khayata (TU Darmstadt), Thomas Schneider (TU Darmstadt)</i>	

**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 Saçiak (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 Kutylowski (NASK National Research Institute, Poland), Oliwier 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)*

<b>Quantum-safe Signatureless DNSSEC .....</b>	<b>267</b>
<i>Aditya Singh Rawat (Ashoka University, India), Mahabir Prasad Jhanwar (Ashoka University, India)</i>	
<b>Ring-LWR based Commitments and ZK-PoKs with Application to Verifiable Quantum-Safe Searchable Symmetric Encryption .....</b>	<b>283</b>
<i>Debadrita Talapatra (Indian Institute of Technology, India), Nimish Mishra (Indian Institute of Technology, India), Debdeep Mukhopadhyay (Indian Institute of Technology, India)</i>	
<b>Practical Deniable Post-Quantum X3DH: A Lightweight Split-KEM for K-Waay .....</b>	<b>298</b>
<i>Guilhem Niot (PQShield SAS, France and Univ Rennes, CNRS, IRISA, France)</i>	
<b>A Quantum-Secure Framework for IoD: Strengthening Authentication and Key-Establishment .....</b>	<b>313</b>
<i>Salman Shamshad (University of Bristol, United Kingdom), Sana Belguith (University of Bristol, United Kingdom), Alma Oracevic (University of Bristol, United Kingdom)</i>	
<b>poqeth: Efficient, Post-Quantum Signature Verification on Ethereum .....</b>	<b>327</b>
<i>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)</i>	

## LLM for Security

<b>Perses: Unlocking Privilege Escalation for Small LLMs via Extensible Heterogeneity .....</b>	<b>344</b>
<i>Dominik M. Weber (Huawei Munich Research Center, Germany), Ioannis Tzachristas (Huawei Munich Research Center, Germany), Aifen Sui (Huawei Munich Research Center, Germany)</i>	
<b>Generalized Adversarial Code-Suggestions: Exploiting Contexts of LLM-based Code-Completion .....</b>	<b>358</b>
<i>Karl Rubel (Karlsruhe Institute of Technology, Germany), Maximilian Noppel (Karlsruhe Institute of Technology, Germany), Christian Wressneger (Karlsruhe Institute of Technology, Germany)</i>	
<b>PentestAgent: Incorporating LLM Agents to Automated Penetration Testing .....</b>	<b>375</b>
<i>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)</i>	
<b>SAFE: A Novel Approach for Software Vulnerability Detection from Enhancing the Capability of Large Language Models .....</b>	<b>392</b>
<i>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)</i>	
<b>Sounds Vishy: Automating Vishing Attacks with AI-Powered Systems .....</b>	<b>407</b>
<i>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)</i>	

<b>SoK: The Privacy Paradox of Large Language Models: Advancements, Privacy Risks, and Mitigation .....</b>	<b>425</b>
---	------------

*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**

<b>ChainMarks: Securing DNN Watermark with Cryptographic Chain.....</b>	<b>442</b>
---	------------

*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)*

<b>Toward Malicious Clients Detection in Federated Learning .....</b>	<b>456</b>
---	------------

*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)*

<b>Nosy Layers, Noisy Fixes: Tackling DRAs in Federated Learning Systems using Explainable AI .....</b>	<b>473</b>
---	------------

*Meghali Nandi (The University of New South Wales (UNSW), Australia and CSIRO's Data61, Australia), Arash Shaghghi (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)*

<b>When Better Features Mean Greater Risks: The Performance-Privacy Trade-Off in Contrastive Learning .....</b>	<b>488</b>
---	------------

*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)*

<b>Unraveling Elevated Data Leakage in Split Learning for Fine-Tuning Stable Diffusion Models .....</b>	<b>501</b>
---	------------

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

<b>Transferable Adversarial Examples with Bayesian Approach.....</b>	<b>517</b>
--	------------

*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**

<b>Glitch in Time: Exploiting Temporal Misalignment of IMU for Eavesdropping.....</b>	<b>530</b>
---	------------

