Giovanni Apruzzese, PhD

University of Liechtenstein ✉
Liechtenstein Business School
Fürst Franz-Josef Strasse 22 m www.uni.li/giovanni.apruzzese
9490 Vaduz—Liechtenstein www.giovanniapruzzese.com

Current Employment

Sept 2022 → now **Assistant Professor** at the *Hilti Chair of Data and Application Security*

Liechtenstein Business School – University of Liechtenstein

Past Work & Education

Jul 2020 → Aug 2022 **PostDoc Researcher** at the *Hilti Chair of Data and Application Security*

Institute of Information Systems – University of Liechtenstein

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 Projects

ASGARD: Analysis System for Gathered Raw Data — H2020 [2016–2020]

EU Project involving dozens of partners, aimed at supporting police forces across Europe with a unified threat intelligence platform. My role was to develop, present, maintain, and document several data analytics tools. The ASGARD project won the "*Collaborative Innovative Technology Award"* in 2022.

ML for Incident Detection and Response — ENISA [2019–2020]

Report by ENISA. I contributed by writing the majority of the publication.

AICA: Autonomous Intelligent Cyber Agent — NATO [2020–2021]

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

SAMLAF: Security Assessment of ML Applications in Finance – FFF [2023–2025]

I am the Principal Investigator, and obtained 80k CHF in funding.

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 (best of its cycle)
2021	**Outstanding Reviewer** of *SecureComm21*
2022	**Highlighted Reviewer** of *ICLR2022* (top 8%)
	Top Reviewer of *NeurIPS2022* (top 10%)
	Outstanding Presentation Award for *IEEE EuroS&P'22*
2023	**Outstanding Reviewer** of *Elsevier FGCS* (top 1%)
	Best Reviewer of *The Web Conf'23* (top 5%)
	Distinguished Reviewer of *USENIX Security'23* (top 5%)

Teaching Activity

University of Liechtenstein

- Lecturer for "*Data and Application Security*—Exercise" [2021–2023]
  Master Degree in Information Systems
- Lecturer for "*Information Systems Development*" [2021–2023]
  Master Degree in Information Systems
- Lecturer for "*Information Management*—Übung & Zahnrad" [2021]
  Bachelor Degree in Business Administration
- Lecturer for "*Systems Analysis and Design*—Übung" [2020, 2022]
  Bachelor Degree in Business Administration

(previously)

- Teaching assistant for "*Computer Security*" [2016–2020]
  Master Degree in Computer Engineering—UniMoRe
- Lecturer for "*Cybersecurity & Machine Learning*" [2020]
  Short Course for CRIT-Research—Italy

Academic Activity (1/2)

Organizing Roles

- Workshop Chair for the IEEE European Symposium on Security and Privacy [2023–2024]
- Publication Chair of the European Symposium on Research in Computer Security [2023]
- Guest Editor for ACM Digital Threats: Research and Practice [2021]
- Online Content Chair for IEEE Int. Symp. on Network Computing and Applications [2020]

PC member

- Network and Distributed Systems Security Symposium (NDSS) [2024]
- USENIX Security Symposium (SEC) [2023]
- ACM Conference on Computer and Communication Security (ACM CCS) [2023]
- IEEE European Symposium on Security and Privacy (EuroS&P) [2023–2024]
- European Symposium on Research in Computer Security (ESORICS) [2023]
- Annual Computer Security Applications Conference (ACSAC) [2023]
- The Web Conference (WWW) [2023–2024]
- IEEE International Conference on Computer Communications and Networks (ICCCN) [2023]
- IEEE Security and Privacy: Deep Learning and Security (DLS) Workshop [2022, 2023]
- ACM CCS: Workshop on Artificial Intelligence Security (AISec) [2021-2023]
- ACM AsiaCCS: Workshop on Robust Malware Analysis (WoRMA) [2022, 2023]
- International Conference on Machine Learning (ICML) [2022]
- Neural Information Processing Systems (NeurIPS) [2021–2023]
- International Conference on Learning Representations (ICLR) [2022–2024]
- EAI Int. Conf. Security and Privacy in Communication Networks (SecureComm) [2021, 2022]
- Conference on Detection of Intrusions, Malware and Vulnerability Assessment (DIMVA) [2020]
- IEEE International Symposium on Network Computing and Applications (NCA) [2018–2021]
- Hawaii International Conference on System Sciences (HICSS) [2021–2024]

Journal Rev.

