Shlomi Dolev
Jonathan Katz
Amnon Meisels (Eds.)

LNCS 13301

Cyber Security, Cryptology, and Machine Learning

6th International Symposium, CSCML 2022
Be’er Sheva, Israel, June 30 – July 1, 2022
Proceedings

Springer

Lecture Notes in Computer Science 13301

More information about this series at https://link.springer.com/bookseries/558

Shlomi Dolev · Jonathan Katz ·
Amnon Meisels (Eds.)

Cyber Security, Cryptology, and Machine Learning

6th International Symposium, CSCML 2022
Be’er Sheva, Israel, June 30 – July 1, 2022
Proceedings

Springer

Editors

Shlomi Dolev
Ben-Gurion University of the Negev
Be'er Sheva, Israel

Jonathan Katz
University of Maryland
College Park, MD, USA

Amnon Meisels
Ben-Gurion University of the Negev
Be'er Sheva, Israel

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-07688-6 ISBN 978-3-031-07689-3 (eBook)
https://doi.org/10.1007/978-3-031-07689-3

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

CSCML, the International Symposium on Cyber Security, Cryptography, and Machine Learning, is an international forum for researchers, entrepreneurs, and practitioners in the theory, design, analysis, implementation, or application of cyber security, cryptography, and machine learning systems and networks and, in particular, of conceptually innovative topics in these research areas. Information technology has become crucial to our everyday lives, an indispensable infrastructure of our society, and therefore a target for attacks by malicious parties. Cyber security is one of the most important fields of research these days because of these developments. Two of the (sometimes competing) fields of research, cryptography and machine learning are the most important building blocks of cyber security.

Topics of interest for CSCML include: cyber security design; secure software development methodologies; formal methods, semantics, and verification of secure systems; fault tolerance, reliability, and availability of distributed secure systems; game-theoretic approaches to secure computing; automatic recovery self-stabilizing and self-organizing systems; communication, authentication, and identification security; cyber security for mobile systems and the Internet of Things; cyber security of corporations; security and privacy for cloud, edge, and fog computing; cryptocurrency; blockchain; cryptography; cryptographic implementation analysis and construction; secure multi-party computation; privacy enhancing technologies and anonymity; post-quantum cryptology and security; machine learning and big data; anomaly detection and malware identification; business intelligence and security; digital forensics, digital rights management; trust management and reputation systems; and information retrieval, risk analysis, and DoS.

The 6th CSCML took place during June 30–July 1, 2022, in Beer-Sheva, Israel. The keynote speakers were Michal Braverman-Blumenstyk, Microsoft Corporate Vice President, Cloud and AI Division CTO, and Israel R&D Center General Manager; Dr. Burt Kaliski, Jr., SVP and Chief Technology Officer at Verisign; and Shlomo Dovrat, Co-founder and General Partner at Viola Ventures. The conference was organized in cooperation with the International Association for Cryptologic Research (IACR), and selected papers will appear in a dedicated special issue of the Journal of Computer and System Sciences.

This volume contains 24 contributions selected by the Program Committee from 51 submissions, and also includes 11 short papers. All submitted papers were read and evaluated by members of the Program Committee assisted by external reviewers. We thank the members of the Program Committee for all their hard work.

We are grateful to the EasyChair system that was used for the reviewing process. We also gratefully acknowledge the support of IBM and Ben-Gurion University of the Negev (BGU), in particular BGU-NHSA, the BGU Lynne and William Frankel Center for Computer Science, the BGU Cyber Security Research Center, and the Department of Computer Science.

March 2022

Shlomi Dolev
Jonathan Katz
Amnon Meisels

Organization

CSCML, the International Symposium on Cyber Security, Cryptography, and Machine Learning, is an international forum for researchers, entrepreneurs, and practitioners in the theory, design, analysis, implementation, and application of cyber security, cryptography, or machine-learning systems.

Founding Steering Committee

Orna Berry	Google Cloud, Israel
Shlomi Dolev (Chair)	Ben-Gurion University of the Negev, Israel
Yuval Elovici	Ben-Gurion University of the Negev, Israel
Bezalel Gavish	Southern Methodist University, USA
Ehud Gudes	Ben-Gurion University of the Negev, Israel
Jonathan Katz	University of Maryland, USA
Rafail Ostrovsky	University of California, Los Angeles, USA
Jeffrey D. Ullman	Stanford University, USA
Kalyan Veeramachaneni	MIT, USA
Yaron Wolfsthal	IBM, Israel
Moti Yung	Columbia University and Google, USA

Organizing Committee

General Chair

Shlomi Dolev	Ben-Gurion University of the Negev, Israel

Program Chairs

Jonathan Katz	University of Maryland, USA
Amnon Meisels	Ben-Gurion University of the Negev, Israel