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

<b>Eradicating the Unseen: Detecting, Exploiting, and Remediating a Path Traversal Vulnerability across GitHub.....</b>	<b>542</b>
<i>Jafar Akhoundali (Leiden University, Netherlands), Hamidreza Hamidi (Technical and Vocational University, Iran), Kristian Rietveld (Leiden University, Netherlands), Olga Gadyatskaya (Leiden University, Netherlands)</i>	
<b>PITCH: AI-assisted Tagging of Deepfake Audio Calls using Challenge-Response.....</b>	<b>559</b>
<i>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)</i>	
<b>Minerva: A File-Based Ransomware Detector .....</b>	<b>576</b>
<i>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)</i>	
<b>Evaluating Robustness of Reference-based Phishing Detectors .....</b>	<b>591</b>
<i>Eunjin Roh (Oregon State University, USA), Sungwoo Jeon (KAIST, Republic of Korea), Sooel Son (KAIST, Republic of Korea), Sanghyun Hong (Oregon State University, USA)</i>	
<b>Comprehensive Evaluation of Cloaking Backdoor Attacks on Object Detector in Real-World .....</b>	<b>605</b>
<i>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)</i>	

## Privacy 1

<b>Enhancing Search Privacy on Tor: Advanced Deep Keyword Fingerprinting Attacks and BurstGuard Defense .....</b>	<b>621</b>
<i>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)</i>	
<b>Robust Locally Differentially Private Graph Analysis .....</b>	<b>635</b>
<i>Amrita Roy Chowdhury (University of Michigan, Ann Arbor, USA), Jacob Imola (University of Copenhagen, Denmark), Kamalika Chaudhuri (UCSD, USA)</i>	
<b>PSP: A Privacy-Preserving Self-certify Pseudonym Protocol for V2X .....</b>	<b>651</b>
<i>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)</i>	

**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 Kutylowski (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)*

<b>Towards Usability of Data with Privacy: A Unified Framework for Privacy-Preserving Data Sharing with High Utility .....</b>	<b>790</b>
<i>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)</i>	

## Blockchain 1

<b>Fast SNARK-based Non-Interactive Distributed Verifiable Random Function with Ethereum Compatibility .....</b>	<b>807</b>
<i>Jia Liu (Enya Labs, USA), Mark Manulis (Universität der Bundeswehr München, Germany)</i>	
<b>VeRange: Verification-efficient Zero-knowledge Range Arguments with Transparent Setup for Blockchain Applications and More.....</b>	<b>823</b>
<i>Yue Zhou (Australian National University, Australia), Sid Chi-Kin Chau (CSIRO, Australia)</i>	
<b>Scalable Time-Lock Puzzle.....</b>	<b>839</b>
<i>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)</i>	
<b>BIP32-Compatible Threshold Wallets.....</b>	<b>856</b>
<i>Poulami Das (Least Authority, Germany), Andreas Erwig (Technische Universität Darmstadt, Germany), Sebastian Faust (Technische Universität Darmstadt, Germany), Philipp-Florens Lehwald (Technische Universität Darmstadt, Germany), Julian Loss (CISPA Helmholtz Center for Information Security, Germany), Ziyang Qu (Technische Universität Darmstadt, Germany), Siavash Riahi (Technische Universität Darmstadt, Germany)</i>	

## Blockchain 2

<b>FIRST: FrontrunNing Resistant Smart ConTracts.....</b>	<b>873</b>
<i>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)</i>	
<b>Mining Attack with Zero Knowledge in the Blockchain .....</b>	<b>890</b>
<i>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)</i>	

**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)*

<b>FP-Rowhammer: DRAM-Based Device Fingerprinting .....</b>	<b>1141</b>
<i>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)</i>	
<b>ProbeShooter: A New Practical Approach for Probe Aiming .....</b>	<b>1158</b>
<i>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)</i>	
<b>GAE4HT: Detecting Hardware Trojans with Graph Autoencoder-Trained on Golden Model Data Flow Graphs .....</b>	<b>1175</b>
<i>Daehyeon Lee (Korea University Seoul, Republic of Korea), Junghee Lee (Korea University Seoul, Republic of Korea)</i>	
<b>Monocle: Transient Execution Proof Memory Views for Runtime Compiled Code.....</b>	<b>1188</b>
<i>Matteo Oldani (ETH Zurich, Switzerland and Oracle Labs, Switzerland), William Blair (Oracle Labs, USA), Shweta Shinde (ETH Zurich, Switzerland), Matthias Neugschwandtner (Oracle Labs, Austria)</i>	
<b>Okapi: Efficiently Safeguarding Speculative Data Accesses in Sandboxed Environments .....</b>	<b>1203</b>
<i>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)</i>	

