July 10–14, 2023
Melbourne, Australia

Association for Computing Machinery

Advancing Computing as a Science & Profession

Conference Handbook

ASIA CCS '23

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

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 **Jianying 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

Conference Website

https://asiaccs2023.org

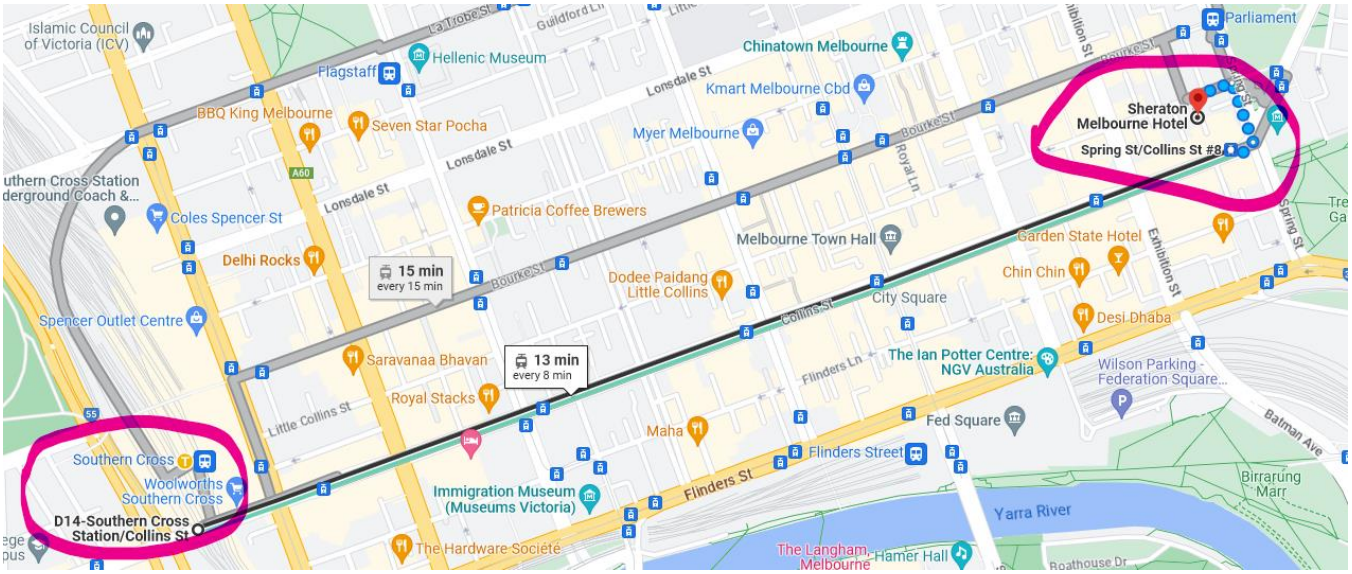
Conference Venue

The 18th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2023) will take place in Sheraton Melbourne Hotel (**Address: 27 Little Collins St, Melbourne VIC 3000**).

Sheraton Melbourne Hotel is located in the heart of Melbourne's CBD. It takes around 20 minutes to drive from Tullamarine Airport to the hotel. The hotel also features convenient public transportation. It is within Melbourne's Free Tram Zone and 300m away from the Parliament Train Station.

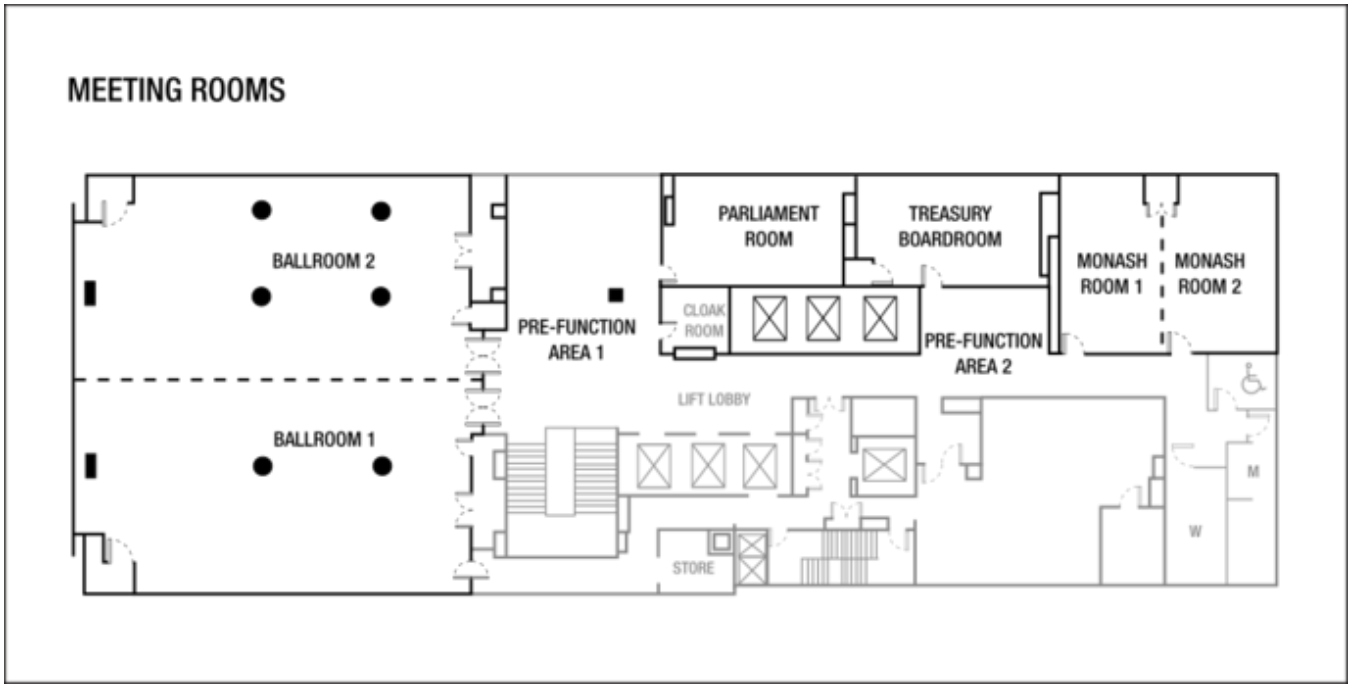
Travel to Venue Site

From the Melbourne Airport, you can catch a taxi or Uber to your hotel / conference venue (Sheraton Melbourne Hotel). Alternatively, you can catch a Skybus which will take you from the Melbourne Airport to Southern Cross Station (in the CBD). Once you depart the Skybus, you can catch a free tram (#11 or #48) at the Southern Cross Station/Collins St to Spring St/Collins St. From there, it is just a few steps walking to Sheraton Melbourne Hotel (See the attached map).



Floor Plan

The conference is held at Level 2 of the hotel. Please refer to the following floor plan for details:



Conference Internet Access

Free Internet access will be provided in the venue. Please turn on Wi-Fi and connect to **MarriottBonvoy** for the free Internet service.

Conference Program

Agenda Overview

Day 0 (Mon) – 10/07

08:30 AM	Registration Open for Workshop
09:00 AM - 05:00 PM	**Workshops** (various location, refer to the **Workshop Schedule** section)
05:30 PM	Registration Open for Conference
06:00 PM - 08:00 PM	Reception for Workshop and Conference (at Ballroom)

Day 1 (Tue) - 11/07

	Ballroom	**Monash Room**
08:30 AM	Registration Open	
09:00 AM - 09:30 AM	Opening	
09:30 AM - 10:30 AM	**Keynote 1: Rethinking IoT Security: Understanding and Mitigating Out-of-Band Vulnerabilities** by Prof. Wenyuan Xu (at **Ballroom**) Session Chair: Joseph Liu (Monash University)	
10:30 AM - 10:55 AM	Morning Tea + Poster	
10:55 AM - 12:10 PM	**Session 1: Applied Cryptography I** *Session Chair: Muhammed Esgin (Monash University)*	**Session 2: Privacy Application** *Session Chair: Hyungjoon (Kevin) Koo (SKKU)*
10:55 AM - 11:20 AM	**Faster TFHE Bootstrapping with Block Binary Keys** *Changmin Lee (Korea Institute For*	**Invasion of location privacy using online map services and smartphone sensors**

