4th International Verification and Security Workshop (IVSW) 2019
Hotel Rodos Palace, Rhodes Island, Greece
Advanced Preliminary Program

Monday July 1, 2019

08:30 – 09:45: FEDFRO Opening Session

08:30 – 08:45: Welcome Message

08:45 – 09:45: FEDFRO 2019 Keynote Talk

The EPI Processor and its Robustness Requirements, Ying-Chih Yang (Atos)

09:45 – 10:00: Break

10:00 – 10:15: IVSW Opening Session

10:15 – 11:00: Session 1: Keynote Talk:

The Role of Machine Learning in Hardware Security, Prof. Yiorgos Makris, University of Texas at Dallas

11:00 – 12:00: Session 2 Intrusion Detection in Embedded Systems: Challenges and emerging solutions

2.1. Distinguished Talk: Issues relating to the practical exploitation of ICMetric security technology
Professor Gareth Howells, University of Kent, UK

2.2. Using Hardware Performance Counters to Detect Control Hijacking Attacks
Miao Yu, Mark Zwolinski and Basel Halak (University of Southampton, UK)

2.3 End-to-end verified constant-time programming, Deian Stephan Univ. of CA-San Diego

12:00- 12:15: Coffee Break

12:15 – 13:15: Special Session 3: Fault Attacks in Cyber-Physical Systems

3.1. A low Cost and Practical Framework for Security Assessment of the Cyber-Physical Systems
Zarha Kazemi, Athanasios Papadimitriou, Ehsan Aerabi, Mosabbah Mushir Ahmed, David Hely and Vincent Beroulle

3.2. Nonlinear Product Codes for Reliability and Security
Batya Karp, Osnat Keren and Ofer Amrani

3.3 Towards Secure and Reliable Cyber-Physical Systems
Francesco Regazzoni

13:15 – 14:30: Lunch

14:30 – 15:30: Joint Session with IOLTS Session 5 – Hardware Security

5.1 On a Concurrent Side Channel and Fault Attack Countermeasure Methodology for modern MCUs,
E.Aerabi (LCIS), A.Papadimitriou (U Grenoble Alpes), D.Hely (LCIS INP GRENOBLE)

5.2 HATE: a HArdware Trojan Emulation Environment for Microprocessor-based Systems,
C.Bolchini, L.Cassano, I.Montalbano, G.Repole, A.Zanetti (Politecnico di Milano), G.Di Natale (TIMA)

5.3 Encrypted Physically Unclonable Function,
E.Vatajelu (TIMA), G.Di Natale (TIMA), B.Halak, M.S.Mispan (U Southampton)

15:30 – 15:45: Break

15:45 – 16:45: Session 4: Distinguished Talks

4.1 Security in printed electronics: challenges and opportunities
Prof. Medi Tahoori -Security, Karlsruhe Institute of Technology

4.2 SMT attack against obfuscated circuits, Prof. Avesta Sasan, George Mason University

16:45 – 17:15: Coffee Break

17:15 – 18:45: Session 5: Panel - Security Concerns of Machine Learning and AI Systems

Organizers: TBD
Moderator: TBD
Panelists: TBD

20:00: Welcome Reception

Tuesday July 2, 2019

08:30 – 09:30: Joint Session with IOLTS Special Session S6 – Hardware Security for Emerging Applications

Organizer: M.Maniatakos (NUYAD),
Moderator: R.Karri (NYU)
S6.1 3D Integration: Another Dimension for Hardware Security, O.Sinanoglu (NYUAD)
S6.2 Reverse Engineering of Flow-Based Microfluidic Biochips, S.Bhattacharjee (NYUAD)
S6.3 JTAG: A Multifaceted Tool for Cyber Security, M.Maniatakos (NYUAD)