- ACM Transactions on Privacy and Security (TOPS)
- ACM Transactions on Sensor Networks (TOSN)
- ACM Digital Threats: Research and Practice (DTRAP)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Engineering Management (TEM)
- IEEE Transactions on Network and Service Management (TNSM)
- IEEE Transactions on Neural Networks and Learning Systems (TNNLS)
- IEEE Transactions on Artificial Intelligence (TAI)
- IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI)
- IEEE Transactions on Industrial Informatics (TII)
- IEEE Communication Surveys and Tutorials (COMST)
- IEEE Intelligent Systems (IS)
- IEEE Security & Privacy (S&P)
- Elsevier Computer and Security (CoSe)
- Elsevier Journal of Information Security and Applications (JISA)
- Elsevier Neural Networks (NeuNet)
- Elsevier Computers and Electrical Engineering
- Elsevier Future Generation Computing Systems (FGCS)
- European Journal of Information Systems (EJIS)

Academic Activity (2/2)

Invited Talks

- Stanford University – Research "Lunch" (Webinar) [May 2023]
  Topic: Is it real, or is it science-fiction? Bridging Adversarial ML Research and Practice.
- University of North Dakota – Research Webinar [2023]
  Topic: Revealing the gap between Research and Practice in Adversarial Machine Learning
- EPFL – Research Seminar [2023]
  Topic: Bridging the Gap between Adversarial ML Research & Practice
- Robust Intelligence – Fireside Chat [2023]
  Topic: Follow-up talk about our SaTML'23 paper
- University of Padua (MSc) – Seminar on Commun. & Netw. Security [2022]
  Topic: Doing Practical Research on Machine Learning and Cybersecurity
- University of Bologna (MSc) – Seminar on Cybersecurity [2022]
  Topic: Some Pragmatic aspects of Machine Learning and Cybersecurity
- Dagstuhl Seminar – Security of Machine Learning [2022]
  Topic: On the (over)use of datasets in ML security research
- Cybersecurity Webinar – hosted by TU Delft [2022]
  Topic: Some Pragmatic aspects of Machine Learning and Cybersecurity
- Technische Universiteit Delft – (MSc.) Seminar in Computer Science [2022]
  Topic: On the Relationship between Machine Learning and Cybersecurity
- 1st Huawei Workshop on Artificial Intelligence for Cyber-Security [2021]
  Topic: The Security of Machine Learning in 5G Network Infrastructures
- Cyber Security Virtual Conference – ICT Security Magazine [2020]
  Topic: Cybersecurity, Machine Learning, Industry 5.0 (panel moderator)

Sess. Chair

- IEEE European Symposium on Security and Privacy [2022, 2023]
- EAI Int. Conf. Security and Privacy in Communication Networks (SecureComm) [2021]
- IEEE Int. Symp. on Network Computing and Applications (NCA) [2019, 2020]

Peer-reviewed Publications (by date) [after joining UniLi]