	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)	*Hyunsoo Kim (NCSOFT, Republic of Korea), Youngbae Jeon (Samsung Research, Republic of Korea), Ji Won Yoon (Korea University, Republic of Korea)*
11:20 AM - 11:45 AM	**Flag: A Framework for Lightweight Robust Secure Aggregation** *Laasya Bangalore (Georgetown University, USA), Mohammad Hossein Faghihi Sereshgi (University of Rochester, USA), Carmit Hazay (Bar-Ilan University, Israel), Muthuramakrishnan Venkitasubramaniam (Georgetown University, USA)*	**Privacy-Preserving Record Linkage for Cardinality Counting** *Nan Wu (Macquarie University and CSIRO's Data61, Australia), Dinusha Vatsalan (Macquarie University, Australia), Mohamed Ali Kaafar (Macquarie University, Australia), Sanath Kumar Ramesh (Open Treatments Foundations, USA)*
11:45 AM - 12:10 PM	**Implementing and Optimizing Matrix Triples with Homomorphic Encryption** *Johannes Mono (Ruhr University Bochum, Germany), Tim Güneysu (Ruhr University Bochum, Germany)*	**Investigating Users' Understanding of Privacy Policies of Virtual Personal Assistant Applications** *Baiqi Chen (The University of Queensland and CSIRO's Data61, Australia), Tingmin Wu (CSIRO's Data61, Australia), Yanjun Zhang (Deakin University, Australia), Mohan Baruwal Chhetri (CSIRO's Data61, Australia), Guangdong Bai (The University of Queensland, Australia)*
12:10 PM - 01:30 PM	Lunch	
01:30 PM - 03:35 PM	**Session 3: Privacy and Machine Learning** *Session Chair: Yansong Gao (CSIRO's Data61)*	**Session 4: Architecture Security I** *Session Chair: Kasper Rasmussen (University of Oxford)*
01:30 PM - 01:55 PM	**RecUP-FL: Reconciling Utility and Privacy in Federated learning via User-configurable Privacy Defense** *Yue Cui (University of Tennessee, USA), Syed Irfan Ali Meerza (University of Tennessee, USA), Zhuohang Li (University of Tennessee, USA), Luyang Liu (Google Research,*	**Cage4Deno: A Fine-Grained Sandbox for Deno Subprocesses** *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*

	USA), Jiaxin Zhang (Intuit AI Research, USA), Jian Liu (University of Tennessee, USA)	*degli Studi di Bergamo, Italy), Stefano Paraboschi (Università degli Studi di Bergamo, Italy)*
01:55 PM - 02:20 PM	**LDL: A Defense for Label-Based Membership Inference Attacks** *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)*	**CacheFX: A Framework for Evaluating Cache Security** *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)*
02:20 PM - 02:45 PM	**Extracting Privacy-Preserving Subgraphs in Federated Graph Learning using Information Bottleneck** *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)*	**Multi-Tag: A Hardware-Software Co-Design for Memory Safety based on Multi-Granular Memory Tagging** *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)*
02:45 PM - 03:10 PM	**LoDen: Making Every Client in Federated Learning a Defender Against the Poisoning Membership Inference Attacks** *Mengyao Ma (The University of Queensland and CSIRO's Data61, Australia), Yanjun Zhang (University of Technology Sydney, Australia), Pathum Chamikara Mahawaga Arachchige (CSIRO's Data61, Australia), Leo Yu Zhang (Griffith University, Australia), Mohan Baruwal Chhetri (CSIRO's Data61, Australia), Guangdong Bai (The University of Queensland, Australia)*	**FlushTime: Towards Mitigating Flush-based Cache Attacks via Collaborating Flush Instructions and Timers on ARMv8-A** *Jingquan Ge (Southern University of Science and Technology, China), Fengwei Zhang (Southern University of Science and Technology, China)*

03:10 PM - 03:35 PM	**Data Privacy Examination against Semi-Supervised Learning** *Jiadong Lou (University of Louisiana at Lafayette, USA), Xu Yuan (University of Louisiana at Lafayette, USA), Miao Pan (University of Louisiana at Lafayette, USA), Hao Wang (Louisiana State University, USA), Nianfeng Tzeng (University of Louisiana at Lafayette, USA)*	**ShowTime: Amplifying Arbitrary CPU Timing Side Channels** *Antoon Purnal (imec-COSIC, KU Leuven, Belgium), Marton Bognar (imec-DistriNet, KU Leuven, Belgium), Frank Piessens (imec-DistriNet, KU Leuven, Belgium), Ingrid Verbauwhede (imec-COSIC, KU Leuven, Belgium)*
03:35 PM - 04:00 PM	Afternoon Tea + Poster	
04:00 PM - 05:40 PM	**Session 5: Software Security I** *Session Chair: Siqi Ma (UNSW)*	**Session 6: Hardware Security** *Session Chair: Antoon Purnal (KU Leuven)*
04:00 PM - 04:25 PM	**Symbolic Modeling of Remote Attestation Protocols for Device and App Integrity on Android** *Abdulla Aldoseri (University of Birmingham UK, University of Bahrain), Tom Chothia (University of Birmingham, UK), Jose Moreira (Valory AG, Switzerland), David Oswald (University of Birmingham, UK)*	**Secure and Efficient Mobile DNN Using Trusted Execution Environments** *Bin Hu (Rutgers University, USA), Yan Wang (Temple University, USA), Jerry Cheng (New York Institute of Technology, USA), Tianming Zhao (Dayton University, USA), Yucheng Xie (Indiana University-Purdue University Indianapolis, USA), Xiaonan Guo (George Mason University, USA), Yingying Chen (Rutgers University, USA)*
04:25 PM - 04:50 PM	**Arvin: Greybox Fuzzing Using Approximate Dynamic CFG Analysis** *Sirus Shahini (University of Utah, USA), Robert Ricci (University of Utah, USA), Mu Zhang (University of Utah, USA), Mathias Payer (EPFL, Switzerland)*	**Stairway To Rainbow** *Gildas Avoine (INSA, CNRS, IRISA, France), Xavier Carpent (University of Nottingham, UK), Diane Leblanc-Albarel (INSA, CNRS, IRISA, France)*
04:50 PM - 05:15 PM	**AbsIntIO: Towards Showing the Absence of Integer Overflows in Binaries using Abstract Interpretation** *Alexander Küchler (Fraunhofer AISEC, Germany), Leon Wenning (TU Munich,*	**EMShepherd: Detecting Adversarial Samples via Side-channel Leakage** *Ruyi Ding (Northeastern University, USA), Cheng Gongye (Northeastern University, USA), Siyue Wang*

	Germany), Florian Wendland (Fraunhofer AISEC, Germany)	*(Northeastern University, USA), A. Adam Ding (Northeastern University, USA), Yunsi Fei (Northeastern University, USA)*
05:15 PM - 05:40 PM	**Eliminating Vulnerabilities by Disabling Unwanted Functionality in Binary Programs** *Mohamad Mansouri (EURECOM, France), Jun Xu (University of Utah, USA), Georgios Portokalidis (Stevens Institute of Technology, USA)*	**Electromagnetic Signal Injection Attacks on Differential Signaling** *Youqian Zhang (University of Oxford, UK), Kasper Rasmussen (University of Oxford, UK)*

Day 2 (Wed) - 12/07

	Ballroom	**Monash Room**
08:30 AM	Registration Open	
09:00 AM - 10:00 AM	**Keynote 2: Formal Methods for Payment Protocols** by Prof. David Basin (at **Ballroom**) Session Chair: Yang Xiang (Swinburne University of Technology)	
10:00 AM - 11:00 AM	**Keynote 3: Model Stealing Attacks and Defenses: Where are we now?** by Prof. N. Asokan (at **Ballroom**) Session Chair: Surya Nepal (CSIRO's Data61)	
11:00 AM - 11:25 AM	Morning Tea	
11:25 AM - 12:40 PM	**Tutorial 1: Custom Memory Functions Demystified: A tutorial of memory corruptions detection using Goshawk** by Xiang Chen, Siqi Ma	**Tutorial 2: Securing Communications in the Post-quantum Era** by Raymond K. Zhao, Sara Jafarbeiki
12:40 PM - 02:00 PM	Lunch	
02:00 PM - 03:40 PM	**Session 7: Applied Cryptography II** *Session Chair: Shangqi Lai (Monash University)*	**Session 8: Software Security II** *Session Chair: Robert Ricci (University of Utah)*

