

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

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA


Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Moti Yung 

Columbia University, New York, NY, USA

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

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>

© Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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	IIT 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
 Marten van Dijk
 Daniele Venturi
 Avishai Wool
 Vassilis Zikas

Bar-Ilan University, Israel
 CWI, The Netherlands
 Sapienza University of Rome, Italy
 Tel Aviv University and AlgoSec, Israel
 Purdue University, USA

External Reviewers

Siddharth Agarwal
 Sohaib Ahmad
 Lior Aronshtam
 Alexander Binun
 Benjamin Bond
 Anirudh Chandramouli

Indian Institute of Science, India
 University of Connecticut, USA
 Sami Shamoon College of Engineering, Israel
 Ben-Gurion University of the Negev, Israel
 Purdue University, USA

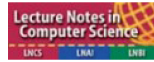
Philip Derbeko
 Duong Do
 Nurit Gal-Oz
 Daniel Khankin
 Manish Kumar
 Thi Kim Phung Lai
 Ximing Li
 Yin Li
 Matan Liber
 Rahul Madhavan
 Truong Son Nguyen
 Kaihua Qin
 Tian Qiu
 Ramakrishnan K.
 Girisha Shankar
 Tammar Shrot
 David Tolpin

The International Institute of Information
 Technology Bangalore, India
 enSilo Inc. Fortinet Company, USA
 Arizona State University, USA
 Sapir Academic College, Israel
 NextSilicon, Israel
 Ben-Gurion University of the Negev, Israel
 New Jersey Institute of Technology, USA
 Jilin University, China
 Dongguan University of Technology, China
 Ben-Gurion University of the Negev, Israel
 Indian Institute of Science, India
 Arizona State University, USA
 Imperial College London, UK
 University of Stuttgart, Germany
 Indian Institute of Science, India
 Indian Institute of Science, India
 Sami Shamoon College of Engineering, Israel
 Offtopia and Ben-Gurion University of the Negev,
 Israel

Nadav Voloch
 Yu Wei
 Trevor Yap

Ben-Gurion University of the Negev, Israel
 Purdue University, USA
 Nanyang Technological University, Singapore

Sponsors



In cooperation with



Contents

Blind Rotation in Fully Homomorphic Encryption with Extended Keys	1
<i>Marc Joye and Pascal Paillier</i>	
Monitoring Time Series with Missing Values: A Deep Probabilistic Approach	19
<i>Oshri Barazani and David Tolpin</i>	
Time, Memory and Accuracy Tradeoffs in Side-Channel Trace Profiling	29
<i>Hen Hayoon and Yossi Oren</i>	
Design of Intrusion Detection System Based on Logical Analysis of Data (LAD) Using Information Gain Ratio	47
<i>Sneha Chauhan and Sugata Gangopadhyay</i>	
Simulating a Coupon Collector	66
<i>Dina Barak-Pelleg and Daniel Berend</i>	
On the Undecidability of the Panopticon Detection Problem	78
<i>Vasiliki Liagkou, Panagiotis E. Nastou, Paul Spirakis, and Yannis C. Stamatiou</i>	
Privacy-Preserving Contrastive Explanations with Local Foil Trees	88
<i>Thijs Veugen, Bart Kamphorst, and Michiel Marcus</i>	
Timing Leakage Analysis of Non-constant-time NTT Implementations with Harvey Butterflies	99
<i>Nir Drucker and Tomer Pelleg</i>	
Predicting the Direction of Changes in the Values of Time Series for Relatively Small Training Samples	118
<i>Sergey Frenkel</i>	
Machine-Learning Based Objective Function Selection for Community Detection	135
<i>Asa Bornstein, Amir Rubin, and Danny Hendler</i>	
Randomness for Randomness Testing	153
<i>Daniel Berend, Shlomi Dolev, and Manish Kumar</i>	

