Giovanni Apruzzese, PhD

University of Liechtenstein
Institute of Information Systems
Fürst-Franz-Josef-Strasse 22
9490 Vaduz – Liechtenstein

✉ giovanni.apruzzese1@gmail.com
giovanni.apruzzese@uni.li
🌍 uni.li/giovanni.apruzzese
linkedin.com/in/giovanniapruzzese

Current Employment

Jul 2020 → now

PostDoc at the *Hilti Chair of Data and Application Security*

Institute of Information Systems – University of Liechtenstein

Aims: Carry out individual research. Teaching duties

Past Work & Education

Nov 2019 → Jun 2020

Research Grant on *Methods and Tools for Cybersecurity Analytics*

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

Aims: Devising innovative ML solutions for enhancing the security of distributed systems.

2016 → 2019

PhD in *Information and Communication Technologies (ICT)*

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

Thesis: *Security Analytics & Machine Learning for CyberDetection: Modern Issues and Novel Solutions*

Tutor: Prof. Michele Colajanni

Main research interests: CyberSecurity; Machine/Deep Learning; Big Data Security Analytics

Jan 2019 → Aug 2019

Visiting Research Scholar at *Dartmouth College* (Hanover, NH, USA)

Advisor: Prof. V.S. Subrahmanian

Topics covered: Adversarial Machine Learning applied to CyberSecurity

2013 → 2016

Master's Degree in *Computer Engineering* (summa cum laude)

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

Thesis: *Big Data Security Analytics for the detection of Advanced Persistent Threats*

Main subjects covered: CyberSecurity; Big Data; Networked Applications, Systems and Services

2010 → 2013

Bachelor's Degree in *Computer Engineering*

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

Thesis: *Using Social Networks for Community Management: the HaloItalia case study*

Main subjects covered: Software Development; Computer Architectures; Mathematics, Management

Research Activity

Short Description

My research combines *cybersecurity* and *big data analytics.* The goal is the detection of malicious activities by means of *machine-* and *deep-learning* techniques. My expertise lies in the analysis of *network*-related data, as well as *phishing* webpages and, more recently, *5G Communications.* I am intrigued by the topic of *adversarial attacks* against ML-powered security systems.

Research Projects

ASGARD: Analysis System for Gathered Raw Data – H2020 (2016 → 2020)

EU Project involving dozens of partners. The goal was supporting the threat intelligence and cyber forensics activities of police forces. My role was to develop, present, maintain, and document several data analytics tools.

ML for Incident Detection and Response – ENISA (2019 → 2020)

Technical Report by ENISA. I contributed by writing the majority of the core document.

AICA: Autonomous Intelligent Cyber Agent – NATO (2020 → now)

I am a member of the AICA Research Group, focusing on the *Stealth and Resilience* section.

Awards and Grants

2016	• **Scholarship** for the *UniMoRe International PhD Course in ICT* (3 years)
2017	• **Short-Term Scientific Mission Grant** by *NESUS COST Action*
	• **License** to practice the *Engineer* profession (Information section)
2018	• **Best Student Paper Award** for *IEEE NCA2018*
2019	• **Grant** for **Best Student Presentation** at the *MLS2019 PhD School*
	• **Best Student Paper Award** for *IEEE NCA2019*
	• **Distinguished International Research Award** at *UniMoRe*
2020	• **Outstanding** PhD Dissertation & Defense

Academic Activity

Teaching

- Teaching assistant for "*Computer Security*" (2016—2020)
  Master Degree in Computer Engineering – University of Modena and Reggio Emilia, Italy
- Teaching assistant for "*Systems Applications & Design*" (2020)
  Bachelor Degree in Business Administration – University of Liechtenstein
- Lecturer for "*Cybersecurity & Machine Learning*" (2020)
  Short Course for CRIT-Research – Italia

Guest Editor

- ACM Digital Threats: Research and Practice
  Special Issue on Offensive Machine Learning (2021)

Academic Activity

Technical Committee

- IEEE International Symposium on Network Computing and Applications
  IEEE NCA (2018, 2019, 2020)
- Conference on Detection of Intrusions, Malware & Vulnerability Assessment
  DIMVA (2020)
- Conference on Secure Communications
  EAI SecureComm (2021)

Reviewer

- ○ IEEE Communication Surveys and Tutorials *(COMST)*
- ○ IEEE Intelligent Systems *(IS)*
- ○ IEEE Transactions on Dependable and Secure Computing *(TDSC)*
- ○ IEEE Transactions on Engineering Management *(TEM)*
- ○ IEEE Transactions on Neural Networks and Learning Systems *(TNNLS)*
- ○ IEEE Transactions on Artificial Intelligence *(TAI)*
- ○ IEEE Access
- ○ IEEE International Conference on Signal Processing and Integrated Networks *(SPIN2018)*
- ○ IEEE International Symposium on Cluster, Cloud and Internet Computing *(CCGrid2020)*
- ○ Elsevier Computer and Security (*CoSe*)
- ○ Elsevier Journal of Information Security and Applications *(JISA)*
- ○ Elsevier Computer Communications *(COMCOM)*
- ○ Elsevier Neural Networks *(NeuNet)*
- ○ Elsevier Computers and Electrical Engineering *(CompElecEng)*
- ○ Elsevier Pervasive and Mobile Computing *(PeMC)*
- ○ Journal of Cyber Security Technology
- ○ ACM Digital Threats: Research and Practice *(DTRAP)*
- ○ Hawaii International Conference on System Sciences *(HICSS54)*
- ○ Springer Soft Computing
- ○ Springer Wireless Networks *(WINE)*
- ○ MDPI Sensors
- ○ MDPI Sustainability
- ○ The Web Conference *(WWW2020)*
- ○ Neural Information Processing Systems *(NeurIPS2020)*

