CSCML 2019

2019INTERNATIONAL SYMPOSIUM ON CYBER SECURITY CRYPTOGRAPHY AND MACHINE LEARNING

JUNE2019 • 27-28 •
BEN-GURION UNIVERSITY ALON BUILDING FOR HI-TECH

PROF. SHLOMI DOLEV
DR. SACHIN LODHA
GENERAL CHAIRS

CSCML 2019

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

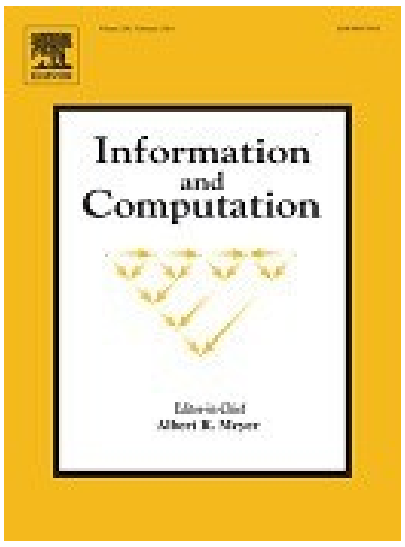
Tech7 Negev Innovation

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

Lecture Notes in Computer Science
LNCS LNAI LNBI

Springer

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH



Wi-Fi: just4visitors

CSCML2019 • June 27

ACADEMIC RESEARCH TRACK • 37/202

CHAIRS PROF. DANNY HENDLER,
PROF. MOTI YUNG

8:30 AM	**GATHERING AND REGISTRATION** **LOCATION:** 2ND FLOOR LOBBY
9:00 AM	**WELCOMING** **LOCATION :**ROOM 202 Prof. Shlomi Dolev
9:15AM	**KEYNOTE INVITED TALK I** **LOCATION:** ROOM 202 How AI is Going to Pull the Table underneath Everything We Know in Cyber Security Prof. Zohar Rozenberg
10:00 AM	**COFFEE BREAK** **LOCATION:** 2ND FLOOR LOBBY
10:30 AM	**ACADEMIC RESEARCH TRACK MORNING SESSION** **LOCATION:** ROOM 202 **MODERATOR:** Prof. Danny Hendler
12:20 AM	**LUNCH BREAK** **LOCATION:** 2ND FLOOR LOBBY
1:00 PM	**ACADEMIC RESEARCH TRACK NOON SESSION** **LOCATION:** ROOM 202 **MODERATOR:** Prof .Ariel Felner
2:45 PM	**COFFEE BREAK** **LOCATION:** 2ND FLOOR LOBBY

Wi-Fi: just4visitors

CSCML2019 • June 27

ACADEMIC RESEARCH TRACK • 37/202

CHAIRS PROF. DANNY HENDLER,
PROF. MOTI YUNG

3:00 PM	**ACADEMIC RESEARCH TRACK AFTERNOON SESSION** **LOCATION:** ROOM 202 **MODERATOR:** Dr. Itai Dinur **CAPTURE THE FLAG MINI-HACKATHON** **LOCATION:** 2ND FLOOR LOBBY **MODERATORS:** Prof. Oded Margalit and Dr. Gera Weiss
4:45 PM	**COFFEE BREAK** **LOCATION:** 2ND FLOOR LOBBY
5:00 PM	**KEYNOTE INVITED TALK II** **LOCATION:** ROOM 202 Cyber Security of Cyber-Physical Systems with Machine Learning Prof. Sandeep Kumar Shukla
5:45 PM	**ENTREPRENEURSHIP PITCH TRACK** **LOCATION:** ROOM 510 Summary of the Track and Naming the Three Best Pitches Finalists **MODERATORS:** Sachin Lodha and Prof. Shlomi Dolev
6:00 PM	**PANEL: From Academia to Entrapanurship and Industry** **LOCATION:** ROOM 202 Ben Gilad, Sandeep Shukla, Snir Hassidim, Itay Katzav **MODERATOR:** Prof .Moti Yung
6:40 PM	**BUSINESS MEETING** **LOCATION:** ROOM 510
7:20 PM	**DINNER** **LOCATION:** 2ND FLOOR LOBBY