- Fiona Koh, Kathrin Grosse, Giovanni Apruzzese: “**Voices from the Frontline: Revealing the AI Practitioners’ viewpoint on the European AI Act**”, *Hawaii International Conference on System Sciences (HICSS)* [2024]
- Jehyun Lee, Zhe Xin, Melanie Ng Pei See, Kanav Sabharwal, Giovanni Apruzzese, Dinil Mon Divakaran: “**Attacking logo-based phishing website detectors with adversarial perturbations**”, *European Symposium on Research in Computer Security (ESORICS)* [2023]
- Johannes Schneider, Giovanni Apruzzese: “**Dual Adversarial Attacks: Fooling Humans and Classifiers**”, *Journal of Information Security and Applications (JISA)* [2023]
- Giovanni Apruzzese, Johannes Schneider, Pavel Laskov: “**SoK: Pragmatic Assessment of Machine Learning for Network Intrusion Detection Systems**”, *IEEE European Symposium on Security and Privacy (EuroS&P)* [2023]
- Pier Paolo Tricomi, Lisa Facciolo, Giovanni Apruzzese, Mauro Conti: “**Attribute Inference Attacks in Online Multiplayer Video Games: A Case Study on Dota2**”, *ACM Conference on Data and Application Security and Privacy* [2023]
- Giovanni Apruzzese, Hyrum Anderson, Savino Dambra, David Freeman, Fabio Pierazzi, Kevin Roundy: “**”Real Attackers Don’t Compute Gradients”: Bridging the Gap between Adversarial ML Research and Practice**”, *IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)* [2023]
- Jacqueline Meyer, Giovanni Apruzzese: “**Cybersecurity in the Smart Grid: Practitioners’ Perspective**”, *Industial Control Systems Security Workshop (ICSS) – co-located with ACSAC’22* [2022]
- [**ARTIFACT: REUSABLE**] Giovanni Apruzzese, Mauro Conti, Ying Yuan: “**SpacePhish: The Evasion Space of Adversarial Attacks against Phishing Website Detectors using Machine Learning**”, *Annual Computer Security Applications Conference (ACSAC)* [2022]
- Giovanni Apruzzese, VS Subrahmanian: “**Mitigating Gray-box adversarial attacks against Phishing Website Detectors**”, *IEEE Transactions on Dependable and Secure Computing (TDSC)* [2022]
- Giovanni Apruzzese, Rodion Vladimirov, Aliya Tastemirova, Pavel Laskov: “**Wild Networks: Exposure of 5G Network Infrastructures to Adversarial Examples**”, *IEEE Transactions on Network and Service Management (TNSM)* [2022]
- Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Bûrdalo Rapa, Athanasios Vasileios Grammatopoulos, Fabio Di Franco: “**The Role of Machine Learning in Cybersecurity**”, *ACM Digital Threats: Research and Practice (DTRAP)* [2022]
- [**OUSTANDING PRESENTATION AWARD**] Giovanni Apruzzese, Aliya Tastemirova, Pavel Laskov: “**SoK: The Impact of Unlabelled Data for Cyberthreat Detection**”, *IEEE European Symposium on Security and Privacy (EuroS&P)* [2022]
- Giovanni Apruzzese, Luca Pajola, Mauro Conti: “**The Cross-evaluation of Machine Learning-based Network Intrusion Detection Systems**”, *IEEE Transactions on Network and Service Management (TNSM)* [2022]
- Johannes Schneider, Giovanni Apruzzese: “**Concept-based Adversarial Attacks: Tricking Classifiers and Humans alike**”, *IEEE Symposium on Security and Privacy: Deep Learning and Security Workshop (S&P DLS)* [2022]
- Giovanni Apruzzese, Mauro Andreolini, Luca Ferretti, Mirco Marchetti, Michele Colajanni: “**Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems**”, *ACM Digital Threats: Research and Practice (DTRAP)* [2021]
- Andrea Corsini, Giovanni Apruzzese, Jay-Yang Shanchieh: “**On the Evaluation of Sequential Machine Learning for Network Intrusion Detection**”, *Int. Conference on Availability, Reliability, Security (ARES)* [2021]
- Martin Husák, Giovanni Apruzzese, Jay-Yang Shanchieh, Gordon Werner: “**Towards an Efficient Detection of Pivoting Activity**”, *2021 IFIP/IEEE Int. Symposium on Integrated Network Management—GraSec Workshop* [2021]
- 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* [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)* [2020]

Peer-reviewed Publications (by date) [before joining UniLi]

- Giovanni Apruzzese, Mauro Andreolini, Mirco Marchetti, Vincenzo Giuseppe Colacino, Giacomo Russo: "**AppCon: Mitigating Evasion Attacks to ML Cyber Detectors**", *Symmetry* [2020]
- Giovanni Apruzzese, Mauro Andreolini, Michele Colajanni, Mirco Marchetti: "**Hardening Random Forest Detectors Against Adversarial Attacks**", *IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI)* [2019]
- [**BEST STUDENT PAPER AWARD**] Giovanni Apruzzese, Michele Colajanni, Mirco Marchetti: "**Evaluating the Effectiveness of Adversarial Attacks against Botnet Detectors**", *IEEE Int. Symposium on Network Computing and Applications (NCA)* [2019]
- Giovanni Apruzzese, Michele Colajanni, Luca Ferretti, Mirco Marchetti: "**Addressing Adversarial Attacks against Security Systems based on Machine Learning**", *IEEE/NATO Int. Conference on Cyber Conflicts (CyCon)* [2019]
- [**BEST STUDENT PAPER AWARD**] Giovanni Apruzzese, Michele Colajanni: "**Evading Botnet Detectors based on Flows and Random Forest with Adversarial Samples**", *IEEE Int. Symposium on Network Computing and Applications (NCA)* [2018]
- Giovanni Apruzzese, Michele Colajanni, Luca Ferretti, Alessandro Guido, Mirco Marchetti: "**On the Effectiveness of Machine and Deep Learning for Cybersecurity**", *IEEE/NATO Int. Conference on Cyber Conflicts (CyCon)* [2018]
- 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)* [2017]
- Giovanni Apruzzese, Mirco Marchetti, Michele Colajanni, Gabriele Gambigliani Zoccoli, Alessandro Guido: "**Identifying malicious hosts involved in periodic communications**", *IEEE Int. Symposium on Network Computing and Applications (NCA)* [2017]
- Fabio Pierazzi, Giovanni Apruzzese, Michele Colajanni, Alessandro Guido, Mirco Marchetti: "**Scalable architecture for online prioritization of cyber threats**", *IEEE/NATO Int. Conference on Cyber Conflicts (CyCon)* [2017]