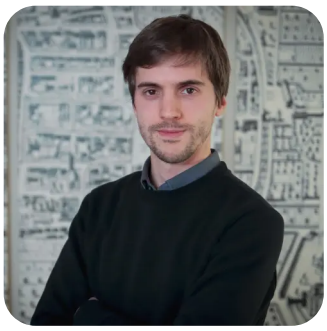

Stefano Berlato

Computer Scientist, PhD

Researcher, De Cifris member.
Keen on cybersecurity, cloud native, and applied cryptography.
Football coach, KH fan, D&D master.

Researcher@FBK | Teaching Assistant@UniTN | Football Coach@PGS Concordia

Last update: 14 June 2024

Research Interests

Working on

Applied Cryptography 5/5 | Authorization 4/5 | Authentication 3/5 | Cloud Native 2/5

Will work on

DevSecOps 1/5

Worked on

Internet of Things 2/5 | Automotive 3/5 | Reverse Engineering 2/5 | Android 3/5

I speak

Italian native | English C1

Experience

Researcher

November 2023 - now

Fondazione Bruno Kessler

Research on applied cryptography, identity and access management, and cybersecurity for cloud native applications. Development of tools for research and demonstration purposes in kotlin. Supervision of interns, BSc and MSc students.

Topics: Applied Cryptography, Authentication, Authorization, DevSecOps, Cloud Native, Kotlin

PhD Student

November 2020 - October 2023

University of Genoa & Fondazione Bruno Kessler

Joint PhD on cryptographic access control in cloud-edge-IoT applications (e.g., Cooperative Connected and Automated Mobility) and design of architectural models for optimal enforcement of cryptographic access control policies.

Topics: Applied Cryptography, Authorization, Internet of Things, Automotive

Research Assistant

October 2018 - October 2020

Fondazione Bruno Kessler

Research activities on access control in the Cloud, mobile and automotive security. Research activities on Cooperative, Connected and Automated Mobility (5G-CARMEN project). Study and design of reverse engineering protections for Java and Android Apps.

Topics: Applied Cryptography, Authorization, Automotive, Reverse Engineering

Intern

July 2018 - October 2018

2ASPIRE

Research and analysis of best practices against malicious Reverse Engineering (RE) to increase the company's knowhow in Android RE antitampering and anti-debugging protections.

Topics: Reverse Engineering, Android

IT Assistant

July 2017 - August 2017

University of Trento

150 hours working contract under the "Information Systems Management" office, Support the deployment of the Digital University project, a new platform serving as Knowledge HUB within the University of Trento.

Topics: None

Intern

June 2016 - September 2016

Heas srl

Design of 2 plugins for the web-based SCADA platform ATVISE® in compliance with high-level HMI industrial standards. Developed gestures and tablet-style functionalities, dynamic object instantiation and linking to PLC data.

Topics: None

Education

PhD

November 2020 - October 2023

University of Genoa & Fondazione Bruno Kessler

PhD in Security, Risk and Vulnerability, Cybersecurity and Reliable Artificial Intelligence curriculum with the thesis "**A Security Service for Performance-Aware End-to-End Protection of Sensitive Data in Cloud Native Applications**".

Master degree

September 2017 - July 2019

University of Trento

Master degree in Computer Science, ICT Innovation - Security&Privacy curriculum (110 cum laude) with the thesis "**A Pragmatic Approach to Handle "Honest but Curious" Cloud Service Providers: Cryptographic Enforcement of Dynamic Access Control Policies**".
Awarded 3rd prize at Thesis Award «Innovating information security» 15th edition - 2019, Clusit.

Bachelor degree

September 2014 - July 2017

University of Trento

Bachelor degree in Computer Science (110 cum laude) with the thesis "**Development of a web based Interface for the Orchestration of Machine Learning Components**".

Research Projects

SERICS

January 2023 - now

Within the SeRiCS ("Security and Rights in CyberSpace") Italian partnership, the project SecCo ("Securing Containers") aims at supporting the secure development and deployment of containerized applications on distributed and heterogeneous architectures, while the project STRIDE ("Secure and TRaceable Identities in Distributed Environments") aims at supporting the secure, protected, and accountable identification of entities and actions through digital identity and access control. Relevant partners are CNR - Consiglio Nazionale delle Ricerche, Telsy S.p.A., ENI, and CINI - Consorzio Interuniversitario Nazionale per l'Informatica.

