Lecture Notes in Computer Science 10332

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

Shlomi Dolev · Sachin Lodha (Eds.)

Cyber Security Cryptography and Machine Learning

First International Conference, CSCML 2017
Beer-Sheva, Israel, June 29–30, 2017
Proceedings

Springer

Editors

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

Sachin Lodha
Tata Consultancy Services (India)
Pune, Maharashtra
India

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-60079-6 ISBN 978-3-319-60080-2 (eBook)
DOI 10.1007/978-3-319-60080-2

Library of Congress Control Number: 2017943048

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing 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 this area. Information technology has become crucial to our everyday life in indispensable infrastructures of our society and therefore is also a target of attacks by malicious parties. Cyber security is one of the most important fields of research today because of these phenomena. The two, sometimes competing, fields of research, cryptography and machine learning, are the most important building blocks of cyber security, as cryptography hides information by avoiding the possibility to extract any useful information pattern while machine learning searches for meaningful information patterns. The subjects covered by the symposium 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; 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 first edition of CSCML took place during June 29–30, 2017, in Beer-Sheva, Israel.

This volume contains 17 contributions selected by the Program Committee and four brief announcements. All submitted papers were read and evaluated by Program Committee members, assisted by external reviewers. We are grateful for the EasyChair system in assisting the reviewing process.

The support of Ben-Gurion University of the Negev (BGU), in particular the BGU Lynne and William Frankel Center for Computer Science, the BGU Cyber Security Research Center, and BGN, also the support of IBM, DELLEMC, JVP, Deutsche Telekom Capital Partners, Glilot, Magma, Pitango, and BaseCamp, is also gratefully acknowledged.

April 2017

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 this field.

Founding Steering Committee

Orna Berry	DELLEMC, Israel
Shlomi Dolev (Chair)	Ben-Gurion University, Israel
Yuval Elovici	Ben-Gurion University, Israel
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 Snapchat, USA

Organizing Committee

Program Chairs

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

Organizing Chair

Timi Budai	Ben-Gurion University of the Negev, Israel

Program Committee

Ran Achituv	Magma Ventures, Israel
Yehuda Afek	Tel-Aviv University, Israel
Adi Akavia	Tel-Aviv Yaffo Academic College, Israel
Amir Averbuch	Tel-Aviv University, Israel
Roberto Baldoni	Università di Roma “La Sapienza”, Italy
Michael Ben-Or	Hebrew University, Israel
Anat Bremler-Barr	IDC Herzliya, Israel
Yves-Alexandre de Montjoye	Imperial College London, UK
Itai Dinur	Ben-Gurion University, Israel
Shlomi Dolev (Co-chair)	Ben-Gurion University, Israel

Karim ElDefrawy	SRI International, USA
Yuval Elovici	Ben-Gurion University, Israel
Felix Freiling	Friedrich-Alexander-Universität, Germany
Ben Gilad	Tata Consultancy Services, Israel
Niv Gilboa	Ben-Gurion University, Israel
Shafi Goldwasser	Weizmann Institute of Science and MIT, USA
Rachel Greenstadt	Drexel University, USA
Ehud Gudes	Ben-Gurion University, Israel
Yaniv Harel	DELLEMC, Israel
Danny Hendler	Ben-Gurion University, Israel
Amir Herzberg	Bar-Ilan University, Israel
Yona Hollander	Fortscale, Israel
Guy Horowitz	Deutsche Telekom Capital Partners, Israel
Stratis Ioannidis	Northeastern University, USA
Yuval Ishai	Technion, Israel
Ayal Itzkovitz	Pitango Venture Capital, Israel
Arik Kleinstein	Glilot Capital Partners, Israel
Vladimir Kolesnikov	Bell Labs, USA
Mark Last	Ben-Gurion University, Israel
Wenke Lee	Georgia Institute of Technology, USA
Sachin Lodha (Co-chair)	Tata Consultancy Services, India
Oded Margalit	IBM, Israel
Aikaterini Mitrokosta	Chalmers University of Technology, Sweden
Kobbi Nissim	Georgetown University, USA
Rita Osadchy	University of Haifa, Israel
Ely Porat	Bar-Ilan University, Israel
Michael Rodeh	Permira and Land & Expand, Israel
Alon Rosen	IDC Herzliya, Israel
Benjamin I.P. Rubinstein	The University of Melbourne, Australia
Galina Schwartz	UC Berkeley, USA
Gil Segev	Hebrew University, Israel
Yossi Shavit	Inno-Negev, Israel
Hans Simon	Ruhr-Universität Bochum, Germany
Doug Tygar	UC Berkeley, USA
Yoav Tzruya	JVP Cyber Labs, Israel
Yael Villa	CISCO, Israel
Michael Waidner	Fraunhofer SIT and TU Darmstadt, Germany
Avishai Wool	Tel-Aviv University, Israel
Moti Yung	Columbia University and Snapchat, USA
Uzy Zwebner	ATP and BaseCamp, Israel

Additional Reviewers

Vijayanand Banahatti	Tata Consultancy Services, India
Silvia Bonomi	Università di Roma “La Sapienza”, Italy
Antonella Del Pozzo	Università di Roma “La Sapienza”, Italy
Manish Shukla	Tata Consultancy Services, India
Ajeet Kumar Singh	Tata Consultancy Services, India

Sponsors

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

FCCS

CBG
Cyber@Ben-Gurion
University of the Negev

BGN Ltd

DELL EMC

BaseCamp
Innovation Center

IBM

JVP

X Organization

T · · CAPITAL PARTNERS

Glilot Capital Partners
Seeds of Intelligence

magma Venture Partners

pitango VENTURE CAPITAL

Contents