Last updated: 03/2024
stefano.longari@polimi.it

Stefano Longari

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 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) **May 2023 —**
Politecnico di Milano *Milan, Italy*
Research topic: Cybersecurity for Industry 4.0, Cyber-physical systems, and critical infrastructure.
Research group: NECSTLab, System security research group.

Postdoctoral Researcher **Jun 2021 — Apr 2023**
Politecnico di Milano *Milan, Italy*
Research topic: Offensive and defensive security techniques for cyber-physical systems.
Research group: NECSTLab, System security research group.

Research Internship **Oct 2019 — Apr 2020**
ESCRYPT GmbH, *Stuttgart, Germany*
Research topic: Research and development of new security techniques for automotive on-board CAN-connected devices.

Education

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

Academic Roles

Specialization Degree Coordinator:
Specialization Degree Title: *"security specialist" specialization degree ("Master universitario di primo livello").* ***2022 — Present***
CEFRIEL and Politecnico di Milano
Number of students: ∼20

Event and Conference Organization:
OWASP Italy Day 2023 ***2023***
OWASP Italy and Politecnico di Milano

Last updated: 03/2024
stefano.longari@polimi.it

Stefano Longari

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 5 scientific publications on journal papers, including 4 top-ranked Q1 journal papers based on SCIMAGO, and 6 peer-reviewed conferences, including 1 top-ranked security conference where the work received an award for its value. 11 publication entries on Scopus. 13 publication entries on Google Scholar.*

Based on Google Scholar: h-index 7 citations 200
Based on Scopus: h-index 6 citations 125

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.**, Pozone, 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.

Last updated: 03/2024
stefano.longari@polimi.it

Stefano Longari

Ricercatore a Tempo Determinato A

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

- **Longari, S.**, Noseda, 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. Pozone, 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 Cyberesecurity (ITASEC)** **2024**
Title: CANter: data-link layer detection of drop-and-spoof attacks on CAN and CAN-FD

Paper presentation at **2024 Symposium on Vehicle Security and Privacy (VehicleSec)** **2024**
Title: Investigating the Impact of Evasion Attacks Against Automotive Intrusion Detection Systems.

Paper presentation at **2024 Symposium on Vehicle Security and Privacy (VehicleSec)** **2024**
Title: Securing LiDAR Communication through Watermark-based Tampering Detection.

Invited Talk at **Hromatka Group** **2023**
Title: Risk and Industrial Security

Invited talk at **HackInBo** **2022**
Title: The CAN Link-Layer, or how we implemented a broken protocol and can we fix it

Invited online talk for **Automotive Security Research Group** **2021**
Title: CAN Error Handling Attacks and Countermeasures

Invited talk at **Hardwear.io** **2019**
Title: It's easier to break than to patch: a stealthy DoS attack against CAN

Paper presentation at **IEEE Vehicular Networking Conference** **2019**
Title: A secure-by-design framework for automotive on-board network risk analysis

Paper presentation at **ACM Workshop on Cyber-Physical Systems Security & Privacy** **2019**
Title: Copycan: An error-handling protocol based intrusion detection system for controller area network

Invited talk at **Infosek conference** **2018**
Title: Automotive Security

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.

Last updated: 03/2024
stefano.longari@polimi.it

Stefano Longari

Ricercatore a Tempo Determinato A

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

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.

Course: **Cybersecurity** **2019 — 2022**
POLI.DESIGN founded by Politecnico di Milano, Fundamentals of the air transport system *Milan, Italy*
Instructor: Stefano Zanero.
Number of students: ∼20.
Hours: ∼10/year.

Course: **Social Engineering** **2021 — Present**
Master universitario di primo livello "Cyber Security and Defence", Università degli Studi di Catania *Milan, Italy*
Course director: Stefano Zanero.
Number of students: ∼10.
Hours: 11/year.

Teaching Assistant:

Course: **Social engineering** **2019 — 2022**
Politecnico di Milano & Bocconi, Cyber Risk Strategy and Governance Master *Milan, Italy*
Instructor: Stefano Zanero.
Number of students: ∼30.
Hours: 16/year.

Last updated: 03/2024
stefano.longari@polimi.it

Stefano Longari

Ricercatore a Tempo Determinato A

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

Course: **Cybersecurity Technologies, Procedures, and Policies** **2023 — 2024**
Politecnico di Milano *Milan, Italy*

Course director: Stefano Zanero.
Number of students: ∼30.
Hours: 20/year.

Course: **Informatica B** **2023 — 2024**
Politecnico di Milano *Milan, Italy*

Course director: Michele Carminati.
Number of students: ∼250.
Hours: 26/year.

Course: **Computer Security** **2019 — 2023**
Politecnico di Milano *Milan, Italy*

Course director: Stefano Zanero / Michele Carminati.
Number of students: ∼200.
Hours: 10/year.

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

Last updated: 03/2024
stefano.longari@polimi.it

Stefano Longari

Ricercatore a Tempo Determinato A

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

Co-Advisor of:

Title: A survey of intrusion detection systems for controller area networks and FPGA evaluation 2022
Author: Nappi Fabio
Advisor: Carminati Michele

Title: Attack detection in industrial robot controllers using Arm TrustZone 2022
Author: Jannone Jacopo
Advisor: Zanero Stefano

Title: Evasion Attacks against Intrusion Detection Systems on Communication Area Network 2022
Author: Noseda Francesco
Advisor: Michele Carminati

Title: CANPass : an extensible framework for bypassing CAN peripherals on unmodified microcontrollers 2021
Author: De Faveri Tron Alvise
Advisor: Stefano Zanero

Title: CANova, a classification-based modular intrusion detection system for CAN 2021
Author: Nichelini Alessandro, Pozzoli Carlo Alberto
Advisor: Zanero Stefano

Title: A feasibility analysis of asymmetric key distribution system for implantable cardioverter defibrillators 2020
Author: Dottino Camilla, Rezzonico Filippo
Advisor: Zanero Stefano

Title: A novel software architecture to secure real-time control systems 2020
Author: Pozone Alessandro
Advisor: Zanero Stefano

Title: A long short-term memory based approach for reverse engineering and classification of CAN signals 2020
Author: Tricarico Andrea
Advisor: Zanero Stefano

Title: Analysis of a distributed ledger framework for automotive positioning applications 2019
Author: Legler Renato
Advisor: Zanero Stefano

Title: Anomaly detection system for automotive CAN using LSTM autoencoders 2019
Author: Nova Valcarcel Daniel Humberto
Advisor: Zanero Stefano

Title: CopyCAN : a traffic monitoring error-based intrusion detection system for controller area network 2019
Author: Penco Matteo
Advisor: Zanero Stefano

Title: A study on CAN filtering techniques 2018
Author: Martino Andrea
Advisor: Zanero Stefano

Title: Explorative techniques and vulnerability assessment on automotive networks 2018
Author: Calin Liviu Razvan
Advisor: Zanero Stefano

Title: A cybersecurity-by-design methodology and tool for vehicular networks 2018
Author: Cannizzo Andrea
Advisor: Zanero Stefano