

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

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

*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

© Springer International Publishing AG 2017

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, express 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.

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, Gilot, 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 Bremner-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 Kleinstei	Gililot 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  
Silvia Bonomi  
Antonella Del Pozzo  
Manish Shukla  
Ajeet Kumar Singh

Tata Consultancy Services, India  
Università di Roma “La Sapienza”, Italy  
Università di Roma “La Sapienza”, Italy  
Tata Consultancy Services, India  
Tata Consultancy Services, India

## Sponsors







# Contents

Efficient, Reusable Fuzzy Extractors from LWE . . . . .	1
<i>Daniel Apon, Chongwon Cho, Karim Eldefrawy, and Jonathan Katz</i>	
GENFACE: Improving Cyber Security Using Realistic Synthetic Face Generation . . . . .	19
<i>Margarita Osadchy, Yan Wang, Orr Dunkelman, Stuart Gibson, Julio Hernandez-Castro, and Christopher Solomon</i>	
Supervised Detection of Infected Machines Using Anti-virus Induced Labels (Extended Abstract) . . . . .	34
<i>Tomer Cohen, Danny Hendler, and Dennis Potashnik</i>	
Building Regular Registers with Rational Malicious Servers and Anonymous Clients . . . . .	50
<i>Antonella Del Pozzo, Silvia Bonomi, Riccardo Lazzeretti, and Roberto Baldoni</i>	
On the Optimality of the Exponential Mechanism . . . . .	68
<i>Francesco Aldà and Hans Ulrich Simon</i>	
On Pairing Inversion of the Self-bilinear Map on Unknown Order Groups . . . . .	86
<i>Hyang-Sook Lee, Seongan Lim, and Ikkwon Yie</i>	
Brief Announcement: Anonymous Credentials Secure to Ephemeral Leakage . . . . .	96
<i>Lukasz Krzywiecki, Marta Wszola, and Mirosław Kutyłowski</i>	
The Combinatorics of Product Scanning Multiplication and Squaring . . . . .	99
<i>Adam L. Young and Moti Yung</i>	
Stylometric Authorship Attribution of Collaborative Documents . . . . .	115
<i>Edwin Dauber, Rebekah Overdorf, and Rachel Greenstadt</i>	
A Distributed Investment Encryption Scheme: Investcoin . . . . .	136
<i>Filipp Valovich</i>	
Physical Layer Security over Wiretap Channels with Random Parameters . . . . .	155
<i>Ziv Goldfeld, Paul Cuff, and Haim H. Permuter</i>	

Assisting Malware Analysis with Symbolic Execution: A Case Study . . . . .	171
<i>Roberto Baldoni, Emilio Coppa, Daniele Cono D'Elia, and Camil Demetrescu</i>	
Brief Announcement: A Consent Management Solution for Enterprises . . . . .	189
<i>Abigail Goldsteen, Shelly Garion, Sima Nadler, Natalia Razinkov, Yosef Moatti, and Paula Ta-Shma</i>	
Brief Announcement: Privacy Preserving Mining of Distributed Data Using a Trusted and Partitioned Third Party . . . . .	193
<i>Nir Maoz and Ehud Gudes</i>	
Brief Announcement: A Technique for Software Robustness Analysis in Systems Exposed to Transient Faults and Attacks. . . . .	196
<i>Sergey Frenkel and Victor Zakharov</i>	
Symmetric-Key Broadcast Encryption: The Multi-sender Case . . . . .	200
<i>Cody Freitag, Jonathan Katz, and Nathan Klein</i>	
A Supervised Auto-Tuning Approach for a Banking Fraud Detection System . . . . .	215
<i>Michele Carminati, Luca Valentini, and Stefano Zanero</i>	
Scalable Attack Path Finding for Increased Security . . . . .	234
<i>Tom Gonda, Rami Puzis, and Bracha Shapira</i>	
Learning Representations for Log Data in Cybersecurity . . . . .	250
<i>Ignacio Arnaldo, Alfredo Cuesta-Infante, Ankit Arun, Mei Lam, Costas Bassias, and Kalyan Veeramachaneni</i>	
Attack Graph Obfuscation . . . . .	269
<i>Hadar Polad, Rami Puzis, and Bracha Shapira</i>	
Malware Triage Based on Static Features and Public APT Reports . . . . .	288
<i>Giuseppe Laurenza, Leonardo Aniello, Riccardo Lazzaretti, and Roberto Baldoni</i>	
<b>Author Index</b> . . . . .	307