UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DOTTORATO DI RICERCA / PHD PROGRAM IN
INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

Activities and Publications Report

PhD Student: Nicola d'Ambrosio

Student DR number: DR996111

PhD Cycle: XXXVII
PhD Cycle Chairman: Prof. Stefano Russo

PhD program student's start date: 1/1/2022
PhD program student's end date: 31/12/2024

Supervisor: Romano Simon Pietro

e-mail: spromano@unina.it

PhD scholarship funding entity:
Italian Ministry of University and Research (MUR) under program PON 2014-2020 and through the project Azione IV.4 - Dottorati e contratti di ricerca su tematiche dell'innovazione (DM 1061, August 10, 2021; CUP: E65F21003690003).

General information

Nicola d'Ambrosio received in year 2021 the Master Science degree in Computer Engineering from the University of Napoli Federico II. He attended a curriculum in Cyber Security within the PhD program in Information Technology and Electrical Engineering. He received a grant from Italian Ministry of University and Research (MUR) under program PON 2014-2020 and through the project Azione IV.4 - Dottorati e contratti di ricerca su tematiche dell'innovazione (DM 1061, August 10, 2021; CUP: E65F21003690003).

Study activities

Attended Courses

Year	Course Title	Type	Credits	Lecturer	Organization
1st	Probability calculus and elements of stochastic modelling	Ad hoc course	4	Massimiliano Giorgio	Scuola Superiore Meridionale
1st	Operations Research: Mathematical Modelling, Optimization Methods and Software Tools	Ad hoc course	4	Adriano Masone	ITEE
1st	Risk Assessment	MSc course	6	Alessandra De Benedctis	Univerisy of Naples Federico II
2nd	Big Data Architecture and Analytics	Ad hoc course	5	Giancarlo Sperlì	ITEE
2nd	Virtualization technologies and their applications	Ad hoc course	5	Luigi De Simone	ITEE
2nd	Operations Research: Mathematical Modelling, Optimization Methods and Software Tools	Ad hoc course	3	Francesco Cotugno	ITEE
3rd	Hands-on Network Intrusion Detection via Machine and Deep Learning	Ad hoc course	4	Antonio Montieri	ITEE

Attended PhD Schools

Year	School title	Location	Credits	Dates	Organization
2st	Complex Networks and Telecommunication	Como, Italy	4	3-7/7/2023	University of Pavia, Italy
3st	Open and programmable 6G networks in the cloud/edge continuum: research challenges and	Lipari, Italy	6	7-13/7/2023	University of Catania, Italy

	experimentation tools in SLICES Research Infrastructures				

Attended Seminars

Year	Seminar Title	Credits	Lecturer	Lecturer affiliation	Organization
1st	RAILS MID-TERM WORKSHOP	1	Multiple Lecturers	Various	ITEE
1st	Project Vac: Can a Text-to-Speech Engine Generate Human Sentiments?	0,4	Prof. V.K. Gubani	Illinois Institute of Technology, USA	ITEE
1st	2nd Workshopon Virtualization Technologies and their Applications (VIRTECH)	0,8	Luigi De Simone	University of Naples Federico II, Italy	ITEE
1st	Fixed Wireless Access	1	Multiple Lecturers	Various	5G Academy
1st	5G Networks in Action - The Private Mobile Era	0,2	Multiple Lecturers	Various	5G Academy
	Human-Multi-Robot Systems: Challenges for Real World Applications	1	Multiple Lecturers	Various	IROS 2022
1st	AR for remote use of Measurement instrumentation	0,2	Multiple Lecturers	Various	5G Academy
1st	Privacy preserving machine learning	0,4	Vittorio Prodomo	University of Naples Federico II, Italy	ITEE
1st	Connecting the dots: Investigating an APT campaign using Splunk	0,4	Antonio Forzieri	Splunk	ITEE
1st	Privacy and Data Protection	0,4	Stefano Mele	Gianni & Origoni	ITEE
1st	IEEE Authorship and Open Access Symposium: Tips and Best Practices to Get Published from IEEE	0,4	Multiple Lecturers	IEEE	IEEE
2nd	IEEE NFV-SDN	2	Multiple Lecturers	Various	University of Dresden, Germany
2nd	Robotics Meets AI & 5G: The Future is Now!	0,3	Bruno Siciliano	University of Naples Federico II, Italy	University of Naples Federico II, Italy
2nd	Migration of legacy IT infrastructures into the cloud.	0,4	Multiple Lecturers	Epsilon s.r.l.	University of Naples Federico II, Italy
2nd	RAILS Final & Roadmapping Events	0,4	Multiple Lecturers	Various	

