europass

Mattia Zago

Date of birth: | **Nationality:** Italian | **Gender:** Male |

About me:
I hold a Ph.D. in cybersecurity and Artificial Intelligence from the University of Murcia in Spain. I have achieved the Engineering title and I have been registered as Engineer in Verona since 2017, where, since 2022 I have acted as Council Member with a special delegation for Digital Transition and Cybersecurity. My current focus is on digital identity and innovative solutions for hybrid federated and decentralized approaches for Web 3.0 identities. Since 2022 I have been a Steward Council Member for the Sovrin Foundation and a Steering Committee Member for the Trust Over IP Foundation.
My research focused on Artificial Intelligence for cybersecurity; specifically, I've been working on i) machine learning solutions for network intrusion detection systems, ii) using big data and sentiment analysis to identify social bots on social media platforms, and iii) anomaly detection in users' behavioral patterns for authentication and authorization purposes.
I also have provable 5+ years of experience as a private technical consultant. I've worked as an IT consultant (sysadmin and DevOps), data scientist, and cybersecurity engineer. I am a lead auditor for ISO/IEC 27001.

WORK EXPERIENCE

31 OCT 2021 – Padova, Italy
SOLUTIONS ARCHITECT – ATHESYS S.R.L.

Cybersecurity consultant.
I'm working for national and multinational large enterprises providing solutions in the cybersecurity space, such as identity management, PKI management, data virtualization, encryption approaches, vulnerability management, and server modernization. I have integrated both centralized, federated, and decentralized identity solutions (Identity and Access Management) with authorization flows (Privileged Access Management) and governance policies (Identity Governance & Administration).

Business or Sector Information and communication |

Address Via Giacinto Andrea Longhin, 29, 35129, Padova, Italy | **Email** mattia.zago@athesys.it |

Website www.athesys.it

31 OCT 2021 – CURRENT – Trento, Italy
SOLUTIONS ARCHITECT – MONOKEE S.R.L.

I lead the research team on the subject of Self-Sovereign Identity. I've lined up the resources and drafted the company's plans for Web 3.0. I represent the company's primary international point of contact. As such, with Monokee, I sit at multiple high-valuable international tables for decentralized identity like the Decentralized Identity Foundation (DIF), the Trust over IP foundation (ToIP, Steering Committee member), and the Sovrin foundation (Steward Council member).

Business or Sector Information and communication | **Department** Research and Development |

Address Via Zeni Fortunato, 8, 38068, Rovereto, Italy | **Email** mattia.zago@monokee.com |

Website www.monokee.com

NOV 2015 – 2021 – Verona, Italy
FREELANCER

I've been working mainly for small and medium businesses in North Italy.

I've provable professional experience in several areas: Consultant, Audit Service, Cyber Security, Cyber security Report, Small Business Consulting, Social Media Training, Software Asset Management, Hardware Asset Management, IT Strategy & Advice, Cloud Solutions, Risk management, Compliance, Security Audit, Threat Intelligence, Vulnerability Assessment, CRM Consultant, Database Services, Cloud Services, Database Management, GDPR Consulting, Information Security, GDPR, Email Solutions, Office 365, Small Business Website Design, Disaster Recovery, Custom software development

Business or Sector Professional, scientific and technical activities |

Address Via Prato Pelagal, 47, 37051, Bovolone, Italy | **Email** work@zagomattia.it | **Website** www.zagomattia.it

31 AUG 2021 – OCT 2021 – Verona, Italy
ISO/IEC 27001 LEAD AUDITOR – FIRST QUALITY ASSURANCE ITALIA

31 JAN 2018 – 30 JAN 2021 – Murcia, Spain
PREDOCTORAL RESEARCHER – UNIVERSITY OF MURCIA - INCIBE - SPANISH NATIONAL CYBERSECURITY INSTITUTE

Ph.D. Candidate with a scholarship for advanced research for cyber security promoted by the Spanish national institute for cyber security - Candidate Code: INCIBEC-2015-02489

I'm working on artificial intelligence approaches to cybersecurity, specifically machine learning solutions for bot detection.
I currently have projects in the following areas:
- Detection of malware in controlled networks using privacy-preserving machine learning algorithms;
- Detection, profiling and attribution of social botnets in social media platforms;
- Seamless authentication and dynamic authorization management;
- Cybersecurity in Cyber Physical Systems;

Business or Sector Education | **Department** Department of Communications and Information Engineering |

Address Faculty of Computer Science, Campus Espinardo, 30100, Murcia, Spain | **Email** mattia.zago@um.es |

Website https://webs.um.es/mattia.zago

APR 2016 – 30 JAN 2018 – Murcia, Spain
PREDOCTORAL RESEARCHER – UNIVERSITY OF MURCIA

28 FEB 2021 – 30 OCT 2021 – Murcia, Spain
RESEARCHER – UNIVERSITY OF MURCIA

I've been working as a Task Leader in the Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises (PALANTIR) Project (grant no 883335).

