europass

Giuseppe Daidone

Email address: giuseppe.daidone@uniroma1.it **Email address:** ingdaidone.business@gmail.com **Phone:** (+39) 3774269117

Website: https://giuseppedaidone.github.io/ **Website:** https://scholar.google.com/citations?user=k932qLEAAAAJ

LinkedIn: https://www.linkedin.com/in/giuseppedaidone/

Gender: Male **Date of birth:** 4 Dec 2000 **Nationality:** Italian

ABOUT MYSELF

Eng. Giuseppe Daidone is a PhD student in the Joint Cybersecurity Program at Sapienza University of Rome and Luiss University.

He has achieved a Bachelor's Degree in Computer Engineering at the University of Bergamo in 2023, with the thesis "Exploration of vulnerabilities found in Electron applications", under the supervision of Prof. S. Paraboschi and Seclab. He has achieved a Master's Degree in Engineering in Computer Science at Sapienza University of Rome in 2025, specializing in Cybersecurity and Deep Learning fields intersection, with the thesis "Adversarial Attacks on Convolutional and Transformer Architectures for Image-based Malware Detection and Classification Tasks", aligned with the objectives of the ArIS (Artificial Intelligence Sandboxing) PNRM Project of NAVARM (Naval Weaponry Direction of the Ministry of Defence) and Telsy, under the supervision of Prof. I. Amerini, co-supervision of Prof. L. Querzoni, and co-examining of Prof. S. Bonomi.

His research interests include adversarial machine learning techniques for designing secure AI models, multimedia forensics for detecting manipulated digital content, and deep learning based techniques for malware analysis. His research project focuses on "Watermarking and Proactive Defense against Malicious Generative AI" in collaboration with the National Cybersecurity Agency (ACN), President of the Council of Ministers. His PhD journey is supervised by Prof. I. Masi at OmnAI Lab, Department of Computer Science, Sapienza, and Prof. I. Amerini at ALCOR Lab, Department of Computer, Control and Management Engineering, Sapienza.

Since 2026, he has been a member of the Italian Intelligence Society (SOCINT) for intelligence studies.

WORK EXPERIENCE

Agenzia per la Cybersicurezza Nazionale (ACN)

City: Rome | **Country:** Italy

[Nov 2025 - Current]

PhD Researcher

Research project: Watermarking and Proactive Defense against Malicious Generative AI.

PhD in Cybersecurity at Sapienza University of Rome, Luiss University, Agenzia per la Cybersicurezza Nazionale (ACN).

EDUCATION & TRAINING

[Nov 2025 - Nov 2028]

Doctor of Philosophy, PhD in Cybersecurity

Sapienza Università di Roma https://www.uniroma1.it/it/

Address: Via Ariosto 2500185, Roma (Italy) | **Field(s) of study:** Information and Communication Technologies | **Level in EQF:** 8

Joint PhD Cybersecurity program by Sapienza University of Rome and Luiss University.

[Nov 2025 - Nov 2028]

Doctor of Philosophy, PhD in Cybersecurity

Luiss Guido Carli University https://www.luiss.it/

Address: Viale Romania 3200197, Roma (Italy) | **Field(s) of study:** Information and Communication Technologies | **Level in EQF:** 8

Joint PhD Cybersecurity program by Sapienza University of Rome and Luiss University.

[Sep 2023 - Jul 2025]

Master's Degree, Engineering in Computer Science

Sapienza Università di Roma https://www.uniroma1.it/it/

Address: Via Ariosto 2500185, Roma (Italy) | **Field(s) of study:** Information and Communication Technologies | **Level in EQF:** 7 | **Number of credits:** 120 | **Thesis:** Adversarial Attacks on Convolutional and Transformer Architectures for Image-based Malware Detection and Classification Tasks

Thesis title: Adversarial Attacks on Convolutional and Transformer Architectures for Image-based Malware Detection and Classification Tasks

Advisor: Prof. I. Amerini

Co-advisor: Prof. L. Querzoni

Co-examiner: Prof. S. Bonomi

Thesis field: Cybersecurity, Deep Learning

Curriculum Studiorum (ENG):