Botnet Attack Identification Based on SDN	162
<i>Avresky Dimiter and Dobrin Dobrev</i>	
Setting Up an Anonymous Gesture Database as Well as Enhancing It with a Verbal Script Simulator for Rehabilitation Applications	170
<i>Yoram Segal and Ofer Hadar</i>	
Fake News Detection in Social Networks Using Machine Learning and Trust	180
<i>Nadav Voloch, Ehud Gudes, Nurit Gal-Oz, Rotem Mitrany, Ofri Shani, and Maayan Shoel</i>	
Reinforcement Based User Scheduling for Cellular Communications	189
<i>Nimrod Gradus, Asaf Cohen, Erez Biton, and Omer Gurwitz</i>	
A Heuristic Framework to Search for Approximate Mutually Unbiased Bases	208
<i>Sreejit Chaudhury, Ajeet Kumar, Subhamoy Maitra, Somjit Roy, and Sourav Sen Gupta</i>	
Counter Mode for Long Messages and a Long Nonce	224
<i>Shay Gueron</i>	
Transfer Learning for Time Series Classification Using Synthetic Data Generation	232
<i>Yarden Rotem, Nathaniel Shimoni, Lior Rokach, and Bracha Shapira</i>	
Non-stopping Junctions via Traffic Scheduling	247
<i>Shlomi Dolev, Ehud Gudes, and Hannah Yair</i>	
Predicting Subscriber Usage: Analyzing Multidimensional Time-Series Using Convolutional Neural Networks	259
<i>Benjamin Azaria and Lee-Ad Gottlieb</i>	
Smart Cybercrime Classification for Digital Forensics with Small Datasets	270
<i>Isfaque Al Kaderi Tuhin, Peter Loh, and Zhengkui Wang</i>	
Auditable, Available and Resilient Private Computation on the Blockchain via MPC	281
<i>Christopher Cordi, Michael P. Frank, Kasimir Gabert, Carollan Helinski, Ryan C. Kao, Vladimir Kolesnikov, Abraham Ladha, and Nicholas Pattengale</i>	

Union Buster: A Cross-Container Covert-Channel Exploiting Union Mounting	300
<i>Novak Boskov, Naor Radami, Trishita Tiwari, and Ari Trachtenberg</i>	
Mutual Accountability Layer: Accountable Anonymity Within Accountable Trust	318
<i>Vanesa Daza, Abida Haque, Alessandra Scafuro, Alexandros Zacharakis, and Arantxa Zapico</i>	
Faster Post-Quantum TLS Handshakes Without Intermediate CA Certificates	337
<i>Panos Kampanakis and Michael Kallitsis</i>	
Enhancing Cybersecurity of Satellites at Sub-THz Bands	356
<i>Rajnish Kumar and Shlomi Arnon</i>	
Polynomial Approximation of Inverse sqrt Function for FHE	366
<i>Samanvaya Panda</i>	
Detecting Clickbait in Online Social Media: You Won't Believe How We Did It	377
<i>Aviad Elyashar, Jorge Bendahan, and Rami Puzis</i>	
Etherless Ethereum Tokens: Simulating Native Tokens in Ethereum	388
<i>John Andrews, Michele Ciampi, and Vassilis Zikas</i>	
A Linear-Time 2-Party Secure Merge Protocol	408
<i>Brett Hemenway Falk, Rohit Nema, and Rafail Ostrovsky</i>	
FairMM: A Fast and Frontrunning-Resistant Crypto Market-Maker	428
<i>Michele Ciampi, Muhammad Ishaq, Malik Magdon-Ismail, Rafail Ostrovsky, and Vassilis Zikas</i>	
In-App Cryptographically-Enforced Selective Access Control for Microsoft Office and Similar Platforms	447
<i>Karim Eldefrawy, Tancrede Lepoint, and Laura Tam</i>	
Differentially-Private "Draw and Discard" Machine Learning: Training Distributed Model from Enormous Crowds	468
<i>Vasyl Pihur, Aleksandra Korolova, Frederick Liu, Subhash Sankuratripati, Moti Yung, Dachuan Huang, and Ruogu Zeng</i>	
Privacy Preserving DCOP Solving by Mediation	487
<i>Pablo Kogan, Tamir Tassa, and Tal Grinshpoun</i>	

BFLUT Bloom Filter for Private Look Up Tables	499
<i>Shlomi Dolev, Ehud Gudes, Erez Segev, Jeffrey Ullman, and Grisha Weintraub</i>	
Author Index	507