

July 10–14, 2023
Melbourne, Australia



Association for
Computing Machinery

Advancing Computing as a Science & Profession



ASIA CCS '23

Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security

Sponsored by:

ACM SIGSAC

General Chairs:

Joseph Liu, Monash University, Australia

Yang Xiang, Swinburne University of Technology, Australia

Program Chairs:

Surya Nepal, Data61, Australia

Gene Tsudik, University of California Irvine, USA

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

ACM COPYRIGHT NOTICE. Copyright © 2023 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.

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: 979-8-4007-0098-9

Message from General Co-Chairs

It is our great pleasure to welcome you to the 18th ACM ASIA Conference on Computer and Communications Security 2022 (ACM ASIACCS 2023). ASIACCS 2023 takes place in Melbourne, Australia on 10th July to 14th July.

As the first post-COVID ASIACCS (travel restrictions of the world have been removed), we decide to organise it as an in-person-only conference, though we also provide an online option for the audience only (not presenter) to participate in. At the time of this writing, registration is still going on, over 200 people have finished registering as in-person.

This year we incorporate multiple programs in the conference. There are six workshops held on the first day of the conference. For the main conference, it includes four keynote talks from world-renowned researchers Prof. Wenyuan Xu, Prof. David Basin, Prof. N. Asokan and Prof. Vanessa Teague, normal (full) paper presentations and posters demonstrated during the tea and lunch break. This year we also add one more program - Tutorial into the conference. The purpose of tutorials is to let distinguished early to mid career researchers in cybersecurity to talk about the state-of-the-art research development of their own focused areas, that may also include their excellent works. We have 4 tutorials in our conference, and the topics covered range from post-quantum and machine learning security to memory corruptions and searchable encryption.

As an in-person conference, we also organise several social events for participants. A reception is held at the first day evening to allow both workshop and conference attendees to join and make networking. A half-day social event followed by the conference banquet is organised on the fourth day of the conference. In order to attract more women to the cybersecurity community, this year we further add a Women's Networking Reception on the third day of the conference. This is organised by some of our female organisation committee members while all attendees (not just restricted to women) are welcome to attend and share their experiences.

We would like to express our deep gratitude to our organisation committee, including Program Chairs Surya Nepal and Gene Tsudik, Local Organisation Chairs Sheng Wen and Xiao Chen, Registration and Finance Chairs Maggie Liu and Xingliang Yuan, Web Chairs Sharif Abuadbba and Shangqi Lai, Publicity Chairs Siqi Ma and Sushmita Ruj, Publication Chairs Seyit Camtepe and Shi-Feng Sun, Workshop Chairs Hyoungshick Kim and Shabnam Kasra, Poster Chairs Guangdong Bai and Wei Wu, Tutorial Chairs Ahmad Salehi Shahraki and Shujie Cui.

We would also like to acknowledge the support from our sponsors including our Platinum Sponsor CSIRO Data 61, Gold Sponsors Cyber Security Cooperative Research Centre (CSCRC) and Monash University Department of Software Systems and Cybersecurity (SSC), Bronze Sponsors Algorand Foundation and LinkStone.

We hope that you enjoy this conference, and wish all the participants a significant experience at ASIACCS 2023 in Melbourne.

General Co-Chairs
Joseph Liu and Yang Xiang

Message from Program Co-Chairs

We are both honored and pleased to have been entrusted to serve as PC Co-Chairs of AsiaCCS'23.

As the first post-pandemic incarnation, AsiaCCS'23 has attracted a large number of high-quality submissions from all over the world, with authors affiliated with diverse academic, non-profit, governmental, and industrial entities. After two rounds of submissions, the conference wound up with an excellent program, covering a broad range of timely and interesting topics in Security, Privacy, and Applied Cryptography.

A total of **429** submissions were received: **204** in the first, and **225** in the second, round, respectively. The reviewing process was facilitated by selfless and dedicated efforts by the PC members (and external reviewers) who collectively did an amazing job providing thorough and thoughtful reviews. Furthermore, some PC members “went the extra mile” by serving as shepherds for papers that required major revisions. The end-result is the total number of **74** accepted submissions, **32** in the first, and **42** in the second, round, respectively.

The 18-session AsiaCCS'23 technical program comprises 74 talks corresponding to accepted papers, a poster session, as well as four impressive keynote talks by internationally prominent and active researchers: N. Asokan, Vanessa Teague, David Basin, and Wenyuan Xu. The program testifies to the level of excellence and the stature of AsiaCCS as the top security venue in the Asia-Pacific region as well as one of the top ones, worldwide.

We offer our deepest gratitude to:

- Every single author of each submission to AsiaCCS'23, whether accepted or not. We thank them for supporting AsiaCCS and for their trust in us and the PC to fairly evaluate their research results.
- The AsiaCCS Steering Committee for their confidence in selecting us as PC Co-Chairs, and their support (especially, by **Jianning Zhou**) throughout the process leading to the conference.
- General Chairs: **Joseph Liu** and **Yang Xiang**, who dealt with (and addressed) numerous logistical and organizational issues.
- Publication Chairs: **Seyit Camtepe** and **Shi-Feng Sun**, for taking care of the proceedings. We especially acknowledge **Seyit** for handling numerous requests from the authors.
- Web Chairs: **Shangqi Lai** and **Sharif Abuadbba** for creating and maintaining the conference website. We are especially indebted to **Sharif** for his extraordinary dedication and the gargantuan amount of work spent on solving a myriad of issues with the website and the submission management system.
- Poster Chairs, **Guangdong Bai** and **Wei Wu**, for taking care of the poster track.
- All PC members and their delegated reviewers, who are the main engine of success and whose hard work yielded the excellent program. Special thanks to the recipients of the “Best Reviewers Award”, **Siqi Ma** and **Alexios Voulimeneas**, for their dedication as both reviewers and shepherds.

In closing, we look forward to the exciting few days in beautiful Melbourne in July and hope that all attendees (physical and remote) enjoy the conference.

PC Co-Chairs
Surya Nepal and Gene Tsudik

Table of Contents

Keynote 1:

Rethinking IoT Security: Understanding and Mitigating Out-of-Band Vulnerabilities	1
<i>Wenyuan Xu (Zhejiang University, China)</i>	

Session 1: Applied Cryptography (I)

Faster TFHE Bootstrapping with Block Binary Keys	2
<i>Changmin Lee (Korea Institute for Advanced Study, South Korea), Seonhong Min (Seoul National University, South Korea), Jinyeong Seo (Seoul National University, South Korea), Yongsoo Song (Seoul National University, South Korea)</i>	
Flag: A Framework for Lightweight Robust Secure Aggregation	14
<i>Laasya Bangalore (Georgetown University, USA), Mohammad Hossein Faghihi Sereshgi (University of Rochester, USA), Carmit Hazay (Bar-Ilan University, Israel), Muthuramakrishnan Venkatasubramaniam (Georgetown University, USA)</i>	
Implementing and Optimizing Matrix Triples with Homomorphic Encryption	29
<i>Johannes Mono (Ruhr University Bochum, Germany), Tim Güneysu (Ruhr University and DFKI GmbH, Germany)</i>	

Session 2: Privacy Application

Invasion of Location Privacy Using Online Map Services and Smartphone Sensors.....	41
<i>Hyunsoo Kim (NCSOFT, Republic of Korea), Youngbae Jeon (Samsung Research, Republic of Korea), Ji Won Yoon (Korea University, Republic of Korea)</i>	
Privacy-Preserving Record Linkage for Cardinality Counting.....	53
<i>Nan Wu (Macquarie University and CSIRO's Data61, Australia), Dinusha Vatsalan (Macquarie University, Australia), Mohamed Ali Kaafar (Macquarie University, Australia), Sanath Kumar Ramesh (OpenTreatments Foundations and CuresDev LLC, USA)</i>	
Investigating Users' Understanding of Privacy Policies of Virtual Personal Assistant Applications	65
<i>Baiqi Chen (The University of Queensland and CSIRO's Data61, Australia), Tingmin Wu (CSIRO's Data61, Australia), Yanjun Zhang (University of Technology Sydney, Australia), Mohan Baruwal Chhetri (CSIRO's Data61, Australia), Guangdong Bai (The University of Queensland, Australia)</i>	

