

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board Members

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, Chennai, 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*

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

*Editors*

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

Sachin Lodha  
Tata Consultancy Services  
Mumbai, India

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

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

© Springer Nature Switzerland AG 2019

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 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, AT&T, 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
Bezael 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 Bremner-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

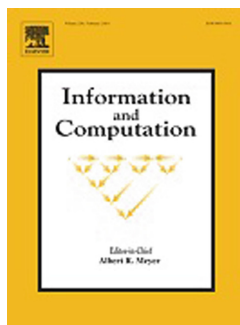
## Additional Reviewers

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

## Sponsors







# Contents

Jamming Strategies in Covert Communication . . . . .	1
<i>Ori Shmuel, Asaf Cohen, and Omer Gurewitz</i>	
Linear Cryptanalysis Reduced Round of Piccolo-80. . . . .	16
<i>Tomer Ashur, Orr Dunkelman, and Nael Masalha</i>	
Continuous Key Agreement with Reduced Bandwidth . . . . .	33
<i>Nir Drucker and Shay Gueron</i>	
Covert Channel Cyber-Attack over Video Stream DCT Payload (Copyright Protection Algorithm for Video and Audio Streams) . . . . .	47
<i>Yoram Segal and Ofer Hadar</i>	
Effects of Weather on Drone to IoT QKD . . . . .	67
<i>Shlomi Arnon and Judy Kupferman</i>	
Malware Classification Using Image Representation . . . . .	75
<i>Ajay Singh, Anand Handa, Nitesh Kumar, and Sandeep Kumar Shukla</i>	
MLDStore: DNNs as Similitude Models for Sharing Big Data (Brief Announcement) . . . . .	93
<i>Philip Derbeko, Shlomi Dolev, and Ehud Gudes</i>	
Cyber Attack Localization in Smart Grids by Graph Modulation (Brief Announcement) . . . . .	97
<i>Elisabeth Drayer and Tirza Routtenberg</i>	
Beyond Replications in Blockchain: On/Off-Blockchain IDA for Storage Efficiency and Confidentiality (Brief Announcement) . . . . .	101
<i>Shlomi Dolev and Yuval Poley</i>	
Self-stabilizing Byzantine Consensus for Blockchain (Brief Announcement) . . . . .	106
<i>Alexander Binun, Shlomi Dolev, and Tal Hadad</i>	
The Advantage of Truncated Permutations . . . . .	111
<i>Shoni Gilboa and Shay Gueron</i>	
Reconstructing C2 Servers for Remote Access Trojans with Symbolic Execution . . . . .	121
<i>Luca Borzacchiello, Emilio Coppa, Daniele Cono D'Elia, and Camil Demetrescu</i>	

Generating a Random String with a Fixed Weight. . . . .	141
<i>Nir Drucker and Shay Gueron</i>	
An Access Control Model for Data Security in Online Social Networks Based on Role and User Credibility. . . . .	156
<i>Nadav Voloch, Priel Levy, Mor Elmakies, and Ehud Gudes</i>	
Enhancing Image Steganalysis with Adversarially Generated Examples . . . . .	169
<i>Kevin Alex Zhang and Kalyan Veeramachaneni</i>	
Controllable Privacy Preserving Blockchain: FiatChain: Distributed Privacy Preserving Cryptocurrency with Law Enforcement Capabilities . . . . .	178
<i>Rami Puzis, Guy Barshap, Polina Zilberman, and Oded Leiba</i>	
A Relay Attack on a Tamper Detection System (Brief Announcement) . . . . .	198
<i>Itai Dinur and Natan Elul</i>	
Amended Cross-Entropy Cost: An Approach for Encouraging Diversity in Classification Ensemble (Brief Announcement) . . . . .	202
<i>Ron Shoham and Haim Permuter</i>	
Governance and Regulations Implications on Machine Learning (Brief Announcement) . . . . .	208
<i>Sima Nadler, Orna Raz, and Marcel Zalmanovici</i>	
Simulating Homomorphic Evaluation of Deep Learning Predictions. . . . .	212
<i>Christina Boura, Nicolas Gama, Mariya Georgieva, and Dimitar Jetchev</i>	
Everything Is in the Name – A URL Based Approach for Phishing Detection . . . . .	231
<i>Harshal Tupsamudre, Ajeet Kumar Singh, and Sachin Lodha</i>	
Network Cloudification (Extended Abstract) . . . . .	249
<i>Yefim Dinitz, Shlomi Dolev, Sergey Frenkel, Alex Binun, and Daniel Khankin</i>	
New Goal Recognition Algorithms Using Attack Graphs . . . . .	260
<i>Reuth Mirsky, Ya'ar Shalom, Ahmad Majadly, Kobi Gal, Rami Puzis, and Ariel Felner</i>	
PeerClear: Peer-to-Peer Bot-net Detection. . . . .	279
<i>Amit Kumar, Nitesh Kumar, Anand Handa, and Sandeep Kumar Shukla</i>	
Rethinking Identification Protocols from the Point of View of the GDPR. . . . .	296
<i>Miroslaw Kutylowski, Łukasz Krzywiecki, and Xiaofeng Chen</i>	

Temporal Pattern-Based Malicious Activity Detection in SCADA Systems  
(Brief Announcement) . . . . . 316  
*Meir Kalech, Amit Shlomo, and Robert Moskovich*

Anonymous Deniable Identification in Ephemeral Setup  
and Leakage Scenarios (Brief Announcement) . . . . . 320  
*Łukasz Krzywiecki, Mirosław Kutylowski, Jakub Pezda,  
and Marcin Słowik*

Randomized and Set-System Based Collusion Resistant Key Predistribution  
Schemes (Brief Announcement) . . . . . 324  
*Vasiliki Liagkou, Paul Spirakis, and Yannis C. Stamatiou*

**Author Index** . . . . . 329