- Dependable Distributed Systems
- Cybersecurity (Low-Level Security + Application-Level Security)
- Algorithm Design
- Laboratory of Advanced Programming
- Artificial Intelligence and Machine Learning
- Data Management
- Human-Computer Interaction*
- Interactive Computer Graphics*
- Computer Vision*
- Project Management*
- Malware Analysis*
- Security Governance*
- Deep Learning*
- Digital Entrepreneurship*

*Optional subjects

[Aug 2019 - Jun 2023]

Bachelor's Degree, Computer Engineering

Università degli Studi di Bergamo www.unibg.it

Address: Viale G. Marconi 524044, Dalmine (Italy) | **Field(s) of study:** Information and Communication Technologies | **Level in EQF:** 6 | **Number of credits:** 180 | **Thesis:** Exploration of vulnerabilities found in Electron applications

Thesis title: Exploration of vulnerabilities found in Electron applications

Advisor: Prof. S. Paraboschi

Thesis field: Cybersecurity

Curriculum Studiorum (IT):

- Analisi Matematica I
- Fisica Generale I

- Chimica
- Programmazione
- Geometria e Algebra Lineare
- Fisica Generale II
- Calcolatori Elettronici
- Programmazione a Oggetti
- Sistemi Operativi
- Analisi Matematica II
- Economia ed Organizzazione Aziendale
- Elettrotecnica
- Statistica
- Fondamenti di Automatica
- Basi di Dati e Web
- Fondamenti di Elettronica
- Fondamenti di Reti e Telecomunicazione
- Modelli Stocastici + Lab. Abilità Informatiche e Telematiche
- Ingegneria del Software
- Databases 2 (ENG)
- Sistemi di Controllo di Gestione
- Embedded and Real Time Systems (ENG)
- Economia del Cambiamento Tecnologico*
- Multimedia Internet (ENG)
- Algebra e Logica
- Tecnologie Cloud e Mobile*

*Optional subjects

[Aug 2014 - Jul 2019] **High School Diploma, Information Technology**

Istituto Tecnico Industriale Leonardo Da Vinci https://www.isdavincitorre.edu.it/

Address: Piazza XXI Aprile91100, Trapani (Italy) | **Field(s) of study:** Information and Communication Technologies | **Level in EQF:** 5

PUBLICATIONS

[2026] **Neutralizing Proactive Defense using Diffusion-based Upsampling**

Reference: Daidone, G. and Bartolucci, F. and Briglia, M. R. and Mirza, M. H. and Lisanti, G. and Masi, I., Neutralizing Proactive Defense using Diffusion-based Upsampling, Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2026.
Authors: Giuseppe Daidone, Filippo Bertolucci, Maria Rosaria Briglia, Mujtaba Hussain Mirza, Giuseppe Lisanti, Iacopo Masi | **Journal Name:** Proceedings of the 2026 ACM Workshop on Information Hiding and Multimedia Security | **Publisher:** ACM

[2026] **Deepfake Detection, Attribution, and Authentication**

Reference: Amerini, I. et al., Deepfake Detection, Attribution, and Authentication: Insights from the FF4ALL Project, ITASEC26, 2026.
Authors: Amerini, Barni, Battiato, Bestagini, Boato, Bongini, Bruni, Casula, Cirillo, Caldelli, Daidone, De Natale, De Nicola, Guarnera, La Cava, Mandelli, Marcialis, Micheletto, Montibeller, Negroni, Orrù, Perazzo, Puglisi, Salvi, Tondi, Tubaro, et al. | **Journal Name:** Proceedings of the Joint National Conference on Cybersecurity (ITASEC & SERICS 2026) | **Volume, Issue and Pages:** Vol. 4198 | **Publisher:** CEUR-WS

[2026] **A Comprehensive Study of Cross-domain Adversarial Robustness and Attack Transferabilityin Image-Based Malware Detection and Classification**

Reference: Daidone, G. and Cirillo, L. and Querzoni, L. and Amerini, I., A Comprehensive

Study of Cross-domain Adversarial Robustness and Attack Transferability in Image-Based Malware Detection and Classification, Image and Vision Computing, 2026.