02:00 PM - 02:25 PM	**On the Cryptographic Fragility of the Telegram Ecosystem** *Theo von Arx (ETH Zurich, Switzerland), Kenneth G. Paterson (ETH Zurich, Switzerland)*	**Benchmarking the Benchmarks** *Marc Miltenberger (Fraunhofer SIT, Germany), Steven Arzt (Fraunhofer SIT, Germany), Philipp Holzinger (Fraunhofer SIT, Germany), Julius Näumann (Fraunhofer SIT, Germany)*
02:25 PM - 02:50 PM	**PSI with computation or Circuit-PSI for Unbalanced Sets from Homomorphic Encryption** *Yongha Son (Samsung SDS, South Korea), Jinhyuck Jeong (Samsung SDS, South Korea)*	**Ember-IO: Effective Firmware Fuzzing with Model-Free Memory Mapped IO** *Guy Farrelly (The University of Adelaide, Australia), Michael Chesser (The University of Adelaide, Australia), Damith C. Ranasinghe (University of Adelaide, Australia)*
02:50 PM - 03:15 PM	**ZEKRA: Zero-Knowledge Control-Flow Attestation** *Heini Bergsson Debes (Technical University of Denmark, Denmark), Edlira Dushku (Aalborg University, Denmark), Thanassis Giannetsos (Ubitech Ltd), Ali Marandi (Technical University of Denmark, Denmark)*	**RaceBench: A Triggerable and Observable Concurrency Bug Benchmark** *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)*
03:15 PM - 03:40 PM	**Overdrive LowGear 2.0: Reduced-Bandwidth MPC without Sacrifice** *Pascal Reisert (University of Stuttgart, Germany), Marc Rivinius (University of Stuttgart, Germany), Toomas Krips (University of Tartu, Estonia), Ralf Kuesters (University of Stuttgart, Germany)*	**BinWrap: Hybrid Protection against Native Node.js Add-ons** *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)*
03:40 PM - 04:05 PM	Afternoon Tea	
04:05 PM - 05:45 PM	**Session 9: Architecture Security II** *Session Chair: William Blair (Boston University)*	**Session 10: User-Centric Security I** *Session Chair: Tina Wu (CSIRO's Data61)*

04:05 PM - 04:30 PM	**Binary Function Clone Search in the Presence of Code Obfuscation and Optimization over Multi-CPU Architectures** *Abdullah Qasem (Concordia University, Canada), Mourad Debbabi (Concordia University, Canada), Bernard Lebel (Thales Research Technologies, , Canada), Marthe Kassouf (Hydro-Québec Research Institute, Canada)*	**Payment with Dispute Resolution: A Protocol for Reimbursing Frauds Victims** *Aydin Abadi (University College London, United Kingdom), Steven J. Murdoch (University College London, United Kingdom)*
04:30 PM - 04:55 PM	**SPEAR-V: Secure and Practical Enclave Architecture for RISC-V** *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)*	**An End-to-End Analysis of Covid-Themed Scams in the Wild** *Behzad Ousat (Florida International University, USA), Mohammad Ali Tofighi (Florida International University, USA), Amin Kharraz (Florida International University, USA)*
04:55 PM - 05:20 PM	**SFITAG: Efficient Software Fault Isolation with Memory Tagging for ARM Kernel Extensions** *Jiwon Seo (Seoul National University, South Korea), Junseung You (Seoul National University, South Korea), Yungi Cho (Seoul National University, South Korea), Yeongpil Cho (Hanyang University, South Korea), Donghyun Kwon (Pusan National University, South Korea), Yunheung Paek (Seoul National University, South Korea)*	**MASCARA: Systematically Generating Memorable And Secure Passphrases** *Avirup Mukherjee (Indian Institute of Technology, Kharagpur, India), Kousshik Murali (Indian Institute of Technology, Kharagpur, India), Shivam Kumar Jha (Indian Institute of Technology, Kharagpur, India), Niloy Ganguly (Indian Institute of Technology, Kharagpur, India), Rahul Chatterjee (University of Wisconsin–Madison, USA), Mainack Mondal (Indian Institute of Technology, Kharagpur, India)*
05:20 PM - 05:45 PM	**An Evaluation Framework for Intrusion Prevention Systems on Serial Data Bus Networks** *Matthew Rogers (MITRE, University of Oxford, USA), Kasper Rasmussen (University of Oxford, UK)*	**How Secure Are The Main Real-World Mix Networks — Case Studies To Explore Vulnerabilities and Usability** *Kun Peng (Huawei Technology Ltd, Australia)*

06:00 PM	Women in Cybersecurity Reception (Venue: Monash Room)

Day 3 (Thu) - 13/07

	Ballroom	Monash Room
09:00 AM - 10:00 AM	**Keynote 4: Democratizing Election Verification: New Methods for Addressing An Ancient Attacker Model** by Prof.Vanessa Teague (at **Ballroom**) Session Chair: Jianying Zhou (Singapore University of Technology and Design)	
10:00 AM - 10:25 AM	Morning Tea	
10:25 AM - 12:30 PM	**Session 11: Machine Learning and Security** *Session Chair: Sanjay Jha (UNSW)*	**Session 12: Applied Cryptography III** *Session Chair: Shabnam Kasra (UNSW)*
10:25 AM - 10:50 AM	**FLAIR: Defense against Model Poisoning Attack in Federated Learning** *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)*	**A New Look at Blockchain Leader Election: Simple, Efficient, Sustainable and Post-Quantum** *Muhammed F. Esgin (Monash University and CSIRO's Data61, Australia), Oguzhan Ersoy (Radboud University and Delft University of Technology, 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)*
10:50 AM - 11:15 AM	**BFU: Bayesian Federated Unlearning with Parameter Self-Sharing** *Weiqi Wang (University of Technology Sydney, Australia), Chenhan Zhang (University of*	**IGA : An Improved Genetic Algorithm to Construct Weightwise (Almost) Perfectly Balanced Boolean Functions with High Weightwise Nonlinearity** *Lili Yan (Tianjin Key Laboratory of*

	Technology Sydney, Australia), An Liu (Soochow University, China), Shui Yu (University of Technology Sydney, Australia)	*Advanced Networking (TANK), Tianjin University, China), Jingyi Cui (School of New Media and Communication, Tianjin University, China), Jian Liu (Tianjin Key Laboratory of Advanced Networking (TANK), Tianjin University, China), Guangquan Xu (Tianjin Key Laboratory of Advanced Networking (TANK), Tianjin University, China), Lidong Han (The Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, China), Alireza Jolfaei (Flinders University, Australia), Xi Zheng (Macquarie University, Australia)*
11:15 AM - 11:40 AM	**SoK: Systematizing Attack Studies in Federated Learning – From Sparseness to Completeness** *Geetanjli 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)*	**FUSE – Flexible File Format and Intermediate Representation for Secure Multi-Party Computation** *Lennart Braun (Aarhus University, Denmark), Moritz Huppert (TU Darmstadt, German), Nora Khayata (TU Darmstadt, German), Thomas Schneider (TU Darmstadt, German), Oleksandr Tkachenko (DFINITY Foundation, Switzerland)*
11:40 AM - 12:05 PM	**Going Haywire: False Friends in Federated Learning and How to Find Them** *William Aiken (University of Ottawa, Canada), Paula Branco (University of Ottawa, Canada), Guy-Vincent Jourdan (University of Ottawa, Canada)*	**A Trade-off SVP-solving Strategy based on a Sharper pnj-BKZ Simulator** *Leizhang Wang (Xidian University, China), Yuntao Wang (Osaka University, Japan), Baocang Wang (Xidian University, China)*
12:05 PM - 12:30 PM	**Deepfake CAPTCHA: A Method for Preventing Fake Calls** *Lior Yasur (Ben-Gurion University, Israel), Guy Frankovits (Ben-Gurion University, Israel), Freddie Grabovski (Ben-Gurion University, Israel), Yisroel Mirsky (Ben-Gurion University, Israel)*	**Communication-Efficient Inner Product Private Join and Compute with Cardinality** *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)
12:30 PM - 10:00 PM	Lunch (Lunch Box) + Social Event + Banquet	

Day 4 (Fri) - 14/07

	Ballroom	**Monash Room**
09:00 AM - 10:15 AM	**Tutorial 3: Recent Advances and Challenges in Membership Inference Attacks on Machine Learning** by Hongsheng Hu, Ruoxi Sun, Shuo Wang, Xuyun Zhang	**Tutorial 4: Symmetric Searchable Encryption: Recent Development and Future Work** by Jianfeng Wang
10:15 AM - 10:40 AM	Morning Tea	
10:40 AM - 12:20 PM	**Session 13: Adversarial Machine Learning** *Session Chair: Saurabh Bagchi (Purdue University)*	**Session 14: Network Security** *Session Chair: Debin Gao (Singapore Management University)*
10:40 AM - 11:05 AM	**Jujutsu: A Two-stage Defense against Adversarial Patch Attacks on Deep Neural Networks** *Zitao Chen (University of British Columbia, , Canada), Pritam Dash (University of British Columbia, Canada), Karthik Pattabiraman (University of British Columbia, Canada)*	**T-TER: Defeating A2 Trojans with Targeted Tamper-Evident Routing** *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)*
11:05 AM - 11:30 AM	**Mitigating Adversarial Attacks by Distributing Different Copies to Different Buyers** *Jiyi Zhang (NUS, Singapore), Han Fang (NUS, Singapore), Wesley Joon-Wie Tann (NUS, Singapore), Ke Xu (Huawei International, Singapore), Chengfang Fang (Huawei Internationa, Singaporel), Ee-Chien Chang (NUS, Singapore)*	**SPARTA: Signal Propagation-based Attack Recognition and Threat Avoidance for Automotive Networks** *Oleg Schell (Robert Bosch GmbH, Germany), Marcel Kneib (Robert Bosch GmbH, Germany)*

