Prof. Ing. Davide Maiorca, Ph.D., Professore Associato[a]

[a]Ultimo aggiornamento: maggio 2025

Informazioni di contatto	Università degli Studi di Cagliari	Telefono: +39 070 675 5758
	Dipartimento di Ingegneria Elettrica ed Elettronica	Fax: +39 070 675 5782
	Research Director @ Joint Lab on Safety and Security of AI (sAIfer Lab)	https://saiferlab.ai/people/davidemaiorca
	Direttore @ ICT4Law and Forensics Lab	https://sites.unica.it/ict4lawforensics
	Piazza d'Armi, 09123, Cagliari, Italia	davide.maiorca@unica.it

Interessi di ricerca: **Analisi e rilevamento di malware su piattaforme Android, X86 e IoT**; **Sicurezza IoT**; **Rilevamento di malware in documenti e contenuti multimediali (PDF, Office, JavaScript)**; **Adversarial Machine Learning**; **Sicurezza Web**.

Formazione

Università degli Studi di Cagliari, Cagliari, Italia

Dottorato di ricerca (Doctor Europaeus), Ingegneria Elettronica, marzo 2016

- Tesi: *Design and Implementation of Robust Systems for Secure Malware Detection*
- Relatore: Prof. Giorgio Giacinto
- Coordinatore del corso di dottorato: Prof. Fabio Roli
- Revisori esterni: Prof. Urko Zurutuza (Mondragon University, Spagna) e Prof. Edgar Weippl (TU Wien, Austria)
- Tesi premiata tra le migliori tesi italiane in Sicurezza Informatica nel 2016 da CLUSIT (Associazione Italiana per la Sicurezza Informatica)

Laurea Magistrale, Ingegneria Elettronica, febbraio 2012

- Votazione finale: 110/110, *e lode*
- Tesi: *A Pattern Recognition System for Malicious PDF Files Detection*
- Relatore: Prof. Giorgio Giacinto

Laurea Triennale, Ingegneria Elettronica, ottobre 2008

- Votazione finale: 110/110

Liceo Scientifico "Antonio Pacinotti", Cagliari, Italia

Diploma di scuola secondaria superiore, luglio 2004

- Votazione finale: 100/100

Posizioni accademiche

Professore Associato gennaio 2025 - Presente
Dipartimento di Ingegneria Elettrica ed Elettronica
Università degli Studi di Cagliari

Ricercatore a tempo determinato di tipo B (RTD-B) gennaio 2022 - dicembre 2024
Dipartimento di Ingegneria Elettrica ed Elettronica
Università degli Studi di Cagliari

Ricercatore a tempo determinato di tipo A (RTD-A) agosto 2019 - dicembre 2021
Dipartimento di Ingegneria Elettrica ed Elettronica
Università degli Studi di Cagliari
Abilitazione Scientifica Nazionale (ING-INF/05) conseguita nel 2021 per il ruolo di Professore Associato

Assegnista di ricerca marzo 2016 - luglio 2019
Dipartimento di Ingegneria Elettrica ed Elettronica
Pattern Recognition and Applications Lab

Dottorando di ricerca gennaio 2013 - marzo 2016
Dipartimento di Ingegneria Elettrica ed Elettronica
Pattern Recognition and Applications Lab
Supervisore: Prof. Giorgio Giacinto

Dottorando in visita novembre 2013 - aprile 2014
Systems Security Group
Ruhr-University of Bochum
Supervisore: Prof. Dr. Thorsten Holz

Assistente di ricerca febbraio 2012 - dicembre 2012
Dipartimento di Ingegneria Elettrica ed Elettronica
Pattern Recognition and Applications Lab
Supervisore: Prof. Giorgio Giacinto

