Lecture Notes in Computer Science 11527

More information about this series at http://www.springer.com/series/7410

Shlomi Dolev · Danny Hendler ·
Sachin Lodha · Moti Yung (Eds.)

Cyber Security Cryptography and Machine Learning

Third International Symposium, CSCML 2019
Beer-Sheva, Israel, June 27–28, 2019
Proceedings

Springer

Editors
Shlomi Dolev
Ben-Gurion University of the Negev
Beer-Sheva, Israel

Danny Hendler
Ben-Gurion University of the Negev
Beer-Sheva, Israel

Sachin Lodha
Tata Consultancy Services
Mumbai, India

Moti Yung
Columbia University and Google
New York, NY, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-20950-6 ISBN 978-3-030-20951-3 (eBook)
https://doi.org/10.1007/978-3-030-20951-3

LNCS Sublibrary: SL4 – Security and Cryptology

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 today 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, 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 and 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 cryptography 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, DoS.

The Third CSCML took place during June 27–28, 2019, in Beer-Sheva, Israel. This year the conference was organized in cooperation with the International Association for Cryptologic Research (IACR) and selected papers will appear in a dedicated special issue in the journal *Information and Computation*.

This volume contains 18 contributions selected by the Program Committee and ten brief announcements. All submitted papers were read and evaluated by Program Committee members, assisted by external reviewers. We are grateful to the EasyChair system in assisting the reviewing process.

The support of Ben-Gurion University of the Negev (BGU), in particular the BGU-NHSA, BGU Lynne and William Frankel Center for Computer Science, the BGU Cyber Security Research Center, Oracle, ATSMA, the Department of Computer Science, Tata Consultancy Services, IBM and BaseCamp, is also gratefully acknowledged.

March 2019

Danny Hendler
Moti Yung
Shlomi Dolev
Sachin Lodha

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, or application of cyber security, cryptography, and machine learning systems and networks, and, in particular, of conceptually innovative topics in the scope.

Founding Steering Committee

Orna Berry	DELLEMC, Israel
Shlomi Dolev (Chair)	Ben-Gurion University, Israel
Yuval Elovici	Ben-Gurion University, Israel
Bezalel Gavish	Southern Methodist University, USA
Ehud Gudes	Ben-Gurion University, Israel
Jonathan Katz	University of Maryland, USA
Rafail Ostrovsky	UCLA, 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 Chairs

Shlomi Dolev	Ben-Gurion University of the Negev
Sachin Lodha	Tata Consultancy Services

Program Chairs

Danny Hendler	Ben-Gurion University of the Negev
Moti Yung	Columbia University and Google

Organizing Chairs

Timi Budai	Ben-Gurion University of the Negev
Simcha Mahler	Ben-Gurion University of the Negev

Program Committee

Ittai Abraham	VMware., Israel
Adi Akavia	Tel Aviv Yaffo Academic College, Israel
Amir Averbuch	Tel Aviv University, Israel
Silvia Bonomi	Sapienza University of Rome, Italy

Anat Bremler-Barr	IDC Herzliya, Israel
Emilio Coppa	PSapienza University of Rome, Italy
Antonella Del Pozzo	CEA List, France
Itai Dinur	Ben-Gurion University, Israel
Orr Dunkelman	University of Haifa, Israel
Karim El Defrawy	SRI International, USA
Bezalel Gavish	Southern Methodist University, USA
Niv Gilboa	Ben-Gurion University, Israel
Ehud Gudes	Ben-Gurion University, Israel
Shay Gueron	University of Haifa, Israel
Danny Hendler (Co-chair)	Ben-Gurion University, Israel
Stratis Ioannidis	Northeastern University, USA
Gene Itkis	MIT Lincoln Laboratory, USA
Bhavana Kanukurthi	IISc, India
Ben Kreuter	Google, USA
Mark Last	Ben-Gurion University, Israel
Ximing Li	South China Agricultural University, China
Yin Li	Fudan University, China
Avi Mendelson	Technion, Israel
Aikaterini Mitrokosta	Chalmers University of Technology, Sweden
Kobbi Nissim	Georgetown University, USA and Ben-Gurion University, Israel
Yossi Oren	Ben-Gurion University, Israel
Chandrasekaran Pandurangan	IIT Madras, India
Haim Permuter	Ben-Gurion University, Israel
Giuseppe Persiano	Università degli Studi di Salerno, Italy
Benny Pinkas	Bar Ilan University, Israel
Christian Riess	FAU, Germany
Or Sattath	Ben-Gurion University, Israel
Elad M. Schiller	Chalmers University of Technology, Sweden
Galina Schwartz	UC Berkeley, USA
Gil Segev	Hebrew University, Israel
Paul Spirakis	University of Liverpool, UK and University Patras, Greece
Kannan Srinathan	IIIT, India
Uri Stemmer	Ben-Gurion University, Israel
Ari Trachtenberg	Boston University, USA
Philippas Tsigas	Chalmers University of Technology, Sweden
Doug Tygar	UC Berkeley, USA
Kalyan Veeramachaneni	MIT LIDS, USA
Colin Wilmott	Nottingham Trent University, UK
Rebecca Wright	Rutgers University, USA
Moti Yung (Co-chair)	Columbia University and Google, USA

Additional Reviewers

Luigi Catuogno
Eran Lambooij
Calvin Newport
Moshe Shechner
Nadav Voloch
Yu Zhang

Sponsors

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

BGU NHSA

FCCS

CBG
Cyber@Ben-Gurion
University of the Negev

ORACLE®
Data Cloud

ATSMA

IBM®

JVP

Innovation
BaseCamp

ELRON

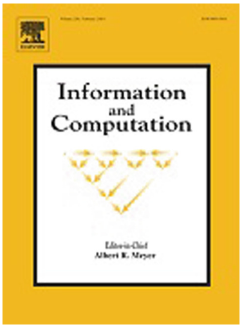
iris capital

Tech7
Negev Innovation

Cyber Week
June 23rd-27th, 2019
Tel Aviv University, Israel

Springer

Lecture Notes in Computer Science
LNCS LNAI LNBI



Information and Computation

Editor-in-Chief
Albert R. Meyer

Contents