11:30 AM - 11:55 AM	**Boost Off/On-Manifold Adversarial Robustness for Deep Learning with Latent Representation Mixup** *Mengdie Huang (Xidian University, China), Yi Xie (Xidian University, China), Xiaofeng Chen (Xidian University, China), Jin Li (Guangzhou University, China), Changyu Dong (Newcastle University, United Kingdom), Zheli Liu (Nankai University, China), Willy Susilo (University of Wollongong, Australia)*	**Investigating Traffic Analysis Attacks on Apple iCloud Private Relay** *Ali Zohaib (UMass Amherst, USA), Jade Sheffey (UMass Amherst, USA), Amir Houmansadr (UMass Amherst, USA)*
11:55 AM - 12:20 PM	**DHBE: Data-free Holistic Backdoor Erasing in Deep Neural Networks via Restricted Adversarial Distillation** *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)*	**A Honey postMessage, but a Heart of Gall: Exploiting Push Service in ServiceWorkers Via postMessage** *Yeomin Jeong (Korea University, South Korea), Woonghee Lee (Korea University, South Korea), Junbeom Hur (Korea University, South Korea)*
12:20 PM - 1:40 PM	Lunch	
01:40 PM - 03:20 PM	**Session 15: Cloud Security** *Session Chair: Aydin Abadi (University College London)*	**Session 16: User-Centric Security II** *Session Chair: Michael V Le (IBM)*
01:40 PM - 02:05 PM	**Secrets Revealed in Container Images: An Internet-wide Study on Occurrence and Impact** *Markus Dahlmanns (RWTH Aachen University, German), Constantin Sander (RWTH Aachen University, German), Robin Decker (RWTH Aachen University, German), Klaus Wehrle (RWTH Aachen University, German)*	**#DM-Me: Susceptibility to Direct Messaging-Based Scams** *Raj Vardhan (Texas A&M University, USA), Alok Chandrawal (Texas A&M University, USA), Phakpoom Chinprutthiwong (Sisaket Rajabhat University, Thailand), Yangyong Zhang (Texas A&M University, USA), Guofei Gu (Texas A&M University, USA)*
02:05 PM - 02:30 PM	**Securing Container-based Clouds with Syscall-aware Scheduling** *Michael V. Le (IBM Research, USA), Salman Ahmed (IBM Research, USA),*	**Do Users Really Know Alexa? Understanding Alexa Skill Security Indicators** *Yangyong Zhang (Texas A&M University, USA), Raj Vardhan (Texas*

	Dan Williams (Virginia Tech, USA), Hani Jamjoom (IBM Research, USA)	*A&M University, USA), Phakpoom Chinprutthiwong (Sisaket Rajabhat University, Thailand), Guofei Gu (Texas A&M University, USA)*
02:30 PM - 02:55 PM	**IOTLB-SC: An Accelerator-Independent Leakage Source in Modern Cloud Systems** *Thore Tiemann (University of Lübeck, Germany), Zane Weissman (Worcester Polytechnic Institute, USA), Thomas Eisenbarth (University of Lübeck, Germany), Berk Sunar (Worcester Polytechnic Institute, USA)*	**Formalising Application-Driven Authentication and Access-Control based on Users' Companion Devices** *Chris Culnane (United Kingdom), Ioana Boureanu (University of Surrey, United Kingdom), Jean Snyman (University of Surrey, United Kingdom), Steve Wesemeyer (University of Surrey, United Kingdom), Helen Treharne (University of Surrey, United Kingdom)*
02:55 PM - 03:20 PM	**Security Properties of Virtual Remotes and SPOOKing their Violations** *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)*	**CryptoShield – Automatic On-Device Mitigation for Crypto API Misuse in Android Applications** *Florian Draschbacher (Graz University of Technology, Austria), Johannes Feichtner (Dynatrace Austria GmbH, Austria)*
03:20 PM - 03:45 PM	Afternoon Tea	
03:45 PM - 05:25 PM	**Session 17: Model Security** *Session Chair: Hung Nguyen (The University of Adelaide)*	**Session 18: Application Security** *Session Chair: Selcuk Uluagac (Florida International University)*
03:45 PM - 04:10 PM	**A Transformer-based Function Symbol Name Inference Model from an Assembly Language for Binary Reversing** *HyunJin Kim (Sungkyunkwan University, South Korea), JinYeong Bak (Sungkyunkwan University, South Korea), Kyunghyun Cho (New York University, USA), Hyungjoon Koo (Sungkyunkwan University, South Korea)*	**ThreadLock: Native Principal Isolation Through Memory Protection Keys** *William Blair (Boston University, USA), William Robertson (Northeastern University, USA), Manuel Egele (Boston University, USA)*

04:10 PM - 04:35 PM	**Masked Language Model Based Textual Adversarial Example Detection** *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, Austraia)*	**Secure Context Switching of Masked Software Implementations** *Barbara Gigerl (Graz University of Technology, Austria), Robert Primas (Graz University of Technology, Austria), Stefan Mangard (Graz University of Technology, Austria)*
04:35 PM - 05:00 PM	**CASSOCK: Viable Backdoor Attacks against DNN in the Wall of Source-Specific Backdoor Defenses** *Shang Wang (Nanjing University of Science and Technology, China), Yansong Gao (Nanjing University of Science and Technology, China), Anmin Fu (Nanjing University of Science and Technology, China), Zhi Zhang (University of Western Australia), Yuqing Zhang (University of Chinese Academy of Sciences, China), Willy Susilo (University of Wollongong, Australia), Dongxi Liu (CSIRO's Data61, Australia)*	**A Scalable Double Oracle Algorithm for Hardening Large Active Directory Systems** *Yumeng Zhang (The University of Adelaide, Australia), Max Ward (The University of Western Australia, Australia), Mingyu Guo (The University of Adelaide, Australia), Hung Nguyen (The University of Adelaide, Australia*
05:00 PM - 05:25 PM	**QUDA: Query-Limited Data-Free Model Extraction** *Zijun Lin (Nanyang Technological University, Singapore), Ke Xu (Huawei International), Chengfang Fang (Huawei International), Huadi Zheng (Huawei Technology), Jaheezuddin Aneez Ahmed (Nanyang Technological University, Singapore), Jie Shi (Huawei International)*	**Uncovering Vulnerabilities of Bluetooth Low Energy IoT from Companion Mobile Apps with Ble-Guuide** *Pallavi Sivakumaran (Royal Holloway, University of London, United Kingdom), Chaoshun Zuo (Ohio State University, USA), Zhiqiang Lin (Ohio State University, USA), Jorge Blasco (Universidad Politécnica de Madrid, Spain)*
05:25 PM - 05:30 PM	Closing	

Workshop Schedule

Overview

02:00 PM – 04:45 PM	**The 10th ACM Asia Public-Key Cryptography Workshop (APKC)** Venue: Treasury
02:00 PM – 04:40 PM	**The 3rd International Symposium on Advanced Security on Software and Systems (ASSS)** Venue: Monash 1
09:00 AM – 05:00 PM	**The 5th ACM International Workshop on Blockchain and Secure Critical Infrastructure (BSCI)** Venue: Parliament
08:50 AM – 01:00 PM	**The 9th ACM Cyber-Physical System Security Workshop (CPSS)** Venue: Monash 1
08:50 AM – 01:25 PM	**The AsiaCCS 2023 Workshop on Secure and Trustworthy Deep Learning Systems (SecTL)** Venue: Treasury
12:50 PM – 05:00 PM	**The 2nd Workshop on the Security Implications of Deepfakes and Cheapfakes (WDC)** Venue: Monash 2

APKC

02:00 PM - 02:05 PM	Welcome
02:05 PM - 02:50 PM	**Keynote: Post-Quantum Zero-Knowledge Proofs and Applications** by Prof. Ron Steinfeld
02:50 PM - 03:05 PM	Coffee Break
03:05 PM - 03:45 PM	**Session 1: Post-Quantum Cryptography**

