

Stefano Longari

Last updated: 06/2024
stefano.longari@polimi.it

Ricercatore a Tempo Determinato A

NECSTLab, DEIB
Politecnico di Milano
Via Ponzio 34/5, 20133, Milan, Italy
Scopus - Google Scholar

I received my Ph.D. degree in Information Technology from Politecnico di Milano in June 2021 with a thesis on the security of automotive systems. I am currently an assistant professor (RTDa) at Politecnico di Milano, working in the system security group at NECST Laboratory inside the Dipartimento di Elettronica, Informazione e Bioingegneria. The focus of my research revolves around offensive and defensive techniques for the security of cyber-physical systems and transportation systems, e.g., automotive, space, industry 4.0, and critical infrastructure. I teach mainly courses and lectures on (cyber-physical) systems security and social engineering.

RESEARCH INTERESTS

My research is centered in the computer security field, traditionally referred to as "systems security." I am particularly interested in the area of cyber-physical systems and how they can be defended against threats by incorporating techniques from multiple fields. My goal, in studying both defensive measures and new attack methods, is to gain a comprehensive understanding of the threat model of this evolving field.

Cyber-physical systems (CPSs) are defined as physical/mechanical systems controlled by computer-based algorithms. Such systems play a crucial role in various critical infrastructures, such as transportation, healthcare, power plants, and manufacturing. The growth in automation of these systems increases the possible end goals of an attacker, while the integration of CPS with the Internet and other communication networks increases the attack surface and the overall amount of exploitable vulnerabilities. Moreover, being CPSs often part of critical infrastructure, attacks on these systems can have serious consequences for both public safety and economic stability. Ensuring the security of CPSs is therefore a critical issue that should be approached at multiple levels. Surely the purely "cyber" element of the system should be secured with well known methodologies, but it is also crucial to analyze the implications of the "physical" one, understanding how the physical world interacts with digital systems and which vulnerabilities this interaction leads to. A multidisciplinary approach towards the security of these systems is therefore necessary, including software, hardware, and communication engineering, machine learning, control systems, and other relevant fields. The development of secure CPS is essential to ensure their reliable operation and to protect against potential threats that could cause harm to individuals, organizations, and society as a whole.

My research interests mainly delve into the security of industrial and manufacturing automation, land - mainly automotive - and air transportation systems, space and satellite systems, and overall critical cyber-physical infrastructures.

RESEARCH EXPERIENCE

Assistant Professor (RTDa) <i>Politecnico di Milano</i> <i>Research topic:</i> Cybersecurity for Industry 4.0, Cyber-physical systems, and critical infrastructure. <i>Research group:</i> NECSTLab, System security research group.	May 2023 — <i>Milan, Italy</i>
Postdoctoral Researcher <i>Politecnico di Milano</i> <i>Research topic:</i> Offensive and defensive security techniques for cyber-physical systems. <i>Research group:</i> NECSTLab, System security research group.	Jun 2021 — Apr 2023 <i>Milan, Italy</i>
Research Internship <i>ESCRYPT GmbH,</i> <i>Research topic:</i> Research and development of new security techniques for automotive on-board CAN-connected devices.	Oct 2019 — Apr 2020 <i>Stuttgart, Germany</i>

EDUCATION

Ph.D. in Information Technology , <i>Politecnico di Milano</i> Dissertation title: <i>On the security of connected automotive systems</i>	Jun 2021
M.Sc. in Computer Science and Engineering , <i>Politecnico di Milano</i> Dissertation title: <i>On the security of connected vehicles</i>	Apr 2018
Bachelor in Computer Science and Engineering , <i>Politecnico di Milano</i>	Sep 2015

ACADEMIC ROLES

Specialization Degree Coordinator: Specialization Degree Title: "security specialist" specialization degree ("Master universitario di primo livello"). <i>CEFRIEL and Politecnico di Milano</i> <i>Number of students:</i> ~20	2022 — Present
Event and Conference Organization: OWASP Italy Day 2023 <i>OWASP Italy and Politecnico di Milano</i>	2023

Stefano Longari

Last updated: 06/2024
stefano.longari@polimi.it

Ricercatore a Tempo Determinato A

NECSTLab, DEIB
Politecnico di Milano
Via Ponzio 34/5, 20133, Milan, Italy
Scopus - Google Scholar

Program Committee:

- Italian conference on Cybersecurity, **ITASEC** 2024
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment, **DIMVA** 2024
- Workshop on Re-design Industrial Control Systems with Security, **RICSS** (in conjunction with Euro S&P) 2023
- Cyber-Physical System Security Workshop, **CPSS** (in conjunction with ASIACCS) 2023
- Workshop on Automotive Cybersecurity, **ACSW** (in conjunction with EURO S&P) 2022 — 2024
- Joint Workshop on CPS & IoT Security and Privacy, **CPSIoTSec** (in conjunction with ACM CCS) 2022

Reviewer:

- IEEE Security and Privacy Symposium, **IEEE S&P** (Subreviewer) 2023 — 2024
- ACM Computers and Communication Security, **ACM CCS** (Subreviewer) 2023 — 2024
- Elsevier Journal of Parallel and Distributed Computing, **JPDC** 2024
- IEEE Transactions on Aerospace and Electronic Systems, **IEEE TAES** 2022 — 2023
- IEEE Internet of Things Journal, **IEEE IoT** 2022
- IEEE Transactions on Dependable and Secure Computing, **IEEE TDSC** 2022
- International Conference on Security for Information Technology and Communications, **SecITC2022** 2022
- IEEE Transactions on Industrial Informatics, **IEEE TII** 2021 — 2022
- Elsevier Computer and Security, **COSE** 2019 — 2024
- IEEE Transactions on Information Forensics and Security, **IEEE T-IFS** 2021
- IEEE Transactions on Emerging Topics in Computing, **IEEE TETC** 2018

PUBLICATIONS

Productivity and Impact Metrics

Scientific Productivity: Author/Co-author of 6 scientific publications on journal papers, including 5 top-ranked Q1 journal papers based on SCIMAGO, and 10 peer-reviewed conferences, including 1 top-ranked security conference where the work received an award for its value. 12 publication entries on Scopus (+2 yet to be published in proceedings). 16 publication entries on Google Scholar.

Based on Google Scholar: h-index 7 citations 214

Based on Scopus: h-index 7 citations 134

Peer-reviewed Journals

- **Longari, S.**, Jannone, J., Carminati, M., Tanelli, M., & Zanero, S. (2024). Janus: A Trusted Execution Environment Approach for Attack Detection in Industrial Robot Controllers. (To be published in) IEEE Transactions on Emerging Topics in Computing.
- **Longari, S.**, Pozzone, A., Leoni, J., Polino, M., Carminati, M., Tanelli, M., & Zanero, S. (2023). CyFence: Securing Cyber-physical Controllers Via Trusted Execution Environment. IEEE Transactions on Emerging Topics in Computing.
- Nichelini, A., Pozzoli, C. A., **Longari, S.**, Carminati, M., & Zanero, S. (2023). Canova: a hybrid intrusion detection framework based on automatic signal classification for can. Computers & Security, 128, 103166.
- Maffiola, D., **Longari, S.**, Carminati, M., Tanelli, M., & Zanero, S. (2021). GOLIATH: A Decentralized Framework for Data Collection in Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems.
- **Longari, S.**, Valcarcel, D. H. N., Zago, M., Carminati, M., & Zanero, S. (2020). CANnolo: An anomaly detection system based on LSTM autoencoders for controller area network. IEEE Transactions on Network and Service Management, 18(2), 1913-1924.
- Zago, M., **Longari, S.**, Tricarico, A., Carminati, M., Pérez, M. G., Pérez, G. M., & Zanero, S. (2020). ReCAN-Dataset for reverse engineering of Controller Area Networks. Data in brief, 29, 105149.

Peer Reviewed Conference Proceedings

- **Longari, S.**, Galletti, G., Holle, J., & Zanero, S. (2024). CANter: data-link layer detection of drop-and-spoof attacks on CAN and CAN FD. (To be published) In Proceedings of the Italian Conference on Cyber Security (ITASEC 2024) (pp. 1-16). CEUR.
- Digregorio, G., Cainazzo, E., **Longari, S.**, Carminati, M., & Zanero, S. (2024, June) Evaluating the Impact of Privacy-Preserving Federated Learning on CAN Intrusion Detection. (To be published) In proceedings of the IEEE Vehicular Technology Conference Spring (VTC Spring 2024).
- Cerracchio, P., **Longari, S.**, Carminati, M., & Zanero, S. (2024, February) Investigating the Impact of Evasion Attacks Against Automotive Intrusion Detection Systems. In Proceedings of the 2024 Symposium on Vehicle Security and Privacy (VehicleSec 2024).
- Marazzi, M., **Longari, S.**, Carminati, M., & Zanero, S. (2024, February) Securing LiDAR Communication through Watermark-based Tampering Detection. In Proceedings of the 2024 Symposium on Vehicle Security and Privacy (VehicleSec 2024).
- **Longari, S.**, Pozzoli, C. A., Nichelini, A., Carminati, M., & Zanero, S. (2023, June). Candito: improving payload-based detection of attacks on controller area networks. In International Symposium on Cyber Security, Cryptology, and Machine Learning (pp. 135-150). Cham: Springer Nature Switzerland.