PUBBLICAZIONI CON PEER REVIEW

1. L. Minnei, G. Piras, A. Sotgiu, M. Pintor, A. Demontis, **D. Maiorca**, B. Biggio. *An Experimental Analysis of Semi-supervised Learning for Malware Detection.* In Proceedings of the Joint National Conference on Cybersecurity (ITASEC & SERICS), 2025.
2. A. Sanna, D. Canavese, L. Regano, **D. Maiorca**, G. Giacinto. *Exposing the Cracks: A Case Study on the Quality of Public Linux Malware Data Sets.* In Proceedings of the Joint National Conference on Cybersecurity (ITASEC & SERICS), 2025.
3. D. Soi, S. L. Sanna, A. Liguori, M. Zuppelli, L. Regano, **D. Maiorca**, L. Caviglione, G. Manco, G. Giacinto. *On the Feasibility of Android Stegomalware: A Detection Study.* In Proceedings of the Joint National Conference on Cybersecurity (ITASEC & SERICS), 2025.
4. L. Pisu, F. Loi, **D. Maiorca**, G. Giacinto. *HTTP/3 will not Save you from Request Smuggling: A Methodology to Detect HTTP/3 Header (mis)Validations.* In Proceedings of the 22nd International Symposium on Network Computing and Applications (NCA), 2024.
5. S. L. Sanna, D. Soi, **D. Maiorca**, G. Fumera, and G. Giacinto. *A Risk Estimation Study of Native Code Vulnerabilities in Android Applications.* In Journal of Cybersecurity, 2024.
6. A. Sanna, F. Cara, **D. Maiorca**, and G. Giacinto. *Oblivion: an open-source system for large-scale analysis of macro-based office malware.* In Journal of Computer Virology and Hacking Techniques, 2024.
7. L. Binosi, P. Mazzini, A. Sanna, M. Carminati, G. Giacinto, R. Lazzeretti, S. Zanero, M.Polino, E. Coppa and **D. Maiorca**. *Do You Trust Your Device? Open Challenges in IoT Security Analysis.* in 21th International Conference on Security and Cryptography (SECRYPT), 2024.
8. E.Massidda, L. Pisu, **D. Maiorca** and G. Giacinto. *Bringing Binary Exploitation at Port 80: Understanding C Vulnerabilities in WebAssembly.* in 21th International Conference on Security and Cryptography (SECRYPT), 2024.
9. D. Soi, L. Regano, **D. Maiorca**, G. Giacinto, and H. Berger. *Can You See It? -NOP! A Practitioners Study.* Poster at Symposium on Usable Privacy and Security (SOUPS) 2024.
10. D. Soi, A. Sanna, **D. Maiorca**, and G. Giacinto. *Enhancing android malware detection explainability through function call graph APIs* in Journal of Information Security and Applications (JISA), vol. 80, February 2024.

11. M. Pintor, G. Orrù, **D. Maiorca**, A. Demontis, L. Demetrio, G.L. Marcialis, B. Biggio, F. Roli. *Cybersecurity and AI: The PRALab Research Experience.* In 3rd Italian CINI Conference on Artificial Intelligence (ITAL-IA), Pisa (Italy), 2023.

12. B. Pala, L. Pisu, S. L. Sanna, **D. Maiorca** and G. Giacinto. *A Targeted Assessment of Cross-Site Scripting Detection Tools.* in 7th Italian Conference on CyberSecurity (ITASEC), 2023.

13. L. Borzacchiello, E. Coppa, **D. Maiorca**, A. Columbu, C. Demetrescu, and G. Giacinto. *Reach Me if You Can: On Native Vulnerability Reachability in Android Apps*, in 27th European Symposium on Research in Computer Security (ESORICS), 2022.

14. A. Janovsky, **D. Maiorca**, D. Macko, V. Matyas, and G. Giacinto. *A Longitudinal Study of Cryptographic API: A Decade of Android Malware*, in 19th International Conference on Security and Cryptography (SECRYPT), 121-133, 2022.

15. F. Meloni, A. Sanna, **D. Maiorca** and G. Giacinto. *Extended Abstract: Effective Call Graph Fingerprinting for the Analysis and Classification of Windows Malware*, in 19th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), Springer, Cagliari, pp. 42-52, 2022.

16. M. Melis, M. Scalas, A. Demontis, **D. Maiorca**, B. Biggio, G. Giacinto, F. Roli. *Do gradient-based explanations tell anything about adversarial robustness to android malware?* in International Journal of Machine Learning and Cybernetics 13(1), 217-232, 2022.

17. G. M. Malandrone, G. Virdis, **D. Maiorca** and G. Giacinto. *PowerDecode: A PowerShell Script Decoder Dedicated to Malware Analysis*, in 5th Italian Conference on CyberSecurity (ITASEC), 2021.