Organizing Chair

Rosemary Franklin	Ben-Gurion University of the Negev, Israel

Program Committee

Gilad Asharov	Bar-Ilan University, Israel
Manuel Barbosa	HASLAB-INESC TEC and FCUP, Portugal
Don Beaver	Meta, Novi Research, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Dor Bitan	University of California, Berkeley, USA
Carlo Blundo	Università degli Studi di Salerno, Italy
Harry Buhrman	CWI, University of Amsterdam, and QuSoft, The Netherlands
Ashish Choudhury	IIIT Bangalore, India
Hadassa Daltrophe	Sami Shamoon College of Engineering, Israel
Stefan Dziembowski	University of Warsaw, Poland
Oren Freifeld	Ben-Gurion University of the Negev, Israel
Felix Freiling	FAU, Germany
Benjamin Fuller	University of Connecticut, USA
Juan A. Garay	Texas A&M University, USA
Craig Gentry	Algorand Foundation, USA
Niv Gilboa	Ben-Gurion University of the Negev, Israel
Ehud Gudes	Ben-Gurion University of the Negev, Israel
Shay Gueron	University of Haifa and Amazon, Israel
David Heath	Georgia Institute of Technology, USA
Gene Itkis	MIT Lincoln Lab and US Military Academy, West Point, USA
Bhavana Kanukurthi	Indian Institute of Science, India
Çetin Kaya Koç	University of California, Santa Barbara, USA
Vladimir Kolesnikov	Georgia Institute of Technology, USA
Benjamin Kreuter	University of Virginia and Google, USA
Ranjit Kumaresan	University of Maryland, USA
Daniel Masny	Meta, USA
Thomas Peyrin	Nanyang Technological University, Singapore
Rami Puzis	Ben-Gurion University of the Negev, Israel
Eyal Ronen	Tel Aviv University, Israel
Alexander Russell	University of Connecticut, USA
Alessandra Scafuro	North Carolina State University, USA
Berry Schoenmakers	Eindhoven University of Technology, The Netherlands
Gil Segev	Hebrew University of Jerusalem, Israel
Qiang Tang	University of Sydney, Australia
Tamir Tassa	The Open University of Israel, Israel
Nikos Triandopoulos	Stevens Institute of Technology, USA
Ni Trieu	Arizona State University, USA
Eran Tromer	Tel Aviv University, Israel

Boaz Tsaban	Bar-Ilan University, Israel
Marten van Dijk	CWI, The Netherlands
Daniele Venturi	Sapienza University of Rome, Italy
Avishai Wool	Tel Aviv University and AlgoSec, Israel
Vassilis Zikas	Purdue University, USA

External Reviewers

Siddharth Agarwal	Indian Institute of Science, India
Sohaib Ahmad	University of Connecticut, USA
Lior Aronshtam	Sami Shamoon College of Engineering, Israel
Alexander Binun	Ben-Gurion University of the Negev, Israel
Benjamin Bond	Purdue University, USA
Anirudh Chandramouli	The International Institute of Information Technology Bangalore, India
Philip Derbeko	enSilo Inc. Fortinet Company, USA
Duong Do	Arizona State University, USA
Nurit Gal-Oz	Sapir Academic College, Israel
Daniel Khankin	NextSilicon, Israel
Manish Kumar	Ben-Gurion University of the Negev, Israel
Thi Kim Phung Lai	New Jersey Institute of Technology, USA
Ximing Li	Jilin University, China
Yin Li	Dongguan University of Technology, China
Matan Liber	Ben-Gurion University of the Negev, Israel
Rahul Madhavan	Indian Institute of Science, India
Truong Son Nguyen	Arizona State University, USA
Kaihua Qin	Imperial College London, UK
Tian Qiu	University of Stuttgart, Germany
Ramakrishnan K.	Indian Institute of Science, India
Girisha Shankar	Indian Institute of Science, India
Tammar Shrot	Sami Shamoon College of Engineering, Israel
David Tolpin	Offtopia and Ben-Gurion University of the Negev, Israel
Nadav Voloch	Ben-Gurion University of the Negev, Israel
Yu Wei	Purdue University, USA
Trevor Yap	Nanyang Technological University, Singapore

Sponsors

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

BGU NHSA

FCCS

IBM

Springer

Lecture Notes in Computer Science
LNCS LNAI LNBI

ELSEVIER

Volume 127 August 2022 ISSN 0022-0000

JOURNAL OF COMPUTER AND SYSTEM SCIENCES

Managing Editor
M. Segal

Editorial Assistant
A. Goldfeld

Editors

J.-Y. Cai	G. Gottlob
A. Chi-Chih Yao	M. Rabin
R. Constable	M. Sharir
D. Dolev	J. Sifakis
R. Fagin	M. Yannakakis
S. Goldwasser	L.A. Zadeh[†]

Available online at www.sciencedirect.com
ScienceDirect

In cooperation with

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH
iacr

Contents