## Fault Injection and Side Channels

<b>FAULT+PROBE: A Generic Rowhammer-based Bit Recovery Attack.....</b>	<b>1219</b>
<i>Kemal Derya (Worcester Polytechnic Institute, USA), M. Caner Tol (Worcester Polytechnic Institute, USA), Berk Sunar (Worcester Polytechnic Institute, USA)</i>	
<b>Three Glitches to Rule One Car: Fault Injection Attacks on a Connected EV .....</b>	<b>1235</b>
<i>Niclas Kühnapfel (TU Berlin, Germany), Christian Werling (TU Berlin, Germany), Hans Niklas Jacob (TU Berlin, Germany), Jean-Pierre Seifert (TU Berlin, Germany)</i>	
<b>AVXProbe: Enhancing Website Fingerprinting with Side-Channel-Assisted Kernel-Level Traces .....</b>	<b>1250</b>
<i>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)</i>	
<b>BranchGauge: Modeling and Quantifying Side-Channel Leakage in Randomization-Based Secure Branch Predictors .....</b>	<b>1265</b>
<i>Quancheng Wang (Wuhan University, China), Ming Tang (Wuhan University, China), Ke Xu (Wuhan University, China), Han Wang (Wuhan University, China)</i>	

**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 Puy (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)*

<b>Can Small-scale Evaluation Reflect Real Ability? A Performance Study of Emerging Biometric Authentication.....</b>	<b>1535</b>
<i>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)</i>	
<b>The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails against Organizations.....</b>	<b>1550</b>
<i>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)</i>	
<b>PRISM: To Fortify Widget Based User-App Data Exchanges Using Android Virtualization Framework.....</b>	<b>1567</b>
<i>YingTat Ng (Singapore Management University, Singapore), Zhe Chen (Singapore Management University, Singapore), Haiqing Qiu (Singapore Management University, Singapore), Xuhua Ding (Singapore Management University, Singapore)</i>	
<b>On the Account Security Risks Posed by Password Strength Meters .....</b>	<b>1582</b>
<i>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 &amp; MPI-SP, USA), Xinyi Zhang (Meta, USA), Yun Lin (Shanghai Jiao Tong University, China), Jin Song Dong (National University of Singapore, Singapore)</i>	

## Software and OS Security

<b>Can You Run My Code? A Close Look at Process Injection in Windows Malware.....</b>	<b>1600</b>
<i>Giorgia Di Pietro (Sapienza University of Rome, Italy), Daniele Cono D'Elia (Sapienza University of Rome, Italy), Leonardo Querzoni (Sapienza University of Rome, Italy)</i>	
<b>CryptoGuard: Lightweight Hybrid Detection and Response to Host-based Cryptojackers in Linux Cloud Environments.....</b>	<b>1617</b>
<i>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)</i>	
<b>Vulnerable Intel GPU Context: Prohibit Complete Context Restore by Modifying Kernel Driver.....</b>	<b>1632</b>
<i>Wonseok Choi (Korea University, Republic of Korea), Youngjoo Shin (Korea University, Republic of Korea)</i>	
<b>Sigy: Breaking Intel SGX Enclaves with Malicious Exceptions &amp; Signals.....</b>	<b>1643</b>
<i>Supraja Sridhara (ETH Zurich, Switzerland), Andrin Bertschi (ETH Zurich, Switzerland), Benedict Schlüter (ETH Zurich, Switzerland), Shweta Shinde (ETH Zurich, Switzerland)</i>	