Wi-Fi: just4visitors

CSCML2019 • June 27 • 37/202

ACADEMIC RESEARCH TRACK MORNING SESSION

10:30 AM	**JAMMING STRATEGIES IN COVERT COMMUNICATION** Ori Shmuel, Asaf Cohen and Omer Gurewitz
10:45 AM	**LINEAR CRYPTANALYSIS REDUCED ROUND OF PICCOLO-80** Tomer Ashur, Orr Dunkelman and Nael Masalha
11:00 AM	**CONTINUOUS KEY AGREEMENT WITH REDUCED BANDWIDTH** Nir Drucker and Shay Gueron
11:15 AM	**COVERT CHANNEL CYBER-ATTACK OVER VIDEO STREAM DCT PAYLOAD** Yoram Segal and Ofer Hadar
11:30 AM	**HACKING IOT AND THE QUANTUM REVOLUTION** Shlomi Arnon and Judy Kupferman
11:45 AM	**MALWARE CLASSIFICATION USING IMAGE REPRESENTATION** Ajay Singh, Anand Handa, Nitesh Kumar and Sandeep Kumar Shukla
12:00 PM	**MLDSTORE: DEEP NEURAL NETWORKS AS SIMILITUDE MODELS FOR SHARING BIG DATA (BRIEF ANNOUNCEMENT)** Philip Derbeko, Shlomi Dolev and Ehud Gudes
12:05 PM	**CYBER ATTACK LOCALIZATION IN SMART GRIDS BY GRAPH MODULATION (BRIEF ANNOUNCEMENT)** Elisabeth Drayer and Tirza Routtenberg
12:10 PM	**BEYOND REPLICATIONS IN BLOCKCHAIN ON/OFF BLOCKCHAIN INFORMATION DISPERSAL FOR MEMORY EFFICIENCY AND DATA CONFIDENTIALITY (BRIEF ANNOUNCEMENT)** Shlomi Dolev and Yuval Poleg
12:15 PM	**SELF-STABILIZING BYZANTINE CONSENSUS FOR BLOCKCHAIN (BRIEF ANNOUNCEMENT)** Alexander Binun, Shlomi Dolev and Tal Hadad

Wi-Fi: just4visitors

CSCML2019 • June 27 • 37/202

ACADEMIC RESEARCH TRACK NOON SESSION

1:00 PM	**THE ADVANTAGE OF TRUNCATED PERMUTATIONS** Shoni Gilboa and Shay Gueron
1:15 PM	**RECONSTRUCTING C2 SERVERS FOR REMOTE ACCESS TROJANS WITH SYMBOLIC EXECUTION** Luca Borzacchiello, Emilio Coppa, Daniele Cono D'Elia and Camil Demetrescu
1:30 PM	**GENERATING A RANDOM STRING WITH A FIXED WEIGHT** Nir Drucker and Shay Gueron
1:45 PM	**AN ACCESS CONTROL MODEL FOR DATA SECURITY IN ONLINE SOCIAL NETWORKS BASED ON ROLE AND USER CREDIBILITY** Nadav Voloch, Priel Levy, Mor Elmakies and Ehud Gudes
2:00 PM	**ENHANCING IMAGE STEGANALYSIS WITH ADVERSARIALLY GENERATED EXAMPLES** Kevin Zhang and Kalyan Veeramachaneni
2:15 PM	**CONTROLLABLE PRIVACY-PRESERVING BLOCKCHAIN-FIATCHAIN: DISTRIBUTED PRIVACY PRESERVING CRYPTOCURRENCY WITH LAW ENFORCEMENT CAPABILITIES** Rami Puzis, Guy Barshap, Polina Zilberman and Oded Leiba
2:30 PM	**A RELAY ATTACK ON A TAMPER DETECTION SYSTEM (BRIEF ANNOUNCEMENT)** Itai Dinur and Natan Elul
2:35 PM	**AMENDED CROSS-ENTROPY COST: AN APPROACH FOR ENCOURAGING DIVERSITY IN CLASSIFICATION ENSEMBLE (BRIEF ANNOUNCEMENT)** Ron Shoham and Haim Permuter
2:40 PM	**GOVERNANCE AND REGULATIONS IMPLICATIONS ON MACHINE LEARNING(BRIEF ANNOUNCEMENT)** Sima Nadler, Orna Raz and Marcel Zalmanovici

