Journal of Computer Security 31 (2023) 419–420
DOI 10.3233/JCS-230950
IOS Press

Special issue: 35th IEEE Computer Security Symposium – CSF 2022

Stefano Calzavara [a,*] and David Naumann [b]
[a] *Università Ca' Foscari Venezia, Italy*
[b] *Stevens Institute of Technology, USA*

This special issue of the Journal of Computer Security comprises six papers that are extended versions of works presented at the 35th IEEE Computer Security Symposium (CSF) in August 2022. The conference was held in Haifa, Israel, as part of the Federated Logic Conference (FLoC). Meeting in person was especially welcome following two years in which CSF was held online due to the pandemic.

Based on reviewer recommendations and feedback during the symposium, the authors of six excellent papers were invited to submit extended papers to JCS. The submitted papers were reviewed following the usual process. The selected papers are representative of the scope and focus of CSF on foundational aspects of computer security, such as formal security models, relationships between security properties and defenses, and principled techniques and tools for design and rigorous analysis of security mechanisms.

In "How Efficient Are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis", the authors study a well known class of attacks, connecting a game-based privacy definition to an entropy-based analysis, and showing that replay attacks are a serious threat against several real-world election systems.

In "Machine-Checked Proofs of Privacy Against Malicious Boards for Selene & Co", the authors formalize a new definition of ballot privacy that encompasses a large class of e-voting schemes, and develop machine-checked proofs of privacy for Selene and similar schemes.

The paper "Symbolic Protocol Verification with Dice: Process Equivalences in the Presence of Probabilities" advances the state of the art in formal protocol verification based on the Dolev-Yao model, which enables effective verification tools by abstracting from probabilities that are negligible (like successful guessing of nonces). Addressing the non-negligible probabilities needed in protocols with randomized control flow, the authors investigate the impact on behavioural equivalences in symbolic models.

In "Universal Optimality and Robust Utility Bounds for Metric Differential Privacy", the authors study optimality of privacy/utility trade-offs using principles from Quantitative Information Flow.

In "A Formal Model of Checked C", the authors formalize a dialect of the C language and prove that it enforces spatial memory safety in the sense that violations can always be blamed on unchecked parts of a program.

In "Flow-Limited Authorization for Consensus, Replication, and Secret Sharing", the authors introduce a core calculus for distributed applications with heterogeneous quorum replication protocols, using

*Corresponding author. E-mail: stefano.calzavara@unive.it.

types to ensure confidentiality, integrity, and availability properties. Additionally, they present an extension to the calculus that supports secret sharing as a form of declassification.

We thank the authors for their work and the referees for timely and informative reviews. In fact some of these papers benefitted from CSF's processes for major revisions and previously rejected papers. Thus there were multiple rounds of review and revision prior to the JCS reviews.

Stefano Calzavara (Università Ca' Foscari Venezia) and
David Naumann (Stevens Institute of Technology)

Guest editors, and PC co-chairs of CSF 2022