3rd	Hominis	1	Multiple Lecturers	Various	University of Naples Federico II, Italy
3rd	1st Workshop on Network Digital Twin for Innovative Networks (NDT4IN)	0,8	Multiple Lecturers	Various	Czech Technical University, Czech Republic
3rd	Introduction to Large Language Models: Evolution and the current state	0,4	Tanmoy Chakraborty	Indian Institute of Technology Delhi, India	ITEE
3rd	Social Network Analysis: Methods and Applications	0,4	Tanmoy Chakraborty	Indian Institute of Technology Delhi, India	ITEE
3rd	QUIC: the secure protocol shaping the future of real-time communication over the Internet	0,8	Lorenzo Miniero	Meetecho	University of Naples Federico II, Italy

Research activities

Nicola d'Ambrosio participated in research activities across various fields related to cybersecurity:

- **CyberRange:** Development of vulnerable environments using deterministic approaches and Large Language Models (LLMs). Additionally, a tool was created to exploit the exposed vulnerability automatically.
- **Blockchain:** Development of applications based on the Web3 paradigm to create secure platforms for data validation, with applications in electronic voting and data collection from IoT devices.
- **DigitalTwin**: Development of digital twins to assess the effectiveness of cutting-edge cybersecurity defense strategies. These infrastructures were integrated with toolkits for capturing network traffic and monitoring system performance.
- **Active Deception and Moving Target Defense:** Development of defense strategies for enterprise and industrial networks aimed at mitigating internal and external threats to network infrastructure. Furthermore, approaches that potential attackers might use to detect the presence of honeypots were studied.
- **STPA and Attack Graphs:** Integration of safety models (STPA) and cybersecurity frameworks (based on NIST 800-53 and MITRE ATT&CK) to evaluate the impact of cyberattacks on critical infrastructures. Moreover, this analysis considers how these hazardous conditions can be triggered using Attack Graphs.
- **Insider Threat:** Use of Bayesian Attack Graphs to analyze the impact and likelihood of insider threats on enterprise infrastructures, with the aim of estimating the costs and benefits of mitigation strategies.
- **OSINT:** Development of tools for extracting and analyzing data from open sources. These tools are made to make it easier to identify illegal activity by collecting, organizing, and analyzing data from open sources.

Tutoring and supplementary teaching activities

During my PhD, I had the opportunity to deliver university lectures for the courses on WebRTC, Network Security, and Data Security, coordinated by Professor Romano Simon Pietro. During these activities, I covered topics such as the use of XML and JavaScript in the WebRTC course, the implementation of TLS (Transport Layer Security) for the Network Security course, and OSINT (Open Source Intelligence) techniques and phishing in the Data Security course. Additionally, I mentored participants at the Academy CyberHack, helping students develop cybersecurity skills. The course adopt a Challenge-Based Learning approach, alternating theoretical lessons with practical projects to promote active learning and the pratical application of acquired knowledge.

Credits summary

PhD Year	Courses	Seminars	Research	Tutoring / Supplementary Teaching
1st	14	6,2	40,6	0
2nd	17	3,1	42,7	0
3rd	10	3,4	40,3	0

Research periods in institutions abroad and/or in companies

PhD Year	Institution / Company	Hosting tutor	Period	Activities
2st	Accenture Cyber Fusion Center, Prague	Jiri Dostal, Security Manager	6 month (2 in remote and 4 on site)	On-field experiments on Automotive Security

PhD Thesis

In the PhD Thesis, Nicola d'Ambrosio proposes integrating risk analysis and active deception to improve the effectiveness of mitigating cyber threats that affect enterprise and industrial networks. In detail, the proposed methodology identifies high-impact cyber risks within the target architecture and leverages the obtained insight to design decoy strategies tailored to the unique characteristics and requirements of the specific infrastructure. Indeed, it is well recognized that cybersecurity lacks a one-size-fits-all solution. Different architectures require customized approaches due to dissimilarity in threat landscapes and infrastructure constraints. However, the underlying methodology remains the same.