18. F. Cara, M. Scalas, G. Giacinto and **D. Maiorca**. *On the Feasibility of Adversarial Sample Creation Using the Android System API*, in Information (MDPI) – Special Issue - New Frontiers in Android Malware Analysis and Detection, 2020.

19. **D. Maiorca**, A. Demontis, B. Biggio, F. Roli, and G. Giacinto. *Adversarial Detection of Flash Malware: Limitations and Open Issues*, in Computers and Security, vol 96, 2020.

20. **D. Maiorca**, B. Biggio and G. Giacinto. *Towards Adversarial Malware Detection: Lessons Learned from PDF-based Attacks*, in ACM Computing Surveys, vol. 52, n. 4, 2019.

21. M. Scalas, **D. Maiorca**, F. Mercaldo, C. Aaron Visaggio, F. Martinelli, and G. Giacinto. *On the Effectiveness of System API-Related Information for Android Ransomware Detection*, in Computers and Security, vol 86, pp. 162-182, 2019.

22. D. Ugarte, **D. Maiorca**, F. Cara, and G. Giacinto. *PowerDrive: Accurate De-Obfuscation and Analysis of PowerShell Malware*, in 16th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), Sprin- ger, Gothenburg, Sweden, pp. 240-259, 2019.

23. A. Demontis, M. Melis, B. Biggio, **D. Maiorca**, D. Arp, K. Rieck, I. Corona, G. Giacinto, and F. Roli, *Yes, Machine Learning Can Be More Secure! A Case Study on Android Malware Detection*, in IEEE Transactions on Dependable and Secure Computing, vol 16, n° 4, pp. 711-724, 2019.

24. **D. Maiorca** and B. Biggio, *Digital Investigation of PDF Files: Unveiling Traces of Embedded Malware*, in IEEE Security and Privacy: Special Issue on Digital Forensics, vol 17, n. 1, pp. 63-71, 2019.

25. B. Kolosnjaji, A. Demontis, B. Biggio, **D. Maiorca**, G. Giacinto, C. Eckert, and F. Roli, *Adversarial Malware Binaries: Evading Deep Learning for Malware Detection in Executables*, in 26th European Signal Processing Conference (EUSIPCO '18), 2018.

26. M. Melis, **D. Maiorca**, B. Biggio, G. Giacinto, and F. Roli, *Explaining Black-box Android Malware Detection*, in 26th European Signal Processing Conference (EUSIPCO '18), 2018.

27. **D. Maiorca**, F. Mercaldo, G. Giacinto. A. Visaggio, F. Martinelli. *R-PackDroid: API Package-Based Characterization and Detection of Mobile Ransomware*, in 32th ACM Symposium on Applied Computing (SAC), Marrakech (Morocco), 2017.

28. **D. Maiorca**, P. Russu, I. Corona, B. Biggio and G. Giacinto. *Detection of Malicious Scripting Code through Discriminant and Adversary-Aware API Analysis*, in 1st Italian Conference on CyberSecurity (ITASEC), 17-20th January 2017, Venice (Italy).

29. J.Hoffmann, T. Rytilahti, **D. Maiorca**, M. Winandy, G. Giacinto and T. Holz. *Evaluating Analysis Tools for Android Apps: Status Quo and Robustness against Obfuscation*, in Proceedings of the 6th ACM Conference on Data and Application Security and Privacy (CODASPY 2016), March 9-11th 2016, New Orleans (USA).

30. T. Hupperich, **D. Maiorca**, M. Kührer, T. Holz, and G. Giacinto, *On the Robustness of Mobile Device Fingerprinting*, in 31st Annual Computer Security and Applica- tions Conference (ACSAC 2015), 7-10th December 2015, Los Angeles, USA, pp. 191-200.

31. M. Aresu, D. Ariu, M. Ahmadi, **D. Maiorca**, and G. Giacinto, *Clustering Android Malware Families by Http Traffic*, in 10h International Conference on Malicious and Unwanted Software (MALCON 2015), October 20-22th 2015, Fajar- do, Puerto Rico, USA.

32. **D. Maiorca**, D. Ariu, I. Corona, and G. Giacinto, *An Evasion Resilient Approach to the Detection of Malicious PDF Files*, in Information Systems Security and Privacy (Communication in Computer and Information Science), vol 576, Springer, 2015, pp. 68-85.