Wi-Fi: just4visitors

CSCML2019 • June 27 • 37/202

ACADEMIC RESEARCH TRACK AFTERNOON SESSION

3:00 PM	**SIMULATING HOMOMORPHIC EVALUATION OF DEEP LEARNING PREDICTIONS** Christina Boura, Nicolas Gama, Mariya Georgieva and Dimitar Jetchev
3:15 PM	**EVERYTHING IS IN THE NAME-A URL BASED APPROACH FOR PHISHING DETECTION** Harshal Tupsamudre, Ajeet Kumar Singh and Sachin Lodha
3:30 PM	**NETWORK CLOUDIFICATION** Yefim Dinitz, Shlomi Dolev, Sergey Frenkel, Alexander Binun and Daniel Khankin
3:45 PM	**NEW GOAL RECOGNITION ALGORITHMS USING ATTACK GRAPHS** Reuth Mirsky, Yaar Shalom, Ahmad Majadly, Kobi Gal, Rami Puzis and Ariel Felner
4:00 PM	**PEERCLEAR: PEER-TO-PEER BOT-NET DETECTION** Amit Kumar, Nitesh Kumar, Anand Handa and Sandeep K. Shukla
4:15 PM	**RETHINKING IDENTIFICATION PROTOCOLS FROM THE POINT OF VIEW OF GDPR** Miroslaw Kutylowski, Lukasz Krzywiecki and Xiaofeng Chen
4:30 PM	**TEMPORAL PATTERN-BASED MALICIOUS ACTIVITY DETECTION IN SCADA SYSTEMS (BRIEF ANNOUNCEMENT)** Meir Kalech, Amit Shlomo and Robert Moskovich
4:35 PM	**ANONYMOUS DENIABLE IDENTIFICATION IN EPHEMERAL SETUP & LEAKAGE SCENARIOS (BRIEF ANNOUNCEMENT)** Łukasz Krzywiecki, Mirosław Kutyłowski, Jakub Pezda and Marcin Slowik
4:40 PM	**RANDOMIZED AND SET-SYSTEM BASED COLLUSION RESISTANT KEY PREDISTRIBUTION SCHEMES(BRIEF ANNOUNCEMENT)** Vasiliki Liagkou, Paul Spirakis and Yannis Stamatiou

Wi-Fi: just4visitors

CSCML2019 • June 27

ENTREPRENEURSHIP PITCH TRACK • 37/510
CHAIR DR. SACHIN LODHA

PH.D. STUDENT RESEARCH TRACK • 37/201
CHAIR PROF. ODED MARGALIT

HACKATHON • 37/LOBBY
MODERATORS PROF. ODED MARGALIT AND DR. GERA WEISS

8:30 AM	**GATHERING AND REGISTRATION** **LOCATION:** 2ND FLOOR LOBBY
9:00 AM	**WELCOMING** **LOCATION:** ROOM 202 Prof. Shlomi Dolev
9:15 AM	**KEYNOTE INVITED TALK I** **LOCATION:** ROOM 202 How AI is Going to Pull the Table underneath Everything We Know in Cyber Security Prof. Zohar Rozenberg
10:00 AM	**COFFEE BREAK** **LOCATION:** 2ND FLOOR LOBBY
10:30 AM	**PH.D. STUDENT RESEARCH TRACK MORNING SESSION** **LOCATION:** ROOM 201 **CHAIR:** Prof. Oded Margalit
12:20 AM	**LUNCH BREAK** **LOCATION:** 2ND FLOOR LOBBY
1:00 PM	**ENTREPRENEURSHIP PITCH TRACK** **LOCATION:** ROOM 510 **CHAIR:** Ben Gilad **PH.D. STUDENT RESEARCH TRACK NOON SESSION** **LOCATION:** ROOM 201 **CHAIR:** Prof. Oded Margalit
2:45 PM	**COFFEE BREAK** **LOCATION:** 2ND FLOOR LOBBY

Wi-Fi: just4visitors

CSCML2019 • June 27

ENTREPRENEURSHIP PITCH TRACK • 37/510
CHAIR DR. SACHIN LODHA

PH.D. STUDENT RESEARCH TRACK • 37/201
CHAIR PROF. ODED MARGALIT

HACKATHON • 37/LOBBY
MODERATORS PROF. ODED MARGALIT AND DR. GERA WEISS

3:00 PM	**CAPTURE THE FLAG MINI-HACKATHON** **LOCATION:** 2ND FLOOR LOBBY **MODERATORS:** Prof. Oded Margalit and Dr. Gera Weiss
4:45 PM	**COFFEE BREAK** **LOCATION:** 2ND FLOOR LOBBY
5:00 PM	**KEYNOTE INVITED TALK II** **LOCATION:** ROOM 202 Cyber Security of Cyber-Physical Systems with Machine Learning Prof. Sandeep Kumar Shukla
5:45 PM	**ENTREPRENEURSHIP PITCH TRACK** **LOCATION:** ROOM 510 Summary of the Track and Naming the Three Best Pitches Finalists **MODERATORS:** Dr. Sachin Lodha and Prof. Shlomi Dolev
6:00 PM	**PANEL: From Academia to Entrapanurship and Industry** **LOCATION:** ROOM 202 Ben Gilad, Sandeep Shukla, Snir Hassidim, Itay Katzav **MODERATOR:** Prof. Moti Yung
6:40 PM	**BUSINESS MEETING** **LOCATION:** ROOM 510
7:20 PM	**DINNER** **LOCATION:** 2ND FLOOR LOBBY