My focus is to design and implement the security services (SECaaS) that will be deployed on-demand.

Project Abstract
The rapid advances in digital technology necessitate finding ways to ensure digital security and help small and medium-sized enterprises (SMEs) recover from cyberattacks. The EU-funded PALANTIR project aims to implement a framework combining privacy assurance, data protection, incident detection and recovery aspects. The project will also focus on cyber-resilience and ensure the SMEs' compliance with the relevant data privacy and protection regulations. The outcomes of the project will provide those enterprises with security tools that will boost their resilience at a reasonable cost.

Business or Sector Education | **Department** Department of Communications and Information Engineering |

Address Faculty of Computer Science, Campus Espinardo s/n, 30100, Murcia, Spain | **Email** mattia.zago@um.es |

Website https://www.palantir-project.eu/

EDUCATION AND TRAINING

2015 – 21 JUL 2021 – Murcia, Spain
PHD COMPUTER SCIENCE – University of Murcia

1. Firstly, a state-of-the-art survey on ML approaches to DGA-based botnet detection; the first chapter reports on supervised and unsupervised algorithms, their features sets, the definition of use cases and experiments, and, ultimately, the outline of multiple research challenges to guide the thesis. Eventually, the experimental findings lay the foundations for ADGs formal and verifiable study.
2. Secondly, a comparative analysis of the data sources to power ML frameworks; the second chapter reports on the published datasets by providing a formal comparison and discussion on multiple orthogonal properties. In the same article, the UMUDGA dataset is introduced as the most complete, balanced, and up-to-date collection of DGAs-related data, featuring 50 malware classes for a total of 30+ million FQDNs. Eventually, the exploratory analysis reported in the article suggests that ML solutions to precisely pinpoint the malware variant based on ADGs pattern recognition are feasible.
3. Thirdly, a virtualised, proof-of-concept framework where the detection of DGA-based botnets is deployed as a security service on edge; the third chapter compares and examines architectural EAI approaches to enable scalable detection in 5G networks and beyond. In the article, the experimental evaluation demonstrates that ADG detection is not only reasonable and achievable, but it is also plausible to expect to have deployed such detection capabilities on the networks' edges and eventually on the user equipments (UEs)

Address Faculty of Computer Science, Campus Espinardo s/n, Murcia, Spain |

Website https://webs.um.es/mattia.zago/phd-thesis-umudga.html |

Field of study Information and Communication Technologies | **Final grade** Approved with honours |

Level in EQF EQF level 8 | **Thesis** Enhancing DGA-based botnet detection beyond 5G with on-edge machine learning |

https://webs.um.es/mattia.zago/phd-thesis-umudga.html

30 SEP 2012 – OCT 2015 – Verona, Italy
MSC COMPUTER SCIENCE AND ENGINEERING – University of Verona

This master thesis will analyze how the Bayesian Theory can be applied to the Intrusion Prevention and Response Strategy research area. I am going to present a brief summary on the graphical security modelling technique, with the objective ofdescribing a common point between the existing formalism and aiming to implement a Security Model Simulator that allows the expert to both run and compare different solutions and approaches to the same problem (or architecture).
The focus of this work is on the simulator, presented in chapter 3, in particular on the technical details of the implementation and on the innate difficulties related to the lack of standard basic structure.

Address Verona, Italy | **Field of study** Information and Communication Technologies (ICTs) not further defined |

Final grade 110 with honors | **Level in EQF** EQF level 7 | **Type of credits** ECTF | **Number of credits** 120 |

Thesis Modeling Cyber-Threats: adopting Bayes' principles in the attack graph theory

2008 – 2011 – Italy
BSC BIOINFORMATICS – University of Verona

Address Italy | **Field of study** Natural sciences, mathematics and statistics not further defined |

Final grade 98/110 | **Level in EQF** EQF level 6 | **Type of credits** ECTF | **Number of credits** 180

LANGUAGE SKILLS

Mother tongue(s): **ITALIAN**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	C1	C2	C1	C1	C2
SPANISH	C1	C1	C1	C1	C1

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

DIGITAL SKILLS

My Digital Skills

Artificial Intelligence

Pandas | Python | Data Science | Machine Learning | Scikit-Learn | Numpy | Deep Learning | Seaborn | Neural Networks and Deep Learning | Keras | Data Preprocessing | Artificial Intelligence | Jupyter Notebook | Data Visualization | TensorFlow | Anaconda | Natural Language Processing | Data Analysis & Data Mining