33. **D. Maiorca**, D. Ariu, I. Corona, M. Aresu, and G. Giacinto, *Stealth Attacks: An Extended Insight into the Obfuscation Effects on Android Malware*, Computers And Security (Elsevier), vol 51 (June), pp. 16-31, 2015.

34. **D. Maiorca**, D. Ariu, I. Corona, and G. Giacinto, *A Structural and Content-Based Approach for a Precise and Robust Detection of Malicious PDF Files*, Proceedings of the 1st International Conference on Information Systems Security and Privacy (ICISSP), 9-11th February 2015, Angers, France, pp. 27-36.

35. I. Corona, **D. Maiorca**, D. Ariu, and G. Giacinto, *Lux0R: Detection of Malicious PDF-embedded JavaScript code through Discriminant Analysis of API References*, in AISec'14: Proceedings of the 2014 ACM Workshop on Artificial Intelligence and Security, co-located with CCS '14, Scottdale, Arizona, USA, 2014.

36. B. Biggio, I. Corona, B. Nelson, B. I. P. Rubinstein, **D. Maiorca**, G. Fumera, G. Giacinto, and F. Roli, *Security Evaluation of Support Vector Machines in Adversarial Environments*, in Support Vector Machines Applications, Y. Ma e Guo, G. Springer International Publishing, 2014, pp. 105-153.

37. B. Biggio, I. Corona, **D. Maiorca**, B. Nelson, N. Srndic, P. Laskov, G. Giacinto, and F. Roli, *Evasion attacks against machine learning at test time*, in European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD), 2013, vol 8190, pagg 387-402.

38. **D. Maiorca**, I. Corona, and G. Giacinto, *Looking at the Bag is not Enough to Find the Bomb: an Evasion of Structural Methods for Malicious PDF Files Detection*, in 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS), Hangzhou, China, 2013.

39. **D. Maiorca**, G. Giacinto, and I. Corona, *A Pattern Recognition System for Malicious PDF Files Detection*, in MLDM - International Conference on Machine Learning and Data Mining, Berlin, 2012, vol 7376, pp. 510-524.

Attività scientifiche

Workshop Chair
- *The 1st Italian Workshop on Capture the Flag for Work (CTF-W) co-Located with ITASEC & SERICS 2025*
- *The 2nd Italian Cyberchallenge.it Workshop, 2024*

Responsabile dell'organizzazione locale
- *The 19th Conference on Detection of Intrusions and Malware & Vulnerability Assessment* (DIMVA 2022)

Guest Editor
- Special Issue - *New Frontiers in Android Malware Analysis and Detection* per la rivista *Information* (MDPI)

Membro del comitato editoriale
- *Information Security Journal: A Global Perspective* (Taylor Francis)
- *Journal of Computer Virology and Hacking Techniques* (Springer)
- *Frontiers in Computer Science - Computer Security*

Membro del Program Committee (conferenze)
- *IEEE Globecom IoTSN*, 2025
- *Digital Forensics Conference Europe (DFRWS)*, 2025
- *APWG Tech Summit*, 2025
- *ACM Symposium on Applied Computing* (Software Protection and Reverse Engineering Track), 2025
- *ACM Conference on Computer and Communications Security (CCS) 2024*
- *Annual Computer Security and Applications Conference* (ACSAC) (2019 e 2022-2025, insieme all'Artifacts Evaluation Committee)
- *6th Italian Conference on CyberSecurity* (ITASEC), 2022-2025
- *European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases* (ECML PKDD) – Journal Track, 2021-2022
- *ACM International Conference on Information Technology for Social Good* (GOODIT), 2021
- *ACM Symposium on Applied Computing* (IoT Track) 2018-2020

Membro del Program Committee (workshop)
- *Workshop on Sustainable security and Awareness For nExt generation infRastructures* (SAFER - Co-located with ARES), 2025.