Related to enterprise networks, this thesis investigates the impact of insider threats through the application of Bayesian threat graph networks. This focus was chosen due to the relative ineffectiveness of traditional risk assessment approaches to covering insider threats compressively. The analysis reveals that insider threats have a significant impact in terms of likelihood and financial

loss and mitigating these threats can yield substantial economic benefits. To address these limitations, the SMASH framework was proposed to seamlessly combine Honeypots and Moving Target Defense as defensive deception techniques within a business network to mitigate risks posed by external and internal threats. Moreover, SDN was utilized in this framework to expose honeypots within the production network without the risk of becoming a pivot for attackers to penetrate the enterprise network infrastructure further. The results demonstrate that the SMASH framework is highly effective in detecting and mitigating malicious activities, ranging from reconnaissance to exploitation, within the enterprise network.
Related to industrial networks, this thesis introduces a novel cyber-resilience model to determine cyber threats and assess their impact on the system. This approach leverages NIST 800-53, MITRE ATT&CK, STPA-Sec, and Attack Graph in order to identify the sequence of malicious actions that can lead to a specific hazardous scenario. To validate this approach, it was applied in an avionic environment by making a UAV (Unmanned Aerial Vehicle) testbed built using the Open System Architecture (OSA). Indeed, this testbed was designed to provide a platform for the broader research community and enable fast prototyping and testing of new features within the same context analyzed in this study. Aligned with the central research theme, this thesis further investigates the integration of Digital Twins, Moving Target Defense (MTD), and STAMP/STPA methodologies to detect malicious actions and isolate attackers within controlled environments. Specifically, the Safe Control Structure (SCS), built using the STAMP/STPA methodology, is employed to identify unauthorized connections. In parallel, MTD redundancy strategies are employed to dynamically redirect attacker traffic to a Digital Twin. Simultaneously, the compromised component is seamlessly replaced with a replica, effectively preventing any disruptions to normal industrial operations. Notably, this approach was also implemented in a hybrid power grid testbed, further demonstrating the versatility and applicability of the proposed methodology in diverse industrial environments.

Research products

Research results appear in 2 paper published and 4 others still under review in international Journals, and 3 contributions to international conferences.

List of scientific publications

International journal papers

- Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano, Alberto Urraro, A Cyber-Resilient Open Architecture for Drone Control, *Computer and Security*, vol. 150, 103410, 2025, DOI: https://doi.org/10.1016/j.cose.2024.104205
- Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano, Including insider threats into risk management through Bayesian threat graph networks, *Computer and Security*, vol. 133, 104205, 2023, DOI: https://doi.org/10.1016/j.cose.2023.103410
- Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano, SCASS: breaking into SCADA Systems Security *Computer and Security (2 round of revision)*
- Nicola d'Ambrosio, Gaetano Perrone, Vittoria Pacchiano, Simon Pietro Romano, ExploDox - Unleashing Exploit-DB Data for Automated Exploits Generation, Journal of Systems & Software (under review)
- Nicola d'Ambrosio, Claudio Lista, Gaetano Perrone, Simon Pietro Romano, SMASH: SDN-MTD Automated System with Honeypot Integration, *Computer Networks (under review)*
- Antonio Avolio, Nicola d'Ambrosio, Gaetano Perrone, Simon Pietro Romano, LLM-assisted generation of vulnerable containers, *Expert Systems with Applications (under review)*

International conference papers

- Francesco Caturano, Nicola d'Ambrosio, Gaetano Perrone, Luigi Previdente, Simon Pietro Romano, ExploitWP2Docker: a Platform for Automating the Generation of Vulnerable WordPress, Environments for Cyber Ranges, *International Conference on Electrical, Computer and Energy Technologies (ICECET),* Prague, Czech Republic, Jul. 2022, IEEE, DOI: https://doi.org/10.1109/ICECET55527.2022.9872859
- Nicola d'Ambrosio, Emma Melluso, Gaetano Perrone, Simon Pietro Romano, A Software-Defined Approach for Mitigating Insider and External Threats via Moving Target Defense, *IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Dresden, Germany, Nov. 2023, pp. 213-219, Publisher, DOI: https://doi.org/10.1109/NFV-SDN59219.2023.10329613
- Raffaele Cuorvo, Nicola d'Ambrosio, Domenico Iorio, Gaetano Perrone, Simon Pietro Romano, Securing Industrial Systems: A Testbed for Cyber-Defense Evaluation and Data Collection, *Workshop on Network Digital Twin for Innovative Networks (NDT4IN),* Prague, Czech Republic, Oct. 2024, Yet to Appear

Date 12/12/2024

PhD student signature 

Supervisor signature