03:05 PM - 03:25 PM	**SoK: On Efficacy of the BGF Decoder for QC-MDPC-based Quantum-Safe Cryptosystems** *Syed Wajid Ali Shah, Mohammad Nosouhi, Lei Pan and Robin Doss*
03:25 PM - 03:45 PM	**Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste** *Elena Dubrova, Kalle Ngo, Joel Gärtner and Ruize Wang*
03:45 PM - 04:00 PM	Coffee Break
04:00 PM - 04:40 PM	**Session 2: Cryptographic Protocols**
04:00 PM - 04:20 PM	**Designated Verifier Signature with Claimability** *Kyosuke Yamashita, Keisuke Hara, Yohei Watanabe, Naoto Yanai and Junji Shikata*
04:20 PM - 04:40 PM	**Few-helping-card Protocols for Some Wider Class of Symmetric Boolean Functions with Arbitrary Ranges** *Hayato Shikata, Daiki Miyahara and Takaaki Mizuki*
04:40 PM - 04:45 PM	Closing Remarks

ASSS

02:00 PM - 02:10 PM	Welcome
02:10 PM - 03:00 PM	**Keynote: Privacy Compliance in Emerging Applications** by Prof. Guangdong Bai
03:00 PM - 03:15 PM	Coffee Break
03:15 PM - 03:55 PM	**Paper Session I**
03:15 PM - 03:35 PM	**SECBlock-IIoT: A Secure Blockchain-enabled Edge Computing Framework for Industrial Internet of Things** *A. S. M. Sanwar Hosen, Pradip Kumar Sharma, Deepak Puthal, In-Ho Ra and Gi Hwan Cho*

03:35 PM - 03:55 PM	**WinkFuzz: model-based script synthesis for fuzzing** *Zian Liu, Chao Chen, Ejaz Ahmed, Jun Zhang and Dongxi Liu*
04:00 PM - 04:40 PM	**Paper Session II**
04:00 PM - 04:20 PM	**A Blockchain-Based False Data Detection Architecture for the Autonomous Vehicular Systems** *Ziaur Rahman, Xun Yi, Ibrahim Khalil, Adnan Anwar and Shantanu Pal*
04:20 PM - 04:40 PM	**BDFL: A Blockchain-enabled FL Framework for Edge-based Smart UAV Delivery Systems** *Chengzu Dong, Zhiyu Xu, Frank Jiang, Shantanu Pal, Chong Zhang, Shiping Chen and Xiao Liu*

BSCI

09:00 AM - 09:10 AM	Workshop Opening
09:10 AM - 09:50 AM	**Keynote: The Dumbo Protocol Family: Making Asynchronous Consensus Real** by Dr. Qiang Tang *Session Chair: Siqi Ma*
09:50 AM - 10:50 AM	**BSCI Session 1**
09:50 AM - 10:10 AM	**ForTrac: A Secure NFT-based Forward Traceability System for Providing Data Accuracy and Completeness** *Fokke Heikamp (Deakin University, Australia), Lei Pan (Deakin University, Australia), Rolando Trujillo (Universitat Rovira i Virgili, Spain), Sushmita Ruj (UNSW, Australia) and Robin Doss (Deakin University, Australia)*
10:10 AM - 10:30 AM	**Trusted Sharing of Autonomous Vehicle Crash Data using Enterprise Blockchain and IPFS** *Akarsh Singh (Indian Institute of Technology Kharagpur, India), Shounak Sural (Carnegie Mellon University, USA), Tirthankar Sengupta (Indian Institute of Technology Kharagpur, India) and Shamik Sural (Indian Institute of Technology Kharagpur, India)*
10:30 AM - 10:50 AM	**Liquid Democracy in DPoS Blockchains** *Chao Li (Beijing Jiaotong University, China), Runhua Xu (Beihang University, China) and Li Duan (Beijing Jiaotong University, China)*

10:50 AM - 11:05 AM	Coffee Break
11:05 AM - 12:05 PM	**BSCI Session 2**
11:05 AM - 11:25 AM	**Blockchain-empowered Search over Encrypted Data with Forward and Backward Privacy** *Shaolong Tang (Beijing Institute of Technology, China), Jie Liu (Beijing Institute of Technology, China), Xiaoyao Luo (Beijing Institute of Technology, China), Peng Jiang (Beijing Institute of Technology, China), Keke Gai (Beijing Institute of Technology, China), Lei Xu (Beijing Institute of Technology, China) and Liehuang Zhu (Beijing Institute of Technology, China)*
11:25 AM - 11:45 AM	**A Framework for User-Centric Visualisation of Blockchain Transactions in Critical Infrastructure** *Samantha Tharani Jeyakumar (Griffith University, Australia), Ryan Ko (The University of Queensland, Australia) and Vallipuram Muthukkumarasamy (Griffith University, Australia)*
11:45 AM - 12:05 PM	**DCSS: A Smart Contract-based Data Continuous Storage Scheme** *Kun Wang (Beihang University, China), Qianhong Wu (Beihang University, China), Tianxu Han (Beihang University, China), Yujue Wang (Beihang University, China), Yingmiao Zhang (Beijing Jiaotong University, China) and Bo Qin (Renmin University of China, China)*
12:05 PM - 01:00 PM	Lunch
01:00 PM - 02:00 PM	**BSCI Session 3**
01:00 PM - 01:20 PM	**Digital Twins and Blockchain for IoT Management** *Mayra Samaniego (University of Saskatchewan, Canada) and Ralph Deters (University of Saskatchewan, Canada)*
01:20 PM - 01:40 PM	**Avoiding the 1 TB Storage Wall: Leveraging Ethereum's DHT to Reduce Peer Storage Needs** *Jean-Philippe Eisenbarth (University of Luxembourg, France), Thibault Cholez (Universite de Lorraine, France) and Olivier Perrin (Universite de Lorraine, France)*
01:40 PM - 02:00 PM	**Decentralized Translator of Trust: Supporting Heterogeneous TEE for Critical Infrastructure Protection** *Rabimba Karanjai (University of Houston, USA), Rowan Collier (Kent State University, USA), Zhimin Gao (University of Houston, USA), Lin Chen (Texas Tech University, USA), Xinxin Fan (IoTex, USA), Taeweon Suh (Korea University, South*

	Korea), Weidong Shi (University of Houston, USA) and Lei Xu (Kent State University, USA)
02:00 PM - 02:15 PM	Coffee Break
02:15 PM - 03:35 PM	**BSCI Session 4**
02:15 PM - 02:35 PM	**A Blockchain-based Co-Simulation Platform for Transparent and Fair Energy Trading and Management** *Ye Chen (Santa Clara University, USA), Peilin Wu (Shenzhen University, China), Yuanliang Li (Concordia University, USA), Yuhong Liu (Santa Clara University, USA), Peng Zhang (Shenzhen University, China), Jun Yan (Concordia University, USA) and Mohsen Ghafouri (Concordia University, USA)*
02:35 PM - 02:55 PM	**An Analysis of Important Factors Affecting the Success of Blockchain Smart Contract Security Vulnerability Scanning Tools** *Cynthia Yi Min Chee (Deakin University, Australia), Shantanu Pal (Deakin University, Australia), Lei Pan (Deakin University, Australia) and Robin Doss (Deakin University, Australia)*
02:55 PM - 03:15 PM	**Efficient Balancing A* Search for Multi-robot Collaboration With Blockchain Consensus** *Erteng Liu (Zhejiang University, China), Rui Shen (Zhejiang University, China), Tianchi Lu (Zhejiang University, China), Jianhai Chen (Zhejiang University, China) and Butian Huang (Hangzhou Yunphant Network Technology co. LTD, China)*
03:15 PM - 03:35 PM	**An Asynchronous Chain and A Variable Bulk Arrival and Asynchronous Bulk Service Model** *Jongho Seol (Middle Geogia State University, USA) and Nohpill Park (Oklahoma State University, USA)*
03:35 PM - 04:15 PM	**BSCI Short Paper & Poster Session**
03:35 PM - 03:55 PM	**Smart contract symbol execution vulnerability detection method based on CFG path pruning** *Yichuan Wang (Xi'an University of Technology, China), Jingjing Zhao (Xi'an University of Technology, China), Yaling Zhang (Xi'an University of Technology, China), Xinhong Hei (Xi'an University of Technology, China) and Lei Zhu (Xi'an University of Technology, China)*
03:55 PM - 04:15 PM	**Fruits Detections Using Single Shot MultiBox Detector** *Md Ali (Rider University, USA), Chris Keller (Rider University, USA) and Michael Huang (Rider University, USA)*