Session 3: Privacy and Machine Learning

RECUP-FL: Reconciling Utility and Privacy in Federated Learning via User-Configurable Privacy Defense	80
<i>Yue Cui (University of Tennessee, US), Syed Irfan Ali Meerza (University of Tennessee, US), Zhuohang Li (University of Tennessee, US), Luyang Liu (Rutgers University, US), Jiaxin Zhang (Intuit AI Research, US), Jian Liu (University of Tennessee, US)</i>	
LDL: A Defense for Label-Based Membership Inference Attacks	95
<i>Arezoo Rajabi (University of Washington, USA), Dinuka Sahabandu (University of Washington, USA), Luyao Niu (University of Washington, USA), Bhaskar Ramasubramanian (Western Washington University, USA), Radha Poovendran (University of Washington, USA)</i>	
Extracting Privacy-Preserving Subgraphs in Federated Graph Learning using Information Bottleneck.....	109
<i>Chenhan Zhang (University of Technology Sydney, Australia), Weiqi Wang (University of Technology Sydney, Australia), James J.Q. Yu (Southern University of Science and Technology, China), Shui Yu (University of Technology Sydney, Australia)</i>	
LoDEN: Making Every Client in Federated Learning a Defender against the Poisoning Membership Inference Attacks	122
<i>Mengyao Ma (The University of Queensland and CSIRO's Data61, Australia), Yanjun Zhang (University of Technology Sydney, Australia), M.A.P. Chamikara (CSIRO's Data61, Australia), Leo Yu Zhang (Griffith University, Australia), Mohan Baruwal Chhetri (CSIRO's Data61, Australia), Guangdong Bai (The University of Queensland, Australia)</i>	
Data Privacy Examination against Semi-Supervised Learning.....	136
<i>Jiadong Lou (University of Louisiana at Lafayette, USA), Xu Yuan (University of Louisiana at Lafayette, USA), Miao Pan (University of Houston, USA), Hao Wang (Louisiana State University, USA), Nian-Feng Tzeng (University of Louisiana at Lafayette, USA)</i>	

Session 4: Architecture Security (I)

Cage4Deno: A Fine-Grained Sandbox for Deno Subprocesses	149
<i>Marco Abbadini (Università degli Studi di Bergamo, Italy), Dario Facchinetti (Università degli Studi di Bergamo, Italy), Gianluca Oldani (Università degli Studi di Bergamo, Italy), Matthew Rossi (Università degli Studi di Bergamo, Italy), Stefano Paraboschi (Università degli Studi di Bergamo, Italy)</i>	
CacheFX: A Framework for Evaluating Cache Security	163
<i>Daniel Genkin (Georgia Institute of Technology, USA), William Kosasih (University of Adelaide, Australia), Fangfei Liu (Intel Labs, USA), Anna Trikalinou (Microsoft, USA), Thomas Unterluggauer (Intel Labs, Austria), Yuval Yarom (Ruhr University Bochum, Germany)</i>	

Multi-Tag: A Hardware-Software Co-Design for Memory Safety based on Multi-Granular Memory Tagging.....	177
<i>Martin Unterguggenberger (Graz University of Technology, Austria), David Schrammel (Graz University of Technology, Austria), Pascal Nasahl (Graz University of Technology, Austria), Robert Schilling (Graz University of Technology, Austria), Lukas Lamster (Graz University of Technology, Austria), Stefan Mangard (Graz University of Technology, Austria)</i>	
FlushTime: Towards Mitigating Flush-based Cache Attacks via Collaborating Flush Instructions and Timers on ARMv8-A.....	190
<i>Jingquan Ge (Southern University of Science and Technology, China), Fengwei Zhang (Southern University of Science and Technology, China)</i>	
ShowTime: Amplifying Arbitrary CPU Timing Side Channels.....	205
<i>Antoon Purnal (imec-COSIC, KU Leuven), Marton Bogнар (imec-DistriNet, KU Leuven), Frank Piessens (imec-DistriNet, KU Leuven), Ingrid Verbauwhede (imec-COSIC, KU Leuven)</i>	

Session 5: Software Security (I)

Symbolic Modeling of Remote Attestation Protocols for Device and App Integrity on Android	218
<i>Abdulla Aldoseri (University of Birmingham and University of Bahrain, UK), Tom Chothia (University of Birmingham, UK), José Moreira (Valory AG, Switzerland), David Oswald (University of Birmingham, UK)</i>	
Arvin: Greybox Fuzzing Using Approximate Dynamic CFG Analysis.....	232
<i>Sirus Shahini (University of Utah), Mu Zhang (University of Utah), Mathias Payer (EPFL), Robert Ricci (University of Utah)</i>	
AbsIntIO: Towards Showing the Absence of Integer Overflows in Binaries using Abstract Interpretation.....	247
<i>Alexander Kuchler (Fraunhofer AISEC, Germany), Leon Wenning (TU München, Germany), Florian Wendland (Fraunhofer AISEC, Germany)</i>	
Eliminating Vulnerabilities by Disabling Unwanted Functionality in Binary Programs.....	259
<i>Mohamad Mansouri (EURECOM, France), Jun Xu (University of Utah, USA), Georgios Portokalidis (Stevens Institute of Technology, USA)</i>	

Session 6: Hardware Security

Secure and Efficient Mobile DNN Using Trusted Execution Environments.....	274
<i>Bin Hu (Rutgers University), Yan Wang (Temple University), Jerry Cheng (New York Institute of Technology), Tianming Zhao (University of Dayton), Yucheng Xie (Indiana University-Purdue University Indianapolis), Xiaonan Guo (George Mason University), Yingying Chen (Rutgers University)</i>	
Stairway to Rainbow	286
<i>Gildas Avoine (INSA, CNRS, IRISA, France), Xavier Carpent (University of Nottingham, UK), Diane Leblanc-Albarel (CNRS, INSA, IRISA, France)</i>	

EMShepherd: Detecting Adversarial Samples via Side-channel Leakage..... 300

Ruyi Ding (Northeastern University), Cheng Gongye (Northeastern University), Siyue Wang (Northeastern University), Aidong Adam Ding (Northeastern University), Yunsi Fei (Northeastern University)

Electromagnetic Signal Injection Attacks on Differential Signaling 314

Youqian Zhang (University of Oxford, UK), Kasper Rasmussen (University of Oxford, UK)

Keynote 2:

Formal Methods for Payment Protocols 326

David Basin (ETH Zurich, Switzerland)

Keynote 3:

Model Stealing Attacks and Defenses: Where Are We Now? 327

N. Asokan (University of Waterloo, Canada and Aalto University, Finland)

Session 7: Applied Cryptography (II)

On the Cryptographic Fragility of the Telegram Ecosystem 328

Theo von Arx (ETH Zurich, Switzerland), Kenneth G. Paterson (ETH Zurich, Switzerland)

PSI with Computation or Circuit-PSI for Unbalanced Sets from Homomorphic Encryption 342

Yongha Son (Samsung SDS, South Korea), Jinhyuck Jeong (Samsung SDS, South Korea)

ZEKRA: Zero-Knowledge Control-Flow Attestation 357

Heini Bergsson Debes (Technical University of Denmark (DTU)), Edlira Dushku (Aalborg University), Thanassis Giannetsos (Ubitech Ltd), Ali Marandi (Technical University of Denmark (DTU))

Overdrive LowGear 2.0: Reduced-Bandwidth MPC without Sacrifice 372

Pascal Reisert (University of Stuttgart, Germany), Marc Rivinius (University of Stuttgart, Germany), Toomas Krips (University of Tartu, Estonia), Ralf Küsters (University of Stuttgart, Germany)

Session 8: Software Security (II)

Benchmarking the Benchmarks..... 387

Marc Miltenberger (Fraunhofer SIT, Germany), Steven Arzt (Fraunhofer SIT, Germany), Philipp Holzinger (Fraunhofer SIT, Germany), Julius Näumann (Fraunhofer SIT, Germany)