- *Workshop on Rethinking Malware Analysis* (WORMA - Co-Located with IEEE Euro S&P), 2024-2025
- *Workshop on Machine Learning for CyberSecurity* (MLCS - Co-located with ECML PKDD), 2022-2023-2024
- *Deep Learning Security and Privacy Workshop* (DLSP - Co-Located with IEEE S&P), 2023-2024
- *Private, Secure, Trustworthy AI workshop* (PriST-AI - Co-Located with ESORICS), 2023
- *ACM Workshop on Robust Malware Analysis* (WORMA - Co-located with ACM ASIACCS), 2022-2024
- *ACM Workshop on Artificial Intelligence and Security* (AISEC - Co-located with ACM CCS) 2017-2023
- *1st European Workshop on Cyber Security Education and Practice* (CSEP - Co-located with IEEE Euro Security and Privacy)

Membro dello Student Program Committee

- *37th IEEE Symposium on Security and Privacy* (IEEE S&P) (2016)

Revisore per riviste

- *ACM Transactions on Privacy and Security* (TOPS) - **Distinguished Reviewer**
- *ACM Computing Surveys*
- *IEEE Transactions on Secure and Dependable Computing*
- *IEEE Transactions on Information Forensics and Security*
- *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*
- *IEEE Transactions on Neural Networks and Learning Systems*
- *IEEE Transactions on Artificial Intelligence*
- *Computers and Security*, Elsevier
- *Journal of Information Security and Applications*, Elsevier
- *Journal of Parallel and Distributed Computing*, Elsevier
- *International Journal on Machine Learning and Cybernetics*, Elsevier
- *IEEE Access*
- *Future Generation Computer Systems*, Elsevier
- *Journal of Systems and Software*, Elsevier
- *Applied Computing and Informatics*, Elsevier
- *Security Informatics*
- *Journal of Cybersecurity*, Oxford Academic

External Sub-Reviewer

- *1st Italian Conference on CyberSecurity* (ITASEC 2017)
- *8th ACM Workshop on Artificial Intelligence and Security* (AISEC 2015)

Relazioni a conferenze

Presentazioni

- Italian Cybercrime Conference (2024)
- 16th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2019)
- 3rd Italian Conference on CyberSecurity (ITASEC 2019)
- 2nd Italian Conference on CyberSecurity (ITASEC 2018)
- 32th ACM Symposium on Applied Computing (SAC 2017)
- 1st International Conference on Information Systems Security and Privacy (ICISSP 2015)
- 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013)

Interventi su invito

- *Keynote speaker* al 2th Workshop on Machine Learning for CyberSecurity (Co-located with ECML PKDD 2020).

Progetti

Principal Investigator

- SETA. *Studying thE impact of anti-analysis Techniques in IoT security evAluations.* Finanziato dal Ministero dell'Università e della Ricerca nell'ambito del bando PRIN (Progetti di Ricerca di Rilevante Interesse Nazionale) attraverso il Piano Nazionale di Ripresa e Resilienza (PNRR). Budget 230, 000€, tasso di accettazione 16%. 2024-2026.

WP Leader

- SERICS. (*Security and Rights in the CyberSpace - Spoke 3 - COVERT*). Finanziato dal Ministero dell'Università e della Ricerca nell'ambito del bando PRIN (Progetti di Ricerca di Rilevante Interesse Nazionale) attraverso il Piano Nazionale di Ripresa e Resilienza (PNRR). 2024-2026.
- SUSTAIN. *Flexible Sensors for secUre and TruSTed crowdsensing environmentAl applicatIoNs.* Finanziato dalla Regione Autonoma della Sardegna. 2023-2025.
- INSIEME. *Intelligent Systems for Integrated Health Management* (2017-2021) – Horizon 2020 – PON 2014/2020 (responsabile dell'unità di lavoro sull'obiettivo 4 - sviluppo del modulo di sicurezza e del supporto server-side).

Project Manager

- PISDAS. *Piattaforma Integrata Servizi Digitali Avanzati Sicuri.* Finanziato dalla Regione Autonoma della Sardegna. Cofinanziato dall'Unione Europea - FESR 2007-2013 (Project Manager per l'Università degli Studi di Cagliari).
- INCLOSEC. *Innovery Cloud Security.* Finanziato dalla Regione Autonoma della Sardegna. Cofinanziato dall'Unione Europea - FESR 2014-2020 (Project Manager per l'Università degli Studi di Cagliari).
- INN-BEDAE. *Innovery Big Energy Data Analytics Efficiency.* Finanziato dalla Regione Autonoma della Sardegna. Cofinanziato dall'Unione Europea - FESR 2014-2020 (Project Manager per l'Università degli Studi di Cagliari).

