Andrea Venturi

Email Personale: andrea.venturi01@gmail.com

Email Istituzionale: andrea.venturi@unimore.it

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

https://orcid.org/0000-0003-3822-968X

Data di nascita: 3 Gennaio 1994

Posizione ed esperienze professionali

Agosto 2023 - in corso

Assegnista di Ricerca

"Applicazioni di AI e ML in ambito cybersecurity", assegno di ricerca junior presso il Dipartimento di Ingegneria "Enzo Ferrari" dell'Universtità degli Studi di Modena e Reggio Emilia.

- Tutor: Prof. Mirco Marchetti

Luglio 2022 - Giugno 2023

Assegnista di Ricerca

"Sistemi e algoritmi di network intrusion detection basati su machine learning e intelligenza artificiale", assegno di ricerca junior presso il Dipartimento di Ingegneria "Enzo Ferrari" dell'Universtità degli Studi di Modena e Reggio Emilia.

- Tutor: Prof. Mirco Marchetti

Luglio 2020 - Giugno 2022

Assegnista di Ricerca

"Machine Learning per la cyber security", assegno di ricerca junior presso il Centro di Ricerca Interdipartimentale per la Sicurezza e la prevenzione dei rischi (CRIS), del Dipartimento di Ingegneria "Enzo Ferrari" dell'Universtità degli Studi di Modena e Reggio Emilia.

- Tutor: Prof. Michele Colajanni

Istruzione e Qualifiche

Novembre 2020 - in corso

PhD in Information and Communication Technologies

"Machine Learning methods for cybersecurity", International Doctorate in ICT, Cycle XXXVI, Computer Engineering and Science Curriculum, Dipartimento di Ingegneria "Enzo Ferrari", Università degli studi di Modena e Reggio Emilia.

- Tutor: Prof. Michele Colajanni
- **Data conseguimento prevista**: Marzo 2024

2020

Laurea Magistrale in Ingegneria Informatica

Dipartimento di Ingegneria Enzo Ferrari, Università degli Studi di Modena e Reggio Emilia, Modena, Italia

- Data Conseguimento Titolo: 7 Aprile 2020
- Curriculum: **Intelligent Cyber Systems**
- Voto: **110/110 e Lode**
- Titolo Tesi: **Sistema di Reinforcement Learning per contrastare l'efficacia di adversarial attack a Intrusion Detection System**, Tesi di Ricerca
- Relatore: Prof. Michele Colajanni
- Correlatore: Ing. Giovanni Apruzzese

2017

Laurea Triennale in Informatica

Dipartimento di Scienze Fisiche, Informatiche e Matematiche, Università degli Studi di Modena e Reggio Emilia, Modena, Italia

- Data Conseguimento Titolo: 19 Aprile 2017
- Voto: **108/110**
- Titolo Tesi: **Sistema di memorizzazione distribuito e scalabile per libreria di analisi dati in Python**
- Relatore: Prof. Michele Colajanni
- Correlatore: Ing. Alessandro Guido

2020 Abilitazione alla professione di Ingegnere

Ingegnere dell'Informazione Sezione A

Skill

Skill Tecniche

Programmazione

- **Python**, C, C++
- Librerie e strumenti: **Pandas**, **Scikit-learn**, **Pytorch**, Keras, DGL, Pytorch Geometric, Matplotlib, Seaborn

Conoscenza dei sistemi operativi **GNU/Linux** e **Windows**

Competenze

- Design e gestione di progetti di ricerca in ambito Machine Learning
- Implementazione di Network Intrusion Detection System basati su moderne tecniche di Machine e Deep Learning
- Riproduzione di metodologie da paper scientifici
- Gestione ed analisi di large-scale data
- Revisore per diverse conferenze e riviste scientifiche

Lingue

- Italiano - Lingua madre
- Inglese - Avanzato
- Spagnolo - Avanzato

Docenze e attività seminariali

Dicembre 2022 Seminario "Machine Learning for Network Intrusion Detection"

- Corso: Cyber Physical Systems - Laurea Triennale in Ingegneria Informatica
  Università di Modena e Reggio Emilia (Sede Mantova)

Dicembre 2021, Novembre 2022 Seminario "Adversarial Machine Learning in Cybersecurity"

- Corso: Cybersecurity (english) - Laurea Magistrale in Ingegneria Informatica
  Università di Bologna

Novembre 2021 Seminario "ML for Malware and Network Intrusion Detection"

- Corso: Cybersecurity (english) - Laurea Magistrale in Ingegneria Informatica
  Università di Bologna

Dicembre 2020, Dicembre 2021, Maggio 2023 Seminario "Machine Learning per la Cybersecurity"

- Corso: Sicurezza Informatica - Laurea Magistrale in Ingegneria Informatica
  Università degli Studi di Modena e Reggio Emilia

Pubblicazioni

- A. Venturi, D. Pellegrini, M. Andreolini, L. Ferretti, M. Marchetti, M. Colajanni. **Practical evaluation of Graph Neural Networks in Network Intrusion Detection.** *CEUR Workshop Proceedings 2023 Italian Conference on Cyber Security, ITASEC'23 (2023).*
- A. Venturi, M. Ferrari, M. Marchetti, M. Colajanni. **"ARGANIDS: a novel Network Intrusion Detection System based on Adversarially Regularized Graph Autoencoder."** *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (SAC). ACM, 2023.*
- A. Venturi, D. Stabili, F. Pollicino, E. Bianchi, M. Marchetti. **"Comparison of Machine Learning-based anomaly detectors for Controller Area Network."** *2022 IEEE 21th International Symposium on Network Computing and Applications (NCA). IEEE, 2022.*
- A. Venturi, C. Zanasi, M. Marchetti, M. Colajanni. **"Robustness Evaluation of Network Intrusion Detection Systems based on Sequential Machine Learning."** *2022 IEEE 21th International Symposium on Network Computing and Applications (NCA). IEEE, 2022.*
- A. Venturi, M. Colajanni, M. Ramilli, G. V. Santangelo (2022). **"Classification of web phishing kits for early detection by platform providers."** arXiv preprint arXiv:2210.08273.
- A. Venturi, C. Zanasi. **"On the feasibility of adversarial machine learning in malware and network intrusion detection."** *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA). IEEE, 2021.*
- 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 (DiB), 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 (TNSM), 2021.*