**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

<b>General Chairs</b>	Huynh Quyet Thang (Hanoi University of Science and Technology, Vietnam) Phan Duong Hieu (Institut Polytechnique de Paris, France)
<b>Program Chairs</b>	Michail Maniatakos (New York University Abu Dhabi, UAE) Yinqian Zhang (Southern University of Science and Technology, China)
<b>Local Organising Chairs</b>	Huynh Thi Thanh Binh (Hanoi University of Science and Technology, Vietnam) Tran Quang Duc (Hanoi University of Science and Technology, Vietnam)
<b>Workshop Chair</b>	Khoa Nguyen (University of Wollongong, Australia)
<b>Poster Chairs</b>	Pham Van Thuan (University of Melbourne, Australia) Yue Duan (Singapore Management University, Singapore)
<b>Sponsorship Chair</b>	Le Xuan Thanh (Hanoi University of Science and Technology, Vietnam)
<b>Web Chair</b>	Tran Hai Anh (Hanoi University of Science and Technology, Vietnam)
<b>Publicity Chairs</b>	Vo Quang Viet (Swinburne University of Technology, Australia) Cao Minh Phuong (University of Illinois at Urbana-Champaign, USA)
<b>Publication Chairs</b>	Dinh Tien Tuan Anh (Deakin University, Australia) Tong Van Van (Hanoi University of Science and Technology, Vietnam)
<b>Steering Committee</b>	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)
<b>Program Committee</b>	Abdelrahman Aly, Technology Innovation Institute, UAE Abhishek Bichawat, 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  
 Hyounghick 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, CISA 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

	<p>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</p>
<b>Poster Reviewers</b>	<p>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)</p>

## ASIA CCS'25 Sponsor and Supporters

### Main Sponsors



### Supporter



### Supporting Partner



### Bronze Sponsor





PDF Download  
3708821.3735342.pdf  
19 January 2026  
Total Citations: 0  
Total Downloads: 926

Latest updates: <https://dl.acm.org/doi/10.1145/3708821.3735342>

POSTER

## POSTER: Transparent Temporally-Specialized System Call Filters

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

Open Access Support provided by:

University of Bergamo

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

# POSTER: Transparent Temporally-Specialized System Call Filters

Matthew Rossi

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

Dario Facchinetti

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

Michele Beretta

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

Stefano Paraboschi

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

## Abstract

Reducing the attack surface of the OS kernel is an effective technique to enhance the security of application workloads. In Linux systems, developers can restrict the set of available system calls by using `seccomp`. Although being widely adopted in browsers, container runtimes, and sandboxing tools, this approach presents some challenges: (i) applying precise filters often requires significant application modifications, which can impede developer productivity, and (ii) the transparent enforcement of filters is bound to use a single, static list with every syscall the application might ever need, resulting in overly permissive and less effective security boundaries.

In this paper, we propose an automated method to generate temporally-specialized `seccomp` filters tailored to the current application state. This significantly enhances the effectiveness of filters, and overcomes the major limitations associated with a single, static filter. We implement our solution by leveraging the eBPF subsystem in the Linux kernel. Specifically, we use in-kernel eBPF programs to monitor the application state and dynamically enable or disable specialized `seccomp` filters in response to state transitions. We discuss how this approach addresses the limitations of state-of-the-art solutions. Finally, we validate the feasibility of our proposal and show that it introduces a limited overhead.

## CCS Concepts

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

## Keywords

Syscall filtering, Temporal specialization, Attack surface reduction, eBPF, Seccomp

## ACM Reference Format:

Matthew Rossi, Michele Beretta, Dario Facchinetti, and Stefano Paraboschi. 2025. POSTER: Transparent Temporally-Specialized System Call Filters. 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/10.1145/3708821.3735342>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

ASIA CCS '25, Hanoi, Vietnam

© 2025 Copyright held by the owner/author(s).

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

<https://doi.org/10.1145/3708821.3735342>

## 1 Introduction

Several research works (e.g., [7, 11]) have shown that access to unnecessary syscalls increases the risk of privilege escalation and correlates with a higher frequency of zero-day vulnerabilities. The reason is that less commonly used kernel APIs are more susceptible to bugs, whereas popular ones are more robust and tested [12].

The introduction of `seccomp` [1] represents a key advancement in safeguarding the kernel from potentially vulnerable unprivileged user space applications. Indeed, `seccomp` enables the specification of a syscall filter that is evaluated by the kernel with minimal overhead whenever an application invokes a syscall. This mechanism is widely employed by various applications, such as browsers, container runtimes, and sandboxing tools. However, it also introduces some challenges. Indeed, once activated, `seccomp` filters can only be further restricted, requiring the implementation of tight security boundaries through significant application restructuring. To become *seccomp-aware*, an application must separate its functions into distinct compartments and manage different security profiles at runtime. In practice, most (if not all) `seccomp` users apply the filter once, often at application startup, and never change it afterwards. This means that all required syscalls are included in a single, overly permissive filter, which exposes a wider attack surface, and diminishes the security benefits. Another issue is that developers often struggle to craft effective syscall filters, since they typically operate at higher level of abstractions (i.e., developers directly invoke library APIs rather than syscalls).

