Presentations and Videos of:

VIRTUAL WORKSHOP ON MACHINE LEARNING & HARDWARE SECURITY

AUGUST 26-27, 2020

Organizer:
Prof. Avi Mendelson, Technion, Israel
Dr. Shivam Bhasin, NTU, Singapore

Objective: Exchange knowledge and research ideas in the area of using machine learning to improve evaluation and reverse engineering techniques.

We hope to:

- Create a community of researchers in these areas
- To expose the researchers to new infrastructures, techniques and research topics
- To establish a common ground for new collaborations and funding opportunities.

Technion
Hiroshi Fujiwara
Cyber Security
Research Center

TECHNION
Israel Institute
of Technology

NANYANG
TECHNOLOGICAL
UNIVERSITY

SoCure
Assuring Hardware
Security by Design
in Systems on Chip

Wednesday - August 26, 2020

Speaker	Talk Title	Link to Presentations	Link to Videos
Dr. Shivam Bhasin **NTU**	Introduction Day 1	🧑‍🏫	▶
Prof Sylvain Guilley **Secure-IC**	On Use of Machine Learning For Detection of Hardware Trojan	🧑‍🏫	▶
Prof. Stjepan Picek **aisylab**	On Use of Machine Learning For Assessment of Side-Channel Attacks	🧑‍🏫	▶
	☕ Break ☕		
Prof. Debdeep Mukhopadhyay **IIT Kharagpur**	On Use of Machine Learning For Assessment of Fault Injection Attacks	🧑‍🏫	▶
Dr. Dirmanto Jap & Dr. Xiaolu Hou **NTU**	On Side-Channel & Fault Attacks against Machine learning	🧑‍🏫	▶
Mr. Stuart Kincaid **Rambus**	Security & Countermeasures - Protecting Against Self-Improving Attacks	🧑‍🏫	▶

Technion
Hiroshi Fujiwara
Cyber Security
Research Center

TECHNION
Israel Institute
of Technology

NANYANG
TECHNOLOGICAL
UNIVERSITY

SOCure
Assuring Hardware
Security by Design
in Systems on Chip

Wednesday - August 26, 2020

Speaker	Talk Title	Link to Presentations	Link to Videos
Dr. Leonid Azriel **Technion**	Overview of algorithmic methods in IC reverse engineering	👨‍🏫	
Prof. Gwee Bah Hwee **NTU**	On Use of Machine Learning for IC Circuit Extraction	👨‍🏫	▶
	☕ Break ☕		
Prof. Alex Bronstein **Technion**	Geometry and learning in shape correspondence problems	👨‍🏫	▶
Mr. Amit Boyarski **Technion**	On Use of Spectral Graph Techniques for Hardware Reverse Engineering	👨‍🏫	▶
Mr. Nils Albartus **MAX PLANCK INSTITUTE** **University Bochum, Germany**	HAL & DANA - The Basis for Netlist Reverse Engineering	👨‍🏫	▶
Prof. Avi Mendelson/ Dr. Shivam Bhasin	Concluding Remarks		▶

Technion
Hiroshi Fujiwara
Cyber Security
Research Center

TECHNION
Israel Institute
of Technology

NANYANG
TECHNOLOGICAL
UNIVERSITY

SOCure
Assuring Hardware
Security by Design
in Systems on Chip