# CCSW '22: The 2022 Cloud Computing Security Workshop

Marten van Dijk
Centrum Wiskunde & Informatica
Marten.van.Dijk@cwi.nl

Francesco Regazzoni
University of Amsterdam and Università della Svizzera italiana,
f.regazzoni@uva.nl; francesco.regazzoni@usi.ch

## ABSTRACT

Clouds and massive-scale computing infrastructures are starting to dominate computing and will likely continue to do so for the foreseeable future. Major cloud operators are now comprising millions of cores hosting substantial fractions of corporate and government IT infrastructure. CCSW is the world's premier forum bringing together researchers and practitioners in all security aspects of cloud-centric and outsourced computing, including:

- Side channel attacks
- Cryptographic protocols for cloud security
- Secure cloud resource virtualization mechanisms
- Secure data management outsourcing (e.g., database as a service)
- Privacy and integrity mechanisms for outsourcing
- Foundations of cloud-centric threat models
- Secure computation outsourcing
- Remote attestation mechanisms in clouds
- Sandboxing and VM-based enforcements
- Trust and policy management in clouds
- Secure identity management mechanisms
- Cloud-aware web service security paradigms and mechanisms
- Cloud-centric regulatory compliance issues and mechanisms
- Business and security risk models and clouds
- Cost and usability models and their interaction with security in clouds
- Scalability of security in global-size clouds
- Binary analysis of software for remote attestation and cloud protection
- Network security (DOS, IDS etc.) mechanisms for cloud contexts
- Security for emerging cloud programming models
- Energy/cost/efficiency of security in clouds
- mOpen hardware for cloud
- Machine learning for cloud protection

CCSW especially encourages novel paradigms and controversial ideas that are not on the above list. The workshop has historically acted as a fertile ground for creative debate and interaction in security-sensitive areas of computing impacted by clouds. This year marked the 13th anniversary of CCSW. In the past decade, CCSW has had a significant impact in our research community.

The complete CCSW'22 workshop proceedings will be available post conference at:
https://dl.acm.org/doi/proceedings/10.1145/3560810

## CCS CONCEPTS

• Computer systems organization~Architectures~Distributed architectures~Cloud computing

• Security and privacy

## KEYWORDS

Cloud computing; security and privacy;

**ACM Reference format:**

Francesco Regazzoni, Marten van Dijk, 2022. CCSW'22: 2022 Cloud Computing Security Workshop**.** In *Proceedings of 2022 Cloud Computing Security Workshop (CCSW'22),* November 7, 2022, Los Angeles, CA, USA, 2 pages. https://doi.org/10.1145/3548606.3563821


ACM ISBN 978-1-4503-9450-5/22/1122/11
https://doi.org/10.1145/3548606.3563821

## 1 Steering Group

The CCSW 2020 Steering Group included:

- Srdjan Capkun, ETH Zurich
- Emiliano De Cristofaro, University College London
- Marten van Dijk, CWI

- Kristin Lauter, Facebook
- Radu Sion, Stony Brook University
- Yinqian Zhang, Ohio State University (chair)

## 2 Programming Committee

We are very grateful to each of our Program Committee members for their great work on a tight timeline. Each submission received at least four reviews. This year's committee included:

- Subhadeep Banik, University of Lugano
- Guoxing Chen, Shanghai Jiao Tong University
- Mayank Varia, Boston University
- Hoda Maleki, Augusta University
- Ulrich Rührmair, LMU Munich and University of Connecticut
- Reihaneh Safavi-Naini, University of Calgary
- Anil Somayaji, Carleton University
- Sean Smith, Dartmouth College
- Dimitrios Papadopoulos, The Hong Kong University of Science and Technology
- Alptekin Küpçü, Koç University
- Joel Coffman, United States Air Force Academy
- Klaus V. Gleissenthall, Vrije Universiteit Amsterdam
- Pierangela Samarati, Universita' degli Studi di Milano
- Fei Chen, Shenzhen University
- Anrin Chakraborti, Duke University
- Giorgos Vasiliadis, Hellenic Mediterranean University and FORTH-ICS
- Chenglu Jin, CWI Amsterdam
- Frank K. Gürkaynak, Microelectronic Design Center, ETH Zürich
- Haibin Zhang, Beijing Institute of Technology
- Ghassan Karame, Ruhr University Bochum
- Meng Yu, Roosevelt University
- Erik-Oliver Blass, Airbus Group Innovations
- Nicolas Alhaddad, Boston University
- Paolo Palmieri, University College Cork
- Sisi Duan, Tsinghua University
- Michael Zohner, HS Fulda
- Bogdan Carbunar, Motorola Labs
- Xiaokuan Zhang, George Mason University
- Nikos Triandopoulos, Stevens Institute of Technology

## 3 Program

Submissions spanned multiple cloud computing security areas, including secure architecture, operating system security, applied cryptography, privacy-preserving of machine learning, and network security. Each paper received at least 4 reviews. The following 5 papers have been accepted for publication after the peer review process:

- A Verifiable Multiparty Computation Solver for the Linear Assignment Problem (And Applications to Air Traffic Management)
- Detecting Anomalous Misconfigurations in AWS Identity and Access Management Policies
- Mitigating Threats Emerging from the Interaction b/w SDN Apps and SDN (Configuration) Datastore
- Contextualizing System Calls in Containers for Anomaly-Based Intrusion Detection
- On Matrix Multiplication with Homomorphic Encryption

In addition, four invited keynotes took place at the workshop. In alphabetical ordering:

- **Roberto Maria Avanzi** (ARM): Cryptographic Protection of Random Access Memory: How Inconspicuous can Hardening Against the most Powerful Adversaries be?
- **Aydin Aysu** (North Carolina State University): Multi-Tenant Cloud FPGAs: Side-Channel Security and Safety
- **Rosario Cammarota** (Intel Lab): Is Revolutionary Hardware and Software for Fully Homomorphic Encryption needed? What else is needed? The lessons learned to date from executing in the DARPA DPRIVE program.
- **Haibin Zhang** (Beijing Institute of Technology): Byzantine Fault Tolerance in the Age of Blockchains and Cloud Computing