Ember-IO: Effective Firmware Fuzzing with Model-Free Memory Mapped IO 401

Guy Farrelly (The University of Adelaide, Australia), Michael Chesser (The University of Adelaide, Australia), Damith C. Ranasinghe (University of Adelaide, Australia)

RaceBench: A Triggerable and Observable Concurrency Bug Benchmark..... 415

Jiashuo Liang (Peking University, China), Ming Yuan (Tsinghua University, China), Zhanzhao Ding (Peking University, China), Siqi Ma (The University of New South Wales, Australia), Xinhui Han (Peking University, China), Chao Zhang (Tsinghua University, China)

BINWRAP: Hybrid Protection against Native Node.js Add-ons..... 429

George Christou (FORTH-ICS, Greece), Grigoris Ntousakis (Brown University, USA), Eric Lahtinen (Aarno Labs, USA), Sotiris Ioannidis (TU Crete, Greece), Vasileios P. Kemerlis (Brown University, USA), Nikos Vasilakis (Brown University, USA)

Session 9: Architecture Security (II)

Binary Function Clone Search in the Presence of Code Obfuscation and Optimization over Multi-CPU Architectures..... 443

Abdullah Qasem (Concordia University, Canada), Mourad Debbabi (Concordia University, Canada), Bernard Lebel (Thales Research and Technologies, Canada), Marthe Kassouf (Hydro-Québec Research Institute, Canada)

SPEAR-V: Secure and Practical Enclave Architecture for RISC-V..... 457

David Schrammel (Graz University of Technology, Austria), Moritz Waser (Graz University of Technology, Austria), Lukas Lamster (Graz University of Technology, Austria), Martin Unterguggenberger (Graz University of Technology, Austria), Stefan Mangard (Graz University of Technology, Austria)

SFITAG: Efficient Software Fault Isolation with Memory Tagging for ARM Kernel Extensions..... 469

Jiwon Seo (Seoul National University, Republic of Korea), Junseung You (Seoul National University, Republic of Korea), Yungi Cho (Seoul National University, Republic of Korea), Yeongpil Cho (Hanyang University, Republic of Korea), Donghyun Kwon (Pusan National University, Republic of Korea), Yunheung Paek (Seoul National University, Republic of Korea)

An Evaluation Framework for Intrusion Prevention Systems on Serial Data Bus Networks 481

Matthew Rogers (University of Oxford, USA), Kasper Rasmussen (University of Oxford, UK)

Session 10: User-Centric Security (I)

#DM-Me: Susceptibility to Direct Messaging-Based Scams 494

Raj Vardhan (Texas A&M University), Alok Chandrawal (Texas A&M University), Phakpoom Chinprutthiwong (Sisaket Rajabhat University), Yangyong Zhang (Texas A&M University), Guofei Gu (Texas A&M University)

An End-to-End Analysis of Covid-Themed Scams in the Wild 509

Behzad Ousat (Florida International University, USA), Mohammad Ali Tofighi (Florida International University, USA), Amin Kharraz (Florida International University, USA)

MASCARA: Systematically Generating Memorable and Secure Passphrases..... 524

Avirup Mukherjee (IIT Kharagpur), Kousshik Murali (IIT Kharagpur), Shivam Kumar Jha (IIT Kharagpur), Niloy Ganguly (IIT Kharagpur), Rahul Chatterjee (University of Wisconsin–Madison), Mainack Mondal (IIT Kharagpur)

How Secure are the Main Real-World Mix Networks — Case Studies to Explore Vulnerabilities and Usability 539

Kun Peng (Huawei Technology Ltd)

Keynote 4:

Democratizing Election Verification: New Methods for Addressing an Ancient Attacker Model ... 552

Vanessa Teague (Australian National University and Democracy Developers Ltd., Australia)

Session 11: Machine Learning and Security

FLAIR: Defense against Model Poisoning Attack in Federated Learning 553

Atul Sharma (Purdue University, USA), Wei Chen (Purdue University, USA), Joshua Zhao (Purdue University, USA), Qiang Qiu (Purdue University, USA), Saurabh Bagchi (Purdue University, USA), Somali Chaterji (Purdue University, USA)

BFU: Bayesian Federated Unlearning with Parameter Self-Sharing 567

Weiqi Wang (University of Technology Sydney), Zhiyi Tian (University of Technology Sydney), Chenhan Zhang (University of Technology Sydney), An Liu (Soochow University), Shui Yu (University of Technology Sydney)

SoK: Systematizing Attack Studies in Federated Learning – From Sparseness to Completeness 579

Geetanjali Sharma (La Trobe University and CSIRO's Data61, Australia), M.A.P. Chamikara (CSIRO's Data61, Australia), Mohan Baruwal Chhetri (CSIRO's Data61, Australia), Yi-Ping Phoebe Chen (La Trobe University, Australia)

Going Haywire: False Friends in Federated Learning and How to Find Them..... 593

William Aiken (University of Ottawa, Canada), Paula Branco (University of Ottawa, Canada), Guy-Vincent Jourdan (University of Ottawa, Canada)

Deepfake CAPTCHA: A Method for Preventing Fake Calls 608

Lior Yasur (Ben-Gurion University of the Negev, Israel), Guy Frankovits (Ben-Gurion University of the Negev, Israel), Fred M. Grabovski (Ben-Gurion University of the Negev, Israel), Yisroel Mirsky (Ben-Gurion University of the Negev, Israel)

Session 12: Applied Cryptography (III)

A New Look at Blockchain Leader Election: Simple, Efficient, Sustainable and Post-Quantum 623

Muhammed F. Esgin (Monash University & CSIRO's Data61, Australia), Oğuzhan Ersoy (Radboud University and Delft University of Technology, The Netherlands), Veronika Kuchta (Florida Atlantic University, USA), Julian Loss (CISPA Helmholtz Center for Information Security, German), Amin Sakzad (Monash University, Australia), Ron Steinfeld (Monash University, Australia), Xiangwen Yang (Monash University, Australia), Raymond K. Zhao (CSIRO's Data61, Australia)

IGA: An Improved Genetic Algorithm to Construct Weightwise (Almost) Perfectly Balanced Boolean Functions with High Weightwise Nonlinearity 638

Lili Yan (Tianjin University, China), Jingyi Cui (Tianjin University, China), Jian Liu (Tianjin University, China), Guangquan Xu (Tianjin University, China), Lidong Han (Hangzhou Normal University, China), Alireza Jolfaei (Flinders University, Australia), Xi Zheng (Macquarie University, Australia)

FUSE – Flexible File Format and Intermediate Representation for Secure Multi-Party Computation 649

Lennart Braun (Aarhus University, Denmark), Moritz Huppert (Technical University of Darmstadt, Germany), Nora Khayata (Technical University of Darmstadt, Germany), Thomas Schneider (Technical University of Darmstadt, Germany), Oleksandr Tkachenko (DFINITY, Switzerland)

A Trade-off SVP-solving Strategy Based on a Sharper pnj-BKZ Simulator 664

Leizhang Wang (Xidian University, China), Yuntao Wang (Osaka University, Japan), Baocang Wang (Xidian University, China)

Communication-Efficient Inner Product Private Join and Compute with Cardinality 678

Koji Chida (Gunma University, Japan), Koki Hamada (NTT Social Informatics Laboratories, Japan), Atsunori Ichikawa (NTT Social Informatics Laboratories, Japan), Masanobu Kii (NTT Social Informatics Laboratories, Japan), Junichi Tomida (NTT Social Informatics Laboratories, Japan)

Session 13: Adversarial Machine Learning

Jujutsu: A Two-stage Defense against Adversarial Patch Attacks on Deep Neural Networks 689

Zitao Chen (University of British Columbia, Canada), Pritam Dash (University of British Columbia, Canada), Karthik Pattabiraman (University of British Columbia, Canada)

Mitigating Adversarial Attacks by Distributing Different Copies to Different Buyers..... 704