Pre-print, post-revision (last update 05/2026).

Authors: Giuseppe Daidone, Lorenzo Cirillo, Leonardo Querzoni, Irene Amerini | **Journal Name:** Image and Vision Computing | **Volume, Issue and Pages:** Special Issue: Security-AI: Attacks on AI Systems in Computer Vision | **Publisher:** Elsevier

CONFERENCES & SEMINARS

[9 Feb 2026 - 12 Feb 2026] **Joint National Conference on Cybersecurity (ITASEC & SERICS)** Faculty of Engineering and Architecture, Piazza d'Armi, Cagliari, Italy

Presenter of the paper *Deepfake Detection, Attribution, and Authentication*.

Link: https://itasec.it/

[2 Feb 2026 - 5 Feb 2026] **CSP-IAS Winter School - Cryptography and Machine Learning** Sala Duomo, OGR Cult, Turin, Italy

Participant.

Link: https://ai4i.it/ias-winter-school-2026/#faculty

PROJECTS

[Mar 2025 - Jun 2025] **SPAICY**

Group project

Digital Entrepreneurship - Professor Andrea Vitaletti

Language: ENG

Mark: 30/30

Link: https://drive.google.com/drive/folders/1fJxUEKQH0TVBsGzJ1yW40wHZWKMRiYNw?usp=sharing

[Dec 2024 - Jan 2025] **Success and Failure Factors in Software Development Projects**

Project Management - Professor Alessandro Annarelli

Language: ENG

Mark: 12/12

Link: https://drive.google.com/drive/folders/1-P0FdxDwA5hLKEm_zNKol5lXUa4sMgkj

[Nov 2024 - Jan 2025] **Data Warehousing and Analysis**

Group project

Data Management - Professor Maurizio Lenzerini and Professor Roberto Maria Delfino

Language: ENG

Mark: 7/8

Links: https://drive.google.com/drive/folders/1qZuh5DDWu4wJT_0ldnSH5H0_GyKbfKAt | https://github.com/Davood-sh/Data-warehouse

[Aug 2024 - Sep 2024] **Layer-wise Depth Integration in RGBD Deepfake Detection**

Computer Vision - Professor Irene Amerini, Professor Luca Maiano and Professor Lorenzo Papa

Language: ENG

Mark: 27/30

Link: https://github.com/GiuseppeDaidone/computer-vision-2324

[Jun 2024 - Jul 2024] **Q-Learning & Deep Q-Network**

Group project

Machine Learning - Professor Fabio Patrizi

Language: ENG

Mark: 30/30

Link: https://drive.google.com/drive/folders/1CAOKYJ42Wqt4_RU_txD9hfE7gnJrshCc?usp=sharing

[Apr 2024 - Jul 2024] **SetOn.**

Group project

Human-Computer Interaction - Professor Tiziana Catarci, Professor Alba Bisante and Professor Valeria Mirabella

Language: ENG

Mark: 30/30

Link: https://drive.google.com/drive/folders/14EOiGNf5JL9kSRgRFfgQSRWuFN_Qk7kB?usp=share_link

[Mar 2024 - Jun 2024] **Computer Graphics Projects**

Interactive Computer Graphics - Professor Paolo Russo

Language: ENG

Mark: 30/30

Links: https://github.com/GiuseppeDaidone/final-project-InteractiveGraphics2324-GiuseppeDaidone | https://drive.google.com/drive/folders/1-1lfkiIv1-DyCsOHLFXzvIybkQB0hYKK

[Jan 2024 - Apr 2024] **FlickTime**

Group project

Laboratory of Advanced Programming - Professor Massimo Mecella

Language: ENG

Mark: Passed

Link: https://github.com/GiuseppeDaidone/flick-time

[Dec 2023 - Jan 2024] **Byzantine Reliable Broadcast — An Adaptive Protocol for the Fault Detection in the Authenticated Double-Echo Broadcast**