Esperienza didattica

Docente titolare (corsi)

- Web Security and Malware Analysis (60 ore - 6 CFU) — 2019-Presente
  Laurea Magistrale in Ingegneria Informatica,
  Cybersecurity and Artificial Intelligence,
  Dipartimento di Ingegneria Elettrica ed Elettronica,
  Università degli Studi di Cagliari, Italia
- Computer Forensics Techniques (30 ore - 5 CFU) — 2019-Presente
  Laurea Magistrale in Ingegneria Informatica,
  Cybersecurity and Artificial Intelligence,
  Dipartimento di Ingegneria Elettrica ed Elettronica,
  Università degli Studi di Cagliari, Italia
- Cybersecurity (25 ore - 5 CFU) — 2022-Presente
  Master universitario di secondo livello in Digitalizzazione del Sistema Elettrico per la Transizione Energetica,
  Università degli Studi di Cagliari e Terna SpA

Docente titolare (seminari)

- Reverse Engineering and Low-Level Program Analysis (Seminario - 24 ore - 3 CFU) — 2019-Presente
  Corso di Dottorato in Ingegneria Elettronica e Informatica,
  Dipartimento di Ingegneria Elettrica ed Elettronica,
  Università degli Studi di Cagliari, Italia
- Introduction to Web Security and Mobile Forensics (8 ore) — 2022
  Master universitario di secondo livello in Security Awareness,
  Università degli Studi di Cagliari, Italia

- Mobile Security (seminario) 2016-2017
  Laurea Magistrale in Ingegneria Elettronica,
  Dipartimento di Ingegneria Elettrica ed Elettronica,
  Università degli Studi di Cagliari, Italia

Assistente alla didattica

- Computer Security 2016-2017
  Docente: Prof. Giorgio Giacinto,
  Laurea Magistrale in Ingegneria Elettronica,
  Dipartimento di Ingegneria Elettrica ed Elettronica,
  Università degli Studi di Cagliari, Italia
- Operating Systems 2014-2017
  Docente: Prof. Giorgio Giacinto,
  Laurea Magistrale in Ingegneria Elettronica,
  Dipartimento di Ingegneria Elettrica ed Elettronica,
  Università degli Studi di Cagliari, Italia
- Calcolatori Elettronici 2012
  Docente: Prof. Fabio Roli
  Laurea Triennale in Ingegneria Elettronica,
  Dipartimento di Ingegneria Elettrica ed Elettronica,
  Università degli Studi di Cagliari, Italia

Assistente per attività di facoltà

- Dipartimento di Ingegneria Elettrica ed Elettronica 2011
  Università degli Studi di Cagliari, Italia

Supervisione di studenti e ricerca

Supervisore di dottorato

- Aurora Arrus, Dottorato Nazionale in CyberSecurity, IMT Lucca, 2024-2027.
- Nicola Deidda, Dottorato Nazionale in CyberSecurity, IMT Lucca, 2024-2027.
- Luca Minnei, Dottorato in Ingegneria Elettronica e Informatica, Università degli Studi di Cagliari, 2024-2027.
- Diego Soi, Dottorato in Ingegneria Elettronica e Informatica, Università degli Studi di Cagliari, 2023-2026.
- Lorenzo Pisu, Dottorato in Ingegneria Elettronica e Informatica, Università degli Studi di Cagliari, 2022-2025.
- Alessandro Sanna, Dottorato in Ingegneria Elettronica e Informatica, Università degli Studi di Cagliari, 2021-2024.

Relatore di tesi

- Federico Moro, *A Comprehensive Study and Tool for Android Memory Analysis*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2024-2025.
- Marta Maria Cossu, *Tools and Techniques for the Acquisition and the Forensic Analysis of Photographic Metadata in iOS*, Laurea Triennale in Ingegneria Elettrica, Elettronica e Informatica, A.A. 2024-2025.
- Bruno Pinna, *Dynamic Malware Analysis in Android: Design and Implementation of the Fridroid Framework*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2024-2025.
- Antonio Aracri, *On the Reliability of Volatile Memory Forensics*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2024-2025.
- Pierangelo Loi, *Exploring the Borderline: A Study on the Behavior and the Detection of Grayware.*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2023-2024.
- Antonio Campus, *Diving into UEFI bootkits: practical implementation of attacks against Bootloaders*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2023-2024.