Jiyi Zhang (National University of Singapore, Singapore), Han Fang (National University of Singapore, Singapore), Wesley Joon-Wie Tann (National University of Singapore, Singapore), Ke Xu (Huawei International, Singapore), Chengfang Fang (Huawei International, Singapore), Ee-Chien Chang (National University of Singapore, Singapore)

Boost Off/On-Manifold Adversarial Robustness for Deep Learning with Latent Representation Mixup..... 716

Mengdie Huang (Xidian University, China), Yi Xie (Xidian University, China), Xiaofeng Chen (Xidian University, China), Jin Li (Guangzhou University, China), Changyu Dong (Newcastle University, UK), Zheli Liu (Nankai University, China), Willy Susilo (University of Wollongong, Australia)

DHBE: Data-free Holistic Backdoor Erasing in Deep Neural Networks via Restricted Adversarial Distillation.....	731
---	------------

Zhicong Yan (Shanghai Jiao Tong University, China), Shenghong Li (Shanghai Jiao Tong University, China), Ruijie Zhao (Shanghai Jiao Tong University, China), Yuan Tian (Shanghai Jiao Tong University, China), Yuanyuan Zhao (Hangzhou Normal University, China)

Session 14: Network Security

T-TER: Defeating A2 Trojans with Targeted Tamper-Evident Routing	746
---	------------

Timothy Trippel (University of Michigan, USA), Kang G. Shin (University of Michigan, USA), Kevin B. Bush (MIT Lincoln Laboratory, USA), Matthew Hicks (Virginia Tech, USA)

SPARTA: Signal Propagation-based Attack Recognition and Threat Avoidance for Automotive Networks	760
---	------------

Oleg Schell (Robert Bosch GmbH), Marcel Kneib (Robert Bosch GmbH)

Investigating Traffic Analysis Attacks on Apple iCloud Private Relay	773
---	------------

Ali Zohaib (University of Massachusetts Amherst, USA), Jade Sheffey (University of Massachusetts Amherst, USA), Amir Houmansadr (University of Massachusetts Amherst, USA)

A Honey postMessage, but a Heart of Gall: Exploiting Push Service in Service Workers Via postMessage.....	785
--	------------

Yeomin Jeong (Korea University, Korea), Woonghee Lee (Korea University, Korea), Junbeom Hur (Korea University, Korea)

Session 15: Cloud Security

Secrets Revealed in Container Images: An Internet-wide Study on Occurrence and Impact.....	797
---	------------

Markus Dahlmanns (RWTH Aachen University, Germany), Constantin Sander (RWTH Aachen University, Germany), Robin Decker (RWTH Aachen University, Germany), Klaus Wehrle (RWTH Aachen University, Germany)

Securing Container-based Clouds with Syscall-aware Scheduling	812
--	------------

Michael V. Le (IBM Research, USA), Salman Ahmed (IBM Research, USA), Dan Williams (IBM Research, USA), Hani Jamjoom (IBM Research, USA)

IOTLB-SC: An Accelerator-Independent Leakage Source in Modern Cloud Systems	827
--	------------

Thore Tiemann (University of Lübeck, Germany), Zane Weissman (Worcester Polytechnic Institute, USA), Thomas Eisenbarth (University of Lübeck, Germany), Berk Sunar (Worcester Polytechnic Institute, USA)

Security Properties of Virtual Remotes and SPOOKing their Violations.....	841
--	------------

Joshua Majors (Purdue University, USA), Edgardo Barsallo Yi (Purdue University, USA), Amiya Maji (Purdue University, USA), Darren Wu (Purdue University, USA), Saurabh Bagchi (Purdue University, USA), Aravind Machiry (Purdue University, USA)

Session 16: User-Centric Security (II)

Payment with Dispute Resolution: A Protocol for Reimbursing Frauds Victims	855
<i>Aydin Abadi (University College London, UK), Steven J. Murdoch (University College London, UK)</i>	
Do Users Really Know Alexa? Understanding Alexa Skill Security Indicators	870
<i>Yangyong Zhang (Texas A&M University), Raj Vardhan (Texas A&M University), Phakpoom Chinprutthiwong (Sisaket Rajabhat University), Guofei Gu (Texas A&M University)</i>	
Formalising Application-Driven Authentication and Access-Control Based on Users’ Companion Devices.....	884
<i>Chris Culnane (Castellate Consulting Ltd, UK), Ioana Boureanu (University of Surrey, UK), Jean Snyman (University of Surrey, UK), Stephan Wesemeyer (University of Surrey, UK), Helen Treharne (University of Surrey, UK)</i>	
CRYPTOSHIELD – Automatic On-Device Mitigation for Crypto API Misuse in Android Applications	899
<i>Florian Draschbacher (Graz University of Technology and Secure Information Technology Center, Austria), Johannes Feichtner (Dynatrace Austria GmbH, Austria)</i>	

Session 17: Model Security

QUDA: Query-Limited Data-Free Model Extraction.....	913
<i>Zijun Lin (Nanyang Technological University, Singapore), Ke Xu (Huawei International, Singapore), Chengfang Fang (Huawei International, Singapore), Huadi Zheng (Huawei Technology, China), Jaheezuddin Aneez Ahmed (Nanyang Technological University, Singapore), Jie Shi (Huawei International, Singapore)</i>	
Masked Language Model Based Textual Adversarial Example Detection	925
<i>Xiaomei Zhang (Southwest University, China), Zhaoxi Zhang (Deakin University, Australia), Qi Zhong (Deakin University, Australia), Xufei Zheng (Southwest University, China), Yanjun Zhang (University of Technology Sydney, Australia), Shengshan Hu (Huazhong University of Science and Technology, China), Leo Yu Zhang (Griffith University, Australia)</i>	
CASSOCK: Viable Backdoor Attacks against DNN in the Wall of Source-Specific Backdoor Defenses	938
<i>Shang Wang (Nanjing University of Science and Technology, China), Yansong Gao (CSIRO’s Data61, Australia and Nanjing University of Science and Technology, China), Anmin Fu (Nanjing University of Science and Technology, China), Zhi Zhang (University of Western Australia and CSIRO’s Data61, Australia), Yuqing Zhang (University of Chinese Academy of Sciences, China), Willy Susilo (University of Wollongong, Australia), Dongxi Liu (CSIRO’s Data61, Australia)</i>	
A Transformer-based Function Symbol Name Inference Model from an Assembly Language for Binary Reversing	951
<i>HyunJin Kim (Sungkyunkwan University, South Korea), JinYeong Bak (Sungkyunkwan University, South Korea), Kyunghyun Cho (New York University, USA), Hyungjoon Koo (Sungkyunkwan University, South Korea)</i>	

Session 18: Application Security

ThreadLock: Native Principal Isolation Through Memory Protection Keys.....	966
<i>William Blair (Boston University, USA), William Robertson (Northeastern University, USA), Manuel Egele (Boston University, USA)</i>	
Secure Context Switching of Masked Software Implementations.....	980
<i>Barbara Gigerl (Graz University of Technology, Austria), Robert Primas (Graz University of Technology, Austria), Stefan Mangard (Graz University of Technology, Austria)</i>	
A Scalable Double Oracle Algorithm for Hardening Large Active Directory Systems.....	993
<i>Yumeng Zhang (The University of Adelaide, Australia), Max Ward (University of Western Australia, Australia), Mingyu Guo (The University of Adelaide, Australia), Hung Nguyen (The University of Adelaide, Australia)</i>	
Uncovering Vulnerabilities of Bluetooth Low Energy IoT from Companion Mobile Apps with BLE-GUIDE	1004
<i>Pallavi Sivakumaran (University of London, United Kingdom), Chaoshun Zuo (The Ohio State University, USA), Zhiqiang Lin (The Ohio State University, USA), Jorge Blasco (Universidad Politécnica de Madrid, Spain)</i>	

Posters:

