



Andrea Venturi

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'Università 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'Università 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'Università degli Studi di Modena e Reggio Emilia.

- Tutor: Prof. Michele Colajanni

Istruzione e Qualifiche

Novembre 2020 - in corso

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, Dipartimento di Ingegneria "Enzo Ferrari", Università degli studi di Modena e Reggio Emilia.

- Tutor: Prof. Michele Colajanni

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

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, Seminario "Machine Learning per la Cybersecurity"
Maggio 2023 • Corso: Sicurezza Informatica - Laurea Magistrale in Ingegneria Informatica
Università degli Studi di Modena e Reggio Emilia

Servizio Accademico

- 2021 Comitato Tecnico
• IEEE Network Computing and Applications (NCA) [2021];
- 2020 - in corso Revisione
• 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];

Pubblicazioni

- A. Venturi, D. Pellegrini, M. Andreolini, L. Ferretti, M. Marchetti, M. Colajanni. **Critical evaluation of Graph Neural Networks in Network Intrusion Detection.** *To appear in Proceedings of 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, 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.*

Skill

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

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

Programming skills

- C, C++, Python
- Esperienza nella progettazione ed implementazione di Intrusion Detection System allo stato dell'arte sfruttando le più moderne tecniche di Machine Learning.
- Esperienza nel trattare ed analizzare grandi quantità di dati (Big Data) attraverso l'uso di algoritmi ad-hoc e tecniche moderne.

Campi di Interesse

- Big data security analytics
- Machine e Deep Learning per la cybersecurity
- Adversarial Machine Learning
- Explainable AI in Cybersecurity