To improve the current scenario, novel research [9, 10] has introduced the promising concept of *temporally-specialized* filters that are tailored around specific application compartments. Despite being innovative, both works have shortcomings. For instance, Ghavamnia et al. [9] provide tools to generate the filters, but still require the developer to restructure the application manually. Jia et al. [10] instead greatly enhance `seccomp`'s flexibility, but their work requires several kernel architectural changes.

This paper advances the state-of-the-art with an approach to enforce temporally-specialized filters that does not require application changes nor kernel modifications. The design relies on the eBPF kernel subsystem, and permits to transparently apply filters to the application based on its current state. In addition, we provide the developer with tools to automatically generate the filters associated with every application state. To this end, the developer is only required to identify functions that trigger state changes (e.g., any

functions that transitions a web server from an initialization to a serving phase), and to run the application in a test environment.

In the following we detail our approach and discuss the experimental evaluation, which confirms the merits of our solution and its limited performance overhead.

## 2 Background

This section provides a concise overview of eBPF, detailing the essential information needed to understand the rest of this paper.

eBPF [5] is a Linux subsystem that allows programs to run within the kernel in response to the execution of kernel functions. Specifically, eBPF programs are attached to designated *hook points*, and are executed whenever these are triggered. This allows for the inspection of the hook’s input arguments and, for functions allowing error injection, the modification of the return value. Essentially, these programs permit to alter the kernel behavior without changing its source code or introducing custom modules. For the purposes of this paper it is important to note that (i) data structures called *maps* can be used to maintain state across multiple invocations of eBPF programs and to share data with user space, and (ii) eBPF programs loaded into the kernel undergo rigorous validation to attest their safety (e.g., a program cannot crash due to memory errors). Modern eBPF development is supported by *frontends* such as libbpf, i.e., frameworks that allow developers to write eBPF programs in a C-like dialect which is then converted into cross-platform bytecode.

## 3 Our approach

This section clarifies the threat model and presents our solution. We begin with a high-level overview, followed by detailed explanations of the generation and enforcement of filters.

*Threat model.* Similarly to the seccomp framework, our proposal limits the set of system calls available to user space applications. We consider the kernel trusted, although it may be affected by vulnerabilities. Our goal is to reduce the attack surface and better defend the kernel against an attacker gaining remote code execution due to vulnerabilities in unprivileged user space applications.

### 3.1 Overview

From a high-level perspective, we replace static filters, traditionally set by manually invoking the seccomp syscall, with dynamic filters enforced through eBPF. This approach requires loading a set of eBPF programs that are evaluated whenever syscalls are invoked. Note that loading eBPF programs into the kernel is a privileged operation, as it demands the CAP\_BPF capability, and hence we delegate this task to a system administrator. This operation occurs only once at application deployment, and simply involves executing the application with a provided loader.

The uploaded eBPF programs operate either (i) in *tracing* mode, in which they collect all syscalls executed by the application and categorize them by application state, enabling the generation of filters, or (ii) in *enforcement* mode, in which the previously generated filters are activated in response to state transitions. Filters are recorded (during tracing) and loaded (during enforcement) in dedicated maps. The architecture of our solution is shown in Figure 1.

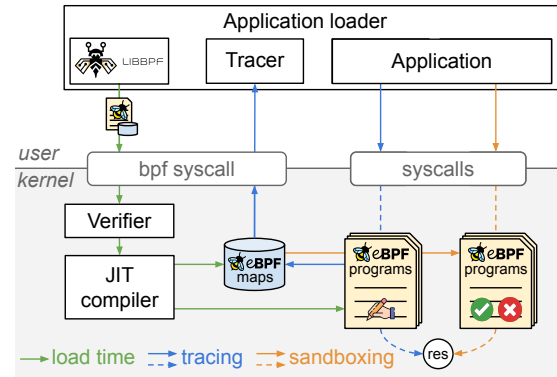


Figure 1: Tracing and sandboxing of a target application

### 3.2 Monitoring the application lifetime

The implementation of our approach presents two primary technical challenges: (i) tracing the processes of the target application, and (ii) detecting transitions in the application’s state.