POSTER: A Cyberspace Study of the Russia-Ukraine War	1016
<i>Gursimran Singh (Rochester Institute of Technology, USA), H. B. Acharya (Rochester Institute of Technology, USA)</i>	
POSTER: A Semi-asynchronous Federated Intrusion Detection Framework for Power Systems	1019
<i>Muhammad Akbar Husnoo (Deakin University), Adnan Anwar (Deakin University), Haftu Tasew Reda (Deakin University, Australia), Nasser Hosseinzadeh (Deakin University, Australia)</i>	
POSTER: Toward Intelligent Cyber Attacks for Moving Target Defense Techniques in Software-Defined Networking.....	1022
<i>Tina Moghaddam (The University of Queensland, Australia), Guowei Yang (The University of Queensland, Australia), Chandra Thapa (CSIRO's Data61, Australia), Seyit Camtepe (CSIRO's Data61, Australia), Dan Dongseong Kim (The University of Queensland, Australia)</i>	
POSTER: A Common Framework for Resilient and Safe Cyber-Physical System Design	1025
<i>Luyao Niu (University of Washington, USA), Abdullah Al Maruf (University of Washington, USA), Andrew Clark (Washington University in St. Louis, USA), J. Sukarno Mertoguno (Georgia Institute of Technology, USA), Radha Poovendran (University of Washington, USA)</i>	

POSTER: Leveraging eBPF to Enhance Sandboxing of WebAssembly Runtimes.....	1028
<i>Marco Abbadini (Università degli Studi di Bergamo, Italy), Michele Beretta (Università degli Studi di Bergamo, Italy), Dario Facchinetti (Università degli Studi di Bergamo, Italy), Gianluca Oldani (Università degli Studi di Bergamo, Italy), Matthew Rossi (Università degli Studi di Bergamo, Italy), Stefano Paraboschi (Università degli Studi di Bergamo, Italy)</i>	
POSTER: ML-Compass: A Comprehensive Assessment Framework for Machine Learning Models.....	1031
<i>Zhibo Jin (The University of Sydney and CSIRO's Data61), Zhiyu Zhu (The University of Sydney and CSIRO's Data61), Hongsheng Hu (CSIRO's Data61), Minhui Xue (CSIRO's Data61), Huaming Chen (The University of Sydney)</i>	
POSTER: Performance Characterization of Binarized Neural Networks in Traffic Fingerprinting	1034
<i>Yiyan Wang (The University of Sydney, Australia), Thilini Dahanayaka (The University of Sydney, Australia), Guillaume Jourjon (CSIRO-Space Astronomy, Australia), Suranga Seneviratne (The University of Sydney, Australia)</i>	
POSTER: On Searching Information Leakage of Python Model Execution to Detect Adversarial Examples.....	1037
<i>Cheng-Yao Guo (National Chengchi University, Taiwan), Fang Yu (National Chengchi University, Taiwan)</i>	
POSTER: A Teacher-Student with Human Feedback Model for Human-AI Collaboration in Cybersecurity	1040
<i>Abdullahi Chowdhury (The University of Adelaide, Australia), Debi Ashenden (The University of Adelaide, Australia), Ganna Pogrebna (The University of Sydney, Australia), Hung Nguyen (The University of Adelaide, Australia)</i>	
POSTER: Security Logs Graph Analytics for Industry Network System.....	1043
<i>Qiaoran Meng (National University of Singapore, Singapore), Nay Oo (NCS Cyber Special Ops-R&D, Singapore), Hoon Wei Lim (NCS Cyber Special Ops-R&D, Singapore), Biplab Sikdar (National University of Singapore, Singapore)</i>	

ASIA CCS'23 Organisation

General Chairs: Joseph Liu (Monash University, Australia)
Yang Xiang (Swinburne University of Technology, Australia)

Program Chairs: Surya Nepal (Data61, Australia)
Gene Tsudik (University of California Irvine, US)

Local Organisation

Chairs: Sheng Wen (Swinburne University of Technology, Australia)
Xiao Chen (Monash University, Australia)

Registration and

Finance Chairs: Maggie Liu (RMIT University, Australia)
Xingliang Yuan (Monash University, Australia)

Web Chairs: Sharif Abuadbba (Data61, Australia)
Shangqi Lai (Monash University, Australia)

Publicity Chairs: Siqi Ma (UNSW Canberra, Australia)
Sushmita Ruj (UNSW Sydney, Australia)

Publication Chairs: Seyit Camtepe (Data61, Australia)
Shi-Feng Sun (Shanghai Jiao Tong University, China)

Workshop Chairs: Hyounghick Kim (Sungkyunkwan University, Korea)
Shabnam Kasra (UNSW Canberra, Australia)

Poster Chairs: Guangdong Bai (University of Queensland, Australia)
Wei Wu (Fujian Normal University, China)

Tutorial Chairs: Ahmad Salehi Shahraki (La Trobe University, Australia)
Shujie Cui (Monash University, Australia)

Steering Committee

Chair: Jianying Zhou (Singapore University of Technology and Design, Singapore)

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)

**Program
Committee:**

Alexios Voulimeneas, KU Leuven, Belgium
Alptekin K p u, Ko  University, Turkey
Angelos Stavrou, Virginia Tech, USA
Anna Lisa Ferrara, University of Molise, Italy
Annabelle McIver, Macquarie University, Australia
Aravind Machiry, Purdue University, USA
Ashish Kundu, Cisco Research, USA
Bet l Durak, Microsoft Research, USA
Bo Chen, Michigan Technological University, USA
Bruno Crispo, University of Trento, Italy
Chao Zhang, Tsinghua University, China
Christopher Wood, Cloudflare, USA
Cristian-Alexandru Staicu, CISP Helmholtz Center, Germany
Cristina Alacraz, University of Malaga, Spain
Damith Ranasinghe, University of Adelaide, Australia
Daniele Antonioli, EURECOM, France
Debdeep Mukhopadhyay, Indian Institute of Technology, Kharagpur, India
Debin Gao, Singapore Management University, Singapore
Di Ma, University of Michigan-Dearborn, USA
Dokyung Song, Yonsei University, Korea
Doowon Kim, University of Tennessee, USA
Edgar Weippl, University of Vienna & SBA Research, Austria
Elisabeth Oswald, University of Klagenfurt, Austria
Gabriele Oligeri, Hamad bin Khalifa University, Qatar
Ghassan Karame, Ruhr University Bochum, Germany
Giovanni Russello, University of Auckland, New Zealand
Guomin Yang, University of Wollongong, Australia
Haehyun Cho, Soongsil University, Korea
Herv  Debar, T l com SudParis, Institut Polytechnique de Paris, France
Hyoungshick Kim, Sungkyunkwan University, Korea
Ileana Buhan, Radboud University Nijmegen, Netherlands
Jie Yang, Florida State University, USA
Jin-Hee Cho, Virginia Tech, USA
Joaquin Garcia-Alfaro, Institut Polytechnique de Paris, France
Jorge Blasco Alis, Royal Holloway, University of London, UK
Jorge Guajardo, Robert Bosch LLC – Research and Technology Center, USA
Juanru Li, Shanghai Jiao Tong University, China
Jun Sakuma, University of Tsukuba, Japan
Junghwan “John” Rhee, University of Central Oklahoma, USA
Kapil Singh, IBM T.J. Watson Research Center, USA
Kari Kostianen, ETH Zurich, Switzerland
Kasper Rasmussen, University of Oxford, UK
Katerina Mitrokotsa, University of St. Gallen, Switzerland
Katsunari Yoshioka, Yokohama National University, Japan
Kiran Balagani, New York Institute of Technology, USA
Kun Sun, George Mason University, USA
Kwok-Yan Lam, Nanyang Technological University, Singapore
Lorenzo De Carli, Worcester Polytechnic Institute, USA
Luca Vigan , King’s College London, UK
Lucas Davi, University of Duisburg-Essen, Germany

