Maria Rigaki
PhD Postdoctoral Researcher
Czech Technical University
Prague, Czech Republic

maria.rigaki@aic.fel.cvut.cz

Experience

Czech Technical University / Postdoctoral Researcher
JANUARY 2026 - , PRAGUE, CZECH REPUBLIC

Czech Technical University / PhD student
FEBRUARY 2018 - DECEMBER 2025, PRAGUE, CZECH REPUBLIC

Member of the Artificial Intelligence Center (AIC) group at FEL, working on the topics of Machine Learning and Cybersecurity. Dissertation topic: "Offensive Applications of Machine Learning in Cybersecurity".

Czech Technical University / Researcher
AUGUST 2017 - SEPTEMBER 2017, PRAGUE, CZECH REPUBLIC

Security Researcher, member of the Stratosphere lab at AIC, working on Machine Learning applications in Network Security.

Ericsson AS / Senior Solution Architect
MARCH 2012 - JULY 2017, OSLO, NORWAY

Solution Architect in the areas of Emergency Response and Critical Infrastructure Protection (CIP) as part of a global team based in Oslo. Technical pre-sales support and project delivery, solution design, and technical subject matter expert in various projects and offerings around the world. Technical evaluation of third-party vendors and potential partners. Lead Architect in portfolio development for Public Safety, including Proof of Concept projects and demonstrations.

Ericsson Greece / Solution Architect & Integrator
AUGUST 2007 - MARCH 2012, ATHENS, GREECE

Solution Architect & Integrator in both pre-sales and delivery phases of various IP Multimedia Subsystem (IMS) projects. Solution design, requirement analysis, customer presentations and demonstrations, customer training in new solutions and products. Lead designer for large IMS provisioning projects in Cyprus and Greece.

Virtual Trip / Senior Software Developer
FEBRUARY 2007 - JULY 2007, ATHENS, GREECE

Product Responsible for Solo Small Server and Gateway. Team leading, design and development of several features for a product that targeted SMEs with the premise

of providing a web-based interface for centralized management of various services, such as Web, Mail, Fax, VPN, VoIP PBX, File server, etc, hosted on a single and low-cost Linux appliance. Technologies: Python, JavaScript, Linux, Apache, Samba, OpenLDAP, Asterisk, Sendmail, etc.

Bytemobile (now Citrix) / Senior Software Developer
MAY 2004 - JANUARY 2007, PATRAS, GREECE

Requirement Analysis, Design, and Development of several features for Bytemobile's products. QA Lead in the local development center, reporting to the Engineering Director and Quality Assurance Managers in the US.

Intracom SA / Software Engineer
JANUARY 1999 -APRIL 2004, PATRAS, GREECE
Multiple positions, starting as a Software Developer and transitioning to technical lead roles and system design.

Education

Luleå University of Technology/ MSc Information Security
AUGUST 2015 - JULY 2017

Thesis: "Adversarial Deep Learning against Intrusion Detection classifiers"
http://www.diva-portal.org/smash/get/diva2:1116037/FULLTEXT01.pdf

University of Patras / Computer Science and Electrical Engineering
GRADUATED JULY 2004, PATRAS, GREECE

Thesis: 'TCP/IPv6 Header Compression for Wireless Networks'

Publications

Rigaki, M., Catania, C. A., & Garcia, S, “Building Adaptative and Transparent Cyber Agents with Local Language Models”, Expert Systems with Applications, 2026, 129987.

M. Rigaki and S. Garcia, “A survey of privacy attacks in machine learning,” ACM Computing Surveys, vol. 56, no. 4, pp 1-34, Nov. 2023, ISSN: 0360-0300. DOI: 10.1145/3624010.

M. Rigaki and S. Garcia, “Stealing and evading malware classifiers and antivirus at low false positive conditions,” Computers & Security, vol. 129, Jun. 2023, ISSN: 0167-4048. DOI: 10.1016/j.cose.2023.103192.

M. Rigaki and S. Garcia, “The power of the meme: Adversarial malware creation with model-based reinforcement learning,” in Computer Security – ESORICS 2023, G. Tsudik, M. Conti, K. Liang, and G. Smaragdakis, Eds., Cham: Springer Nature Switzerland, 2024, pp. 44–64, ISBN: 978-3-031-51482-1. DOI: 10.1007/978-3-031-51482-1_3.

M. Rigaki, O. Lukáš, C. Catania, and S. Garcia, “Out of the Cage: How Stochastic Parrots Win in Cyber Security Environments,” in Proceedings of the 16th International Conference on Agents and Artificial Intelligence - Volume 3: ICAART, Roma, Italy: SciTePress, Jul. 2024, pp. 774–781, ISBN: 978-989-758-680-4. DOI: 10.5220/0012391800003636.

M. Rigaki, O. Lukáš, C. Catania, and S. Garcia, “Prompt. exploit. repeat: Automating network security testing with llms,” in Agents and Artificial Intelligence, Cham: Springer Nature Switzerland, 2025, pp. 15–36, ISBN: 978-3-031-87330-0. DOI: 10.1007/978-3-031-87330-0_2.

M. Rigaki, C. Catania, and S. Garcia, "Hackphyr: A Local Fine-Tuned LLM Agent for Network Security Environments", 2024. *Under review.* Pre-print: https://arxiv.org/abs/2409.11276

M. Rigaki and S. Garcia, "Bringing a GAN to a Knife-fight: Adapting Malware Communication to Avoid Detection," in 2018 IEEE Security and Privacy Workshops (SPW), pp. 70-75. IEEE, 2018. DOI: 10.1109/SPW.2018.00019.

V. Valeros, M. Rigaki, and S. Garcia, "Machete: Dissecting the Operations of a Cyber Espionage Group in Latin America," in 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 464-473. IEEE, 2019. DOI: 10.1109/EuroSPW.2019.00058.

F. Palau, C. Catania, J. Guerra, S. García, and M. Rigaki, "Detecting DNS threats: A Deep Learning Model to Rule Them All," in XX Simposio Argentino de Inteligencia Artificial (ASAI 2019)-JAIIO 48 (Salta). 2019.

Selected Projects

- **AVAST LAB projekt - 13141/830/8301955C000 (2019-2021)**
  - Research in continual learning for malware detections

- **Research Center for Informatics (2021-2022):**
  - Research on privacy attacks on machine learning models
  - Model extraction attacks against malware classifiers

- **FEEL: Federated Learning for Network Security (2021)**:
  - Lead PI on a small project that focused on federated learning of network intrusion detection classifiers

- **AI Dojo (2022-2025)**:
  - Development of the AI-dojo network security environment
  - Research on LLM-based attacking agents for network security environments

Grants & Awards

Lead PI for CESNET Grant for “FEEL: Federated Learning for Network Security” project (2021).

Best poster award in Transylvanian Machine Learning Summer School (Summer 2018)

Security Conference presentations: Security Sessions ‘18, Blackhoodie #4 (2018), VirusBulletin (2019), CyberSec & AI (2021), ShaktiCon (2023), BSides Prague (2024)