Wi-Fi: just4visitors

CSCML2019 • June 27 • 37/201

ENTREPRENEURSHIP PITCH TRACK • 37/510

CHAIR DR. SACHIN LODHA

3:00 PM	**Algorithm and IoT nitrate sensor to optimize agriculture yields and protect the environment** Shlomi Arnon
3:10 PM	**SocPro: Social Protector for Online Social Networks** Nadav Voloch
3:20 PM	**Cryptopus: Crypto currency monitoring application** Nadav Voloch
3:30 PM	**Computational Nano-robots as *In-Vivo* Medicine.** Ram Prasadh Narayanan
3:40 PM	**AdaptiveClimb – Adaptive Policy for Cache Replacement** Marina Sadesky
3:50 PM	**Exploiting compressed video domain redundancy for cyber protection and compression efficiency (casting covert channel in compressed video)** Yoram Segal/Ofer Hadar
4:00 PM	**Secret Computing: Privacy Preserving Machine Learning and Analytics** Nicolas Gama, Inpher and Mariya Georgieva, Inpher
4:10 PM	**Managing an Operating Theatre as a Multi-Agent System** Amnon Miseles
4:20 PM	**Stick ‘n Grip: A revolutionary robot gripper for the e-commerce industry** Amir Shapiro

PH.D. STUDENT RESEARCH TRACK MORNING SESSION

10:30 AM	**Towards in-vivo Energy Harvesting Computational Nanorobots** Shlomi Dolev and Ram Prasadh Narayanan
10:50 AM	**LOCALIZATION OF DATA INJECTION ATTACKS ON DISTRIBUTED M-ESTIMATION** Or Shalom, Amir Leshem and Anna Scaglione
11:10 AM	**A New Family of Trapdoor Functions for Single Database Information-theoretic Private Block Retrieval** Radhakrishna Bhat and N R Sunitha
11:30 AM	**Self-Stabilizing Local Load Balancing** Shlomi Dolev and Manish Kumar
11:50 AM	**Assume, Guarantee or Repair** Hadar Frenkel, Orna Grumberg, Corina Pasareanu and Sarai Sheinvald

PH.D. STUDENT RESEARCH TRACK NOON SESSION

1:00 PM	**Reinforcement Learning Method for Computing the Capacity of Communication Channels with Feedback** Ziv Aharoni, Oron Sabag and Haim Permuter
1:20 PM	**Visual Analytics for Unsupervised Anomaly Detection of Multivariate Sensor Streams** Efrat Vilenski and Jonathan Rosenblatt
1:40 PM	**Sampling for effective DB activity monitoring anomaly detection** Hagit Grushka, Ofer Biller, Bracha Shapira, Lior Rokach and Oded Sofer
2:00 PM	**Information-Theoretically Secure Quantum Gate Computation and Applications** Dor Bitan and Shlomi Dolev
2:20 PM	**A Factored Approach to Contingent Multi-Agent Planning** Shashank shekhar

CSCML2019 • June 28 • 37/LOBBY

FILED SEMINAR MITZPE RAMON AND SDE BOKER

7:50 AM	**GATHERING** **LOCATION:** 37/LOBBY
8:00 AM	**TRANSPORTATION TO MITZPE RAMON**
9:00 AM	**TOUR AT THE MITZPE RAMON CRATER**
10:45 AM	**FIELD SEMINAR KEYNOTE INVITED TALK** Overview of Cybersecurity & Privacy Work in TCS Speakers: Manish Shukla, Arun Jindal, Harshal Tupsamudre and Nitesh Emmadi
11:15 AM	**DISCUSSION** ACADEMIC RESEARCH AND ENTREPRENEURSHIP
11:45 AM	**LUNCH BREAK AT SDE BOKER**
12:15 PM	**JEEP TOUR AT SDE BOKER AND CIN SPRINGS**
2:15 PM	**TRANSPORTATION TO BE'ER SHEVA TRAIN STATION**

Dear Guest, we hope that you enjoyed your time here.

Please return your badge at the end of the conference.

Thank you.