09:30 – 09:45: Break

09:45 – 10:45: Joint Session with IOLTS Session 7 – Attacks

7.1 QuSecNets: Quantization-based Defense Mechanism for Securing Deep Neural Network against Adversarial Attacks,
F.Khalid (TU Wien), H.Ali, H.A.Tariq (NUST), M.A.Hanif, S.Rehman (TU Wien), R.Ahmed (NUST), M.Shafique (TU Wien)
7.2 TrISec: Training Data-Unaware Imperceptible Security Attacks on Deep Neural Networks,
F.Khalid, M.A.Hanif, S.Rehman (TU Wien), R.Ahmed (NUST), M.Shafique (TU Wien)
7.3 LED Alert: Supply Chain Threats for Stealthy Data Exfiltration in Industrial Control Systems,
D.Tychalas, A.Keliris, M.Maniatakos (NYU-AD)

10:45 – 11:00: Coffee Break

11:00 – 11:45: Session 6: Keynote Talk:

Prof. Massimo Alioto, National University of Singapore

11:45 – 12:15: Session 7: Distinguished Talk:

Dr. Yervant Zorian, Synopsys

12:15 – 12:30: Break

12:30 – 13:30: Session 8: IC Counterfeits Mitigation Techniques

8.1. Detection of Recycled ICs through On-Chip Leakage Current Sensors
Daniele Rossi (University of Hertfordshire, Hatfield, UK) and Saqib Khursheed (University of Liverpool, Liverpool, UK)
8.2. Two-Stage Architectures for Resilient Lightweight PUFs
Haibo Su, Mark Zwolinski and Basel Halak (University of Southampton, UK))
8.3. On the Reliability of the Ring Oscillator Physically Unclonable Functions
Honorio Martin, Elena-Ioana Vatajelu, Giorgio Di Natale and Osnat Keren

13:30 – 15:00: Lunch

15:00 – 16:00: Session 9: Security of Cyber-Physical Systems

9.1. A Two-Flights Mutual Authentication for Energy-Constrained IoT Devices
Yildiran Yilmaz and Basel Halak (University of Southampton, UK)
9.2. An overview of Platform and Ecosystem Level of Security Threats and their effects on security of the underlying hardware
Kumar Mangipudi. (Intel, United States)
9.3 Title TBD, Fareena Saqib, Univ. of North Carolina

16:30: Social Event & Dinner

Wednesday July 3, 2019

08:30 – 09:30: Special Session 10: A Comprehensive Approach to a Trusted Test Infrastructure

10.1 An Industrial Approach to Secure Testing
Jerome Quevremont, Marc Merandat, Nicolas Valette
10.2 Authenticated Access to Scan Chains
Vincent Reynaud, Paolo Maistri, Regis Leveugle
10.3 Encryption Techniques for Test Infrastructures
Emanuele Valea, Marie-Lise Flottes, Sophie Dupuis, Bruno Rouzeyre, Giorgio Di Natale

09:30 – 10:15: Session 11: Keynote Talk

Prof. Ramesh Kari, New York University

10:15-10:30 coffee break

10:30 – 11:30: Session12: Secure Hardware Design and Test

12.1 Restricting Switching Activity Using Logic Locking to Improve Power Analysis-Based Trojan Detection
Arash Nejat, Zahra Kazemi, Vincent Beroulle, David Hely and Mahdi Fazeli.
12.2 Verification of Physical Chip Layouts Using GDSII Design Data
Aayush Singla, Bernhard Lippmann and Helmut Graeb
12.3 Dynamic Adjustment of Test-Sequence Duration for Increasing the Functional Coverage
Zacharias Takakis, Dimitrios Mangiras, Chrysostomos Nicopoulos and Giorgos Dimitrakopoulos

11:30-11:35 Short Break

11:35 – 12:15: Session 13 Emerging Security Technologies

13.1 Memresistive Devices for Hardware Security Primitives
Nan Du, Mahdi Kiani, Xianyue Zhao, Danilo Bürger, Oliver G. Schmidt, Ramona Ecke, Stefan E. Schulz, Heidemarie Schmidt, Ilia Polian (TU Chemnitz, Fraunhofer ENAS, IPHT, University of Stutgart),
13.2 Spintronic Devices for Hardware Security Primitives
Elena-Ioana Vatajelu, Giorgio Di Natale

12:15-12:45 Session 14 - Embedded Tutorial:

Security Validation, Sohrab Aftabjahani, Intel USA

12:45: Closing Remarks

12:45-14:15 Lunch