Stefano Longari

Last updated: 06/2024
stefano.longari@polimi.it

Ricercatore a Tempo Determinato A

NECSTLab, DEIB
Politecnico di Milano
Via Ponzio 34/5, 20133, Milan, Italy
Scopus - Google Scholar

- **Longari, S.**, Nosedà, F., Carminati, M., & Zanero, S. (2023, June). Evaluating the Robustness of Automotive Intrusion Detection Systems Against Evasion Attacks. In International Symposium on Cyber Security, Cryptology, and Machine Learning (pp. 337-352). Cham: Springer Nature Switzerland.
- Avanzi, D., **Longari, S.**, Polino, M., Carminati, M., Zanchettin, Tanelli, M., & Zanero, S. (2023). Task Aware Intrusion Detection for Industrial Robots. In Proceedings of the Italian Conference on Cyber Security (ITASEC 2023) (pp. 1-16). CEUR.
- de Faveri Tron, A., **Longari, S.**, Carminati, M., Polino, M., & Zanero, S. (2022, November). 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 (pp. 711-723).
- **Longari, S.**, Penco, M., Carminati, M., & Zanero, S. (2019, November). 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 (pp. 39-50).
- **Longari, S.**, Cannizzo, A., Carminati, M., & Zanero, S. (2019, December). A secure-by-design framework for automotive on-board network risk analysis. In 2019 IEEE Vehicular Networking Conference (VNC) (pp. 1-8). IEEE.

Awards

- Best Paper Runner Up, Securing LiDAR Communication through Watermark-based Tampering Detection. 2024 Symposium on Vehicle Security and Privacy (VehicleSec 2024).
- Best Paper Honorable Mention, CANflict: Exploiting Peripheral Conflicts for Data-Link Layer Attacks on Automotive Networks. 2022 ACM SIGSAC Conference on Computer and Communications Security.

Patents

- Sistema di riconoscimento di manomissione del codice di un sistema di controllo mediante uso di processori con memoria trusted (Computer-implemented real-time control system for controlling a physical system or device), International application ref: WO2023002321A1. Numero di deposito italiano: 102021000018998. **S. Longari**, A. Pozzone, M. Tanelli, S. Zanero. Published 2023. 01. 26.
- Submitted: Verfahren zum Erkennen eines Angriffs auf einen zu sichernden Busteilnehmer, Überwachungseinheit und Bussystem (Method for detecting an attack on a to be protected bus node, monitoring system and the bus). Registration number: DE 102022207911.6. **S. Longari**, J. Holle. Registered on 01.08.2022.

SPEAKER ACTIVITY

Paper presentation at Italian Conference on Cybersecurity (ITASEC)	2024
<i>Title: CANter: data-link layer detection of drop-and-spoof attacks on CAN and CAN-FD</i>	
Paper presentation at 2024 Symposium on Vehicle Security and Privacy (VehicleSec)	2024
<i>Title: Investigating the Impact of Evasion Attacks Against Automotive Intrusion Detection Systems.</i>	
Paper presentation at 2024 Symposium on Vehicle Security and Privacy (VehicleSec)	2024
<i>Title: Securing LiDAR Communication through Watermark-based Tampering Detection.</i>	
Invited Talk at Hromatka Group	2023
<i>Title: Risk and Industrial Security</i>	
Invited talk at HackInBo	2022
<i>Title: The CAN Link-Layer, or how we implemented a broken protocol and can we fix it</i>	
Invited online talk for Automotive Security Research Group	2021
<i>Title: CAN Error Handling Attacks and Countermeasures</i>	
Invited talk at Hardwear.io	2019
<i>Title: It's easier to break than to patch: a stealthy DoS attack against CAN</i>	
Paper presentation at IEEE Vehicular Networking Conference	2019
<i>Title: A secure-by-design framework for automotive on-board network risk analysis</i>	
Paper presentation at ACM Workshop on Cyber-Physical Systems Security & Privacy	2019
<i>Title: Copycan: An error-handling protocol based intrusion detection system for controller area network</i>	
Invited talk at Infosek conference	2018
<i>Title: Automotive Security</i>	

PROJECTS

European Projects:

AHEAD: AI-informed Holistic EVs integration Approaches for Distribution grids 2024 — 2028
Role: Task Leader.

Stefano Longari

Last updated: 06/2024
stefano.longari@polimi.it

Ricercatore a Tempo Determinato A

NECSTLab, DEIB
Politecnico di Milano
Via Ponzio 34/5, 20133, Milan, Italy
Scopus - Google Scholar

SARIL: Sustainability And Resilience for Infrastructure and Logistics networks Role: Participant.	2023 — 2026
KEEPER: Key Code based on Nanomaterials to Protect Services and Products Role: Participant.	2024 — 2027
PNRR Projects: MICS: Made in Italy Circolare e Sostenibile Role: Participant.	2023 — 2025

TEACHING ACTIVITIES

Professor:

Course: Human and Physical aspects of Security 2024 —
Politecnico di Milano & Bocconi, Computer Science and Engineering & Cyber Risk Strategy and Governance Master Milan, Italy
Number of students: ~N/A.
Hours: 50/year.

Course: Social engineering 2023 — 2024
Politecnico di Milano & Bocconi, Cyber Risk Strategy and Governance Master Milan, Italy
Number of students: ~30.
Hours: 16/year.

Lecturer:

Course: Cybersecurity 2022 — Present
CEFRIEL & Politecnico di Milano, "security specialist" specialization degree ("Master universitario di primo livello"). Milan, Italy
Course director: Stefano Longari.
Number of students: ~25.
Hours: 110/year.

Course: Cybersecurity Technologies, Procedures and Policies 2023 — Present
Politecnico di Milano & Bocconi, Cyber Risk Strategy and Governance Master Milan, Italy
Course director: Stefano Zanero.
Number of students: ~30.
Hours: 17/year.

Course: Social engineering 2023
Politecnico di Milano & Bocconi, Cyber Risk Strategy and Governance Master Milan, Italy
Instructor: Stefano Longari.
Number of students: ~30.
Hours: 16/year.

Course: Cybersecurity 2019 — Present
CEFRIEL and Politecnico di Milano, "security specialist" specialization degree ("Master universitario di primo livello"). Milan, Italy
Topic: Automotive Security.
Course director: Michele Carminati.
Number of students: ~25.
Hours: 8/year.

Course: Automation and control in vehicles 2021
Politecnico di Milano Milan, Italy
Topic: Security of connected vehicles.
Instructor: Sergio Savaresi.
Number of students: ~50.
Hours: 2/year.

Course: Computer Security 2022
Politecnico di Milano for Microdata Milan, Italy
Course director: Luciano Baresi.
Number of students: ~10.
Hours: 8/year.

Stefano Longari

Last updated: 06/2024
stefano.longari@polimi.it

Ricercatore a Tempo Determinato A

NECSTLab, DEIB
Politecnico di Milano
Via Ponzio 34/5, 20133, Milan, Italy
Scopus - Google Scholar

Course: Cybersecurity <i>POLI.DESIGN founded by Politecnico di Milano, Fundamentals of the air transport system</i> Instructor: Stefano Zanero. Number of students: ~20. Hours: ~10/year.	2019 — 2022 Milan, Italy
Course: Social Engineering <i>Master universitario di primo livello "Cyber Security and Defence", Università degli Studi di Catania</i> Course director: Stefano Zanero. Number of students: ~10. Hours: 11/year.	2021 — Present Milan, Italy
Teaching Assistant: Course: Social engineering <i>Politecnico di Milano & Bocconi, Cyber Risk Strategy and Governance Master</i> Instructor: Stefano Zanero. Number of students: ~30. Hours: 16/year.	2019 — 2022 Milan, Italy
Course: Cybersecurity Technologies, Procedures, and Policies <i>Politecnico di Milano</i> Course director: Stefano Zanero. Number of students: ~30. Hours: 20/year.	2023 — 2024 Milan, Italy
Course: Informatica B <i>Politecnico di Milano</i> Course director: Michele Carminati. Number of students: ~250. Hours: 26/year.	2023 — 2024 Milan, Italy
Course: Computer Security <i>Politecnico di Milano</i> Course director: Stefano Zanero / Michele Carminati. Number of students: ~200. Hours: 10/year.	2019 — 2023 Milan, Italy

ADVISOR ACTIVITY

Advisor of:

Title: CANPak: An Intrusion Detection System against Stealthier Attacks for Controller Area Network	2024
Author: Abbasi Sikandar Mehmood	
Title: Meeting Proof Protocol: a Protocol for Physical Anchor Systems	2024
Author: Sironi Mattia	
Title: Empirical Security Evaluation of Digital Therapeutic Applications	2024
Author: Gervasio Dario Alex	
Title: Micro-Mobility Security: A Systematic Approach via Mobile App Analysis	2024
Author: Balossini Marco	
Title: CANtera: A novel real-world dataset on advanced CAN attacks for intrusion detection systems	2024
Author: Valencic Jas	
Title: Evaluation of Graph-based IDS Based on Outlier Detection Methods for CAN-bus	2024
Author: Balalipour Pedram	
Title: On the feasibility of Adversarial Attacks against IDSs in Automotive CAN	2024
Author: Montalbano Ivan	
Title: Location inference through social media and social relationships	2023
Author: Rizzi Matteo	
Title: Panettone: evaluating federated learning implementations of can intrusion detection systems	2023
Author: Cainazzo Elisabetta	
Title: A Blockchain-based framework to enhance air traffic control security using ADS-B protocol.	2023
Author: Saputelli Edoardo	
Title: A Comprehensive Study of Cyber Threats and Countermeasures in Micromobility.	2023
Author: Rosati Nicholas	
Title: Exploring gradient-based evasion techniques against automotive intrusion detection systems	2023
Author: Cerracchio Paolo	
Title: Towards Secure Electronic Voting : a Literature Review on E-Voting Systems and Attacks.	2023
Author: Barelli Riccardo	
Title: Securing Lidar communication in autonomous vehicles through watermark-based tampering detection	2023
Author: Marazzi Michele	

Stefano Longari

Last updated: 06/2024
stefano.longari@polimi.it

Ricercatore a Tempo Determinato A

NECSTLab, DEIB
Politecnico di Milano
Via Ponzio 34/5, 20133, Milan, Italy
Scopus - Google Scholar

Co-Advisor of:

<i>Title:</i> A survey of intrusion detection systems for controller area networks and FPGA evaluation	2022
<i>Author:</i> Nappi Fabio	
<i>Advisor:</i> Carminati Michele	
<i>Title:</i> Attack detection in industrial robot controllers using Arm TrustZone	2022
<i>Author:</i> Jannone Jacopo	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> Evasion Attacks against Intrusion Detection Systems on Communication Area Network	2022
<i>Author:</i> Nosedà Francesco	
<i>Advisor:</i> Michele Carminati	
<i>Title:</i> CANPass : an extensible framework for bypassing CAN peripherals on unmodified microcontrollers	2021
<i>Author:</i> De Faveri Tron Alvise	
<i>Advisor:</i> Stefano Zanero	
<i>Title:</i> CANova, a classification-based modular intrusion detection system for CAN	2021
<i>Author:</i> Nichelini Alessandro, Pozzoli Carlo Alberto	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> A feasibility analysis of asymmetric key distribution system for implantable cardioverter defibrillators	2020
<i>Author:</i> Dottino Camilla, Rezzonico Filippo	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> A novel software architecture to secure real-time control systems	2020
<i>Author:</i> Pozzone Alessandro	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> A long short-term memory based approach for reverse engineering and classification of CAN signals	2020
<i>Author:</i> Tricarico Andrea	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> Analysis of a distributed ledger framework for automotive positioning applications	2019
<i>Author:</i> Legler Renato	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> Anomaly detection system for automotive CAN using LSTM autoencoders	2019
<i>Author:</i> Nova Valcarcel Daniel Humberto	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> CopyCAN : a traffic monitoring error-based intrusion detection system for controller area network	2019
<i>Author:</i> Penco Matteo	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> A study on CAN filtering techniques	2018
<i>Author:</i> Martino Andrea	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> Explorative techniques and vulnerability assessment on automotive networks	2018
<i>Author:</i> Calin Liviu Razvan	
<i>Advisor:</i> Zanero Stefano	
<i>Title:</i> A cybersecurity-by-design methodology and tool for vehicular networks	2018
<i>Author:</i> Cannizzo Andrea	
<i>Advisor:</i> Zanero Stefano	