04:15 PM - 04:20 PM	Closing Remark

CPSS

08:50 AM - 09:00 AM	Opening
09:00 AM - 10:00 AM	**Keynote I: Data security & privacy in IoT MGC Architectures** by Prof. Robert Deng *Session Chair: Jianying Zhou*
10:00 AM - 11:00 AM	**Keynote II: Digital twins: double insecurity for industrial scenarios** by Prof. Cristina Alcaraz *Session Chair: Jianying Zhou*
11:00 AM - 11:15 AM	Coffee Break
11:15 AM - 12:00 AM	**Session I: Intrusion Detection in Cyber-Physical Systems** *Session Chair: Rodrigo Roman*
11:15 AM - 11:30 AM	**PAID: Perturbed Image Attacks Analysis and Intrusion Detection Mechanism for Autonomous Driving Systems** *K. Z. Teng, T. Limbasiya, F. Turrin, Y. L. Aung, S. Chattopadhyay, J. Zhou and M. Conti*
11:30 AM - 11:45 AM	**A Practical Intrusion Detection System Trained on Ambiguously Labeled Data for Enhancing IIoT Security** *W. Yang, Z. Chu, J. Fan, Z. Liu and K. Y. Lam*
11:45 AM - 12:00 PM	**Anomaly Detection Framework for Securing Next Generation Networks of Platoons of Autonomous Vehicles in a Vehicle-to-Everything System** *S. Nazat and M. Abdallah*
12:00 PM - 12:45 PM	**Session II: Cybersecurity in Industrial Control Systems** *Session Chair: Jianying Zhou*
12:00 PM - 12:15 PM	**Blind Concealment from Reconstruction-based Attack Detectors for Industrial Control Systems via Backdoor Attacks** *T. Walita, A. Erba, J. H. Castellanos and N. O. Tippenhauer*

12:15 PM - 12:30 PM	**Preventing Reverse Engineering of Control Programs in Industrial Control Systems** *S. Banerjee, S. D. Galbraith, T. Khan, J. H. Castellanos and G. Russello*
12:30 PM - 12:45 PM	**ICSML: Industrial Control Systems ML Framework for native inference using IEC 61131-3 code** *C. Doumanidis, P. Rajput and M. Maniatakos*
12:45 PM - 01:00 PM	Conclusion

SecTL

08:50 AM - 09:00 AM	Opening
09:00 AM - 10:00 AM	**Keynote I: Attacking Machine Learning Models** by Prof. Yang Zhang *Session Chair: Jason Xue*
10:00 AM - 11:00 AM	**Keynote II: Adversarial Attacks and Defenses in Deep Learning: from a Perspective of Cybersecurity** by Prof. Tianqing Zhu *Session Chair: Shangqi Lai*
11:00 AM - 11:15 AM	Coffee Break
11:15 AM - 11:45 AM	**Session I: Privacy-Preserving Machine Learning** *Session Chair: Xiaoning (Maggie) Liu*
11:15 AM - 11:30 AM	**Privacy-Enhanced Knowledge Transfer with Collaborative Split Learning over Teacher Ensembles** *Ziyao Liu (Nanyang Technological University), Jiale Guo (Nanyang Technological University), Mengmeng Yang (Data61, CSIRO), Wenzhuo Yang (Nanyang Technological University), Jiani Fan (Nanyang Technological University), Kwok-Yan Lam (Nanyang Technological University)*
11:30 AM - 11:45 AM	**Privacy-Preserving Distributed Machine Learning Made Faster** *Zoe L. Jiang (Harbin Institute of Technology, Shenzhen & Peng Cheng Laboratory), Jiajing Gu (Harbin Institute of Technology, Shenzhen), Hongxiao Wang (University of Hong Kong); Yulin Wu (Harbin Institute of Technology, Shenzhen & Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies), Junbin Fang (Jinan University), Siu-Ming Yiu (The University of*

	Hong Kong), Wenjian Luo (Harbin Institute of Technology, Shenzhen & Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies), Xuan Wang (Harbin Institute of Technology, Shenzhen & Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies)
11:45 AM - 12:15 PM	**Session II: Security in On-device Machine Learning** *Session Chair: Ruoxi Sun*
11:45 PM - 12:00 PM	**Beyond the Model: Data Pre-processing Attack to Deep Learning Models in Android Apps** *Ye Sang (Monash University), Yujin Huang (Monash University), Shuo Huang (Monash University), Helei Cui (Northwestern Polytechnical University)*
12:00 PM - 12:15 PM	**Energy-Latency Attacks to On-Device Neural Networks via Sponge Poisoning** *Zijian Wang (Monash University), Shuo Hang (Monash University), Yujin Huang (Monash University), Helei Cui (Northwestern Polytechnical University)*
12:15 PM - 12:45 PM	**Session III: Attacks and Defences** *Session Chair: Tingmin (Tina) Wu*
12:15 PM - 12:30 PM	**Multi-class Detection for Off The Shelf transfer-based Black Box Attacks** *Niklas Bunzel (Fraunhofer SIT/ ATHENE), Dominic Böringer (TU-Darmstadt)*
12:30 PM - 12:45 PM	**Membership Inference Vulnerabilities in Peer to Peer Federated Learning** *Alka Luqman (Nanyang Technological University), Anupam Chattopadhyay (Nanyang Technological University), Kwok-Yan Lam (Nanyang Technological University)*
12:45 PM - 01:15 PM	**Session III: Adversarial Attacks in Physical World** *Session Chair: Huaming Chen*
12:45 PM - 01:00 PM	**Toward Evaluating the Robustness of Deep Learning Based Rain Removal Algorithm in Autonomous Driving** *Yiming Qin (Monash University), Jincheng Hu (Loughborough University), Bang Wu (Monash University)*
01:00 PM -01:15 PM	**A First Look at the Security of EEG-based Systems and Intelligent Algorithms under Physical Signal Injections** *Md Imran Hossen (University of Louisiana at Lafayette), Yazhou Tu (University of Louisiana at Lafayette), Xiali Hei (University of Louisiana at Lafayette)*

01:15 PM - 01:25 PM	Conclusion

WDC

12:50 PM - 01:00 PM	Welcome (Sharif Abuadbba)
01:00 PM - 01:45 PM	**Keynote: Temporal Evolution of Human Perceptions and Detection of Deepfakes: An Empirical Study** by Prof. Ganna Pogrebna *Session Chair: Sharif Abuadbba*
01:45 PM - 02:30 PM	**Full & Short Papers** *Session Chair: Shahroz Tariq*
01:45 PM - 02:00 PM	**On the Application of Synthetic Media to Penetration Testing** *Nathalia Soares, Steven Seiden, Ibrahim Baggili and Andrew Webb*
02:00 PM - 02:15 PM	**Exploiting Inconsistencies in Object Representations for DeepFake Video Detection** *Kishor Kumar Bhaumik and Simon S. Woo*
02:15 PM - 02:30 PM	**Deepfake in the Metaverse: Security Implications for Virtual Gaming, Meetings, and Offices** *Shahroz Tariq, Alsharif Abuadbba and Kristen Moore*
02:30 PM - 02:45 PM	Coffee Break
02:45 PM - 03:45 PM	**Panel Discussion: Security Implications of Deepfakes and Potential Threats** *Panel Members: Kendra Vant (Xero), Asher Flynn (Monash University), Rob Cover (RMIT University), Shahroz Tariq (CSIRO's Data61)* *Moderator: Sharif Abuadbba*
03:45 PM - 04:30 PM	**Poster and Discussion Papers** *Session Chair: Kristen Moore*
03:45 PM - 04:00 PM	**The Threat of Real Time Deepfakes** *Guy Frankovits and Yisroel Mirsky*

04:00 PM - 04:15 PM	**Why Do Facial Deepfake Detectors Fail?** *Binh Le, Shahroz Tariq, Alsharif Abuadbba, Kristen Moore and Simon Woo*
04:15 PM - 04:30 PM	**GAN Discriminator based Audio Deepfake Detection** *Thien Phuc Doan, Kihun Hong and Souhwan Jung*
04:30 PM - 05:00 PM	Closing Remarks (Kristen Moore) and Networking

Access to Proceedings

Please visit here for the proceedings, open access will be offered during the conference time.

Keynote Speakers

Main Conference

Prof. Vanessa Teague

Associate Professor (Adj.), Australian National University; Thinking Cybersecurity Pty. Ltd., and Democracy Developers Ltd, Australia

Vanessa Teague's research focuses primarily on cryptographic methods for achieving security and privacy, particularly for issues of public interest such as election integrity and the protection of government data. She was part of the team (with Chris Culnane and Ben Rubinstein) who discovered the easy re-identification of doctors and patients in the Medicare/PBS open dataset released by the Australian Department of Health. She has co-designed numerous protocols for improved election integrity in e-voting systems, and co-discovered serious weaknesses in the cryptography of deployed e-voting systems in New South Wales, Western Australia and Switzerland. She lives and works on Wurundjeri land in Southeastern Australia (near Melbourne). In 2023 she founded Democracy Developers Ltd, an Australian not-for-profit that builds open-source software for supporting democracy.