Dependable Distributed Systems - Professor Silvia Bonomi and Professor Giovanni Farina

Language: ENG

Mark: 3/3

Link: https://github.com/GiuseppeDaidone/AdaptiveByzantineReliableBroadcast

[Oct 2023 - Dec 2023] **Cybersecurity Reports**

Cybersecurity - Professor Fabrizio D'Amore

Language: ENG

Mark: 2/2

Link: https://drive.google.com/drive/folders/10L0Wr6D-Vt3ewtxUrBhHuSB7H3FuI2zm?usp=dri

ve_link

[Mar 2022 - May 2022] **Cloud and Mobile Technologies**

Group project

Tecnologie Cloud e Mobile - Professor Giuseppe Psaila and Professor Marco Della Vedova

Language: IT

Mark: 10/12

Link: https://github.com/GiuseppeDaidone/unibg-tcm22

[Nov 2021 - Jan 2022] **Management Control System**

Group project

Sistemi di Controllo di Gestione - Professor Mattia Cattaneo and Professor Nicolò Avogadro

Language: IT

Mark: 25/30

Link: https://drive.google.com/drive/folders/1nVj-FShhWFgUkzL9XJCe9C78MGKdnQMJ

[Nov 2021 - Jan 2022] **Software Engineering**

Group project

Ingegneria del Software - Professor angelo Gargantini, Professor Silvia Bonfanti and Professor Patrizia Scandurra

Language: IT

Mark: 5/5

Link: https://github.com/GiuseppeDaidone/IngSwUnibg21

[Feb 2021 - Jun 2021] **DataBase and Web Pages**

Basi di Dati e Web - Professor Stefano Paraboschi

Language: IT

Mark: 2,5/2,5

Link: https://drive.google.com/drive/folders/1RIwBohVqTlAR_OCK51iS85nqk6TtTfOV

[Apr 2021 - Jun 2021] **Statistics Temporal Trend**

Group project

Modelli Stocastici - Professor Francesco Finazzi and Professor Frank Yannick Massoda Tchoussi

Language: IT

Mark: 30 cum laude (33)/30

Link: https://drive.google.com/drive/folders/18_mTkE2T_UWXrwoJp862BO194l7gDrK_

[Feb 2021 - Apr 2021] **Statistics Advanced Regression and Splines**

Group project

Modelli Stocastici - Professor Francesco Finazzi and Professor Frank Yannick Massoda Tchoussi

Language: IT

Mark: 23/30

Link: https://drive.google.com/drive/folders/1aPVeqVQ8k6ylaBdz6DlTduttgbsYwbYs

Statistics Linear Regression

Group project

Statistica - Professor Alessandro Fassò and Professor Paolo Maranzano
Language: IT
Link: https://drive.google.com/drive/folders/1oLJwyMrtJGXDJvXZyGo_zGUpwnJO0o1v

[Apr 2020 - Jun 2020] **Java Application**

Programmazione ad Oggetti - Professor Angelo Michele Gargantini
Language: IT
Mark: 30/30
Link: https://drive.google.com/drive/folders/1jzC27eUQVOW_i9s3B6yCgbKk3Z6CL8Qq

[Apr 2020 - Jun 2020] **Java Thread Sync**

Sistemi Operativi - Professor Patrizia Scandurra
Language: IT
Mark: 12,5/13
Link: https://drive.google.com/drive/folders/1Ur33Y6wuwLzNzJWGHvQiDnECqwhmi2Yv

[Apr 2020 - May 2020] **MIPS Assembly**

Group project
Calcolatori Elettronici - Professor Giuseppe Coldani
Language: IT
Mark: 2/2
Link: https://drive.google.com/drive/folders/1ta9rkFsiaxVVb-mrefsS5lDQoDuZLLpO

NETWORKS AND MEMBERSHIPS

[1 Feb 2026 - Current] **Società Italiana di Intelligence (SOCINT)**

Associate

[1 Apr 2026 - Current] **ACM SIGMM**

Member

LANGUAGE SKILLS

Mother tongue(s): Italian

Other language(s):

