Andrea Venturi

Personal Email: andrea.venturi01@gmail.com

Institutional Email: andrea.venturi@unimore.it

https://www.linkedin.com/in/andreaventuri01/

Skype: andrea.venturi01@gmail.com

Born on: January 3rd, 1994

Actual position and professional experience

July 2020 - now

Research Grant

"Machine Learning for cyber security", junior research grant at Interdepartment Research Center on Security and Safety (CRIS), Department of Engineering "Enzo Ferrari", University of Modena and Reggio Emilia.

- Tutor: Prof. Michele Colajanni

Education and Qualifications

November 2020 - now

PhD Student

"Novel methodologies for the cybersecurity of the future", International Doctorate in Information and Communication Technologies (ICT), Cycle XXXVI, Computer Engineering and Science Curriculum, Department of Engineering "Enzo Ferrari", University of Modena and Reggio Emilia.

- Tutor: Prof. Michele Colajanni

2020

Master's Degree in Computer Engineering

Department of Engineering "Enzo Ferrari", University of Modena and Reggio Emilia, Modena, Italia

- 7 Aprile 2020
- Curriculum: **Intelligent Cyber Systems**
- Graduation mark: **110/110 cum Laude**
- Thesis: **Sistema di Reinforcement Learning per contrastare l'efficacia di adversarial attack a Intrusion Detection System**
- Advisor: Prof. Michele Colajanni
- Co-Advisor: Ing. Giovanni Apruzzese

2017

Bachelor's Degree in Computer Science

Department of Physics, Computer Science and Mathematics, University of Modena and Reggio Emilia, Modena, Italia

- 19 Aprile 2017
- Graduation mark: **108/110**
- Thesis: **Sistema di memorizzazione distribuito e scalabile per libreria di analisi dati in Python**
- Advisor: Prof. Michele Colajanni
- Co-Advisor: Ing. Alessandro Guido

2020

License to practice the profession of Engineer

Information Engineer Section A

Teaching activities

December 2021

Seminar "Adversarial Machine Learning in Cybersecurity"

- Course: Cybersecurity (english) - Master's Degree in Computer Engineering - **University of Bologna**

November 2021

Seminar "ML for Malware and Network Intrusion Detection"

- Course: Cybersecurity (english) - Master's Degree in Computer Engineering - **University of Bologna**

December 2020

Seminar "Machine Learning for Cybersecurity"

- Course: Computer Security - Master's Degree in Computer Engineering - **University of Modena and Reggio Emilia**

Academic activities

2021

Technical Committee member

- IEEE Network Computing and Applications (NCA) [2021];

2020 - now

Reviewer

- IEEE Network Computing and Applications (NCA) [2020 - 2021];
- IEEE Transaction on Network and Service Management (TNSM) [2021];
- Elsevier Journal of Information Security and Applications (JISAS) [2021];

Publications

- A. Venturi, C. Zanasi. **"On the feasibility of adversarial machine learning in malware and network intrusion detection."** *IEEE Network Computing and Applications (NCA), November 2021.*
- G.Apruzzese, M. Andreolini, M. Marchetti, A. Venturi, M. Colajanni. **"Deep Reinforcement Adversarial Learning against Botnet Evasion Attacks."** *IEEE Transactions on Network and Service Management, December 2020*
- A. Venturi, G.Apruzzese, M. Andreolini, M. Colajanni, M. Marchetti. **"DReLAB - Deep REinforcement Learning Adversarial Botnet: A benchmark dataset for adversarial attacks against botnet Intrusion Detection Systems."** *Elsevier Data in Brief, February 2021*

Skills

Lingue

- Italian - Native
- English - Proficient
- Spanish - Advanced

Technical Skills

Operating Systems: **GNU/Linux** e **Windows**

Programming skills

- C, C++, Java, Python, Javascript
- Experience in designing and implementing of state-of-the-art level Intrusion Detection Systems leveraging modern Machine Learning techniques.
- Experience in treating big data and analyzing them through ad-hoc algorithms and modern techniques.
- Experience in designing and implementing modern Computer Vision techniques for Image/Video Recognition, Segmentation and Tracking.

Research Interests

- Big data security analytics
- Machine and Deep Learning for cybersecurity
- Adversarial Machine Learning
- Explainable AI in Cybersecurity