Lucca Hirschi, Inria, France
Mads Dam, KTH Royal Institute of Technology, Sweden
Mahmoud Ammar, Huawei Research, Germany
Man Ho Au, University of Hong Kong, Hong Kong
Mark Manulis, Universität der Bundeswehr München, Germany
Mathieu Cunche, INSA-Lyon / Inria, France
Mathy Vanhoef, KU Leuven, Belgium
Melek Önen, EURECOM, France
Michael Sirivianos, Cyprus University of Technology, Cyprus
Mitsuaki Akiyama, NTT, Japan
Miyako Ohkubo, NIICT, Japan
Mohammad Mannan, Concordia University, Canada
Mu Zhang, University of Utah, USA
Muhammad Ikram, Macquarie University, Australia
Muhammed Esgin, Monash University, Australia
Ning Zhang, Washington University in St. Louis, USA
Nuno Santos, INESC-ID / Instituto Superior Técnico, Portugal
Olga Gadyatskaya, Leiden University, The Netherlands
Qi Li, Tsinghua University, China
Qiang Tang, University of Sydney, Australia
Rahmadi Trimananda, University of California, Irvine, USA
Reza Curtmola, New Jersey Institute of Technology, USA
Rishab Nithyanand, University of Iowa, USA
Roberto Guanciale, KTH, Sweden
Rolf Oppliger, eSECURITY Technologies, Switzerland
Sanjay Jha, UNSW, Australia
Satoshi Obana, Hosei University, Japan
Satyanarayana Vusirikala, DFINITY, USA
Saurabh Bagchi, Purdue University & KeyByte, USA
Selcuk Uluagac, Florida International University, USA
Seung Geol Choi, US Naval Academy, USA
Shabnam Kasra Kermanshahi, RMIT, Australia
Shuohuai Xu, University of Colorado Colorado Springs, USA
Siqi Ma, UNSW, Australia
Stefan Katzenbeisser, University of Passau, Germany
Steven Galbraith, University of Auckland, New Zealand
Sven Dietrich, City University of New York, USA
Tatsuya Mori, Waseda University, Japan
Thorsten Strufe, KIT, Germany
Tingmin Wu, Data61, CSIRO, Australia
Vanessa Daza, Pompeu Fabra University, Spain
Veelasha Moonsamy, Ruhr University Bochum, Germany
William Robertson, Northeastern University, USA
Willy Susilo, University of Wollongong, Australia
Xavier Carpent, University of Nottingham, UK
Xiapu Luo, Hong Kong Polytechnic University, China
Xingliang Yuan, Monash University, Australia
Youngee Park, San Jose State University, USA
Yuan Hong, Illinois Institute of Technology, USA
Zhi Zhang, Data61, CSIRO, Australia
Zhen Huang, DePaul University, USA

**External
Reviewers:**

Ziyao Liu, NTU, Singapore
Feng Li, NTU, Singapore
Jiabo Wang, NTU, Singapore
Jiani Fan, NTU, Singapore
Niusen Chen, Michigan Technological University, USA
Caleb Rother, Michigan Technological University, USA
Harsh Singh, Michigan Technological University, USA
Weijing You, Fujian Normal University, China
Xinyu Zhang, Monash University, Australia
Shangqi Lai, Monash University, Australia
Maxime Buser, Kudelski Security, Switzerland
Mafalda Ferreira, INESC-ID / Instituto Superior Técnico, Portugal
Daniela Lopes, INESC-ID / Instituto Superior Técnico, Portugal
Íris Damião, LIP Lisboa / Instituto Superior Técnico, Portugal
Jia Liu, ENYA Labs, UK
Daniel Klischies, Ruhr University Bochum, Germany
Philipp Mackensen, Ruhr University Bochum, Germany
Abbas Acar, Florida International University, Germany
Shawn Emery, UCCS, USA
Ekzhin Ear, UCCS, USA
Rosana Montanez Rodriguez, UCCS, USA
Takashi Nishide, University of Tsukuba, Japan
Kazuma Ohara, NIAIST, Japan
Shi Bai, Florida Atlantic University, USA
Kelong Cong, KU Leuven, Belgium
Duhyeong Kim, Intel, USA
Yi-Fu Lai, University of Auckland, New Zealand
Frederik Vercauteren, KU Leuven, Belgium
Joshua Zhao, Purdue University, USA
Chris Gutierrez, Intel, USA
Fahad Arshad, VMWare, USA
Ahaan Dabholkar, Purdue University, USA
Johannes Ernst, University of St. Gallen, Switzerland
Shihua Sun, Virginia Technology, USA
Tolga Atalay, Virginia Technology, USA
Akira Kanaoka, Toho University, Japan
Daniel Collins, EPFL, Switzerland
Koji Nuida, Kyushu University, Japan
Haiyang Xue, University of Hong Kong, Hong Kong
Kexin Hu, Chinese Academy of Sciences, China
Nadeem Ahmed, UNSW, Australia
Ryo Lijima, Waseda University, Japan
Sayntan Mukherjee, University of St. Gallen, Switzerland
Srinath Setty, Microsoft Research, USA
Takuya Watanabe, Waseda University, Japan
Tapas Pal, NTT Corporation, Japan
Hanwen Feng, University of Sydney, Australia
Jason (Minhui) Xue, CSIRO's Data61, Australia
Jawad Ahmed, UNSW, Australia

Junichi Tomida, NTT, Japan
Kazuki Yoneyama, Ibaraki University, Japan
Kazuma Ohara, AIST, Japan
Keewoo Lee, Seoul National University, Korea
Kristen Moore, CSIRO's Data61, Australia
Masaya Yasuda, Rikkyo University, Japan
Shuo Wang, CSIRO's Data61, Australia
Takasha Nishide, Tsukuba University, Japan
Jeremy D. Seideman, American Express, USA
Jiakun Liu, Singapore Management University, Singapore

Poster

Reviewers: Naipeng Dong, Qinglei Kong, Juanru Li, Chao Lin, Chamikara Mahawaga Arachchige, Mark Huasong Meng, Jianting Ning, Qiang Tang, Sin Gee Teo, Viet Vo, Kailong Wang, Guowei Yang, Leo Yu Zhang, Ying Zhang

ASIA CCS'23 Sponsor and Supporters

Sponsor:



**Platinum
Supporter:**



**Gold
Supporters:**



MONASH
INFORMATION
TECHNOLOGY

MONASH
SOFTWARE
SYSTEMS AND
CYBERSECURITY

**Bronze
Supporters:**



LinkStone
Creating More Secure Identity Management



POSTER: Leveraging eBPF to enhance sandboxing of WebAssembly runtimes

Marco Abbadini
marco.abbadini@unibg.it
Università degli Studi di Bergamo
Bergamo, Italy

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

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

Gianluca Oldani
gianluca.oldani@unibg.it
Università degli Studi di Bergamo
Bergamo, Italy

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

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

ABSTRACT

WebAssembly is a binary instruction format designed as a portable compilation target enabling the deployment of untrusted code in a safe and efficient manner. While it was originally designed to be run inside web browsers, modern runtimes like Wasmtime and WasmEdge can execute WebAssembly directly on various systems. In order to access system resources with a universal hostcall interface, a standardization effort named WebAssembly System Interface (WASI) is currently undergoing. With specific regard to the file system, runtimes must prevent hostcalls to access arbitrary locations, thus they introduce security checks to only permit access to a pre-defined list of directories. This approach not only suffers from poor granularity, it is also error-prone and has led to several security issues. In this work we replace the security checks in hostcall wrappers with eBPF programs, enabling the introduction of fine-grained per-module policies. Preliminary experiments confirm that our approach introduces limited overhead to existing runtimes.

CCS CONCEPTS

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

KEYWORDS

Sandboxing, Access control, WebAssembly runtime, eBPF

ACM Reference Format:

Marco Abbadini, Michele Beretta, Dario Facchinetti, Gianluca Oldani, Matthew Rossi, and Stefano Paraboschi. 2023. POSTER: Leveraging eBPF to enhance sandboxing of WebAssembly runtimes. In *ACM ASIA Conference on Computer and Communications Security (ASIA CCS '23)*, July 10–14, 2023, Melbourne, VIC, Australia. ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3579856.3592831>



This work is licensed under a Creative Commons Attribution International 4.0 License.