- Aurora Arrus, *Advanced Emulation-Based Analysis of Linux Malware*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2023-2024.
- Maria Chessa, *Securing Against Ransomware: A Study on the Effectiveness of Detection and Mitigation Tools*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2023-2024.
- Emmanuele Massidda, *Bringing Binary Exploitation to Port 80: Understanding C Vulnerabilities in WebAssembly*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2023-2024.
- Matteo Asuni, *Effective Graphical Visualization of Vulnerabilities in C and C++ Programs* , Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2023-2024.
- Amal Golli, *A Comprehensive Analysis of Cloud Security Posture Management Practices*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2022-2023.
- Nicola Crobu, *An Ethical Dilemma: Study and Categorization of Deceptive Android Applications*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2022-2023.
- Maria Jose Baffigo, *Study And Analysis of Automatic Unpacking Techniques for Malware Detection*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2021-2022.
- Bruno Pala, *Analysis and Evaluation of Web Application Vulnerability Scanners against Cross Site Scripting*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2021-2022.
- Gianluca Pala, *On the Effectiveness of Graphs for Android Malware Detection*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2021-2022.
- Diego Soi, *An Explainable Deep Learning approach for the detection of Android Malware*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2021-2022.
- Federico Loi, *Are Italian.tweets safe? Study and analysis of Italian URLs on Twitter*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2021-2022.
- Lorenzo Pisu, *A security assessment of the server-side template injection vulnerability*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2021-2022.
- Silvia Lucia Sanna, *A risk estimation study of native code vulnerabilities in Android applications*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2020-2021.
- Luca Minnei, *Study and analysis of Adware applications on the Android platform*, Laurea Triennale in Informatica, A.A. 2020-2021.
- Filippo Pitzalis, *Study and Analysis of Native Libraries Embedded in Android Malware*, Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2019-2020.
- Luca Puzzoni, *Studio ed Analisi di Librerie Crittografiche impiegate da Malware Android*. Laurea Triennale in Informatica, A.A. 2019-2020.
- Alessandro Sanna, *Dynamic Analysis and Instrumentation of Interaction-based Office Malware*. Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2019-2020.
- Francesco Meloni, *Advanced Call Graph Fingerprinting for the Analysis and Classification of Windows Malware*. Laurea Magistrale in Ingegneria Informatica, CyberSecurity and Artificial Intelligence, A.A. 2019-2020.
- Giuseppe Malandrone, *Studio e Sviluppo di un Rilevatore di Attacchi Avanzati Basati su PowerShell*. Laurea Magistrale in Ingegneria Elettronica, A.A. 2018-2019.

Correlatore di tesi

- Laura Pucci, *A Study of Machine Learning-Based Android Malware Detectors*. Relatore: Prof. Giorgio Giacinto. Laurea Triennale in Ingegneria Elettrica, Elettronica e Informatica, A.A. 2018-2019.
- Lorenzo Mulas, *Studio ed analisi di applicazioni grayware nella piattaforma Android*. Relatore: Prof. Giorgio Giacinto. Laurea Triennale in Ingegneria Elettrica, Elettronica e Informatica, A.A. 2018-2019.
- Fabrizio Cara, *Malware Stealth: Studio e Creazione di Attacchi Evasivi Contro Dispositivi Android*. Relatore: Prof. Giorgio Giacinto. Laurea Magistrale in Ingegneria delle Telecomunicazioni, A.A. 2017-2018.
- Michele Scalas, *Study and Development of an Android Application for Automatic Ransomware Detection*. Relatore: Prof. Giorgio Giacinto. Laurea Magistrale in Ingegneria delle Telecomunicazioni, A.A. 2016-2017.
- Alessandro Medda, *Studio e sviluppo di un analizzatore avanzato per la rilevazione di attacchi Flash*. Relatore: Prof. Giorgio Giacinto. Laurea Magistrale in Ingegneria delle Telecomunicazioni, A.A. 2015-2016.
- Efisio Caschili, *Studio ed Implementazione di un sistema di Pattern Recognition per la rilevazione di malware Office*. Relatore: Prof. Giorgio Giacinto. Laurea Magistrale in Ingegneria delle Telecomunicazioni, A.A. 2014-2015.
- Maria Elena Chiappe, *Static Analysis and Detection of Malicious ActionScript Files through Structural and Content-Based Analysis*. Relatore: Prof. Giorgio Giacinto. Laurea Triennale in Ingegneria Elettrica ed Elettronica, A.A. 2014-2015.
- Marco Aresu, *Analysis and Test of Advanced Techniques to the Evasion of Android Malware Detectors*. Relatore: Prof. Giorgio Giacinto. Laurea Magistrale in Ingegneria delle Telecomunicazioni, A.A. 2013-2014.
- Simone Moro, *Advanced Attacks on the Android Platform. Analysis, Development and Implementation of Deliberately Vulnerable Software*. Relatore: Prof. Giorgio Giacinto. Laurea Magistrale in Ingegneria delle Telecomunicazioni, A.A. 2012-2013.
- Luigi Meloni, *Analysis and Detection of Obfuscated Android Malware*. Relatore: Prof. Giorgio Giacinto. Laurea Magistrale in Ingegneria Elettronica, A.A. 2012-2013.
- Antonio Cau, *Analysis of the Mobile Botnets Characteristics and Detection Tools*. Relatore: Prof. Giorgio Giacinto. Laurea Triennale in Ingegneria Elettronica, A.A. 2012-2013.
- Roberta Mameli, *Analysis and Test of Evasion Techniques against PDF Malware Detectors*. Relatore: Prof. Giorgio Giacinto. Laurea Triennale in Ingegneria Elettronica, A.A. 2012-2013.
- Mauro Marongiu, *Development and Test of a System for the Detection of Malicious Javascript Files*. Relatore: Prof. Giorgio Giacinto. Laurea Magistrale in Ingegneria Elettronica, Università degli Studi di Cagliari, Italia. A.A. 2011-2012.