Topics: Attribute-based Encryption, Cloud Native, DevSecOps, Authorization, Applied Cryptography

METAfora

January 2022 - now

METAfora wants to implement new and innovative models of digital identity management and use, placing itself in the strategic confluence between the evolutions of European regulations

on the subject, thus a regulated and top-down context, and the dynamics of growth and evolution arising from below, understood as the whole world that is now described as metaverse.

Topics: Applied Cryptography, Attribute-based Encryption

FAMILIAR

August 2023 - now

The project aims to conceive and develop a platform (called Familiar) that enables the creation of a coordination system for Long Term Care (LTC) services using innovative digital technologies, with a specific focus on the field of dementia. The ultimate goal is to enhance the quality of life for patients and increase support for their families. Relevant partners are Zucchetti Healthcare, Shifton, SDA Bocconi, Upipa, AIP – Associazione Italiana di Psicogeriatria.

Topics: Applied Cryptography, Authentication, Authorization, Blockchain, Cloud

5G CARMEN

November 2018 - October 2021

The 5G-CARMEN (5G for Connected and Automated Road Mobility in the European UnioN) project is a medium-term effort to significantly drive the research, implementation, and demonstration of refined 5G solutions for the Cooperative, Connected, and Automated Mobility. Relevant partners are Deutsche Telekom AG, BMW Group, Centro Ricerche FIAT, TIM, NOKIA, and Qualcomm.

Topics: Automotive, Authorization, Blockchain, Internet of Things

Teaching, Seminars, and Outreach Events

Teaching Assistant

September 2020 - now

University of Trento

Teaching Assistant for the Computer Science course "Programmazione 1"; preparation of lectures and exams, marking and grading of exams.

Seminar

February 2024

I.I.S. TRON ZANELLA

Seminar "I Perché e i Come della Ricerca: Il Lavoro del Ricercatore nel Campo della Sicurezza Informatica" at the Tron-Zanella high school.

Teacher

October 2023 - November 2023

University of Genoa

Lecturer in advanced applications for access control in the "Cybersecurity and Critical Infrastructure Protection" professional specialization course.

Guest Lecturer

May 2023

University of Trento

Guest lecture in data security for applications based on cloud-edge computing in the "Fog and Cloud Computing" master course at the University of Trento.

Guest Lecturer

April 2022 - March 2023

University of Genoa

Guest lecture in zero trust in authorization – cryptographic enforcement of access control policies – in the "Digital Identity: Enrollment, Authentication, and All That" PhD course at the University of Genoa.

Publications

Stefano Berlato, Matteo Rizzi, Matteo Franzil, Silvio Cretti, Pietro De Matteis, Roberto Carbone **Work-in-Progress: A Sidecar Proxy for Usable and Performance-Adaptable End-to-End Protection of Communications in Cloud Native Applications** in 1st Workshop on Operating Systems and Virtualization Security (OSVS 2024)

Stefano Berlato, Silvio Cretti, Domenico Siracusa, Silvio Ranise **Multi-Objective Microservice Orchestration: Balancing Security and Performance in CCAM** in 27th Conference on Innovation in Clouds, Internet and Networks (ICIN 2024)

Davide Pizzolotto, Stefano Berlato, Mariano Ceccato **Mitigating Debugger-based Attacks to Java Applications with Self-Debugging** in ACM Transactions on Software Engineering and Methodology (TOSEM)

Stefano Berlato, Umberto Morelli, Roberto Carbone, Silvio Ranise **End-to-End Protection of IoT Communications Through Cryptographic Enforcement of Access Control Policies** in 36th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2022)

Stefano Berlato, Marco Centenaro, Silvio Ranise **Smart Card-Based Identity Management Protocols for V2V and V2I Communications in CCAM: a Systematic Literature Review** in IEEE Transactions on Intelligent Transportation Systems (T-ITS)

Stefano Berlato, Roberto Carbone, Adam J. Lee, Silvio Ranise **Formal Modelling and Automated TradeOff Analysis of Enforcement Architectures for Cryptographic Access Control in the Cloud** in ACM Transactions on Privacy and Security (TOPS)

Marco Centenaro, Stefano Berlato, Roberto Carbone, Gianfranco Burzio, Giuseppe Faranda Cordella, Roberto Riggio, and Silvio Ranise **Safety-Related Cooperative, Connected, and Automated Mobility Services: Interplay Between Functional and Security Requirements** in IEEE Vehicular Technology Magazine (VTM)