Prof. Wenyuan Xu

Professor, Zhejiang University, China

Wenyuan Xu is a Professor in the College of Electrical Engineering at Zhejiang University. She received her Ph.D. in Electrical and Computer Engineering from Rutgers University in 200 7. Prior to joining Zhejiang University in 2013, she was a tenured faculty member in the Department of Computer Science and Engineering at the University of South Carolina in the United States. Her research focuses on embedded systems security, smart systems security, and IoT security. She is a recipient of the National Science Fund for Distinguished Young Scholars of China, the NSF CAREER award, and various best-paper awards including ACM CCS 2017 and ACM AsiaCCS 2018. In addition, she is a program committee co-chair for NDSS 2022-2023 and USENIX Security 2024, and serves as an associate editor for IEEE TMC, ACM TOSN, and TPS.

Prof. David Basin

Professor, ETH Zurich, Switzerland

David Basin is a full professor of Computer Science at ETH Zurich, since 2003. His research areas are Information Security and Software Engineering. He is the founding director of the ZISC, the Zurich Information Security Center, which he led from 2003-2011. He served as Editor-in-Chief of the ACM Transactions on Privacy and Security (2015-2020) and of Springer-Verlag's book series on Information Security and Cryptography (2008-present). He has co-founded three security companies, is on the board of directors of Anapaya Systems AG, and on various management and scientific advisory boards. He is an IEEE Fellow and an ACM Fellow.

Prof. N. Asokan

Professor and David R. Cheriton Chair, The University of Waterloo, Canada

N. Asokan is a professor of computer science and a David R. Cheriton Chair at the University of Waterloo where he also serves as the executive director of the Cybersecurity and Privacy Institute. Asokan is an ACM Fellow and an IEEE Fellow. More information about his work is on his website at https://asokan.org/asokan/.

Workshops

APKC

Prof. Ron Steinfeld

Associate Professor, Monash University, Australia

Ron Steinfeld received his Ph.D. degree in Computer Science in 2003 from Monash University, Australia. Since 2020, he is an Associate Professor at the Department of Software Systems and Cybersecurity, Monash University, Australia.

Following his Ph.D. Ron worked as a postdoctoral research fellow in cryptography and information security at Macquarie University, Australia, holding the positions of Macquarie University Research Fellow in cryptography and information security (2007-2009), and ARC Australian Research Fellow in cryptogra phy and information security (2009-2012). Ron completed his ARC Research Fellowship at Monash University (2012-2014), where he was Senior Lecturer until 2019. His main research interests are in the design and analysis of cryptographic algorithms and protocols, and in particular in the area of quantum-safe cryptography and its applications.

He has over 20 years of research experience in cryptography and information security. He has published more than 80 research papers in international refereed conferences and journals, more than 15 of which have each been cited over 100 times. He received the ASIACRYPT 2015 best paper award. He has served on the technical Program Committee of numerous international conferences in cryptography, is serving as the Program Co-Chair of ASIACRYPT 2023 and is an editorial board member of the journal 'Designs Codes and Cryptography', and has consulted in cryptography design for the software industry.

ASSS

Prof. Guangdong Bai

Associate Professor, The University of Queensland, Australia

Guangdong Bai is an Associate Professor in The University of Queensland, Australia. He obtained his PhD degree from National University of Singapore, and MS and BS degrees from Peking University.

His research areas are Security and Software Engineering. He has served as program/general (co-)chair of international c onferences such as NSS, ICECCS, and ICFEM.

BSCI

Dr. Qiang Tang

Senior Lecturer (equal to U.S. Associate Professor), The University of Sydney, Australia

Dr.Qiang Tang is currently Senior Lecturer (equal to U.S. Associate Professor) at the University of Sydney. From 2016.8 – 2020.12, he was an assistant professor at New Jersey Institute of Technology and director of JD-NJIT-ISCAS Joint Blockchain Research Lab. Before joining NJIT, he was a postdoc at Cornell. His research spans broadly on cryptography, and blockchain technology, and his work appeared mostly in top security/crypto/distributed computing venues such as Crypto, Eurocrypt, CCS, USENIX Sec, NDSS, PODC and others. He won a few prestigious awards including SOAR Prize, MIT Technical Review 35 Chinese Innovators under 35, Google Faculty Award, NJIT Research Award and more. His research is supported by various federal agencies and big tech, as well as leading blockchain foundations including Ethereum, Stellar, Filecoin, Algorand and more.

CPSS

Prof. Robert Deng

AXA Chair Professor of Cybersecurity, Singapore Management University, Singapore

Robert Deng is AXA Chair Professor of Cybersecurity, Director of Secure Mobile Centre, and Deputy Dean for Faculty & Research, School of Computing and Information Systems, Singapore Management University (SMU). His research interests are in the areas of data security and privacy, network security, and applied cryptography. He received the Outstanding University Researcher Award from National University of Singapore, Lee Kuan Yew Fellowship for Research Excellence from SMU, and Asia-Pacific Information Security Leadership Achievements Community Service Star from International Information Systems Security Certification Consortium. He is a Fellow of IEEE and Fellow of Academy of Engineering Singapore.

Prof. Cristina Alacaraz

Associate Professor, University of Malaga, Spain

Cristina Alcaraz is an Associate Professor in the Computer Science Department at UMA. She has been awarded two competitive postdoctoral fellowships: Marie-Curie in 2012 and Ramon-y-Cajal in 2015 and was a guest researcher at NIST (2011-2012), visiting later the Royal Holloway (2012-2014, under the Marie-Curie fellowship), UCBM (2017, Rome) and the University of Piraeus (2019 and 2022, Athens). She is interested in the security of cyber-physical systems, Industry 4.0/5.0, smart grids, IIoT and digital twins, focusing the research on situational awareness, advanced detection and resilience. She has published 75+ papers, is a member of the editorial boards of 8+ international journals in the area (e.g., IEEE Transactions on Industrial Informatics, IEEE Transactions on Dependable and Secure Computing, ACM Distributed Ledger Technologies, IEEE Networking Letters, IJCIP, IJIS, among others), received the Women in Homeland Security Award by the IEEE SMC TC on Homeland Security in 2021 and she is the Vice-Chair of IEEE ComSoc SIG on Green Digital Twin Network.

SecTL

Prof. Yang Zhang

Tenured Faculty (equiv. Professor), CISPA Helmholtz Center for Information Security, Germany

Yang Zhang (https://yangzhangalmo.github.io/) is a tenured faculty (equivalent to full professor) at CISPA Helmholtz Center for Information Security, Germany. His research concentrates on trustworthy machine learning. Moreover, he works on measuring and understanding misinformation and unsafe content like hateful memes on the Internet. Over the years, he has published multiple papers at top venues in computer science, including CCS, NDSS, Oakland, and USENIX Security. His work has received the NDSS 2019 distinguished paper award and the CCS 2022 best paper award runner-up.

Prof. Tianqing Zhu

Associate Professor, The University of Technology Sydney, Australia

Tianqing Zhu holds BEng and MEng degrees from Wuhan University, Wuhan, China in 2000 and 2004, respectively. And a PhD in Computer Science from Deakin University, Australia (2014). She is currently an Associate Professor with the School of Computer Science at the University of Technology Sydney, Australia. She is serving as an Australian Research Council College of Expert from 2021. Prior to that, she was a Lecturer with the School of Information Technology, Deakin University, from 2014 to 2018. Her research interests include privacy-preserving and AI security.

WDC

Prof. Ganna Pogrebna

Executive Director/Professor (Honorary), The Artificial Intelligence and Cyber Futures Institute, Charles Sturt University and The University of Sydney, Australia

Ganna Pogrebna is a pioneer in behavioural data science. She is Executive Director of the Artificial Intelligence and Cyber Futures Institute at Charles Sturt University, Honorary Professor at the University of Sydney, and Lead for Behavioural Data Science at the Alan Turing Institute. Blending behavioural science, AI, computer science, data analytics, engineering, and business model innovation, Ganna helps businesses, cities, charities, and individuals to better understand why they make decisions they make and how they can optimize their behaviour to achieve higher profit, better social outcomes, as well as flourish and bolster their wellbeing. Her recent projects focus on smart technological and social systems, cybersecurity, human-computer and human-data interactions, and business models. Her most impactful projects concentrated on cybersecurity as a behavioural science as well as applications of behavioural data science to media industry . Her digital security risk-tolerance scale (CyberDoSpeRT) is widely used in Australia and abroad. Ganna's contributions to risk analytics and modelling was recognized by the Leverhulme Research Fellowship award. In January 2020, she was also named as the winner of TechWomen100 – the prize awarded to leading female experts in Science, Technology, Engineering and Mathematics in the UK. She is also named as one of 20+ Inspiring Data Scientists by the AI Time Journal. Ganna runs the Data Driven blog on YouTube as well as Inclusion AI blog. Her work is regularly covered by the traditional as well as social media. Ganna is one of the contributors to the Oxford Handbook of AI Ethics. She is also currently co-editing the Cambridge Handbook of Behavioural Data Science, which is due to be published in 2023 by Cambridge University Press.