English

LISTENING: C2 **READING:** C2 **WRITING:** C2

SPOKEN PRODUCTION: C2 **SPOKEN INTERACTION:** C2

French

LISTENING: A2 **READING:** A2 **WRITING:** A2

SPOKEN PRODUCTION: A2 **SPOKEN INTERACTION:** A2

LICENSES AND CERTIFICATIONS

[Sep 2025] **IBM - Security Operations Center**

Link:
https://www.credly.com/badges/ae2e53ca-3be1-473f-9cc0-29a378d97c29/public_url

[Sep 2025] **IBM - Threat Intelligence and Hunting**

Link:
https://www.credly.com/badges/5fdd71c8-aaef-4999-9eed-9ca5eb532cad/public_url

[Sep 2025] **IBM - Quantum Enigmas**

Link:
https://www.credly.com/badges/6072743d-fcc8-4d9f-9da8-7ad9c0c8ea1e/public_url

[Apr 2025] **IBM - Cyber Academy Fundamentals**

ID: URL-2AFFFF0091A3

Link:
https://skills.yourlearning.ibm.com/certificate/share/ba5d15b27cewogICJvYmplY3RJZCIgOiAiVVJMLTJBRkZGRjAwOTFBMyIsCiAgImxlYXJuZXJDTlVNIiA6ICI0NTUwOTY1UkVHIiwKICAib2JqZWN0VHlwZSIgOiAiQUNUSVZJVFkiCn00bd9f5b1b0-10

[Sep 2021] **Criminal Psychology Fundamentals**

Course by Margit Averdijk.

[Sep 2021] **Guide to sqlmap**

Course by Cybr.

[Sep 2021] **Ethical hacking with Hak5 devices**

Course by David Bombal.

[Sep 2021] **Fundamentals of Computer Hacking**

Course by infySEC.

[Sep 2021] **Introduction to OS Command Injection**

Course by Cybr.

[Sep 2021] **A.I. (Artificial Intelligence)**

Course by Nikola Milosevic.

[Sep 2021] **SQL Injection Attacks**

Course by Cybr.

[Sep 2021] **Introduction to Application Security (AppSec)**

Course by Cybr.

[Oct 2019] **Google - Digital Marketing**

ID: FR3 DS4 ZBH

Link: https://learndigital.withgoogle.com/digitaltraining/validate-certificate-code

[May 2019] **ESOL International I**

ID: 601/5516/4

[May 2019] **English Certification ISE II**

ID: 601/5516/4

[Sep 2017] **EF English Education First B1 - online test**

[Jun 2017 - Jul 2020] **ECDL Full Standard Certification**

[Mar 2017] **Corso di Formazione su "Salute e Sicurezza nei Luoghi di Lavoro"**

ID: 2308/ll-h

[Feb 2017 - Mar 2019] **CSE / Salvamento Agency - Basic Life Support with Defibrillation Certification**

[Feb 2017] **Certification of General English Standard at Cambridge Study Centre course - level B2**

HONOURS AND AWARDS

[31 Dec 2024] **Borsa di Studio (Scholarship) DiSCo Lazio - a.y. 2024/2025 Awarding institution:** DiSCo Lazio

[31 Mar 2024] **Borsa di Studio (Scholarship) DiSCo Lazio - a.y. 2023/2024 Awarding institution:** DiSCo Lazio

[30 Nov 2022] **Borsa di Studio (Scholarship) Università degli Studi di Bergamo - a.a. 2021/2022 Awarding institution:** Università degli Studi di Bergamo

[31 Dec 2021] **Borsa di Studio (Scholarship) Università degli Studi di Bergamo - a.a. 2020/2021 Awarding institution:** Università degli Studi di Bergamo

[30 Mar 2021] **Borsa di Studio (Scholarship) Università degli Studi di Bergamo - a.a. 2019/2020 Awarding institution:** Università degli Studi di Bergamo