ASIA CCS '23, July 10–14, 2023, Melbourne, VIC, Australia
© 2023 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0098-9/23/07.
<https://doi.org/10.1145/3579856.3592831>

1 INTRODUCTION

WebAssembly (Wasm) [15] is a popular binary instruction format that enables the execution of untrusted code in a safe, isolated environment. Moreover, it is a portable compilation target for different languages, and can be executed efficiently on a wide range of platforms without the need of dedicated hardware. Wasm was originally meant to be run inside web browsers, but given the considerable advantages it brings, many runtimes that allow execution in stand-alone mode have been developed recently. Popular examples are Wasmtime, WasmEdge, Wasmer, and WAMR.

To answer the developers' need to access resources of the host system from within the runtime, a standardization effort called WebAssembly System Interface (WASI) [28] is undergoing. Its goal is to provide a stable and multi-platform system interface. To be WASI-compliant, each runtime must implement all the calls defined in the interface with dedicated functions, which are named hostcalls. However, implementing these functions is non-trivial, since (i) the code must not introduce violations to the Wasm memory model, and (ii) it is possible to break the separation between the system and the isolated environment in which the Wasm module is executed. The solution adopted by current runtimes leverages WASI Libc [27], a library providing POSIX-compatible APIs built on top of hostcalls.

Currently, every WASI-compliant runtime implements the proposed file system interface with a libpreopen-like layer [21]. Whenever the runtime receives a request to open a file, it first checks whether the path belongs to the authorized list of directories, then it opens the file on behalf of the Wasm program, redirecting the content to the caller. Previous work [7, 16, 18] proved the approach to be error-prone, leaving the system unprotected when a vulnerability was introduced in a hostcall wrapper (Figure 1). Moreover, this approach provides limited flexibility, as it is associated with directory-based granularity instead of file-based. Lastly, in order to audit the policy regulating resource access, one must find the permissions by looking at the code. We claim that there is no practical advantage in having several implementations of the same access control checks for different runtimes. Our idea is to replace the user-space runtime-specific security checks with a single in-kernel implementation that leverages eBPF [26]. There are considerable advantages in doing so: (i) it permits to decouple the implementation of hostcall wrappers and the access control details, minimizing the risk of bugs [3, 17, 25], (ii) it enables the introduction of per-module policies with file-based granularity, and (iii) it fulfills

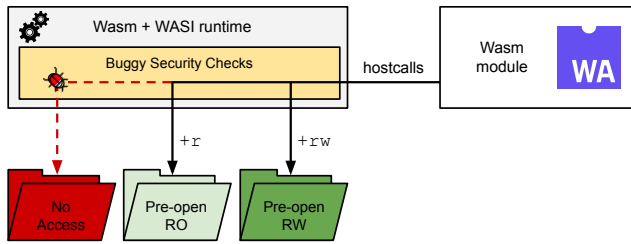


Figure 1: Current implementation of WASI by runtimes. A bug present in a hostcall wrapper permits the module to read the unauthorized directory on the left (red dotted arrow)

Wasm’s promise of portability as eBPF programs are portable across different kernel versions [22] and also operating systems, thanks to Microsoft’s undergoing effort to port eBPF to Windows [20].

2 THREAT MODEL

Our assumptions reflect the threat model employed by Wasm runtimes. We assume that the code executed by the runtime is either untrusted or it is trusted but potentially affected by security vulnerabilities due to bugs. The goal of the attacker providing the code is to bypass the security checks enforced by the runtime to get access to the host file system. To fulfill this objective, the attacker can leverage the interface provided by WASI and send any argument. Runtime escapes caused by memory corruption or alteration of the program flow are out of scope of our work, since protection can be provided by other existing solutions (e.g., [7]).

3 ARCHITECTURE

Our analysis starts from the scenario illustrated in Figure 1. Currently, WASI-compliant runtimes implement dedicated user-space wrappers to enforce the security boundaries of hostcalls. File system access is granted by the user on a set of pre-opened directories that are specified via CLI before the Wasm module is run (e.g., with the `--dir` option). We follow a similar approach, asking the user to state the permissions of each Wasm module in a JSON policy file. Contrary to existing runtimes, permissions can be granted with file-based granularity. Three permissions are available: (i) read to open and read a file, (ii) write to modify, truncate and append content to a file, and (iii) delete to remove the file. When permissions are related to a directory, `read` translates to listing its content, `write` allows to create and delete files within it. We extended the Wasmtime and WasmEdge runtimes to load the policy at startup, and, instead of pre-opening the directories available to the Wasm module, we enforce the policy with eBPF. eBPF code is split into programs attached to a kernel- or user-space function called *hook point* and executed whenever the hook is reached. Programs have visibility of function parameters, they can persist state and share it with user space using *maps*, and most of all they can enforce security checks based on this information. Once the policy is encoded inside the map and the eBPF programs are loaded, the runtime instantiates the Wasm module selected by the user (arrow **A** in Figure 2). At this stage, the modified runtime invokes a dedicated user probe specifying as a parameter the policy that confines the loaded Wasm module (**B**). The argument is captured by a dedicated eBPF program

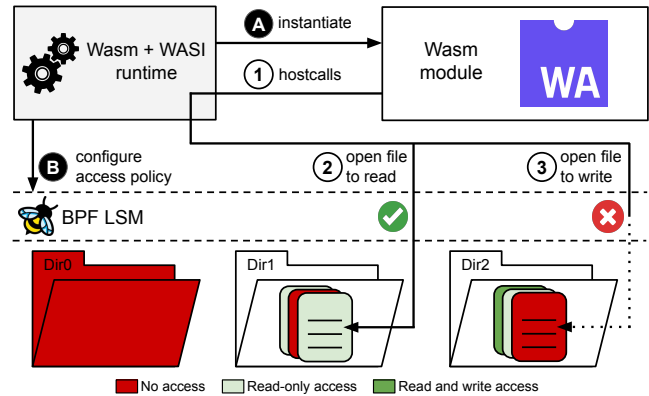


Figure 2: Workflow of our proposal. The runtime instantiates the Wasm module (A**), and configures the associated policy calling the traced user probe (**B**). After the Wasm module is run, all the hostcalls issued by the program (**1**) are restricted by eBPF (**2**, **3**)**

that also annotates the identifier of the thread running the Wasm interpreter in a tracing map. We highlight that the policy is activated before the runtime executes the module (i.e., before untrusted code is interpreted). The consequence is that, from this point on, all the hostcalls performed by the Wasm module are restricted by our eBPF programs (arrows **2**, **3**). The eBPF programs that make the security decisions are evaluated every time a file-related kernel security hook is reached (e.g., `security_file_open`), and any access decision is enforced at kernel level. When an unauthorized request is performed by the Wasm code (**3**), the related eBPF program detects the violation and denies the request, returning to the caller a permission denied error. When the execution of untrusted Wasm code terminates, another eBPF program is responsible for removing the access restriction from the thread executing the Wasm runtime. No further intervention from the runtime is required, as the maps and the eBPF programs are automatically removed from the kernel immediately after the process running the runtime terminates.

This architecture offers several advantages. First, it eliminates the risks coming from buggy user-space security checks (e.g., wrong filepath resolution [19], wrong directory removal [8]). Then, by leveraging kernel hook points [26], our approach allows the runtime developer to focus on the interaction between Wasm code and the memory unsafe system call, leaving aside authorizations and policy-related issues. Lastly, access constraints can be audited by simply looking at the JSON policy, instead of inspecting the code.

