UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

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

Activities and Publications Report

PhD Student: Vittorio Orbinato

Student ID: DR995144

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

PhD program student's start date: 01/11/2020
PhD program student's end date: 31/10/2023

Supervisor: prof. Domenico Cotroneo

e-mail: cotroneo@unina.it

Co-supervisor: prof. Roberto Natella

e-mail: roberto.natella@unina.it

PhD scholarship funding entity: MUR PON

General information

Vittorio Orbinato received in year 2020 the Master Science degree in Computer Engineering from the University of Napoli Federico II. He attended a curriculum in Computer Engineering within the PhD program in Information Technology and Electrical Engineering. He received a grant from the Ministry of University and Research (MUR) under the "PON Ricerca e Innovazione 2014-2020 – Dottorati innovativi con caratterizzazione industriale".

Study activities

Attended Courses

Year	Course Title	Type	Credits	Lecturer	Organization
1st	Scientific programming and visualization with Python	Ad hoc course	2.0	Prof. Alessio Botta	DiSt
1st	Data Management	MSc course	6.0	Prof. Flora Amato	DIETI
1st	Intelligenza Artificiale	MSc course	6.0	Prof. Flora Amato	DIETI
1st	Strategic Orientation for STEM Research & Writing	Ad hoc course	5.0	Dr. Chie Shin Fraser	ITEE
2nd	Virtualization Technologies and their Applications	Ad hoc course	5.0	Dr. Luigi De Simone	ITEE

Attended PhD Schools

Year	School title	Location	Credits	Dates	Organization
1st	5G International PhD School	Virtual	3.0	01-03/12/2020	Consorzio Nazionale Interuniversitario per le Telecomunicazioni

Attended Seminars

Year	Seminar Title	Credits	Lecturer	Lecturer affiliation	Organization
1st	Robot Manipulation and Control	0.5	Prof. Bruno Siciliano	DIETI	Prof. Bruno Siciliano (DIETI)
1st	Digital Project Management: practices, processes, techniques, tools and scientific approach	0.2	Prof. Dario Carotenuto	Project Management Institute	Data Science MSc & DIETI
1st	#andràtuttobene: Images, Texts, Emojis & Geodata in a Sentiment Analysis Pipeline	0.3	Dr. Serena Pelosi	University of Salerno	Data Science MSc & DIETI
1st	Patent Searching Best Practices with IEEE Xplore	0.2	Dr. Eszter Lukacs	IEEE	IEEE

1st	How to Get Published with IEEE	0.3	Dr. Eszter Lukacs	IEEE	IEEE
1st	At the Nexus of Big Data, Machine Intelligence and Human Cognition	0.2	Prof. George S. Djorgovski	California Institute Of Technology	Data Science MSc & DIETI
1st	Exploiting Deep Learning and Probabilistic Modeling for Behavior Analytics	0.2	Prof. Giuseppe Manco	ICAR - CNR	Data Science MSc & DIETI
1st	GDPR basics for computer scientists	0.3	Dr. Rigo Wenning	European Research Consortium for Informatics and Mathematics	DIETI
1st	Data Driven Transformation in WINDTRE through Managers' voice	0.4	Marcello Savarese, Erica Bertone	WINDTRE	Data Science MSc & DIETI
1st	From Photometric Redshift to Improved Weather Forecasts: an interdisciplinary view on machine learning	0.2	Dr. Kai Polsterer	Heidelberg Institute for Theoretical Studies (HITS)	Data Science MSc & DIETI
1st	Cybercrime and electronic evidence	0.2	Eng. Matteo Lucchetti	Cyber 4.0	Data Science MSc & DIETI
1st	AI LEGAL: Artificial Intelligence for notary's sector	0.2	Dr. Salvatore Palange	FLUEL	Data Science MSc & DIETI
1st	The era of Industry 4.0: new frontiers in business model innovation	0.2	Dr. Marco Balzano	Ca' Foscari University	Data Science MSc & DIETI
1st	Machine learning: causality lost in translation	0.3	Dr. Edwin A. Valentijn	Rijksuniversiteit Groningen	Data Science MSc & DIETI
1st	Approaches to Graph Machine Learning	0.2	Dr. Miroslav Cepek	Oracle Labs	Data Science MSc & DIETI
1st	Visual Interaction and Communication in Data Science	0.4	Dr. Marco Quartulli	Vicomtech	Data Science MSc & DIETI
1st	Dai mainframe all'IoT: una retrospettiva sull'evoluzione delle architetture di calcolo	0.4	Prof. Antonino Mazzeo	DIETI	Prof. Alessandro Cilardo (DIETI)
1st	Big data and Computational Linguistics	0.4	Prof. Francesco Cutugno	DIETI	Data Science MSc & DIETI

