# Dimitrios Tychalas

**Ph.D. Candidate**
Electrical and Computer Engineering
New York University
Tandon School of Engineering
New York, USA

**Contact:**
245 18th Street, Brooklyn,
11215, NY, USA
Email: dimitris.tychalas@nyu.edu
Web: https://wp.nyu.edu/ditihala/
Cell (US) : +1 (646) 610 3282
Cell (UAE): +971 (50) 764 5007

## Education

**New York University Tandon School of Engineering** 2016-(exp.)2021
Electrical and Computer Engineering Department
- **Ph.D. Candidate**
  Topic: "Emulation-Assisted Automated Security Assessment of Industrial Control Systems"
  Advisor: Prof. Michail Maniatakos

**University of Thessaly** 2010-2015
School of Electrical and Computer Engineering
- **Dipl.Ing.** in Computer Engineering
  Thesis: "A hardware implementation of the entropy encoding technique CABAC on reconfigurable architectures"
  Advisor : Prof. Nikolaos Bellas

## Professional Experience

**Security Research Intern** Summer 2018
Intel Product Assurance and Security (IPAS) Team
Intel Corporation
Hillsboro, OR, USA

**Graduate Research Assistant** 2016-present
Modern Microprocessor Architectures (MoMA) Lab
New York University Abu Dhabi
Abu Dhabi, UAE

**Research Assistant** 2015-2016
Modern Microprocessor Architectures (MoMA) Lab
New York University Abu Dhabi
Abu Dhabi, UAE

## Skills

**Areas of Interest**
- Computer Architecture
- Systems Security
- Real-Time Embedded Systems
- Static/Dynamic Software Security Assessment Techniques
- Hardware Assisted Information Security
- Cache-based Side-Channels

**Programming**
- Hardware Design : Verilog, VHDL
- General Programming : C, Python, MIPS/ARM/x86 Assembly

**Computer Skills**
- Operating systems: Linux, MS Windows
- Hardware Design: Xilinx ISE/Vivado/HLS, Icarus Verilog, GTK Wave
- SGX Development: Microsoft Visual Studio, Intel SGX SDK
- Security Assessment Tools: AFL, AFL-Unicorn, Libfuzzer, angr
- Misc tools: QEMU, Ghidra, IDA Pro, gnu gdb
- Misc: bash, LaTeX, MS Office, Basic web design (HTML, CSS)

**Selected Coursework**

**Graduate level**

- Advanced Computer Architecture
- Advanced Hardware Design
- Advanced Compiler Topics
- Information Security and Privacy
- Hardware Security
- Application Security

**Selected Publications**

[1] **Dimitrios Tychalas**, Nektarios Georgios Tsoutsos, and Michail Maniatakos. "SGXCrypter: IP protection for portable executables using Intel's SGX technology." Design Automation Conference, 2017 22nd Asia and South Pacific (ASP-DAC). IEEE, 2017. (link)

[2] **Dimitrios Tychalas**, and Michail Maniatakos. "Open Platform Systems Under Scrutiny: A Cybersecurity Analysis of the Device Tree" 25th International Conference on Electronics, Circuits and Systems (ICECS). IEEE, 2018. (link)

[3] **Dimitrios Tychalas**, Anastasis Keliris, and Michail Maniatakos. "LED Alert: Supply Chain Threats for Stealthy Data Exfiltration in Industrial Control Systems" 25th International Symposium on On-Line Testing And Robust System Design (IOLTS). IEEE, 2019. (link)

[4] **Dimitrios Tychalas**, and Michail Maniatakos. "IFFSET: In-Field Fuzzing of Industrial Control Systems using System Emulation" Design, Automation & Test in Europe (DATE). IEEE, 2020. (link)

[5] **Dimitrios Tychalas**, Anastasis Keliris, and Michail Maniatakos, "Stealthy Information Leakage through Peripheral Exploitation in Modern Embedded Systems", Transactions on Device and Materials Reliability (TDMR). IEEE, 2020. (link)

[6] **Dimitrios Tychalas**, and Michail Maniatakos. "Potentially Leaky Controller: Examining Cache Side-Channel Attacks in Programmable Logic Controllers" 38th International Conference on Computer Design (ICCD). IEEE, 2020. (link)

[7] **Dimitrios Tychalas**, Hadjer Benkraouda, and Michail Maniatakos. "ICSFuzz: Manipulating I/Os and Repurposing Binary Code to Enable Instrumented Fuzzing in ICS Control Applications", In 30th USENIX Security Symposium (USENIX Security 21), 2021. (link)

[8] Prashant Rajput, Esha Sarkar, **Dimitrios Tychalas**, and Michail Maniatakos. "Remote Non-Intrusive Malware Detection for PLCs based on Chain of Trust Rooted in Hardware", in 6th IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2021. (link)

[9] **Dimitrios Tychalas**, and Michail Maniatakos "Stuxnet-in-a-Box: In-Field Emulation and Fuzzing of PLCs to Uncover the Next Zero-Day Threat in Industrial Control Systems.", Black Hat Asia 21 (2021) (link)

**Honors and Awards**

**Global Ph.D. Student Fellowship (5-year)** 2016-present
New York University Abu Dhabi (NYUAD)

**Academic Activities**

**Teaching Assistant** Fall 2016
EL-GY 6463: Advanced Hardware Design
Performed as a TA during the latter half of the Advanced Hardware Design class taught by Prof. Ramesh Karri at NYU Tandon School of Engineering, being the only student finishing the final class project before the midterm exam.

**Teaching Assistant** Fall 2017
ENGR-UH 3511: Computer Organization and Architecture
Designed and delivered the Lab part of the undergraduate Computer Organization and Architecture class taught by Prof. Michail Maniatakos at NYUAD.

**Mentorship**

- Supervised IIT Kanpur undergraduate student project Summer 2018
  Student: Ritesh Kumar
  Topic: ARM-based cache side-channel exploitation.
- Supervised NYUAD undergraduate student summer internship Summer 2020
  Student: Ibrahim Suleiman
  Topic: Software emulation for dedicated PLC I/O modules
- Supervised NYUAD undergraduate student summner internship Summer 2020
  Student: Berwin Gan
  Topic: Reverse engineering of Codesys 3.x PLC binaries through symbolic execution

**Technical Subreviewer**

- Journals
  - IEEE TIFS (2016, 2017)
  - IEEE SCIS (2017)
  - IEEE TDSC (2018)
  - IEEE DTIS (2018)
  - ACM TECS (2018, 2019)
- Conferences
  - ACM/EDAC/IEEE DAC (2016)
  - IEEE/ACM ICCAD (2016, 2017)
  - ACM AsiaCCS (2017, 2018)
  - IEEE ASPDAC (2018)
  - IEEE DATE (2019, 2020)
  - IEEE/ACM MICRO (2020, 2021)
  - USENIX Security (2021)

**Memberships** **Institute of Electrical and Electronic Engineers (IEEE)** 2015-present

**Languages**

- **Greek**: Native
- **English**: Fluent