4 EXPERIMENTS

To investigate the overhead introduced by our solution we implemented it in WasmEdge and Wasmtime, two industrial state-of-the-art Wasm runtimes. The evaluation has been performed in the following test environment: an Ubuntu 22.04 LTS server powered by an AMD Ryzen 2950X CPU with 16 cores, 128 GB RAM, and 2 TB SSD. In order to assess the performance, we tested one of the most popular binaries that can be compiled to Wasm with support to WASI: `utils coreutils`, the porting of the `coreutils` in Rust [9]. First, we compiled the `coreutils` with the `wasm32-wasi` target, and applied runtime-specific optimization (with `wasmedgec` [2])

Utility	WasmEdge	WasmEdge*	Wasmtime	Wasmtime*
head	32	34 (+6.25%)	14	16 (+14.29%)
sum	134	137 (+2.24%)	130	136 (+4.62%)
tac	149	150 (+0.67%)	152	155 (+1.97%)
wc	285	287 (+0.70%)	309	310 (+0.32%)
shuf	298	300 (+0.67%)	356	358 (+0.56%)
ls	512	526 (+2.73%)	1077	1113 (+3.34%)
seq	1155	1157 (+0.17%)	1526	1533 (+0.46%)
cut	1403	1411 (+0.57%)	359	360 (+0.28%)
join	1601	1603 (+0.12%)	2054	2065 (+0.54%)
split	4416	4694 (+6.30%)	4933	4998 (+1.32%)

Table 1: Average execution time in ms of the coreutils with-out and with* our approach (% overhead in parenthesis)

for WasmEdge and with `wasmtime compile` [1] for Wasmtime) to further speed up the code. Then, we reproduced the benchmarks reported in the coreutils repository, with the exception of those that are not portable to WASI due to temporary lack of support (e.g., the `dd` utility needs to spawn threads, a feature that is yet to be implemented [11]). Finally, we repeated the experiments with our protection in place. The Hyperfine benchmarking tool [10] was used to log measures, and 1000 runs were performed (with 100 warmups). As shown from the results in Table 1, our approach introduces a limited overhead, ranging from an additional 0.12% to 6.30% for WasmEdge, and from 0.28% to 14.29% for Wasmtime. As expected, the highest overhead is experienced by short-living utilities (e.g., `head`). We also observe that there are notable differences between the WasmEdge and Wasmtime test execution time for some utilities (e.g., `ls` and `cut`); from our analysis these differences are mostly caused by the specific post-compilation optimizations.

5 RELATED WORK

There are several successful solutions that leverage Wasm to sandbox untrusted code [14, 23, 24]. RLBox [23] is a framework that facilitates the isolation of third-party libraries in pre-existing software. eWASM [24] optimizes the execution of Wasm in embedded systems with constrained resources. Sledge [14] enables efficient Wasm-based serverless execution on the edge. The use of our approach for restricting access to the file system within these frameworks can strengthen their security assurance.

The memory safety guarantees of Wasm depend on the runtime implementation [18]. Hence, Bosamiya et al. [7] explore the problem of producing probably safe sandboxes. WaVe [16] explains that any interaction with the unsafe interfaces exposed by WASI can introduce security and safety violations. Thus, the authors proposed a verified secure runtime system implementing WASI. However, both works require to redesign the runtime toolchain, while our solution can be directly integrated into existing runtimes.

The academic and industrial communities have investigated the use of eBPF for the isolation of software [4, 5, 12, 13]. *BPFBox* [13] and *BPFContain* [12] use an eBPF daemon to confine processes and services. *Cilium* [4] provides eBPF-based networking, observability and security for container workloads. *Falco* [5] enables lightweight threat detection in the cluster. These solutions highlight the potential of eBPF, and provide a simple and flexible confinement of system

resources. However, they focus on containers or services, while our solution aims at enforcing fine-grained per-sandbox policies.

6 CONCLUSIONS

The results achieved by our approach are promising: not only it permits to introduce fine-grained policies to restrict file system access, it is also associated with a limited overhead which is aligned with the needs of a modern sandbox. The protection is currently applied only to the file system, but our approach has the potential to be extended also to network sockets, which are in the first stage of the standardization process [6]. We believe this could be an interesting line of research for future work.

ACKNOWLEDGMENTS

We thank the reviewers for their valuable comments and feedback. This work was supported by the European Commission in the HE program within the GLACIATION project (No 101070141).

REFERENCES

- [1] 2023. CLI Options - Wasmtime. <https://docs.wasmtime.dev/cli-options.html>
- [2] 2023. wasmedgec AOT Compiler - WasmEdge. <https://wasmedge.org/book/en/cli/wasmedgec.html>
- [3] M. Abbadini, D. Facchinetti, G. Oldani, M. Rossi, and S. Paraboschi. 2023. Cage4Deno: A Fine-Grained Sandbox for Deno Subprocesses. In *ASIACCS*.
- [4] The Cilium Authors. 2023. Cilium. <https://cilium.io>
- [5] The Falco Authors. 2022. Falco. <https://falco.org>
- [6] D. Bakker. 2023. wasi-sockets. <https://github.com/WebAssembly/wasi-sockets>
- [7] J. Bosamiya, W. S. Lim, and B. Parno. 2022. Provably-Safe Multilingual Software Sandboxing using WebAssembly. In *USENIX Security*.
- [8] B. Coenen. 2021. feat(wasi): add rename for a directory + fix remove_dir. <https://github.com/wasmerio/wasmer/commit/e0e12f9d9ff41a512e44bd497324e>
- [9] The coreutils Authors. 2023. uutils coreutils. <https://github.com/uutils/coreutils>
- [10] P. David. 2023. hyperfine. <https://github.com/sharkdp/hyperfine>
- [11] A. Ene, M. Kolny, and A. Brown. 2023. wasi-threads. <https://github.com/WebAssembly/wasi-threads>
- [12] W. Findlay, D. Barrera, and A. Somayaji. 2021. BPFContain: Fixing the Soft Underbelly of Container Security. *arXiv* (2021).
- [13] W. Findlay, A. Somayaji, and D. Barrera. 2020. bpfbox: Simple Precise Process Confinement with eBPF. In *Cloud Computing Security Workshop*.
- [14] P. K. Gadealli, S. McBride, G. Peach, L. Cherkasova, and G. Parmer. 2020. Sledge: A Serverless-First, Light-Weight Wasm Runtime for the Edge. In *International Middleware Conference*.
- [15] A. Haas, A. Rossberg, D. L. Schuff, B. L. Titzer, M. Holman, D. Gohman, L. Wagner, A. Zakai, and JF Bastien. 2017. Bringing the web up to speed with WebAssembly. In *Programming Language Design and Implementation*.
- [16] E. Johnson, E. Laufer, Z. Zhao, D. Gohman, S. Narayan, S. Savage, D. Stefan, and F. Brown. 2022. WaVe: A Verifiably Secure WebAssembly Sandboxing Runtime. In *IEEE Security and Privacy*.
- [17] M. Kehoe. 2022. eBPF: The Next Power Tool of SREs. USENIX Association.
- [18] D. Lehmann, J. Kinder, and M. Pradel. 2020. Everything old is new again: Binary security of webassembly. In *USENIX Security*.
- [19] M. McCaskey. 2019. Prevent parent directory from being opened without being preopened wasi. <https://github.com/wasmerio/wasmer/pull/463>
- [20] Microsoft. 2023. eBPF for Windows. <https://microsoft.github.io/ebpf-for-windows/>
- [21] MUSEC. 2023. libpreopen. <https://github.com/musec/libpreopen>
- [22] A. Nakryiko. 2021. BPF CO-RE. <https://nakryiko.com/posts/bpf-core-reference-guide/>
- [23] S. Narayan, C. Disselkoe, T. Garfinkel, N. Froyd, E. Rahm, S. Lerner, H. Shacham, and D. Stefan. 2020. Retrofitting Fine Grain Isolation in the Firefox Renderer. In *USENIX Security*.
- [24] G. Peach, R. Pan, Z. Wu, G. Parmer, C. Haster, and L. Cherkasova. 2020. eWASM: Practical Software Fault Isolation for Reliable Embedded Devices. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2020).
- [25] M. Rossi, D. Facchinetti, E. Bacis, M. Rosa, and S. Paraboschi. 2021. SEApp: Bringing Mandatory Access Control to Android Apps. In *USENIX Security*.
- [26] The kernel development community. 2023. LSM eBPF Programs. https://docs.kernel.org/bpf/prog_lsm.html
- [27] WebAssembly. 2023. WASI Libc. <https://github.com/WebAssembly/wasi-libc>
- [28] WebAssembly. 2023. The WebAssembly System Interface. <https://wasi.dev>