Andreas Heider-Aviet, Danny Roswin Ollik, Stefano Berlato, Silvio Ranise, Roberto Carbone, Van Thanh Le, Nabil El Ioini, Claus Pahl, Hamid R. Barzegar **Blockchain Based RAN Data Sharing** in IEEE International Conference on Smart Data Services 2021 (SMDS 2021)

Stefano Berlato, Roberto Carbone, Silvio Ranise **Cryptographic Enforcement of Access Control Policies in the Cloud: Implementation and Experimental Assessment** in 18th International Conference on Security and Cryptography (SECRYPT 2021)

Marco Centenaro, Stefano Berlato, Roberto Carbone, Gianfranco Burzio, Giuseppe Faranda Cordella, Silvio Ranise, Roberto Riggio **Security Considerations on 5G-Enabled Back-Situation Awareness for CCAM** in IEEE 3rd 5G World Forum (5GWF 2020)

Stefano Berlato, Roberto Carbone, Adam J. Lee, Silvio Ranise **Exploring Architectures for Cryptographic Access Control Enforcement in the Cloud for Fun and Optimization** in 15th ACM ASIA Conference on Computer and Communications Security (ASIACCS 2020)

Stefano Berlato, Mariano Ceccato **A Large-Scale Study on the Adoption of Anti-Debugging and Anti-Tampering Protections in Android Apps** in Journal of Information Security and Applications (JISA), Issue number 52

Supervised Theses

Simone Brunello **Cryptographic Access Control for Balancing Trust, Protection, and Performance** Bachelor in Computer Science at the University of Trento (2024)

Ion Andy Ditu **Leveraging Trusted Execution Environment for Efficient Revocation and Security in Cryptographic Access Control** Bachelor in Computer Science at the University of Trento (2023)

Erica Elia **A Key Recovery Protocol based on Threshold Secret Sharing for Cryptographic Access Control in the Cloud: The CryptoAC Use Case** Master in Mathematics at the University of Trento (2023)

Enrico Marconi **Combining Blockchain-as-a-Service and Cryptographic Access Control for Secure Data Sharing Across Multiple Organizations** Bachelor in Computer Science at the University of Trento (2022)

Alessandro Colombo **Attribute Based Encryption for Advanced Data Protection in IoT with MQTT** Bachelor in Computer Science at the University of Trento (2022)

Veronica Cristiano **Key Management for Cryptographic Enforcement of Access Control Policies in the Cloud: The CryptoAC Use Case** Master in Mathematics at the University of Trento (2021)

Chaudhry Muhammad Suleman **Cyber-security Risk Assessment for Cooperative, Connected and Automated Mobility: Application to Cooperative Lane Merging** Master in Computer Science at the University of Trento (2021)

Open Source Projects

Kotlin Multiplatform for OpenABE

March 2022 - now

A wrapper allowing to easily use the OpenABE library for Attribute-based Encryption (ABE) from Kotlin multiplatform.

Repository: /kABE

Technologies: Kotlin, React.js

Joni

February 2018 - July 2018

University project for building Joni, a tool meant to help blind and visually impaired people to keep in touch with the world. The project comprised the validation of the business idea through concrete analysis on the field and market research with the goal to make news and podcasts accessible by the blind community.

Repository: /joni

Technologies: Raspberry Pi, Python

Glumo

February 2017 - June 2017

University project for building an Android app, called Glumo, to help people who suffer from diabetes with features like automatic alarms and emergency SMS. The project comprised the design of monitoring services with direct bluetooth connection with modern glycemic sensors.

Repository: /glumo

Technologies: Android, Arduino, Bluetooth

Eater

February 2016 - June 2016

University project for building a web application for finding and reviewing restaurants. The project comprised the Agile design and development of the web application with a Java backend, the implementation of the Model-View-Control (MVC) and the DAO pattern for decoupling logic and storage.

Repository: /eater

Technologies: Java, Apache, SQL

Editorial Work and Community Service

2024
Reviewer for: IEEE - TIFS · ICIN · WWW · ITASEC · DBSec

2023
Reviewer for: EURASIP - JIS · DBSec · ITASEC · SECRYPT · CODASPY · SACMAT · ICISS · FPS

2022
Reviewer for: CODASPY · SECRYPT · DBSec · FedCSIS · ICISSP · FPS

2021
Reviewer for: Elsevier - JISA · SECRYPT · DPM · SACMAT · ITASEC · DBSec · FPS

2020
Reviewer for: SECRYPT · FPS · ICISS · DPM · DBSec · SACMAT

2019
Reviewer for: ICISS