Social Events

Women in Cybersecurity Reception

Day 2 (Wed) – 12/07, 6:00 PM (at Monash Room)

Overview

The Women in Security Reception is co-located with ACM AsiaCCS and is being sponsored by ACM. The event is chaired by Sushmita Ruj and Siqi Ma. The event will be hosted on 12 July 2023, 6-8 pm. The event consists of a panel and a follow-up networking reception.

The purpose of the panel is to discuss ways to improve the participation of women in security. Since most of our participants are already pursuing a career in security, we will also discuss how they can continue to make valuable and impactful contributions to the community.

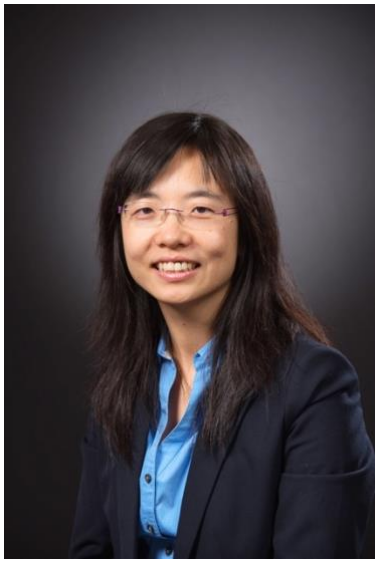
We have got an excellent line of panellists for the event, moderated by Dr. Sushmita Ruj, UNSW, Sydney.

Speaker Info

Vanessa Teague

Associate Professor (Adj.), Australian National University; Thinking Cybersecurity Pty. Ltd., and Democracy Developers Ltd, Australia

Vanessa Teague's research focuses primarily on cryptographic methods for achieving security and privacy, particularly for issues of public interest such as election integrity and the protection of government data. She was part of the team (with Chris Culnane and Ben Rubinstein) who discovered the easy re-identification of doctors and patients in the Medicare/PBS open dataset released by the Australian Department of Health. She has co-designed numerous protocols for improved election integrity in e-voting systems, and co-discovered serious weaknesses in the cryptography of deployed e-voting systems in New South Wales, Western Australia and Switzerland. She lives and works on Wurundjeri land in Southeastern Australia (near Melbourne). In 2023 she founded Democracy Developers Ltd, an Australian not-for-profit that builds open-source software for supporting democracy.



Yuhong Liu

Associate Professor, Department of Computer Science and Engineering, Santa Clara University, U.S.

Yuhong Liu, Associate Professor at the Department of Computer Science and Engineering, Santa Clara University, received her B.S. and M.S. degree from Beijing University of Posts and Telecommunications in 2004 and 2007 respectively, and the Ph.D. degree from University of Rhode Island in 2012. She is the recipient of the 2019 Researcher of the Year Award at School of Engineering, Santa Clara University, and the 2013 University of Rhode Island Graduate School Excellence in Doctoral Research Award. Her research interests include trustworthy computing and cyber security of emerging applications, such as online social media, Internet-of-things and Blockchain. She has published over 90 papers on prestigious journals and peer reviewed conferences. She has contributed as an organizing committee member and/or a TPC member for over 30 conferences. She is actively contributing to professional societies including IEEE and Asia-Pacific Signal and Information Processing Association (APSIPA). She is currently serving as an IEEE Computer Society Distinguished Visitor (2022-2023), the Chair of IEEE Computer Society Special Technical Communities (STC) Executive Committee Board (2022), and the Chair of the IEEE Computer Society Technical Meeting Request Committee. She is also a member of the Multimedia Security and Forensics (MSF) TC for APSIPA, Associate Editor of APSIPA Transactions on Signal and Information Processing, and an APSIPA Distinguished Lecturer (2021-2022).

Cindy He

Industry and Innovation Manager, Institutional Transaction Banking division, ANZ Bank, Australia

Cindy He is an Industry and Innovation Manager in the Institutional Transaction Banking division at ANZ Bank. She leads projects and partnerships related to the application of emerging technologies in global payments, trade and supply chains, with consideration for security and automation. Her recent work has focused on blockchain and AI/ML.

She is also in industry advisory groups and committees where technology, digital transformation and human-centred initiatives intersect. She's currently in an advisory committee to the Attorney General's Department, advising on the use of technologies to improve public policy development and delivery of government services.

Somali Chaterji

Assistant Professor, Purdue University, U.S.

Somali Chaterji (pronounced shoh-MAH-lee CHA-ter-jee) is an Assistant Professor in Ag. and Biological Engineering and in the Elmore Family School of Electrical and Computer Engineering at Purdue University, USA. Dr. Chaterji is also the founder and CEO of KeyByte, a blazing fast cloud computing company established in 2021. Dr. Chaterji leads ICAN, the Innovatory of Cells and Neural Machines, at Purdue University in the little college town of West Lafayette, south of Chicago. She won the NSF (National Science Foundation) CAREER award from the Computing Directorate (Cyber-Physical Program) in January 2022, which focuses on optimizing large convolutional neural networks for computer vision applications on IoT devices, which she calls IoST (Internet of Small Things). Her work has appeared at computer vision, computer systems, and computational genomics venues, such as CVPR, OSDI, and EuroSys, and now in Asia-CCS where she is working to secure decentralized learning that is suitable for IoST. She belives in security by design and security through graceful degradation for safety-critical systems such as for autonomous transportation systems. She encourages early engagement in research and embraces problem-solving with an open mind, tenacity, and fuzzy boundaries between work and life to suit her style. She also recommends cultivating a passion outside the circumference of one's career. This could be the secret elixir to maintaining sanity and stoking one's passion in the long haul. After all, life isn't merely a string of sprints, it's a marathon that tests your grit and perseverance. So, be sure to intersperse your race with unhurried strolls, picturesque detours and thrilling deadline-induced dashes to the finish line.

Moderator

Sushmita Ruj

Faculty of Engineering Lead, the UNSW Institute for Cybersecurity, IfCyber; Senior Lecturer, School of Computer Science and Engineering, UNSW Sydney, Australia

Sushmita Ruj is the Faculty of Engineering Lead at the UNSW Institute for Cybersecurity, IfCyber and Senior Lecturer at the School of Computer Science and Engineering, UNSW, Sydney. Her research interests are in applied cryptography, post quantum cryptography, blockchains and privacy enhancing technologies. She designs practical, efficient, and provably secure protocols that can be deployed in real-world applications.

She has won several competitive grants like Samsung GRO Award, NetApp Faculty Fellowship, Cisco Academic Grant and IBM Research grant. She is an Associate Editor of the Transactions on Information Forensics and Security.

Before joining UNSW, she was a Senior Research Scientist at CSIRO's Data61, an Associate Professor at Indian Statistical Institute and an Assistant Professor at Indian Institute of Technology, IIT, Indore.

Sushmita is a senior member of both ACM and IEEE.

Goldfields Town Tour

Day 3 (Thu) – 13/07, 12:30 PM

We are pleased to announce this year's AsiaCCS will feature a social event at renowned Sovereign Hill.

Sovereign Hill is one of the most premier tourist attractions in Victoria. It is a living museum that showcases the history of Ballarat as a goldfields town during the gold rush era in Victoria.

Banquet (Day 3 – 13/07)

Day 3 (Thu) – 13/07, 12:30 PM

The banquet will be held at RACV Goldfields Resort, which is close to the social event venue.

After exploring the Winter Exclusive event (Winter Wonderlights) at Sovereign Hill, we will arrange the shuttle bus to the banquet site.

Shuttle Bus Info for Attendees

The shuttle bus service between the Sheraton Melbourne Hotel, the social event venue and the RACV Resort will be provided. To participate the social event and banquet, please gather at the pick-up point at 12:30 pm, 13 Jul (Thu).

Acknowledgement

We appreciate all organisation/program committee members and external reviewers for their time and energy that goes into reviewing and preparing this year's ASIACCS conference.

We would also like to acknowledge our external sponsors and supporters for their generous support of the AISACCS'23 Conference. Without the help of our partners, we will not be able to produce such an enriching conference program.

ASIACCS'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:	Hyoungshick 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 Küpçü, Koç University, Turkey
Angelos Stavrou, Virginia Tech, USA
Anna Lisa Ferrara, University of Molise, Italy
Annabelle Mclver, Macquarie University, Australia
Aravind Machiry, Purdue University, USA
Ashish Kundu, Cisco Research, USA
Betül 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, CISPA Helmholtz Center, Germany
Cristina Alacaraz, 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
Hervé Debar, Télécom 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 Kostiainen, 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 Viganò, 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
Vanesa 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
Younghee 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:

Bronze Supporters: