# Michele Carminati

*Curriculum Vitae - Short*

*Politecnico di Milano, DEIB*
*Via Ponzio, 34/5 - 20133 Milano - Italy*
*+39 02 2399-4041*
*michele.carminati@polimi.it*
*Scopus Profile - Google scholar*

## Contents



## Highlights

| | | |
|---|---|---|
| **Research** | *Positions* | Associate Professor, Politecnico di Milano, DEIB (13/01/2025-Today). |
| | | Assistant Professor, Tenure Track (RTD-B), Politecnico di Milano, DEIB (10/2022—01/2025). |
| | | Assistant Professor (RTD-A), Politecnico di Milano, DEIB (03-09/2022). |
| | | Research Assistant & Adjunct Professor, Politecnico di Milano, DEIB (02/2017-02/2022). |
| | *Qualification* | National Scientific Qualification (**ASN**) for the role of Associate Professor in the scientific-disciplinary sector GSD 09/IINF-05 - Information Processing Systems (since 15/06/2023). |
| | *Publications* | 14 journals papers, 11 top-ranked Q1 (SCIMAGO), 2 in class A, and 6 in class B (CORE2020). |
| | | 30 conference papers, 2 in class A++, 1 in class A+, 4 in class A (GSS ranking). |
| | *Bibliometrics* | *Google Scholar*: h-index 17, citations 796 (accessed November 5, 2024). |
| | | *Scopus*: h-index 12, citations 443 (accessed November 5, 2024). |
| | | 72 co-authors (according to Scopus). |
| | *Conf. Activities* | Publication Chair for DIMVA 2023-2025. |
| | | Program Committee: DIMVA 2023–2025, ACM ASIA CCS 2024, ACSAC 2024 |
| **Teaching** | *Lecturer* | *Computer Security*, M.Sc. program at PoliMi (since 2017/18). |
| | | *Advanced Research Topic in Cybersecurity*, Ph.D. program at PoliMi (since 2022/23). |
| | | *Informatica B*, B.Sc. program at PoliMi (since 2022/23). |
| | | *Computer and Network Security*, Cybersecurity Professional Master's Degree ("Master universitario di primo livello") at PoliMi/CEFRIEL (since 2019). |
| | | *Fraud Analysis and Detection*, Cybersecurity Professional Master's Degree ("Master universitario di primo livello") at PoliMi/CEFRIEL (since 2019). |
| | | *Computer and Network Security*, Cybersecurity Professional Master's Degree ("Master universitario di primo livello") at MIP PoliMi (since 2019). |
| | | *AI and Cyber Security*, Cybersecurity Professional Master's Degree ("Master universitario di primo livello") at PoliMi/CEFRIEL (2020). |
| | *Teaching Assist.* | *Digital Forensics and Cybercrime*, M.Sc. program at PoliMi/Bocconi (since 2019/20). |
| | | *Cyber Security Technologies, Procedures, and Policies*, M.Sc. program at PoliMi/Bocconi (since 2019/20). |
| | | *Computer Security*, M.Sc. program at PoliMi (2014-2017). |
| | | *Privacy and Security*, M.Sc. program at PoliMi (2016-2018). |
| | Supervision | Advisor of 3/Co-advisor of 5 Doctoral Students at PoliMi. |
| | | Opponent Member of 3 Doctoral Examination Committees at PoliMi. |
| | | Advisor/Co-advisor of 60+ Master Students at PoliMi. |
| **Projects** | Research | Principal Contact Coordinator (from 2019): RAMSES (HE, 2016-2020). |
| | | Principal Investigator: *AI-RESCUE* (PNRR, 172k€, 2024-2026), *FARE* (PRIN PNRR, 128k€, 2024-2025), *SHIELDED* (PRIN PNRR, 85k€, 2023-2025). |
| | | Investigator: *SOCRATE* (2023-2025), *COVERT* (PNRR 2023-2025), *SETA* (PRIN PNRR, 2023-2025). |
| | Industrial | Principal Investigator: Trenord (15k€, 2024-2025) |
| | | Co-PI: Google.org Impact Challenge: Tech for Social Good (550k€, 2023-2025), Trenord (2022-2023), Napier Ltd. (previously Fortytwo Data Ltd.) (2017-2019) |
| **Tech. Transfer** | Spinoff | Co-founder of **Banksealer** (in 2016), Spinoff of Politecnico di Milano, delivering novel fraud detection solutions for banking and payment systems |

## Selected Publications

### Peer-Reviewed Journals

2015 **M. Carminati**, R. Caron, F. Maggi, I. Epifani, and S. Zanero, *"BankSealer: A decision support system for online banking fraud analysis and investigation"*. In: *Comput. Secur.*, (2015), doi:10.1016/j.cose.2015.04.002, url: https://doi.org/10.1016/j.cose.2015.04.002. *Citations:* 130 [*Google Scholar*] - 67 [*Scopus*]. *Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 125; [CORE2020] **B**.
**Role**: Primary ideator, investigator, and developer. I designed the tools, experimentally validated the research questions, and authored the paper.
**Research Relevance**: This paper presents a decision support system for online banking fraud analysis, modeling individual spending habits to accurately detect complex fraud patterns, as demonstrated in real-world attack scenarios.

2018 **M. Carminati**, M. Polino, A. Continella, A. Lanzi, F. Maggi, and S. Zanero, *"Security Evaluation of a Banking Fraud Analysis System"*. In: *ACM Trans. Priv. Secur.*, (2018), doi:10.1145/3178370, url: https://doi.org/10.1145/3178370. *Citations:* 43 [*Google Scholar*] - 26 [*Scopus*]. *Ranking:* [Scimago 2023] **Q1**, *SJR* 0.79, *H-index* 26; [CORE2020] **A**.
**Role**: Primary ideator, investigator, and developer, extending previous research with comprehensive data exploration and rigorous experimental evaluation. I developed the tools, validated key research questions, and authored the paper.
**Research Relevance**: This paper presents an in-depth analysis of fraud detection systems, assessing how modeling granularity influences detection performance and resilience against mimicry attacks.

2021 S. Longari, D. H. N. Valcarcel, M. Zago, **M. Carminati**, and S. Zanero, *"CANnolo: An Anomaly Detection System Based on LSTM Autoencoders for Controller Area Network"*. In: *IEEE Trans. Netw. Serv. Manag.*, (2021), doi:10.1109/TNSM.2020.3038991, url: https://doi.org/10.1109/TNSM.2020.3038991. *Citations:* 112 [*Google Scholar*] - 80 [*Scopus*]. *Ranking:* [Scimago 2023] **Q1**, *SJR* 1.76, *H-index* 73; [CORE2020] n.a..
**Role**: Contributed to the conceptualization and methodology design alongside Stefano Longari and assisted in writing through reviews and edits across multiple submission rounds.
**Research Relevance**: This paper presents an intrusion detection system (IDS) using LSTM-autoencoders to detect anomalies in Controller Area Network (CAN) networks. Evaluated on simulated attacks over real-world data, it outperforms state-of-the-art methods.

2022 N. Galloro, M. Polino, **M. Carminati**, A. Continella, and S. Zanero, *"A Systematical and longitudinal study of evasive behaviors in windows malware"*. In: *Comput. Secur.*, (2022), doi:10.1016/J.COSE.2021.102550, url: https://doi.org/10.1016/J.COSE.2021.102550. *Citations:* 54 [*Google Scholar*] - 28 [*Scopus*]. *Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 125; [CORE2020] **B**.
**Role**: Contributed to the conceptualization and design of the methodology, co-advised Nicola Galloro during his Ph.D. and conducted a longitudinal analysis of evasive techniques using OSINT sources. Additionally, I contributed to writing through reviews and edits across multiple submission rounds.
**Research Relevance**: This paper examines malware evasive techniques over a decade, identifying trends and differentiating malware-specific behaviors, offering valuable insights for enhancing security measures.

2022 D. Maffiola, S. Longari, **M. Carminati**, M. Tanelli, and S. Zanero, *"GOLIATH: A Decentralized Framework for Data Collection in Intelligent Transportation Systems"*. In: *IEEE Trans. Intell. Transp. Syst.*, (2022), doi:10.1109/TITS.2021.3123824, url: https://doi.org/10.1109/TITS.2021.3123824. *Citations:* 12 [*Google Scholar*] - 7 [*Scopus*]. *Ranking:* [Scimago 2023] **Q1**, *SJR* 2.58, *H-index* 201; [CORE2020] n.a..
**Role**: Contributed to the conceptualization and design of the methodology alongside Stefano Longari, co-supervised D. Maffiola's master's thesis on framework implementation, and assisted in writing through reviews and edits across multiple submission rounds.
**Research Relevance**: This paper introduces GOLIATH, a blockchain-based framework for decentralized traffic data collection in Intelligent Transportation Systems, enhancing trust and resilience in vehicle data exchange.

2023 T. Paladini, F. Monti, M. Polino, **M. Carminati**, and S. Zanero, *"Fraud Detection under Siege: Practical Poisoning Attacks and Defense Strategies"*. In: *ACM Trans. Priv. Secur.*, (2023), doi:10.1145/3613244, url: https://doi.org/10.1145/3613244. *Citations:* 2 [*Google Scholar*] - 0 [*Scopus*]. *Ranking:* [Scimago 2023] **Q1**, *SJR* 0.79, *H-index* 26; [CORE2020] **A**.
**Role**: Advised T. Paladini during his Ph.D., contributed to the conceptualization and design of the methodology, and supported paper writing through reviews and edits across multiple submission rounds.
**Research Relevance**: This paper investigates adversarial attacks in fraud detection, proposing a novel poisoning attack and an effective countermeasure that mitigates fraud losses, even with limited attacker knowledge.

### Peer-Reviewed Conference Proceedings

2014 **M. Carminati**, R. Caron, F. Maggi, I. Epifani, and S. Zanero. *"BankSealer: An Online Banking Fraud Analysis and Decision Support System"*. In: *ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings*, 2014, doi:10.1007/978-3-642-55415-5_32, url: https://doi.org/10.1007/978-3-642-55415-5_32. *Acceptance Rate: 17.9% (27/151). Citations:* 40 [*Google Scholar*], 22 [*Scopus*]. *Ranking: GGS Class* 3, *GGS Rating* B-, *CORE* B, *LiveSHINE* B , *MA* C [GGS].
**Role**: Primary ideator, investigator, and developer. This tool, as the first output of my Ph.D., was fully developed, validated, and authored by me.
**Research Relevance**: This paper introduces a white-box, semi-supervised approach for online banking fraud detection, utilizing an ensemble of user spending profiles to rank suspicious transactions. Evaluation on real-world data demonstrates that the approach effectively prioritizes complex fraud cases as "top priority."

2020 **M. Carminati**, L. Santini, M. Polino, and S. Zanero. *"Evasion Attacks against Banking Fraud Detection Systems"*. In: *23rd International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2020, San Sebastian, Spain, October 14-15, 2020*, 2020, isbn:978-1-939133-18-2, url: https://www.usenix.org/conference/raid2020/presentation/carminati. *Acceptance Rate: 23.2% (70/302). Citations:* 26 [*Google Scholar*], 18 [*Scopus*]. *Ranking: GGS Class* 1, *GGS Rating* A+, *CORE* A, *LiveSHINE* A+ , *MA* A+ [GGS].
**Role**: Ideator and investigator of This paper, implemented through Luca Santini's master's thesis under my advisorship. I wrote the initial draft and refined the paper through multiple rounds of reviews and edits.
**Research Relevance**: This paper pioneers the application of adversarial machine learning (AML) techniques in banking fraud detection, addressing key challenges and introducing a novel evasion attack approach. It evaluates the security of several state-of-the-art fraud detection systems across varying levels of attacker knowledge.

2020 A. Erba, R. Taormina, S. Galelli, M. Pogliani, **M. Carminati**, S. Zanero, and N. O. Tippenhauer. *"Constrained Concealment Attacks against Reconstruction-based Anomaly Detectors in Industrial Control Systems"*. In: *ACSAC '20: Annual Computer Security Applications Conference, Virtual Event / Austin, TX, USA, 7-11 December, 2020*, 2020, doi:10.1145/3427228.3427660, url: https://doi.org/10.1145/3427228.3427660. *Acceptance Rate: 23.2% (70/302). Citations:* 63 [*Google Scholar*], 34 [*Scopus*]. *Ranking: GGS Class* 2, *GGS Rating* A, *CORE* n.c., *LiveSHINE* A+ , *MA* A+ [GGS].
**Role**: Ideator of the research and supervisor of Dario Ferrari's master's thesis, which focused on implementing the infrastructure for large-scale web-based analysis. I also contributed to writing through reviews and edits across multiple submission rounds.
**Research Relevance**: This paper analyzes popular NoSQL databases to automatically identify misconfigurations that pose security and privacy risks without exposing sensitive data. The study uncovered 12,276 misconfigured databases.

2020 D. Ferrari, **M. Carminati**, M. Polino, and S. Zanero. *"NoSQL Breakdown: A Large-scale Analysis of Misconfigured NoSQL Services"*. In: *ACSAC '20: Annual Computer Security Applications Conference, Virtual Event / Austin, TX, USA, 7-11 December, 2020*, 2020, doi:10.1145/3427228.3427260, url: https://doi.org/10.1145/3427228.3427260. *Acceptance Rate: 25.6% (31/121). Citations:* 15 [*Google Scholar*], 9 [*Scopus*]. *Ranking: GGS Class* 2, *GGS Rating* A, *CORE* n.c., *LiveSHINE* A+ , *MA* A+ [GGS].
**Role**: Ideator of the research and supervisor of Dario Ferrari's master thesis, which focused on implementing the infrastructure for large-scale web-based analysis. Also contributed to writing through reviews and edits across submission rounds.
**Research Relevance**: This paper examines popular NoSQL databases to automatically identify misconfigurations that pose security and privacy risks, without exposing sensitive data. The study uncovered 12,276 misconfigured databases.

2022 A. d. F. Tron, S. Longari, **M. Carminati**, M. Polino, and S. Zanero. *"CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks"*. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, 2022, doi:10.1145/3548606.3560618, url: https://doi.org/10.1145/3548606.3560618. *Acceptance Rate: 22.3% (879/196). Citations:* 22 [*Google Scholar*], 11 [*Scopus*]. *Ranking: GGS Class* 1, *GGS Rating* A++, *CORE* A++, *LiveSHINE* A++ , *MA* A++ [GGS].
**Role**: Contributed to conceptualizing the final approach to achieve the research goals explored in A. d. F. Tron's master's thesis and supported the paper's development through reviews and edits across multiple submission rounds.
**Research Relevance**: This paper introduces CANflict, a technique for executing stealthy CAN bus attacks from a compromised ECU, uncovering critical link-layer vulnerabilities and informing advancements in automotive security.

2023 T. Paladini, M. d. L. Bernasconi, **M. Carminati**, M. Polino, F. Trovò, and S. Zanero. *"Advancing Fraud Detection Systems Through Online Learning"*. In: *Machine Learning and Knowledge Discovery in Databases: Applied Data Science and Demo Track - European Conference, ECML PKDD 2023, Turin, Italy, September 18-22, 2023, Proceedings, Part VI*, 2023, doi:10.1007/978-3-031-43427-3_17, url: https://doi.org/10.1007/978-3-031-43427-3_17. *Acceptance Rate: 24% (58/241). Citations:* 3 [*Google Scholar*], 1 [*Scopus*]. *Ranking: GGS Class* 2, *GGS Rating* A, *CORE* A, *LiveSHINE* A+ , *MA* A [GGS].
**Role**: Advised T. Paladini during his Ph.D., contributing to the conceptualization and design of the methodology, and supported the paper's development through reviews and edits across multiple submission rounds.
**Research Relevance**: This paper introduces an adaptive online learning approach for fraud detection, enhancing resilience against evolving attacker behaviors in financial transactions.

# Michele Carminati

*Curriculum Vitae et Studiorum*

*Politecnico di Milano, DEIB*
*Via Ponzio, 34/5 - 20133 Milano - Italy*
*+39 02 2399-4041*
*michele.carminati@polimi.it*
*Scopus Profile - Google scholar*

## Short Biography

I received my Ph.D. degree *cum laude* in Information Technology from the Politecnico di Milano, Italy, where I am currently an Associate Professor as part of the System Security group within the Dipartimento di Elettronica, Informazione e Bioingegneria. My research primarily focuses on applying **Machine Learning** (ML) and **Artificial Intelligence** (AI) techniques to the field of **cybersecurity**. Recently, I have also explored the **security of machine learning models** and the application of **federated learning** to cybersecurity. I am actively involved in research projects funded by the European Union and co-founded Banksealer, a Fintech spin-off of the Politecnico di Milano.

## Research Interest

My research is positioned within the field of **cybersecurity**, focusing on the application of **Machine Learning** (ML) and **Artificial Intelligence** (AI) techniques across various domains, including *cyber threat intelligence*, *cyber-physical systems*, *automotive security*, *binary and malware analysis*, and *fraud and intrusion detection*.
ML and AI play a crucial role in cybersecurity for several reasons. First, the adversarial nature of the field creates a continuous race between defenders and attackers, who are constantly working to either fix or exploit vulnerabilities. Moreover, the cybersecurity landscape is rapidly evolving due to the rise of financially motivated cybercrime and the increasing complexity and interconnectivity of systems, which make them harder to protect. However, these systems also generate vast, rich datasets, which ML and AI can leverage to address these challenges. My research focuses on applying these techniques to automate the analysis of large-scale datasets related to security phenomena, with the goal of detecting threats, analyzing them, and generating actionable threat intelligence.
Nevertheless, as previously mentioned, we operate in an adversarial environment where determined attackers constantly seek to exploit vulnerabilities in computer systems. Adversaries can manipulate ML models to evade detection and circumvent defenses. This growing area of research, known as **adversarial machine learning**, explores how attackers, with varying degrees of knowledge and access, can carry out different attacks to achieve malicious objectives. Many ML algorithms are not designed with security in mind and may be vulnerable to attacks such as *evasion* or *poisoning* attacks. Therefore, it is critical to consider such threat models when designing and building ML systems for security purposes.
My initial research interest was in **financial fraud detection**, where I focused on analyzing advanced financial threats and developing frameworks for promptly identifying and detecting fraudulent transactions. Subsequently, I transitioned to the **security of machine learning models**, studying the robustness of these models in adversarial settings. More recently, I have also explored the security of **federated learning** systems, which aim to train ML models across multiple decentralized computing nodes that hold local data without sharing it. This approach is particularly relevant in the cybersecurity domain, where data privacy is a significant concern, and data sharing is often restricted due to legal or privacy constraints.

## Education

- **Ph.D. Degree in Information Technology**, *cum laude*. *2013-2017*
  *Institution:* Politecnico di Milano, Milan, Italy.
  *Dissertation Title*: Internet Banking Fraud Analysis and Detection.
  *Advisor:* Prof. Stefano Zanero.
- **M.Sc. (Laurea Magistrale) in Computer Science and Engineering**, *110/110 cum laude*. *2010-2013*
  *Institution:* Politecnico di Milano, Milan, Italy.
  *Advisor:* Prof. Stefano Zanero.
- **B.Sc. (Laurea di Primo Livello) in Computer Science and Engineering**, *109/110*. *2007-2010*
  *Institution:* Politecnico di Milano, Milan, Italy.
  *Advisor:* Prof. Giovanni Agosta.

## Research Experience

- **Associate Professor**, Politecnico di Milano, Milan, Italy. *13/01/2025-Today*
  Dipartimento di Elettronica, Informazione e Bioingegneria.
  *Research Topic:* Machine Learning for Cybersecurity and Security of Machine Learning.
- **Assistant Professor, Tenure Track (RTD-B)**, Politecnico di Milano, Milan, Italy. *10/2022-01/2025*
  Dipartimento di Elettronica, Informazione e Bioingegneria.
  *Research Topic:* Machine Learning for Cybersecurity and Security of Machine Learning.

- **Assistant Professor (RTD-A)**, Politecnico di Milano, Milan, Italy. *03/2022-09/2022*
  Dipartimento di Elettronica, Informazione e Bioingegneria.
  *Research Topic:* Application of machine learning techniques to cybersecurity.
- **Adjunct Professor (Professore a contratto)**, Politecnico di Milano, Milan, Italy. *2017/18-03/2022*
  Dipartimento di Elettronica, Informazione e Bioingegneria.
- **Research Assistant**, Politecnico di Milano, Milan, Italy. *02/2017-02/2022*
  *Research Topic:* Application of machine learning techniques to fraud detection.
  *Head of Research*: Stefano Zanero.
- **Visiting Research Assistant**, Università Svizzera Italiana, Lugano, Switzerland. *03/2019-06/2019*
  *Research Topic:* Anomaly Log Detection.
  *Head of Research*: Dr. Davide Eynard.
- **Visiting Research Assistant**, Northeastern University, Boston, USA. *09/2015-03/2016*
  *Research Topic:* Web security - Analysis of malicious advertisement.
  *Head of Research*: Engin Kirda and William Robertson.

## Teaching Activities

### Lecturer

- *Course: Computer Security* [5 CFU] *2018-Today*
  M.Sc. in Computer Science and Engineering, Biomedical, Telecommunication, and Geoinformatics Engineering.
  Politecnico di Milano, Milan, Italy.
  *Number of students:* 300 (2024), *Student Evaluation:* 3.2/4 (2023).
- *Course: Advanced Research Topics in Cybersecurity* [5 CFU] *a.a. 2022/23, 2024/25*
  Ph.D. program, Politecnico di Milano, Milan, Italy.
- *Course: Informatica B* [7 CFU] *2023-Today*
  B.Sc. in Mechanical and Energetic Engineering, Politecnico di Milano, Milan, Italy.
  *Number of students:* 252 (2024), *Student Evaluation:* 3.2/4 (2023).
- *Course: Computer and Network Security* [ 100 hours - year] *2019-2024*
  Cybersecurity Professional Master's Degree ("Master universitario di primo livello").
  CEFRIEL & Politecnico di Milano, Milan, Italy.
  *Specialization degree director:* Prof. Stefano Zanero. *Number of students:* ~25.
- *Course: Fraud Analysis and Detection* [24 hours - year] *2019-2024*
  Cybersecurity Professional Master's Degree ("Master universitario di primo livello"),
  CEFRIEL & Politecnico di Milano, Milan, Italy.
  *Specialization degree director:* Prof. Stefano Zanero. *Number of students:* ~25.
- *Course: Computer and Network Security* [16 hours - year] *2021-Today*
  Professional Master's Degree in business analytics and big data ("Master universitario di primo livello").
  MIP Politecnico di Milano, Graduate School of Business, Milan, Italy. *Number of students:* ~25.
- *Course: AI and Cyber Security* [24 hours] *2020*
  Professional Master's Degree in "Artificial Intelligence" ("Master universitario di primo livello"),
  CEFRIEL & Politecnico di Milano, Milan, Italy.
  *Specialization degree director:* Prof. Matteo Matteucci. *Number of students:* ~25.

### Teaching Assistant

- *Course: Digital Forensics and Cybercrime* [5 CFU] *2020-Today*
  M.Sc. in Computer Science and Engineering and in Cyber Risk Strategy and Governance,
  Politecnico di Milano & Università Bocconi, Milan, Italy.
  *Course Lecturer*: Stefano Zanero. *Number of students:* 182 (2024).
- *Course: Cyber Security Technologies, Procedures and Policies* [5 CFU] *2019-2023*
  M.Sc. in Cyber Risk Strategy and Governance, Politecnico di Milano & Università Bocconi, Milan, Italy.
  *Course Lecturer*: Stefano Zanero. *Number of students:* 54 (2022).
- *Course: Privacy and Security* [5 CFU] *2016-2018*
  M.Sc. in Computer Science and Engineering, Politecnico di Milano, Como, Italy.
  *Course Lecturer*: Stefano Zanero. *Number of students:* 41 (2018).
- *Course: Computer Security* [5 CFU] *2016-2017*
  M.Sc. in Computer Science and Engineering, Politecnico di Milano, Milan, Italy.
  *Course Lecturer*: Stefano Zanero. *Number of students:* 192 (2017).

- *Course: Computer Security* [5 CFU] *2014-2016*
  M.Sc. in Computer Science and Engineering,
  Politecnico di Milano, Milan, Italy.
  *Course Lecturer*: Federico Maggi. *Number of students:* 161 (2016).

### Tutor

- *Course: Informatica* course. [8 hours - year] *a.a. 2018/19*
  B.Sc. in Computer Science and Engineering, Politecnico di Milano, Milan, Italy.
  *Course Lecturer*: Marco Lattuada. *Number of students:* ~10.

### Trainings

- *AI and ML for Fraud Detection* (HITB+ CyberWeek) - 3 day training, ADNEC, Abu Dhabi, UAE *2021*
  *Description:* The course covers insights and practical implementation of fraud detection models.
  *Role:* Trainer.
- *Cyberchallenge.it* (https://cyberchallenge.it/) *2018–2023*
  *Description:* Training program in cybersecurity for high-school and undergraduate student.
  *Role:* Local Co-organizer.

## Academic Service

### Abilitazione Scientifica Nazionale

- ASN II Fascia, GSD 09/IINF-05-Information Processing Systems. *25/06/2023*

### Memberships and Associations

- IEEE member *2017-2024*
- IEEE Computer Society Member *2022-2024*
- ACM member *2022-2024*

### Coordination

- **Specialization Degree Coordinator** *2022-Today*
  *Cybersecurity Professional Master's Degree ("Master universitario di primo livello")*,
  CEFRIEL & Politecnico di Milano, Milan, Italy.
  *Number of students:* ~30 (2023).

### Conference Organizing Committee

- **Publication Chair**
  Conference on Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA. *2023-2025*
- **Publication Co-Chair**
  Italian Conference on Cybersecurity, ITASEC 2025. *2025*
- **Program Co-Chair**
  OWASP Italy Day 2023, OWASP IT 2023. *2023*

### Conference Program Committee

- Conference on Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA. *2023-2025*
- IEEE International Conference on Cyber Security and Resilience, CSR. *2022-2025*
- ACM ASIA Conference on Computer and Communications Security, ASIA CCS. *2024*
- International Conferences on Trust, Security and Privacy in Computing and Communications, TrustCom. *2022-2024*
- Annual Computer Security Applications Conference, ACSAC. *2024*
- International Conferences on High Performance Computing and Communications, IEEE HPCC. *2024*
- International Conference on Security for Information Technology and Communications, SECITC. *2022-2024*
- International Conference on Attacks and Defenses for Internet-of-Things, ADIoT 2024. *2024*
- IEEE International Conference on Embedded and Ubiquitous Computing, EUC 2024. *2024*
- IEEE International Conference on Ubiquitous Intelligence and Computing, UIC 2024. *2024*
- IEEE International Conference on Computational Science and Engineering, CSE 2024. *2024*
- IEEE International Conference on Artificial Intelligence Testing, AITest 2024. *2024*
- International Symposium on Cyber Security, Cryptology and Machine Learning, CSCML 2024. *2024*
- International workshop on Blockchain for Process and Information Science, B4PIS24 2024. *2024*
- The First IEEE International Workshop on Testing and Evaluation of Large Language Models, TELLMe 2024. *2024*
- IEEE European Symposium on Security and Privacy [Poster], EURO S&P. *2023-2024*
- EAI International Conference on Artificial Intelligence for CyberSecurity, EAI AICSEC 2023. *2023*

- The 21st IEEE International Symposium on Parallel and Distributed Processing with Applications, ISPA 2023. *2023*
- 26th Information Security Conference, ISC 2023. *2023*
- International Workshop on AI-driven Trustworthy, Secure, and Privacy-Preserving Computing, AIDTSP 2023. *2023*
- International Conference on Information Systems Security, ICISS. *2021-2022*
- The Italian Conference on CyberSecurity, ITASEC. *2017-2018, 2020*
- Workshop on Machine Learning for Cyber-Crime Investigation and Cybersecurity, MaL2CSec. *2019*
- **S&P** (Oakland), IEEE Symposium on Security and Privacy. *2018*
  Student Shadow Technical Program Committee, New York

### Journals Reviewer

- Elsevier Journal of Paralled and Distributed Computing, JPDC. *2024*
- IEEE Transactions on Neural Networks and Learning Systems, IEEE TNNLS. *2024*
- IEEE Transactions on Information Forensics and Security, IEEE T-IFS. *2024*
- ACM Transactions on the Web, ACM TWEB. *2024*
- ACM Transactions on Autonomous and Adaptive Systems, ACM TAAS. *2023-2024*
- IEEE Transactions on Information Forensics and Security, IEEE TIFS. *2023*
- IEEE Transactions on Automation Science and Engineering IEEE TASE. *2023*
- Springer The Journal of Supercomputing *2023*
- IEEE Transactions on Cloud Computing TCC *2022*
- ACM Transactions on Privacy and Security ACM TOPS *2022*
- IEEE Access *2020–2022*
- Elsevier Computers & Security, COSE *2019–2023*
- IEEE Transactions on Intelligent Transportation Systems, TITS *2020-2022*
- Elsevier Future Generation Computer Systems, FGCS *2019–2021*
- IEEE Transactions on Network and Service Management, TNSM *2020*
- IEEE Transactions on Computational Social Systems, TCSS *2020*
- ACM Transactions on Knowledge Discovery from Data, TKDD *2020-2022*
- IEEE Transactions on Engineering Management, TEM *2020*
- IEEE Transactions on Industrial Informatics, TII *2018*

### External Reviewer

- The European Symposium on Research in Computer Security, ESORICS *2023-2024*
- The International Symposium on Research in Attacks, Intrusions and Defenses, RAID *2023-2024*
- Annual Computer Security Applications Conference, ACSAC 2023 *2023*
- 14th USENIX Workshop on Offensive Technologies, WOOT 2020 *2020*
- International Conference on Information Systems Security, ICIS 2019 *2019*
- IEEE International Conference on Malicious and Unwanted Software, MALCON 2019 *2019*
- IEEE International Conference On Trust, Security And Privacy In Computing And Communications, IEEE TrustCom *2018–2019*
- The 12th International Symposium on Applied Reconfigurable Computing, ARC 2016 *2016*
- The 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA 2016 *2016*
- The WISTP International Conference on Information Security Theory and Practice Series, WISTP 2015 *2015*
- The 10th International Conference on Information Systems Security, ICISS 2014 *2014*
- The 2nd IEEE International Workshop on Reliability and Security Data Analysis, RSDA 2014 *2014*

### Editorial Task

- **Publication Chair** *2023-2024*
  Conference on Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA
- **Associate Editor** *2024*
  Journal: Journal of Parallel and Distributed Computing, JPDC.
- **Executive Guest Editor** *2024*
  *Title:* Special Issue: Secure and Efficient Distributed Computation for Emerging Systems on the Edge
  Journal: Journal of Parallel and Distributed Computing, JPDC.
- **Editorial Board Member-Review Editor** *2022-Today*
  Frontiers in Big Data

### Attended Conference

- 21th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2024, Lausanne, Switzerland.
- 20th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2023, Hamburg, Germany.
- ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA.
- Italian Conference on Cybersecurity, ITASEC 2022, Rome, Italy.
- Annual Computer Security Applications Conference, ACSAC 2020, Virtual Event / Austin, TX, USA.
- 23rd International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2020, Virtual Event / San Sebastian, Spain.
- 40th IEEE Symposium on Security and Privacy, S&P 2019, San Francisco, USA.
- 39th IEEE Symposium on Security and Privacy, S&P 2018, San Francisco, USA.
- 15th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2018, Saclay, France.
- 23rd ACM Conference on Computer and Communications Security, CCS 2016, Hofburg Palace, Vienna, Austria.
- 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2015, Milan, Italy.
- International Conference on ICT Systems Security and Privacy Protection, IFIP SEC 2014, Marrakech, Morocco.

## Institutional Responsibilities and Commission of Trust

### Doctoral defense Committee

- Lorenzo Binosi, "New Approaches and New Techniques for the Security of Software Applications" *2024*
  *Ph.D. Committee:* Michele Carminati - Polimi (Chair), Martina Linderhofen - TU Wien, Davide Balzarotti - Eurecom.
  *Advisor:* Stefano Zanero.
- Alberto Zeni "A Framework for the Aided Design of High-Performance Genome Analysis Applications on Heterogeneous Architectures"
  Guido Walter di Donato "Leveraging Heterogeneous Hardware Acceleration From High-Level Programming Languages: The Case For Biomedical Informatics" *2024*
  *Ph.D. Committee:* Prof. Michele Carminati (Chair) - Polimi, Prof. Dionysios Pnevmatikatos - ECE, National Technical University of Athens, Prof. Juergen Becker - Karlsruhe Institute of Technology.
  *Advisor:* Marco Domenico Santambrogio.
- Mattia Zago. "Enhancing DGA-based botnet detection beyond 5G with on-edge machine learning - Aprendizaje Automático en el Edge para la Mejora de la Detección de Botnets DGA en Redes 5G y Futuras" *2021*
  *Ph.D. Committee:* Lorenzo Fernández Maimó - University of Murcia (Chair), Victor A. Villagra - Universidad Politecnica de Madrid, Prof. Michele Carminati - Polimi.
  *Advisors:* Manuel Gil Pérez, Gregorio Martínez Pérez.

### M.Sc. Degree Committees

M.Sc. Degree Committees **Member or Chair**, Politecnico di Milano, Milan, Italy. *2018-Today*

M.Sc. Degree Committees **Member**, Università Bocconi, Milan, Italy. *2022-Today*

### B.Sc. Degree Committees

B.Sc. Degree Committees **Member**, Politecnico di Milano, Milan, Italy. *2018-Today*

### Specialization Degree Committee (Master)

"Security Specialist" specialization degree Committee **Member**, Politecnico di Milano, Milan, Italy *2019-Today*

### Others

**Member of the Electoral Committee of the CS IEEE Italy Section** *2022,2024*

## Technology Transfer

### Development of Products

*Product name:* Banksealer.
*Website:* https://banksealer.com/
*Role:* Software designer and developer.
*Industrial and Societal Impact:* Deployed in 1 financial institution and 2 Companies.

### Startup and Spinoffs

*Company name:* Banksealer S.r.l.
*Website:* https://banksealer.com/
*Founded:* 2016
*Description:* Fintech spinoff of Politecnico di Milano delivering novel fraud detection solutions for banking and payment systems, based in Milano, Italy.
*Role:* **Co-Founder** and **Scientific Advisor**
*Co-founders:* Alvise Biffi, Stefano Zanero, Daniele Gallingani, Claudio Caletti.

## Research Projects and Funding

### Competitive Research Projects

- *Project Title:* **AI-RESCUE - Science and engineering Of Security of Artificial Intelligence - Bando a Cascata PNRR SOS_AI - Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 3 "Attacks and Defences"**
  *Principal Investigator:* Michele Carminati
  *Period:* *2024-2026*
  *Role:* **Principal Investigator**
  *Funding:* The MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU funded the project 1.2M EUR, 172k EUR of which for the research group at DEIB.
- *Project Title:* **SOCRATE**
  *Principal Investigator:* Stefano Longari, The previous principal investigator (2023-2024), Mario Polino left the project.
  *Period:* *2023-2025*
  *Role:* **Research Team Member**
  *Funding:* The Agenzia Spaziale Italiana funded the project 112k EUR, of which 56k EUR for the research group at DEIB.
- *Project Title:* **COVERT - In searCh Of eVidence of stEalth cybeR Threats - Bando a Cascata PNRRR - Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 3 "Attacks and Defences"**
  *Principal Investigator:* Stefano Zanero
  *Period:* *2024-2025*
  *Role:* **Research Team Member**
  *Funding:* The MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU funded the project 1M EUR, 60k EUR of which for the research group at DEIB.
- *Project Title:* **Google.org Impact Challenge: Tech for Social Good**
  *Principal Investigators:* Stefano Zanero and Michele Carminati
  *Period:* *2023-2026*
  *Role:* **Co-Principal Investigator**
  *Funding:* Tides Foundation funded the project 1M EUR, 550k EUR of which for the research group at DEIB.
- *Project Title:* **PRIN 2022 PNRR project "SHIELDED: Secure, Trustworthy, and Efficient Federated Learning for Intrusion Detection at the Edge"**
  *Principal Investigator:* Francesco Malandrino
  *Period:* *2023–2025*
  *Role:* **Local Principal Investigator**
  *Funding:* The MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU funded the project 240k EUR, 85k EUR of which for the research group at DEIB.
- *Project Title:* **PRIN PNRR 2022 project "SETA: Studying thE impact of anti-analysis Techniques in IoT security evAluations"**
  *Principal Investigator:* Davide Maiorca
  *Period:* *2023-2025*
  *Role:* **Research Team Member**
  *Funding:* The MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU funded the project 229k EUR, 76k EUR of which for the research group at DEIB.
- *Project Title:* **PRIN 2022 project "FARE: Firmware Analysis for vulneRability dEtection"**
  *Principal Investigator:* Emilio Coppa
  *Period:* *2024-2025*
  *Role:* **Local Principal Investigator** The previous principal investigator (2023-2024), Mario Polino left the project.
  *Funding:* The MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU funded the project 256k EUR, 128k EUR of which for the research group at DEIB.

- *Project Title:* **EU HORIZON TRUSTROKE**: TRUSTWORTHY AI FOR IMPROVEMENT OF STROKE OUTCOMES
  *Local Principal Investigators:* Prof. Stefano Zanero and Prof. Alessandro Cesare Redondi
  *Period:* *2023-2027*
  *Roles:*
  – **Task leader** of the task *T2.4 Security and privacy design*.
  *Funding:* The European Union financed the project with approximately 6M EUR, 300k EUR of which for the research group at DEIB.
- *Project Title:* **European H2020 Project "RAMSES"**: Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware - https://ramses2020.eu/
  *Local Principal Investigators:* Prof. Stefano Zanero and Michele Carminati
  *Period:* *2016-2020*
  *Roles:*
  – **WP leader** of WP6 (Forensic analysis of malware monetization techniques).
  – **Task leader** of the following tasks: T6.1 (New methods for Bitcoin deanonymization) and T6.3 (Automatic forensic analysis of malware monetization).
  – **Project Coordinator** *2019-2020*: Due to the bankrupcy of the original coordinator, POLIMI acquired the coordination of the project and I was selected as primary coordinator.
  *Funding:* The European Union financed the project with approximately 3M EUR, 280k EUR of which for the research group at DEIB.
- *Project Title:* **ISSES Information Security Services Education in Serbia, Erasmus+ Programme** - https://isses.etf.bg.ac.rs/
  *Local Principal Investigator:* Prof. Stefano Zanero
  *Period:* *2017-2021*
  *Role:* **Research Team Member**, delivering seminars and preparing course material.
- *Project Title:* **European Marie Curie RISE Project "PROTASIS"** - https://www.protasis.eu/
  *Local Principal Investigator:* Prof. Stefano Zanero
  *Period:* *2016-2020*
  *Role:* **Research Team Member**
  *Funding:* The European Union financed the project with approximately 3M EUR, 320k EUR of which for the research group at DEIB.
- *Project Title:* **PRIN project "TENACE: Protecting National Critical Infrastructures From Cyber Threats"** - http://www.diag.uniroma1.it// tenace/
  *Local Principal Investigator:* Prof. Stefano Zanero
  *Period:* *2013-2016*
  *Role:* **Research Team Member** working on financial fraud detection.
  *Funding:* 77k EUR for the research group at DEIB.
- *Project Title:* **FACE Formal Avenue for Chasing malwarE (MIUR FIRB 2013)** - face-project.it
  *Topics*: Malware analysis and defense methodologies.
  *Local Principal Investigators*: Federico Maggi and Stefano Zanero
  *Period:* *2014-2016*
  *Role:* **Research Team Member** working on banking Trojan analysis and detection.

### Industrial-funded Research Projects

- **Research Agreement** with Trenord S.r.l.
  *Period:* *2024*
  *Role:* **Principal Investigator**
  *Research Topic:* Fraud and anomaly detection for e-ticketing systems.
  *Funding:* 15k EUR for the research group at DEIB.
- **Research Agreement** with Trenord S.r.l.
  *Local Principal Investigators:* Prof. Stefano Zanero.
  *Period:* *2021*
  *Role:* **Research Team Member** working on fraud and anomaly detection.
  *Funding:* 20k EUR for the research group at DEIB.
- **Research Agreement** with Napier ltd. (previously Fortytwo Data ltd.)
  *Local Principal Investigators:* Prof. Stefano Zanero and **Michele Carminati**.
  *Period:* *2017–2019*
  *Role:* **Local Principal Investigator** working on anti-money laundering.
  *Funding:* 45k EUR for the research group at DEIB.

# Publications

## Productivity and Impact Metrics

- **Scientific Productivity 49** publications entries on Google Scholar - **40** publications entries on Scopus, 72 co-authors according to Scopus:
  Author/Co-author of **14** scientific publications on journal papers, including **11 top-ranked Q1** journal papers based on SCIMAGO (i.e., *Computer & Security*, *ACM Transactions on Privacy and Security*, *IEEE Transactions on Network and Service Management*, *IEEE Transactions on Intelligent Transportation Systems*,and *IEEE Transactions on Emerging Topics in Computing*. )
  Author/Co-author of **25** scientific publications on peer-reviewed conferences and **5** on workshops, including , 2 in class A++, 1 in class A+, 3 in class A according to GGS conf. ranking (including the *Annual Computer Security Applications Conference (ACSAC)*, *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, *ECML PKDD*, and *Conference on Computer and Communications Security (CCS)*);
- **Publication Impact**
  *Based on Google Scholar*: h-index 17, citations 796.
  *Based on Scopus*: h-index 12, citations 443.

## Peer-Reviewed Journal Publications

[J1] **M. Carminati**, R. Caron, F. Maggi, I. Epifani, and S. Zanero, *"BankSealer: A decision support system for online banking fraud analysis and investigation"*. In: *Comput. Secur.*, (2015), doi:10.1016/j.cose.2015.04.002, url: https://doi.org/10.1016/j.cose.2015.04.002.
*Citations:* 130 [*Google Scholar*] - 67 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 125; [CORE2020] **B**.

[J2] A. Continella, **M. Carminati**, M. Polino, A. Lanzi, S. Zanero, and F. Maggi, *"Prometheus: Analyzing WebInject-based information stealers"*. In: *J. Comput. Secur.*, (2017), doi:10.3233/JCS-15773, url: https://doi.org/10.3233/JCS-15773.
*Citations:* 31 [*Google Scholar*] - 12 [*Scopus*].
*Ranking:* [Scimago 2023] **Q3**, *SJR* 0.34, *H-index* 59; [CORE2020] **B**.

[J3] **M. Carminati**, M. Polino, A. Continella, A. Lanzi, F. Maggi, and S. Zanero, *"Security Evaluation of a Banking Fraud Analysis System"*. In: *ACM Trans. Priv. Secur.*, (2018), doi:10.1145/3178370, url: https://doi.org/10.1145/3178370.
*Citations:* 43 [*Google Scholar*] - 26 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 0.79, *H-index* 26; [CORE2020] **A**.

[J4] M. Zago, S. Longari, A. Tricarico, **M. Carminati**, M. . Pérez, G. . Pérez, and S. Zanero, *"ReCAN – Dataset for reverse engineering of Controller Area Networks"*. In: *Data in Brief*, (2020), doi:https://doi.org/10.1016/j.dib.2020.105149, url: https://doi.org/https://doi.org/10.1016/j.dib.2020.105149.
*Citations:* 26 [*Google Scholar*] - 15 [*Scopus*].
*Ranking:* [Scimago 2023] **Q3**, *SJR* 0.21, *H-index* 52; [CORE2020] n.a..

[J5] S. Longari, D. H. N. Valcarcel, M. Zago, **M. Carminati**, and S. Zanero, *"CANnolo: An Anomaly Detection System Based on LSTM Autoencoders for Controller Area Network"*. In: *IEEE Trans. Netw. Serv. Manag.*, (2021), doi:10.1109/TNSM.2020.3038991, url: https://doi.org/10.1109/TNSM.2020.3038991.
*Citations:* 112 [*Google Scholar*] - 80 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 1.76, *H-index* 73; [CORE2020] n.a..

[J6] N. Galloro, M. Polino, **M. Carminati**, A. Continella, and S. Zanero, *"A Systematical and longitudinal study of evasive behaviors in windows malware"*. In: *Comput. Secur.*, (2022), doi:10.1016/J.COSE.2021.102550, url: https://doi.org/10.1016/J.COSE.2021.102550.
*Citations:* 54 [*Google Scholar*] - 28 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 125; [CORE2020] **B**.

[J7] D. Maffiola, S. Longari, **M. Carminati**, M. Tanelli, and S. Zanero, *"GOLIATH: A Decentralized Framework for Data Collection in Intelligent Transportation Systems"*. In: *IEEE Trans. Intell. Transp. Syst.*, (2022), doi:10.1109/TITS.2021.3123824, url: https://doi.org/10.1109/TITS.2021.3123824.
*Citations:* 12 [*Google Scholar*] - 7 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 2.58, *H-index* 201; [CORE2020] n.a..

[J8] D. Labanca, L. Primerano, M. Markland-Montgomery, M. Polino, **M. Carminati**, and S. Zanero, *"Amaretto: An Active Learning Framework for Money Laundering Detection"*. In: *IEEE Access*, (2022), doi:10.1109/ACCESS.2022.3167699, url: https://doi.org/10.1109/ACCESS.2022.3167699.
*Citations:* 29 [*Google Scholar*] - 13 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 0.96, *H-index* 242; [CORE2020] n.a..

[J9] T. Paladini, F. Monti, M. Polino, **M. Carminati**, and S. Zanero, *"Fraud Detection under Siege: Practical Poisoning Attacks and Defense Strategies"*. In: *ACM Trans. Priv. Secur.*, (2023), doi:10.1145/3613244, url: https://doi.org/10.1145/3613244.
*Citations:* 2 [*Google Scholar*] - 0 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 0.79, *H-index* 26; [CORE2020] **A**.

[J10] L. Binosi, M. Polino, **M. Carminati**, and S. Zanero, *"BINO: Automatic recognition of inline binary functions from template classes"*. In: *Comput. Secur.*, (2023), doi:10.1016/J.COSE.2023.103312, url: https://doi.org/10.1016/J.COSE.2023.103312.
*Citations:* 5 [*Google Scholar*] - 1 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 125; [CORE2020] **B**.

[J11] A. Nichelini, C. A. Pozzoli, S. Longari, **M. Carminati**, and S. Zanero, *"CANova: A hybrid intrusion detection framework based on automatic signal classification for CAN"*. In: *Comput. Secur.*, (2023), doi:10.1016/J.COSE.2023.103166, url: https://doi.org/10.1016/J.COSE.2023.103166.
*Citations:* 19 [*Google Scholar*] - 13 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 125; [CORE2020] **B**.

[J12] S. Longari, A. Pozone, J. Leoni, M. Polino, **M. Carminati**, M. Tanelli, and S. Zanero, *"CyFence: Securing Cyber-Physical Controllers via Trusted Execution Environment"*. In: *IEEE Trans. Emerg. Top. Comput.*, (2024), doi:10.1109/TETC.2023.3268412, url: https://doi.org/10.1109/TETC.2023.3268412.
*Citations:* 1 [*Google Scholar*] - 1 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 61; [CORE2020] n.a..

[J13] M. D'Onghia, M. Salvadore, B. M. Nespoli, **M. Carminati**, M. Polino, and S. Zanero, *"Apicula: Static detection of API calls in generic streams of bytes"*. In: *Comput. Secur.*, (2022), doi:10.1016/J.COSE.2022.102775, url: https://doi.org/10.1016/J.COSE.2022.102775.
*Citations:* 7 [*Google Scholar*] - 4 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 125; [CORE2020] **B**.

[J14] S. Longari, J. Jannone, M. Polino, **M. Carminati**, A. Zanchettin, M. Tanelli, and S. Zanero, *"Janus: A Trusted Execution Environment Approach for Attack Detection in Industrial Robot Controllers"*. In: *IEEE Transactions on Emerging Topics in Computing*, (2024), doi:10.1109/TETC.2024.3390435, url: https://doi.org/10.1109/TETC.2024.3390435.
*Citations:* 1 [*Google Scholar*] - 0 [*Scopus*].
*Ranking:* [Scimago 2023] **Q1**, *SJR* 1.57, *H-index* 61; [CORE2020] n.a..

### Peer-Reviewed Conference Proceedings

[C1] **M. Carminati**, R. Caron, F. Maggi, I. Epifani, and S. Zanero. *"BankSealer: An Online Banking Fraud Analysis and Decision Support System"*. In: *ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings, 2014*, doi:10.1007/978-3-642-55415-5_32, url: https://doi.org/10.1007/978-3-642-55415-5_32.
*Acceptance Rate: 17.9% (27/151).*
*Citations:* 40 [*Google Scholar*], 22 [*Scopus*].
*Ranking: GGS Class* 3, *GGS Rating* B-, *CORE* B, *LiveSHINE* B , *MA* C [GGS].

[C2] **M. Carminati**, L. Valentini, and S. Zanero. *"A Supervised Auto-Tuning Approach for a Banking Fraud Detection System"*. In: *Cyber Security Cryptography and Machine Learning - First International Conference, CSCML 2017, Beer-Sheva, Israel, June 29-30, 2017, Proceedings, 2017*, doi:10.1007/978-3-319-60080-2_17, url: https://doi.org/10.1007/978-3-319-60080-2_17.
*Citations:* 10 [*Google Scholar*], 10 [*Scopus*].
*Ranking: GGS Class* n.a, *GGS Rating* n.a, *CORE* n.a, *LiveSHINE* n.a , *MA* n.a [GGS].

[C3] P. D. Nicolao, M. Pogliani, M. Polino, **M. Carminati**, D. Quarta, and S. Zanero. *"ELISA: ELiciting ISA of Raw Binaries for Fine-Grained Code and Data Separation"*. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 15th International Conference, DIMVA 2018, Saclay, France, June 28-29, 2018, Proceedings, 2018*, doi:10.1007/978-3-319-93411-2_16, url: https://doi.org/10.1007/978-3-319-93411-2_16.
*Acceptance Rate: 30.5% (18/59).*
*Citations:* 17 [*Google Scholar*], 9 [*Scopus*].
*Ranking: GGS Class* 3, *GGS Rating* B, *CORE* C, *LiveSHINE* A- , *MA* A- [GGS].

[C4] **M. Carminati**, A. Baggio, F. Maggi, U. Spagnolini, and S. Zanero. *"FraudBuster: Temporal Analysis and Detection of Advanced Financial Frauds"*. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 15th International Conference, DIMVA 2018, Saclay, France, June 28-29, 2018, Proceedings, 2018*, doi:10.1007/978-3-319-93411-2_10, url: https://doi.org/10.1007/978-3-319-93411-2_10.
*Acceptance Rate: 30.5% (18/59).*
*Citations:* 17 [*Google Scholar*], 12 [*Scopus*].
*Ranking: GGS Class* 3, *GGS Rating* B, *CORE* C, *LiveSHINE* A- , *MA* A- [GGS].

[C5] S. Longari, A. Cannizzo, **M. Carminati**, and S. Zanero. *"A Secure-by-Design Framework for Automotive On-board Network Risk Analysis"*. In: *2019 IEEE Vehicular Networking Conference, VNC 2019, Los Angeles, CA, USA, December 4-6, 2019, 2019*, doi:10.1109/VNC48660.2019.9062783, url: https://doi.org/10.1109/VNC48660.2019.9062783.
*Citations:* 19 [*Google Scholar*], 17 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n. a., *CORE* n. a., *LiveSHINE* B, *MA* C [GGS].

[C6] **M. Carminati**, L. Santini, M. Polino, and S. Zanero. *"Evasion Attacks against Banking Fraud Detection Systems"*. In: *23rd International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2020, San Sebastian, Spain, October 14-15, 2020, 2020*, isbn:978-1-939133-18-2, url: https://www.usenix.org/conference/raid2020/presentation/carminati.
*Acceptance Rate: 23.2% (70/302)*.
*Citations:* 26 [*Google Scholar*], 18 [*Scopus*].
*Ranking: GGS Class* 1, *GGS Rating* A+, *CORE* A, *LiveSHINE* A+ , *MA* A+ [GGS].

[C7] A. Erba, R. Taormina, S. Galelli, M. Pogliani, **M. Carminati**, S. Zanero, and N. O. Tippenhauer. *"Constrained Concealment Attacks against Reconstruction-based Anomaly Detectors in Industrial Control Systems"*. In: *ACSAC '20: Annual Computer Security Applications Conference, Virtual Event / Austin, TX, USA, 7-11 December, 2020, 2020*, doi:10.1145/3427228.3427660, url: https://doi.org/10.1145/3427228.3427660.
*Acceptance Rate: 23.2% (70/302)*.
*Citations:* 63 [*Google Scholar*], 34 [*Scopus*].
*Ranking: GGS Class* 2, *GGS Rating* A, *CORE* n.c., *LiveSHINE* A+ , *MA* A+ [GGS].

[C8] D. Ferrari, **M. Carminati**, M. Polino, and S. Zanero. *"NoSQL Breakdown: A Large-scale Analysis of Misconfigured NoSQL Services"*. In: *ACSAC '20: Annual Computer Security Applications Conference, Virtual Event / Austin, TX, USA, 7-11 December, 2020, 2020*, doi:10.1145/3427228.3427260, url: https://doi.org/10.1145/3427228.3427260.
*Acceptance Rate: 25.6% (31/121)*.
*Citations:* 15 [*Google Scholar*], 9 [*Scopus*].
*Ranking: GGS Class* 2, *GGS Rating* A, *CORE* n.c., *LiveSHINE* A+ , *MA* A+ [GGS].

[C9] J. F. Rodriguez, M. Papale, **M. Carminati**, and S. Zanero. *"A Natural Language Processing Approach for Financial Fraud Detection"*. In: *Proceedings of the Italian Conference on Cybersecurity (ITASEC 2022), Rome, Italy, June 20-23, 2022, 2022*, url: https://ceur-ws.org/Vol-3260/paper10.pdf.
*Citations:* 10 [*Google Scholar*], 4 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a. , *MA* n.a. [GGS].

[C10] A. d. F. Tron, S. Longari, **M. Carminati**, M. Polino, and S. Zanero. *"CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks"*. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022, 2022*, doi:10.1145/3548606.3560618, url: https://doi.org/10.1145/3548606.3560618.
*Acceptance Rate: 22.3% (879/196)*.
*Citations:* 22 [*Google Scholar*], 11 [*Scopus*].
*Ranking: GGS Class* 1, *GGS Rating* A++, *CORE* A++, *LiveSHINE* A++ , *MA* A++ [GGS].

[C11] T. Paladini, M. d. L. Bernasconi, **M. Carminati**, M. Polino, F. Trovò, and S. Zanero. *"Advancing Fraud Detection Systems Through Online Learning"*. In: *Machine Learning and Knowledge Discovery in Databases: Applied Data Science and Demo Track - European Conference, ECML PKDD 2023, Turin, Italy, September 18-22, 2023, Proceedings, Part VI, 2023*, doi:10.1007/978-3-031-43427-3_17, url: https://doi.org/10.1007/978-3-031-43427-3_17.
*Acceptance Rate: 24% (58/241)*.
*Citations:* 3 [*Google Scholar*], 1 [*Scopus*].
*Ranking: GGS Class* 2, *GGS Rating* A, *CORE* A, *LiveSHINE* A+ , *MA* A [GGS].

[C12] M. P. Tatulli, T. Paladini, M. D'Onghia, **M. Carminati**, and S. Zanero. *"HAMLET: A Transformer Based Approach for Money Laundering Detection"*. In: *Cyber Security, Cryptology, and Machine Learning - 7th International Symposium, CSCML 2023, Be'er Sheva, Israel, June 29-30, 2023, Proceedings, 2023*, doi:10.1007/978-3-031-34671-2_17, url: https://doi.org/10.1007/978-3-031-34671-2_17.
*Citations:* 5 [*Google Scholar*], 2 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a. , *MA* n.a. [GGS].

[C13] S. Longari, F. Noseda, **M. Carminati**, and S. Zanero. *"Evaluating the Robustness of Automotive Intrusion Detection Systems Against Evasion Attacks"*. In: *Cyber Security, Cryptology, and Machine Learning - 7th International Symposium, CSCML 2023, Be'er Sheva, Israel, June 29-30, 2023, Proceedings, 2023*, doi:10.1007/978-3-031-34671-2_24, url: https://doi.org/10.1007/978-3-031-34671-2_24.
*Citations:* 1 [*Google Scholar*], 0 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a. , *MA* n.a. [GGS].

[C14] S. Longari, C. A. Pozzoli, A. Nichelini, **M. Carminati**, and S. Zanero. *"CANdito: Improving Payload-Based Detection of Attacks on Controller Area Networks"*. In: *Cyber Security, Cryptology, and Machine Learning - 7th International Symposium, CSCML 2023, Be'er Sheva, Israel, June 29-30, 2023, Proceedings, 2023*, doi:10.1007/978-3-031-34671-2_10, url: https://doi.org/10.1007/978-3-031-34671-2_10.
*Citations:* 7 [*Google Scholar*], 2 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a. , *MA* n.a. [GGS].

[C15] A. Bertani, M. Bonelli, L. Binosi, **M. Carminati**, S. Zanero, and M. Polino. *"Untangle: Aiding Global Function Pointer Hijacking for Post-CET Binary Exploitation"*. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 20th International Conference, DIMVA 2023, Hamburg, Germany, July 12-14, 2023, Proceedings*, *2023*, doi:10.1007/978-3-031-35504-2_13, url: https://doi.org/10.1007/978-3-031-35504-2_13.
*Acceptance Rate: 28% (13/46)*.
*Citations:* 3 [*Google Scholar*], 1 [*Scopus*].
*Ranking: GGS Class* 3, *GGS Rating* B, *CORE* C, *LiveSHINE* A- , *MA* A- [GGS].

[C16] D. Avanzi, S. Longari, M. Polino, **M. Carminati**, A. M. Zanchettin, M. Tanelli, and S. Zanero. *"Task Aware Intrusion Detection for Industrial Robots"*. In: *Proceedings of the Italian Conference on Cyber Security (ITASEC 2023), Bari, Italy, May 2-5, 2023*, *2023*, url: https://ceur-ws.org/Vol-3488/paper03.pdf.
*Citations:* 0 [*Google Scholar*], 0 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a. , *MA* n.a. [GGS].

[C17] L. Binosi, L. Rullo, M. Polino, **M. Carminati**, and S. Zanero. *"Rainfuzz: Reinforcement-Learning Driven Heat-Maps for Boosting Coverage-Guided Fuzzing"*. In: *Proceedings of the 12th International Conference on Pattern Recognition Applications and Methods, ICPRAM 2023, Lisbon, Portugal, February 22-24, 2023*, *2023*, doi:10.5220/0011625300003411, url: https://doi.org/10.5220/0011625300003411.
*Citations:* 3 [*Google Scholar*], 3 [*Scopus*].
*Ranking: GGS Class* w.i.p., *GGS Rating* w.i.p., *CORE* C, *LiveSHINE* n.a. , *MA* C [GGS].

[C18] T. Paladini, L. Ferro, M. Polino, S. Zanero, and **M. Carminati**. *"You Might Have Known It Earlier: Analyzing the Role of Underground Forums in Threat Intelligence"*. In: *The 27th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2024, Padua, Italy, 30 September 2024- 2 October 2024*, *2024*, doi:10.1145/3678890.3678930, url: https://doi.org/10.1145/3678890.3678930.
*Citations:* 0 [*Google Scholar*], 0 [*Scopus*].
*Ranking: GGS Class* 1, *GGS Rating* A+, *CORE* A, *LiveSHINE* A+ , *MA* A+ [GGS].

[C19] G. Digregorio, S. Maccarrone, M. D'Onghia, L. Gallo, **M. Carminati**, M. Polino, and S. Zanero. *"Tarallo: Evading Behavioral Malware Detectors in the Problem Space"*. In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 21st International Conference, DIMVA 2024, Lausanne, Switzerland, July 17-19, 2024, Proceedings*, *2024*, doi:10.1007/978-3-031-64171-8_7, url: https://doi.org/10.1007/978-3-031-64171-8_7.
*Citations:* 0 [*Google Scholar*], 0 [*Scopus*].
*Ranking: GGS Class* 3, *GGS Rating* B, *CORE* C, *LiveSHINE* A- , *MA* A- [GGS].

[C20] 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: *Proceedings of the 21st International Conference on Security and Cryptography, SECRYPT 2024, Dijon, France, July 8-10, 2024*, *2024*, doi:10.5220/0012856200003767, url: https://doi.org/10.5220/0012856200003767.
*Citations:* 0 [*Google Scholar*], 0 [*Scopus*].
*Ranking: GGS Class* w.i.p., *GGS Rating* w.i.p., *CORE* B, *LiveSHINE* C , *MA* C [GGS].

[C21] P. Cerracchio, S. Longari, **M. Carminati**, and S. Zanero. *"Investigating the Impact of Evasion Attacks Against Automotive Intrusion Detection Systems"*. In: *Symposium on Vehicles Security and Privacy (VehicleSec) 2024*, *2024*, url: https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-56-paper.pdf.
*Citations:* 1 [*Google Scholar*], n.a. [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a., *MA* n.a. [GGS].

[C22] M. Marazzi, S. Longari, **M. Carminati**, and S. Zanero. *"Securing LiDAR Communication through Watermark-based Tampering Detection"*. In: *Symposium on Vehicles Security and Privacy (VehicleSec) 2024*, *2024*, url: https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-55-paper.pdf.
*Citations:* 0 [*Google Scholar*], n.a. [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a., *MA* n.a. [GGS].

[C23] G. Digregorio, E. Cainazzo, S. Longari, **M. Carminati**, and S. Zanero. *"Evaluating the Impact of Privacy-Preserving Federated Learning on CAN Intrusion Detection"*. In: *99th IEEE Vehicular Technology Conference, VTC Spring 2024, Singapore, June 24-27, 2024*, *2024*, doi:10.1109/VTC2024-SPRING62846.2024.10683636, url: https://doi.org/10.1109/VTC2024-SPRING62846.2024.10683636.
*Citations:* 0 [*Google Scholar*], 0 [*Scopus*].
*Ranking: GGS Class* 2, *GGS Rating* A, *CORE* B, *LiveSHINE* A+ , *MA* A+ [GGS].

[C24] L. Binosi, G. Barzasi, **M. Carminati**, S. Zanero, and M. Polino. *"The Illusion of Randomness: An Empirical Analysis of Address Space Layout Randomization Implementations"*. *To Appear In*: *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security, CCS 2024, Salt Lake City, UTAH, USA, October 14-18, 2024*, *2024*.
*Citations:* n.a. [*Google Scholar*], n.a. [*Scopus*].
*Ranking: GGS Class* 1, *GGS Rating* A++, *CORE* A++, *LiveSHINE* A++ , *MA* A++ [GGS].

[C25] D. R. Santos, A. S. Aillet, A. Boiano, U. Milasheuski, L. Giusti, M. D. Gennaro, S. Kianoush, L. Barbieri, M. Nicoli, **M. Carminati**, A. E. C. Redondi, S. Savazzi, and L. Serio. *"A Federated Learning Platform as a Service for Advancing Stroke Management in European Clinical Centers"*. *To Appear In*: *2024 IEEE International Conference on E-health Networking, Application & Services (HealthCom), 2024*.
*Citations:* n.a. [*Google Scholar*], n.a. [*Scopus*].
*Ranking: GGS Class* w.i.p., *GGS Rating* w.i.p., *CORE* C, *LiveSHINE* C , *MA* C [GGS].

### Peer-reviewed Workshops

[W1] G. Viglianisi, **M. Carminati**, M. Polino, A. Continella, and S. Zanero. *"SysTaint: Assisting Reversing of Malicious Network Communications"*. In: *Proceedings of the 8th Software Security, Protection, and Reverse Engineering Workshop, San Juan, PR, USA, December 3-4, 2018, 2018*, doi:10.1145/3289239.3289245, url: https://doi.org/10.1145/3289239.3289245.
*Citations:* 4 [*Google Scholar*], 1 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a. , *MA* n.a. [GGS].

[W2] S. Longari, M. Penco, **M. Carminati**, and S. Zanero. *"CopyCAN: An Error-Handling Protocol based Intrusion Detection System for Controller Area Network"*. In: *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy, CPS-SPC@CCS 2019, London, UK, November 11, 2019, 2019*, doi:10.1145/3338499.3357362, url: https://doi.org/10.1145/3338499.3357362.
*Citations:* 27 [*Google Scholar*], 16 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a. , *MA* n.a. [GGS].

[W3] R. Remigio, A. Bertani, M. Polino, **M. Carminati**, and S. Zanero. *"The Good, the Bad, and the Binary: An LSTM-Based Method for Section Boundary Detection in Firmware Analysis"*. In: *Advances in Information and Computer Security - 18th International Workshop on Security, IWSEC 2023, Yokohama, Japan, August 29-31, 2023, Proceedings, 2023*, doi:10.1007/978-3-031-41326-1_2, url: https://doi.org/10.1007/978-3-031-41326-1_2.
*Citations:* 1 [*Google Scholar*], 1 [*Scopus*].
*Ranking: GGS Class* w.i.p., *GGS Rating* w.i.p., *CORE* n.c., *LiveSHINE* n.c., *MA* B [GGS].

[W4] M. D'Onghia, F. D. Cesare, L. Gallo, **M. Carminati**, M. Polino, and S. Zanero. *"Lookin' Out My Backdoor! Investigating Backdooring Attacks Against DL-driven Malware Detectors"*. In: *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security, AISec 2023, Copenhagen, Denmark, 30 November 2023, 2023*, doi:10.1145/3605764.3623919, url: https://doi.org/10.1145/3605764.3623919.
*Citations:* 3 [*Google Scholar*], 1 [*Scopus*].
*Ranking: GGS Class* w.i.p., *GGS Rating* w.i.p., *CORE* n.a., *LiveSHINE* C , *MA* n.a. [GGS].

[W5] A. Boiano, M. D. Gennaro, L. Barbieri, **M. Carminati**, M. Nicoli, A. E. C. Redondi, S. Kianoush, U. Milasheuski, S. Savazzi, A. S. Aillet, D. R. Santos, and L. Serio. *"A Secure and Trustworthy Network Architecture for Federated Learning Healthcare Applications"*. *To Appear In*: *2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) - The Twelfth international workshop on e-Health Pervasive Wireless Applications and Services e-HPWAS'24, 2024*.
*Citations:* 0 [*Google Scholar*], 0 [*Scopus*].
*Ranking: GGS Class* n.a., *GGS Rating* n.a., *CORE* n.a., *LiveSHINE* n.a., *MA* n.a. [GGS].

### Posters

[P1] **M. Carminati**, R. Caron, F. Maggi, I. Epifani, and S. Zanero. *"Poster: BankSealer: A Decision Support System For Internet Banking Fraud Analysis and Investigation"*. In: **International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment**, **DIMVA 2015**, 2015.

[P2] N. Mariani, A. Continella, M. Pogliani, **M. Carminati**, F. Maggi, and S. Zanero. *"Poster: Detecting WebInjects through Live Memory Inspection"*. In: **Proceedings of the IEEE Symposium on Security and Privacy (SP)**, 2017. url
*Citations:* 2 [*Google Scholar*], 0 [*Scopus*].

### Preprint/ArXiv

[X1] A. Erba, R. Taormina, S. Galelli, M. Pogliani, **M. Carminati**, S. Zanero, and N. O. Tippenhauer. *"Real-time Evasion Attacks with Physical Constraints on Deep Learning-based Anomaly Detectors in Industrial Control Systems"*. , *2019*, doi:doi.org/10.48550/arXiv.1907.07487, url: https://doi.org/10.48550/arXiv.1907.07487.
*Citations:* 24 [*Google Scholar*].

[X2] A. d. F. Tron, S. Longari, **M. Carminati**, M. Polino, and S. Zanero. *"CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks"*. , *2022*, doi:10.48550/arXiv.2209.09557, url: https://doi.org/10.48550/arXiv.2209.09557.

[X3] S. Longari, A. Nichelini, C. A. Pozzoli, **M. Carminati**, and S. Zanero. *"CANdito: Improving Payload-based Detection of Attacks on Controller Area Networks"*. , *2022*, doi:10.48550/arXiv.2208.06628, url: https://doi.org/10.48550/arXiv.2208.06628.

[X4] L. Binosi, G. Barzasi, **M. Carminati**, S. Zanero, and M. Polino. *"The Illusion of Randomness: An Empirical Analysis of Address Space Layout Randomization Implementations"*. , *2024*, doi:10.48550/ARXIV.2408.15107, url: https://doi.org/10.48550/ARXIV.2408.15107.

[X5] A. Boiano, M. D. Gennaro, L. Barbieri, **M. Carminati**, M. Nicoli, A. Redondi, S. Savazzi, A. S. Aillet, D. R. Santos, and L. Serio. *"A Secure and Trustworthy Network Architecture for Federated Learning Healthcare Applications"*. , *2024*, doi:10.48550/ARXIV.2404.11698, url: https://doi.org/10.48550/ARXIV.2404.11698.

[X6] D. Reis Santos, A. Sund Aillet, A. Boiano, U. Milasheuski, L. Giusti, M. Di Gennaro, S. Kianoush, L. Barbieri, M. Nicoli, **M. Carminati**, and others. *"A Federated Learning Platform as a Service for Advancing Stroke Management in European Clinical Centers"*. , *2024*, doi:doi.org/10.48550/arXiv.2410.13869, url: https://doi.org/10.48550/arXiv.2410.13869.

*Citations were collected on 05/11/2024.*

## Awards & Scholarship

- **ZOOX AutoDriving Security Award Runner-up!**
  Paper: "Securing Lidar Communication through Watermark-based Tampering Detection"
  **Symposium on Vehicles Security and Privacy (VehicleSec)** *2024*
- **Best Industrial Paper Award**
  Paper: "Rainfuzz: Reinforcement-Learning Driven Heat-Maps for Boosting Coverage-Guided Fuzzing"
  **12th International Conference on Pattern Recognition Applications and Methods, ICPRAM 2023** *2023*
- **Best Paper Honorable Mention (Top 20 Best Papers)**
  Paper: "CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks"
  **2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022,** *2022*
- Startup Competition Digital 360 Award, Winner "Banking Innovation" *2016*
- Startup Competition Security Rockstars, Finalist *2016*
- Ph.D. scholarship from "M.I.U.R". *2013–2016*
- Best M.Sc. Thesis Nominee at "Premio tesi ClusIT", third place. *2013*
- "Yves Deswarte" **Best Student Paper Award**
  Paper: "BankSealer: An Online Banking Fraud Analysis and Decision Support System"
  **29th IFIP SEC TC 11 International Conference**, **IFIP SEC 2014** *2014*

## Talks and Seminars

### Invited Talks

- *"RAMSES: Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware"*
  DG HOME 14th CoU Thematic Workshops, Bao Congress Center, Rue Félix Hap 11, 1040 Etterbeek, Bruxelles. *2019*
- *"RAMSES: Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware"*
  DG HOME 12th CoU Meeting on Forensics, Bao Congress Center, Rue Félix Hap 11, 1040 Etterbeek, Bruxelles. *2018*
- *"Machine Learning for Fraud Detection"*
  Digital Payments: how safe are they? Risks, opportunities and implications, Milan Fintech District, Milan, Italy. *2018*
- *"A Supervised Auto-Tuning Approach for a Banking Fraud Detection System"*
  Italian Conference on Cyber Security, ITASEC 2018, Milan, Italy. *2018*
- *"Machine Learning for Fraud Detection"*
  Cyber Crime: La minaccia Invisibile che minaccia il mondo
  Osservatori.net Digital Innovation Event, Milan, Italy. *2017*
- *"BankSealer: A Decision Support System For Internet Banking Fraud Analysis and Investigation"*
  IV Conference on Application Security and Modern Technologies
  Sicurezza e Governance nell'era dell'Internet of Things, Università Ca' Foscari, Venice, Italy. *2016*
- *"BankSealer: An Online Banking Fraud Analysis and Decision Support System"*
  Microsoft Research, Mountain View, Palo Alto, USA. *2015*
- *"BankSealer: An Online Banking Fraud Analysis and Decision Support System"*
  Infosek Conference, Nova Gorica, Slovenia. *2014*

### Conference Talks

- *"Natural Language Processing Approach for Financial Fraud Detection"*
  AI for Security and Security of AI Workshop
  AISAI 2022 - ITASEC 2022, Rome, Italy. *2022*
- *"Evasion Attacks against Banking Fraud Detection Systems"*
  Italian Conference on Cybersecurity
  ITASEC 2022, Rome, Italy. *2022*
- *"NoSQL Breakdown: A Large-scaleAnalysis of Misconfigured NoSQL Services"*
  Annual Computer Security Applications Conference
  ACSAC 20, Virtual Event / Austin, TX, USA. *2020*

- *"Evasion Attacks againstBanking Fraud Detection Systems"*
  23rd International Symposium on Research inAttacks, Intrusions and Defenses,
  RAID 2020, Virtual Event / San Sebastian, Spain. *2020*
- *"FraudBuster: Temporal Analysis and Detection of Advanced Financial Frauds"*
  International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment,
  DIMVA 2018, Campus Paris-Saclay, France. *2018*
- *"BankSealer: An Online Banking Fraud Analysis and Decision Support System"*
  International Conference on ICT Systems Security and Privacy Protection
  IFIP SEC 2014, Marrakech, Morocco. *2014*

### Seminar

- *"Security of Federated Learning Systems"*
  TRUSTroke WP2 review and seminars, CERN, Geneve *2023*
- *"Evasion Attacks against Banking Fraud Detection Systems"*
  Huawei - AI4Sec Research Seminar, Virtual Event *2022*
- *"Machine Learning for Fraud Detection"*
  *Course:* Advanced Topics in Computer Security
  CSE – Ph.D. level, Politecnico di Milano, Milan, Italy. *2017-2018*

## Advisor Activity

### Ph.D. Advisor

- **Advisor** of 3 Ph.D. Students:

  Tommaso Paladini, "Analysis and Applications of Machine Learning-based Cybercrime Investigation, Detection, and Prevention Techniques" *2022-Today*

  Marco Di Gennaro, "Security of Machine and Federated Learning Systems" *2024-Today*

  Francesco Panebianco, "Artificial Intelligence for Cybersecurity" *2024-Today*

- **Co-Advisor** of 5 Ph.D. Students:

  Stefano Longari, "On the security of connected automotive systems" *2017-2020*

  Alessandro Bertani, "Architetture di sicurezza per sottosistemi di memoria in applicazioni datacenter" *2022-Today*

  Gabriele Digregorio, "Offensive and Defensive Cybersecurity for Critical Infrastructures" *2023-Today*

  Daniele Mammone, "Cybersecurity of cyberphysical systems" *2023-Today*

  Juri Sacchetta, "New methodologies to assess the security of binary applications" *2024-Today*

### Advisor of M.Sc. Thesis

- **Advisor** of 26 M.Sc. Thesis:

  Domenico Putignano, "A quantitative analysis of the relevance of underground forums in cyber threat intelligence" *2024*

  Davide Biarese, "AdvBench: a framework to evaluate adversarial attacks against fraud detection systems" *2024*

  Michele Albanese, "Guided Risk Assessment Tool: Model Research to Implementation" *2024*

  Alessandro Bagnacani, "Improving the extraction of threat actor behavior from cyber threat intelligence reports" *2024*

  Laura Amabili, "On the impact of dataset construction to malware detection models performance and robustness" *2024*

  Marco Di Gennaro, "Packhero: leveraging graph-based analysis for packer identification" *2024*

  Lara Ferro, "Unveiling the potential of hacker forums in cyber threat intelligence: a longitudinal analysis of emerging threats in discussions" *2024*

  Giovanni Dragonetti, "A graph-based approach for the application and evaluation of address clustering heuristics on the Bitcoin blockchain" *2023*

  Federica Marchetti, "A study of machine learning algorithms for detecting ticket forgery fraud in public transportation" *2023*

  Marco Tagliafierro, "Adversarial attacks against federated learning systems: a review" *2023*

  Alessio Battaglia, "Adversarial machine learning techniques in Fraud Detection: a Survey" *2023*

  Marco Pianta, "Amatriciana: A Temporal Graph Neural Networks-based Framework for Money Laundering Detection" *2023*

  Luca Maniscalchi, "FraudBench: A Benchmarking Software for Fraud Detection Systems" *2023*

  Salvatore Maccarrone, Gabriele Digregorio, "tarallo: an end-to-end framework for malware behavior obfuscation" *2023*

  Francesco Cermaria, "Cost-aware adversarial attacks and defenses for tabular data" *2023*

  Francesco Nicotera, "Enhancing cybersecurity through vulnerability assessment and penetration testing: a case study analysis on an Italian automotive distribution company" *2023*

  Tommaso Paladini, "RAD-X: an adversarial training approach for Fraud Detection Systems" *2022*

Fabio Nappi, "A survey of intrusion detection systems for controller area networks and FPGA evaluation" *2022*

Filippo Maria Benati, "An analysis of defense mechanisms against evasion attacks in the fraud detection domain" *2022*

Marco Di Gloria, "ANNtivirus: dissecting antivirus programs through neural network explainability" *2022*

Andrea Maria Ventura, "Improving poisoning attacks against banking fraud detection systems" *2022*

Francesco Noseda, "Evasion attacks against Intrusion Detection Systems on Communication Area Network" *2022*

PILLARELLA, ROSAMARIA, "A holistic generative adversarial network-based methodology for synthetic banking dataset generation" *2021*

Maria Paola Tatulli, "HAMLET: Hierarchical Anti Money Laundering Encoder Transformer" *2021*

Grotti Pietro, "Novel Evasion Attacks against Banking Fraud Detection Systems" *2021*

Francesco Monti, "Poisoning attacks against banking fraud detection systems" *2020*

### Co-advisor of M.Sc. Thesis

- **Co-advisor** of 45 M.Sc. Thesis:

Sidoti Migliore, Francesco, "A study on windows malware evasion strategies in the context of sandboxes and packers" *2024*

Gervasio, Dario Alex, "Empirical security evaluation of digital therapeutic applications" *2024*

Mileto, Alessandro, "On the performance of hypervisor-assisted memory monitoring for code unpacking detection" *2024*

Saputelli, Edoardo, "A blockchain-based framework to enhance air traffic control security using ADS-B protocol" *2023*

Morabito, Nicholas, "Analysis of evasive behavior against a sandbox" *2023*

Barotti, Matteo, "Emego: enhancing malware evasion through genetic optimization" *2023*

Cerracchio, Paolo, "Exploring gradient-based evasion techniques against automotive intrusion detection systems" *2023*

Marazzi, Michele, "Securing Lidar communication in autonomous vehicles through watermark-based tampering detection" *2023*

Cainazzo, Elisabetta, "Panettone: evaluating federated learning implementations of CAN intrusion detection systems" *2023*

Curcio, Cesare, "A game theoretical approach to the fraud detection problem" *2022*

Coccia, Giorgio, "A study of evasive behaviors in commercial packers" *2022*

Benati, Filippo Maria, "An analysis of defence mechanisms against evasion attacks in the fraud detection domain" *2022*

Pellizzi, Kristopher Francesco, "Memtrace: a dynamic memory overlaps tracing tool" *2022*

Ciaccia, Giuseppe, "MPT-Mon: a memory monitoring technique based on page tables supervision" *2022*

Fioravanti, Tommaso, "Evaluation of quantum machine learning algorithms for cybersecurity" *2022*

Jannone, Jacopo, "Attack detection in industrial robot controllers using Arm TrustZone" *2022*

Gozzini, Stefano, "PINvader: a dynamic analysis tool for evasive techniques detection and bypass in 64-bit Windows binaries" *2022*

Di Cesare, Federico, "TriggerOne: backdoor-injection attacks on pre-trained models for malware detection" *2022*

Puce, Gabriele"A digital twin simulation framework for cyber physical system and anomaly detection" *2021*

Dottino, Camilla; Rezzonico, Filippo, "A feasibility analysis of asymmetric key distribution system for implantable cardioverter defibrillators" *2020*

Remigio, Riccardo, "A methodology to reconstruct information and enable static analysis in raw binaries" *2020*

Fernandez Rodriguez, Javier, "A natural language processing approach to fraud detection" *2020*

Papale, Michele, "An ensemble approach for banking fraud detection" *2020*

Bova, Salvatore, "An evaluation of anti-evasion techniques implemented in malware analysis sandboxes and debuggers" *2020*

Ferrari, Dario, "NoSQL breakdown: a large-scale analysis of misconfigured NoSQL services" *2020*

Patuelli, Simone, "Towards understanding alternative and mainstream news dissemination on social media: the case of the 2018 Italian election" *2020*

Labanca, Danilo, "Amaretto: an active learning framework for money laundering detection" *2019*

Salvadore, Matteo; Nespoli, Benedetto Maria, "Apicula: static detection of API call in malware memory" *2019*

Mortillaro, Luca, "Crave 2.0: toward scalable and reproducible antivirus analyses" *2019*

Santini, Luca, "Evasion attacks against banking fraud detection systems" *2019*

Zheng, Shihao, "Labelless concept drift detection and explanation" *2019*

Termignone, Gabriele, "Towards automated cutting of binaries" *2019*

Giossi, Gabriele Oliviero; Mosca, Paolo, "MALwhere: a memory forensics platform for financial malware analysis and classification" *2019*

Jegher, Andrea, "WMD: a scalable web-malware detection system" *2019*

Bucci, Giovanni, "RansomScan: extracting intelligence from ransomware families" *2018*

Gnecco, Enrico, "BitAnalyzer: a framework for extracting intelligence from the blockchain" *2018*

Bulloni, Matteo, "FraudCleaner: an unsupervised ensemble approach for money laundering and financial fraud detection" *2018*

Dignani, Alessandro, "FraudsDigger: an active learning tool for online banking fraud detection" *2018*

Perillo, Salvatore, "Improving the extraction of knowledge from the blockchain" *2018*

Innocenti, Tommaso, "Less is more (secure) deprecator: automated reduction of the attack surface in modern browsers" *2018*

Belhaj, Marouan, "FraudKiller: an online fraud detection system for digital marketplaces" *2017*

Baggio, Alessandro, "FraudBuster: time-based analysis of Internet banking fraud" *2016*

Biondani, Andrea, "Fraudhunter: a supervised fraud detection tool for Internet banking transactions" *2016*

Ricci, Michele, "Versatile processing platform for embedded energy spectroscopy" *2016*

Valentini, Luca, "Genetic algorithms for optimizing Internet banking fraud detection" *2015*

### Professional Master's Degree ("Master universitario di primo livello")

- **Academic tutor** of 12 Professional Master's Degree thesis

*2019-2024*

Milano, January 14, 2025

Michele Carminati

---

- Autorizzo il trattamento dei dati personali contenuti nel mio curriculum vitae in base all'art. 13 del GDPR 679/16
- Il sottoscritto, Michele Carminati, consapevole delle sanzioni penali previste dall'art. 76 T.U. N. 445 del 28.12.2000 sulle disposizioni legislative e regolamentari in materia di documentazione amministrativa nel caso di mendaci dichiarazioni o esibizione di atti falsi o contenenti dati non rispondenti a verità, dichiara sotto la propria responsabilità che quanto sopra riportato risponde a verità.