1st	Sensoria Health	0.2	Dr. Stefano Rossotti	Sensoria Health	Data Science MSc & DIETI
1st	The coming revolution of Data Driven Discovery (a fourth Methodological Paradigm of Science)	0.3	Prof. Giuseppe Longo	Unina	Scuola Superiore Meridionale
1st	Distributional Semantics Methods: how Linguistics features can improve the semantic representation	0.3	Dr. Alessandro Maisto	University of Salerno	Data Science MSc & DIETI
1st	Ethics of quantification	0.4	Dr. Andrea Saltelli	Open University of Catalonia	Data Science MSc & DIETI
1st	Risk assessment in real life: experiences from the railway domain	0.3	Emilia Di Martino, Diego Gerbasio, Claudio Mazzariello, Aniello Paolillo	HITACHI Rail	Prof. Valeria Vittorini (DIETI)
1st	Sadas Engine, an innovative DBMS for the Data Warehouse, great performance in the VLDB environment	0.4	Eng. Luca De Rosa	SADAS	Data Science MSc & DIETI
1st	Qiskit: state of the art and tools for Quantum Computers from IBM	0.4	Dr. Federico Accetta	IBM Italy	Prof. A. S. Cacciapuoti (DIETI)
1st	Second Quantum Revolution: innovation trends and expected industrial impacts	0.4	Dr. Antonio Manzalin	TIM	Prof. A. S. Cacciapuoti (DIETI)
2nd	Connecting the dots: Investigating an APT campaign using Splunk	0.4	Dr. Antonio Forzieri	Splunk	Proff. D. Cotroneo, S. P. Romano, R. Natella
2nd	Threat Hunting Essentials	0.4	Dr. Artem Artemov	Group-IB	Proff. D. Cotroneo, S. P. Romano, R. Natella
2nd	Threat Hunting Use Cases	0.4	Dr. Vladimir Kurdin	Group-IB	Proff. D. Cotroneo, S. P. Romano, R. Natella
2nd	Privacy-preserving Machine Learning	0.4	Dr. Vittorio Prodomo	DIETI	Proff. D. Cotroneo, S. P. Romano, R. Natella
3rd	Cybercrime and Information Warfare: National and International Actors	0.4	Dr. Pierluigi Paganini	ENISA	Proff. D. Cotroneo, S.P. Romano, R. Natella
3rd	Privacy and Data Protection	0.4	Dr. Stefano Mele	Gianni & Origoni	Proff. D. Cotroneo, S. P. Romano, R. Natella

3rd	Crash Course on Data Excellence	0.4	Dr. Roberto Maranca	Schneider Electric	Data Science MSc & DIETI
3rd	How to Publish Under the CARE-CRUI Open Access Agreement with IEEE	0.3	Nino Grizzuti, Eszter Lukacs, Stefano Bianco	CARE-CRUI and Unina, IEEE, CARE-CRUI and INFN	CARE-CRUI and IEEE
3rd	Open-source software e sicurezza della software supply chain	0.4	Antonino Sabetta, Serena Ponta	SAP	Prof. Roberto Natella
3rd	Ricerca e formazione nella società della transizione digitale	1.0			CINI

Research activities

Vittorio Orbinato participated in the research on cybersecurity-related topics, focusing on offensive security and adversary emulation. In particular, his research focused on the two main issues of adversary emulation: i) limited representativeness of real-world attackers and scenarios, and ii) lack of integration with Cyber Threat Intelligence (CTI). His research efforts have resulted in developing solutions to bridge these gaps in the cybersecurity landscape: a CTI-driven framework for adversary emulation. This framework enables the automatic extraction of adversarial tactics, techniques, and procedures (TTPs) from unstructured CTI to generate adversary emulation plans. Such plans can be used to emulate the behavior of complex APTs on *Laccolith*, a novel hypervisor-based adversary emulation solution equipped with anti-detection capabilities. Laccolith has been extensively evaluated against state-of-the-art solutions for adversary emulation in terms of detectability, i.e., their ability to evade the most popular detection mechanisms, e.g., anti-viruses (AVs), Endpoint Detection and Response (EDR).