Attività Capture the Flag (CTF)

Fondatore e Presidente dell'associazione Sardinia Len 2024-Presente

CTF Player e Capitano del team Srdnlen 2019-Presente

- Miglior ranking CTFTime: 47° posto (2023, classifica mondiale)
- Secondo posto a Cybercup.it (https://cybercup.it/) nel 2023 e 2024.
- Migliori risultati CTF: 1° posto in K!nd4SUS CTF 2025, HackDay 2025 - Finals, UlisseCTF 2025, Snake CTF 2023; 2° posto in UniVsThreats 25 CTF, HackDay 2025 - Qualifications, Hackappatoi CTF '22 e Team Italy CTF '22; 3° posto in L3akCTF 2024, RITSEC CTF 2023, Killer Queen CTF 2021 e PBjar CTF '21.
- Sito web: `https://srdnlen.it`

Didattica, coaching e organizzazione CTF 2019-Presente

- Responsabile del progetto CyberChallenge.it per l'Università degli Studi di Cagliari (2020-Presente).

- Docente per il progetto CyberChallenge.it per l'Università degli Studi di Cagliari (reverse engineering e binary exploitation) - (2019-Presente)
- Coach del team dell'Università degli Studi di Cagliari per le finali Attack and Defense del progetto CyberChallenge.it (vincitore nel 2021).
- Organizzatore del progetto Cybercup.it (https://cybercup.it) (2023-Presente).
- Organizzatore del Srdnlen CTF (https://ctftime.org/event/1766).
- Trainer per ENISA Team Europe, 2024.
- Trainer per Team Italy, 2024.

ATTIVITÀ AGGIUNTIVE

Visite all'estero

- Docente presso la Jordan University e la Princess Sumaya University of Technology (Computer and Mobile Forensics - febbraio 2020).
- Visiting Researcher presso Masaryk University - Prof. Vashek Matyas (gennaio-febbraio 2020)

Consulenze forensi

- Consulente tecnico di parte (CTP) per procedimenti giudiziari

Affiliazioni

- ACM (2016-Presente)
- IEEE (Student Member 2013-2016, Member 2016-Presente)
- Computer Society (2016-Presente)
- IEEE Systems, Man and Cybernetics (SMC) (2013-Presente)
- CVPL (2013-Presente)
- INSTICC (2022)
- Ordine degli Ingegneri della Provincia di Cagliari (n. 7994) (2013-Presente)

Altri ruoli

- Chair dell'IEEE Cagliari Student Branch (2013-2015)
- Chair dell'IEEE Cagliari Systems, Man and Cybernetics (SMC) Society Chapter (2014-2015)

Autorizzo il trattamento dei dati personali contenuti nel mio curriculum vitae in base al D. Lgs. 196/2003, coordinato con il D. Lgs. 101/2018, e al Regolamento UE 2016/679.