Processes are traced by injecting in the kernel a set of eBPF programs to monitor the application’s lifetime. These programs are attached to the sched\_process\_fork and the sched\_process\_exit tracepoints, which are triggered by both the fork and clone syscalls, and also at process termination. Using the application’s main thread id as a starting point, the eBPF programs track all child processes by adding or removing their ids in a TYPE\_HASH map.

To detect transitions we rely on eBPF’s ability to probe user space processes. Specifically, a second set of eBPF programs are activated when the application executes a transitioning function. These programs maintain the mapping between application threads and states. Every thread is associated with a single state, but multiple threads with their respective states and syscalls may coexist at runtime. We consider the definition of state transition functions a developer-provided input, which entails sharing its name with the system administrator. No application changes are required.

### 3.3 Generating the filters

To generate the filters, the developer runs the application in a test environment with a provided binary, which (i) prepares a process for the application’s execution, (ii) records its process id in the application monitoring maps detailed in § 3.2, and (iii) launches the application via an execve syscall. An eBPF program is attached to the tp\_btf/sys\_enter tracepoint to capture all the syscalls issued by the application. When executed, it first reconstructs the mapping between thread id and application state using the monitoring maps, and then extracts the requested syscall id, storing it in a backing array. Upon application termination, this information is retrieved by the tracer to generate the corresponding filters (see Figure 1).

### 3.4 Activating the filters

The generated filters (§ 3.3) are applied at runtime without modifying the application’s structure or manually invoking the seccomp syscall. The developer just provides the system administrator with the application binary and the generated filters. The system administrator then executes the application binary using the provided

**Table 1: Performance of local web servers without syscall filtering, with seccomp, and with our eBPF-based solution**

Software	P99 latency [ms]			Throughput [req/s]		
	Native	Seccomp	eBPF	Native	Seccomp	eBPF
Apache 2.4.58	18.64	19.11	19.51	3.46K	2.72K	2.39K
Lighttpd 1.4.74	2.79	2.91	3.34	5.45K	5.23K	4.69K
Nginx 1.24.0	6.32	6.58	6.96	3.09K	2.99K	2.93K

loader (§ 3.1). This process is sufficient to enforce the filters automatically at runtime, and requires no additional actions.

Filter enforcement is handled by a separate eBPF program attached to kernel probes that monitors all syscalls issued by the application’s threads. If a thread’s application state does not allow a specific syscall, i.e., it is absent from the backing array representing the filter, the eBPF program invokes the `bpf_override_return` helper function to inject an error. This means that the kernel code implementing the syscall is not run at all, and instead a permission denied error is returned, resulting in a failed syscall invocation.

## 4 Evaluation

To test our approach, we first isolated the overhead introduced by eBPF with a microbenchmark that measures the performance of the lightweight `getpid` syscall, and then evaluated the impact of syscall filtering on popular web servers (Apache, Lighttpd, Nginx). In both experiments, we compared a test without protections (native case) against the use of seccomp and our eBPF-based solution. Experiments were conducted on an Ubuntu 24.04 server, kernel 6.8.0, an AMD 7985WX CPU, 256 GiB of DDR5 RAM, and 2 TB SSD.

*Microbenchmark.* In this preliminary experiment we measured the time to execute the `getpid` syscall over 1 million invocations. The average time was 207 ns when running without protections, 241 ns (+16.4%) with seccomp, and 309 (+28.2% w.r.t. seccomp) with our solution. This result was expected, since `getpid` is one of the shortest-lived syscalls, and because seccomp is currently the most efficient approach to filter syscalls directly within the kernel.

*Web server.* In this test we evaluated the overhead introduced by syscall filtering techniques on web servers. In detail, we used `Wrk`<sup>1</sup> to request the default web server page for 30 seconds, using 100 connections parallelized over 12 threads. Table 1 reports the 99th percentile of latency and the average throughput in the three different configurations. The result we obtained are promising: comparing our solution with seccomp, latency increased by 2.1% (−12.1% throughput) for Apache, by 14.7% (−10.3% throughput) for Lighttpd, and by 5.8% (−2.0% throughput) for Nginx.

