Andrea Venturi

Email Personale: andrea.venturi01@gmail.com

Email Istituzionale: andrea.venturi@unimore.it

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

Skype: andrea.venturi01@gmail.com

Data di nascita: 3 Gennaio 1994

Posizione ed esperienze professionali

Luglio 2020 - in corso

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 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

2020

Abilitazione alla professione di Ingegnere

Ingegnere dell'Informazione Sezione A

Docenze e attività seminariali

Dicembre 2021

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

Seminario ”Machine Learning per la Cybersecurity”

- 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, C. Zanasi. **”On the feasibility of adversarial machine learning in malware and network intrusion detection.”** *IEEE Network Computing and Applications (NCA), Novembre 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, Gennaio 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, Febbraio 2021*.

Skills

Lingue

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

Skill Tecniche

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

Programming skills

- C, C++, Java, Python, Javascript
- 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.
- Esperienza nella progettazione ed implementazione delle più importanti tecniche di Computer Vision per Image/Video Recognition, Segmentation e Tracking.

Campi di Interesse

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