Tutoring and supplementary teaching activities

Sistemi Operativi, SSD: ING-INF/05, Tutor: prof. Domenico Cotroneo, CdL Ingegneria Informatica

Credits summary

PhD Year	Courses	Seminars	Research	Tutoring / Supplementary Teaching
1st	22.0	7.8	35.0	0
2nd	5.0	1.6	53.4	1.6
3rd	0	2.9	57.1	0

Research periods in institutions abroad and/or in companies

PhD Year	Institution / Company	Hosting tutor	Period	Activities
2nd	University of Coimbra, Coimbra, Portugal	Prof. Marco Vieira	18/05/22 – 19/12/22	Research on intrusion injection in virtualized systems for security assessment purposes.
2nd/3rd	System Management S.p.A, Napoli, Italy	Dr. Fabio Cornevilli	01/03/22 – 30/04/22, 01/01/23 – 30/06/23 (remote)	Development of a hypervisor-based adversary emulation platform with anti-detection capabilities. Experimental evaluation of its detectability.

PhD Thesis

In the ever-evolving landscape of cybersecurity, the challenges faced by organizations in safeguarding their digital assets and data have grown exponentially. Traditional reactive security measures, which focus on responding to attackers after they have breached the perimeter, are no longer sufficient in the current dynamic threat environment, resulting in delayed detection and business damage.

To effectively protect against Advanced Persistent Threats (APTs), organizations must shift their paradigm toward proactive security measures. *Adversary emulation* is the pivotal strategy within this landscape, i.e., a strategy that emulates the TTPs employed by real-world threat actors to anticipate their moves and enhance defensive capabilities accordingly.

Unfortunately, adversary emulation also presents some drawbacks that limit its adoption. First, the scenarios emulated with this paradigm are *not representative* of real-world threat actors. Currently, adversary emulation lacks integration with Cyber Threat Intelligence (CTI) to provide insights into the TTPs employed by APTs. This happens since CTI still comes in unstructured forms, e.g., threat and incident reports written by security analysts, making it challenging to automatically process this information to replicate the attackers' behavior.

Second, security practitioners cannot rely upon open-source adversary emulation tools to effectively emulate APTs. These solutions only provide educational emulation, without being able to evade basic detection countermeasures in actual deployment scenarios.

To address these issues, this dissertation devises a **CTI-driven framework for adversary emulation**. The framework provides a pipeline to **automatically extract attack techniques** from CTI documents and **generate adversary emulation plans**. In addition, it offers a novel solution for adversary emulation *(Laccolith*) able to perform malicious actions in a non-detectable way, to emulate the behavior of complex APTs realistically. Laccolith was tested against multiple AV/EDR solutions to assess its effectiveness for adversary emulation.

Publications

Research results appear in 3 contributions to international conferences, with 1 paper for an international journal and 1 contribution to an international conference under review.

List of scientific publications

International journal papers

V. Orbinato, M.C. Feliciano, D. Cotroneo, R. Natella,
Laccolith: Hypervisor-Based Adversary Emulation with Anti-Detection,
Transactions on Dependable and Secure Computing (TDSC), (**under review after revision**)

International conference papers

V. Orbinato,
A next-generation platform for Cyber Range-as-a-Service,
2021 IEEE 32nd International Symposium on Software Reliability Engineering Workshops (ISSREW),
Wuhan, China, Oct. 2021, pp. 314-318, DOI: 10.1109/ISSREW53611.2021.00094.

P. Liguori, E. Al-Hossami, V. Orbinato, R. Natella, S. Shaikh, D. Cotroneo, B. Cukic,
EVIL: Exploiting Software via Natural Language,
2021 IEEE 32nd International Symposium on Software Reliability Engineering (ISSRE),
Wuhan, China, Oct. 2021, pp. 321-332, DOI: 10.1109/ISSRE52982.2021.00042.

V. Orbinato, M. Barbaraci, R. Natella, D. Cotroneo,
Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study,
2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE),
Charlotte, North Carolina, Oct./Nov. 2022, pp. 181-192, DOI: 10.1109/ISSRE55969.2022.00027.

V. Orbinato, F.C. Grasso, R. Natella, D. Cotroneo,
Vulnerability Prediction on Binary Code via Neural Decompilation,
54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), (**under review)**

Date 20/10/2023

PhD student signature 

Supervisor signature _____