## 5 Related Work

While seccomp remains a fundamental technique to safeguard the kernel, recent research has explored precise *temporal specialization* [9, 10] to enhance its effectiveness, with the goal of enabling fine-grained seccomp filters, tailored to specific application states. Although innovative, these approaches have limitations. For instance, Ghavamnia et al. [9] propose the generation of temporally-specialized policies, but the solution requires developers to make

applications seccomp-aware. Jia et al. [10] significantly enhance seccomp’s programmability, but introduce several kernel architectural changes, hindering adoption. Extensive research [7, 13, 14] has also investigated user space solutions. This offers great flexibility, but it incurs substantial overhead due to frequent context switches between kernel and user space. A promising binary rewriting technique named *zpoline* [15] can be used to avoid them, but unfortunately it cannot filter syscalls issued by dynamic libraries.

The automatic generation of syscall filters has also been widely studied. Proposed methods fall into two main categories: static and dynamic generators. Static generators [6, 8] extract the syscalls required by an application directly from its code, whereas dynamic generators [2–4] are based on runtime application monitoring. Both approaches have limitations. For instance, static generators struggle with interpreters or managed runtimes, while the coverage of dynamic generators depends on the runtime tests conducted.

## 6 Conclusions and future work

This paper proposed an approach to transparently apply temporally-specialized seccomp filters, without requiring modifications to the application or to the kernel. Preliminary results confirmed the introduction of a limited overhead. In future work we aim to explore various hooking strategies and investigate the integration of our solution into orchestration frameworks.

## 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] 2025. *Seccomp BPF*. [https://docs.kernel.org/userspace-api/seccomp\\_filter.html](https://docs.kernel.org/userspace-api/seccomp_filter.html)
- [2] 2025. *Slim Toolkit*. <https://slimtoolkit.org/>
- [3] M. Abbadini, M. Beretta, D. Facchinetti, G. Oldani, M. Rossi, and S. Paraboschi. 2023. Lightweight Cloud Application Sandboxing. In *CLOUDCOM*.
- [4] M. Abbadini, D. Facchinetti, G. Oldani, M. Rossi, and S. Paraboschi. 2023. NatiSand: Native Code Sandboxing for JavaScript Runtimes. In *RAID*.
- [5] J. Corbet. 2014. *BPF: the universal in-kernel virtual machine*. <https://lwn.net/Articles/599755/>
- [6] N. DeMarinis, K. Williams-King, D. Jin, R. Fonseca, and V.P. Kemerlis. 2020. Sysfilter: Automated system call filtering for commodity software. In *RAID*.
- [7] T. Garfinkel, B. Pfaff, and M. Rosenblum. 2004. Ostia: A delegating architecture for secure system call interposition. In *NDSS*.
- [8] S. Ghavamnia, T. Palit, A. Benameur, and M. Polychronakis. 2020. Confine: Automated system call policy generation for container attack surface reduction. In *RAID*.
- [9] S. Ghavamnia, T. Palit, S. Mishra, and M. Polychronakis. 2020. Temporal system call specialization for attack surface reduction. In *USENIX*.
- [10] J. Jia, Y. ZhuFei, D. Williams, A. Arcangeli, C. Canella, H. Franke, T. Feldman-Fitzthum, D. Skarlatos, D. Gruss, and T. Xu. 2023. Programmable system call security with eBPF. *arXiv* (2023).
- [11] V. Kemerlis, Vasileios P., M. Polychronakis, and A. D. Keromytis. 2014. ret2dir: Rethinking kernel isolation. In *USENIX*.
- [12] Y. Li, B. Dolan-Gavitt, S. Weber, and J. Justin. 2017. Lock-in-Pop: Securing privileged operating system kernels by keeping on the beaten path. In *USENIX ATC*.
- [13] C. Linn, M. Rajagopalan, S. Baker, C. Collberg, and S. Debray and J.H. Hartman. 2005. Protecting Against Unexpected System Calls. In *USENIX*.
- [14] S. Pailoor, X. Wang, H. Shacham, and I. Dillig. 2020. Automated policy synthesis for system call sandboxing. *OOPSLA* (2020).
- [15] K. Yasukata, H. Tazaki, P.L. Aublin, and K. Ishiguro. 2023. *zpoline*: a system call hook mechanism based on binary rewriting. In *USENIX ATC*.

<sup>1</sup><https://github.com/wg/wrk>