Conference Session Chair

- IEEE International Symposium on Network Computing and Applications 2019
  Sessions 4, 5, 9: Networking, IoT and Industry 4.0, Secure and Resilient Systems
- Cyber Security Virtual Conference 2020 (*ICT Security Magazine*)
  Panel: Machine Learning and Industry 5.0 – Opportunities, Risks and Solutions

Languages

native • **Italian**
proficient • **English**
basic • **French**, **German**

Other Work Experiences

2012 → 2014

- **Administrator** of *HaloItalia*

  I was one of the administrators of the website *HaloItalia.it.* As such, I had to perform multiple duties of critical importance, including: the management of the staff; the management of the official social media pages (Facebook and YouTube) of the website; the production and editing of multimedia content (videos, images); the management of partnerships with external organizations (with the goal of providing sponsorships, fundings and visibility for the portal); the supervision and management (from both a technical- and social-side) of live events; the writing of news articles and reports before and after each event (both live and online).

  My work greatly contributed to the growth of HaloItalia, which increased its number of active users and views by over 1000%. In addition, I managed to secure year-long collaborations with *VideoGamesParty.it* which guaranteed proper prizes for the winners of each live event that we organized.

2016

- **Internship** at *BPER Services*

  For my MSc thesis, I spent 4 months as an intern in the main operation and information center of Banca Popolare dell'Emilia Romagna (BPER), a major Italian bank. Here, I witnessed the workflow of professional and experienced Network and Security operators. During my internship, I developed a tool that, by leveraging the APIs provided by the adopted SIEM, aided the network security personnel by prioritizing the most dangerous activities and incidents that occurred within the monitored network.

  The tool allowed the analysts to quickly determine which hosts required manual inspection.

2016

- **Independent Software Developer**, remotely working for *ATI Compressori*

  After obtaining my MSc degree and before starting my PhD Program, I was commissioned the development of a piece of software by *ATI Compressori*, the Italian leading company for air compressors. The program I developed had the goal of supporting the personnel during their auditing-tasks; more specifically, it had to show how the energy consumption of a given set of air compressors would have changed if one (or more) units were replaced by newer and/or more appropriate machines. The final version of the program (written in Python) came with a GUI (built with TKinter).

  The developed software is still being used by ATI Compressori even in 2019.

Publications

- Giovanni Apruzzese, Fabio Pierazzi, Michele Colajanni, Mirco Marchetti,
  “Detection and Threat Prioritization of Pivoting Attacks in Large Networks”,
  IEEE Transactions on Emerging Topics in Computing (TETC), October 2017
- Giovanni Apruzzese, Mauro Andreolini, Michele Colajanni, Mirco Marchetti,
  “Hardening Random Forest Detectors Against Adversarial Attacks”,
  IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI), May 2020
- Giovanni Apruzzese, Mauro Andreolini, Mirco Marchetti, Andrea Venturi, Michele Colajanni,
  “Deep Reinforcement Adversarial Learning against Botnet Evasion Attacks”,
  IEEE Transactions on Network and Service Management (TNSM), October 2020
- Giovanni Apruzzese, Michele Colajanni,
  “Evading Botnet Detectors based on Flows and Random Forest with Adversarial Samples”,
  Proc. of the 17th IEEE International Symposium on Network Computing and Applications (IEEE NCA18),
  Cambridge, MA, USA, November 2018 [**BEST STUDENT PAPER AWARD**]
- Giovanni Apruzzese, Michele Colajanni, Mirco Marchetti,
  “Evaluating the Effectiveness of Adversarial Attacks against Botnet Detectors”,
  Proc. of the 18th IEEE International Symposium on Network Computing and Applications (IEEE NCA19),
  Cambridge, MA, USA, September 2019 [**BEST STUDENT PAPER AWARD**]
- Giovanni Apruzzese, Michele Colajanni, Luca Ferretti, Alessandro Guido, Mirco Marchetti,
  “On the Effectiveness of Machine and Deep Learning for Cybersecurity”,
  Proc. of the 10th NATO International Conference on Cyber Conflicts (Cycon 2018),
  Tallinn, Estonia, May 2018
- Giovanni Apruzzese, Michele Colajanni, Luca Ferretti, Mirco Marchetti,
  “Addressing adversarial attacks against security systems based on machine learning”,
  Proc. of the 11th NATO International Conference on Cyber Conflicts (Cycon 2019),
  Tallinn, Estonia, May 2019
- Giovanni Apruzzese, Mirco Marchetti, Michele Colajanni, Gabriele Gambigliani Zoccoli, Alessandro Guido,
  “Identifying malicious hosts involved in periodic communications”,
  Proc. of the 16th IEEE International Symposium on Network Computing and Applications (IEEE NCA17),
  Cambridge, MA, USA, November 2017
- Giovanni Apruzzese, Mauro Andreolini, Mirco Marchetti, Vincenzo Giuseppe Colacino, Giacomo Russo,
  “AppCon: Mitigating Evasion Attacks to ML Cyber Detectors”,
  Symmetry, April 2020
- Andrea Venturi, Giovanni Apruzzese, Mauro Andreolini, Michele Colajanni, Mirco Marchetti,
  “DReLAB - Deep REinforcement Learning Adversarial Botnet: A benchmark dataset for adversarial attacks against botnet Intrusion Detection Systems”,
  Elsevier Data in Brief, December 2020
- Fabio Pierazzi, Giovanni Apruzzese, Michele Colajanni, Alessandro Guido, Mirco Marchetti,
  “Scalable architecture for online prioritization of cyber threats”,
  Proc. of the 9th NATO International Conference on Cyber Conflicts (CyCon 2017),
  Tallinn, Estonia, June 2017