Cybersecurity

Encryption, PKI, TLS | ISO 27001 Foundation certified | Cybersecurity | Resilience | Privileged Account Management (PAM) | SPID CNN and electronic signature advanced user (Certified Italian Webmail) | DNS | Advanced understanding of cryptography ((worked with HSMs, SSL certificates, OpenSSL etc)) | Risk Management

System Administration

Docker | Linux : routing eth interfaces , ssh remote connection | Linux | VPS admin, cPanel and Plesk | Proxmox VE | pfSense | Server SysAdmin

DevOps

SQL | Laravel FrameWork | PHP | Java | Versioning: Git, Github | Software Engineering | NoSQL | MySQL | Object-Oriented Programming | Microservices | MongoDB | Flask | RESTful api | Web Development | SQLite

Miscellaneous

LaTeX | Intermediate skills in graphic design (Adobe Photoshop Adobe Illustrator Adobe InDesign)

Digital Identity

Hyperledger Fabric | Self-Sovereign Identity | Hyperledger Indy | Identity and Access Management (IAM) | SAML 2 | Protocol and standard literate (Kerberos, OIDC, OAuth, SAML) | Privileged Access Management | IAM | OpenId Connect | Hyperledger Besu | Identity Governance & Administration (IGA) | oAuth | SCIM

NETWORKS AND MEMBERSHIPS

MAY 2022
Steering Committee Member

Trust over IP Foundation https://trustoverip.org/

SEP 2022
Steward Council Member

Sovrin Foundation https://sovrin.org/

JAN 2017 – CURRENT
Ordine degli Ingegneri

Verona
Unique identifier: VR-A-4783

In 2021 I've been coordinating the Cybersecurity Webinar Series, featuring four events:
- Privacy and message services
- Mobile security
- Industry 4.0 and explainable security
- Fake news and social bots

Since 2022 I've been elected as Council Member with special mandate for Digital Transition and Cybersecurity. I also coordinate the ICT and Teachers working groups.
https://ingegneri.vr.it/amministrazione-trasparente/organizzazione/consiglio-2022-2026/

PROJECTS

NOV 2017 – CURRENT
Research project - BotBusters

https://webs.um.es/mattia.zago/botbusters.html
Social networks are a primary source of news and information that can be steered, distorted, and influenced. Recent scandals such as Cambridge Analytics proved that social media users are prone to such direct manipulation. Among the weapons available to perform these anti-democracy attacks, Social Bots are beyond question the most powerful one. These autonomous entities constitute coordinated armies that sneakily manipulate and deceive real users. Thus, our research identifies five significant challenges that the research community needs to face toward tackling Social Bots activities in four individual but comparable scenarios. To address these key challenges, we propose, elaborate, and evaluate a mix of remedies in the form of a proof-of-concept platform combining the agility of artificial intelligence with human analysts' expertise to detect and shield against Social Bots interference.

Research project - UMUDGA

https://webs.um.es/mattia.zago/phd-thesis-umudga.html
With the first commercially available 5G infrastructures, worldwide's attention is shifting to the next generation of theorised technologies that might be finally deployable. In this context, the cybersecurity of edge equipment and end-devices must be a top priority as botnets see their spread remarkably increase. Most of them rely on algorithmically generated domain names (AGDs) to evade detection and remain shrouded from intrusion detection systems, via the so-called Domain Generation Algorithm (DGA). Despite the issue, by applying concepts such as distributed computing and federated learning, the cybersecurity community has prototyped and developed dynamic and scalable solutions that leverage the increased capabilities and connectivity of edge devices.
This article proposes a lightweight and privacy-preserving framework that pushes the intelligence modules to the edges aiming to achieve early DGA-based botnet detection in mobile and edge-oriented scenarios. Experimental results prove the deployability of such architecture at all levels, including resource-constrained end-devices.

AUG 2019 – CURRENT
Research project - Automotive

https://webs.um.es/mattia.zago/automotive.html
Automotive security has gained significant traction in the last decade thanks to the development of new connectivity features that have brought the vehicle from an isolated environment to an externally facing domain. Researchers have shown that modern vehicles are vulnerable to multiple types of attacks leveraging remote, direct and indirect physical access, which allow attackers to gain control and affect safety-critical systems. Conversely, Intrusion Detection Systems (IDSs) have been proposed by both industry and academia to identify attacks and anomalous behaviours. In this paper, we propose CANnolo, an IDS based on Long Short-Term Memory (LSTM)-autoencoders to identify anomalies in Controller Area Networks (CANs). During a training phase, CANnolo automatically analyzes the CAN streams and builds a model of the legitimate data sequences. Then, it detects anomalies by computing the difference between the reconstructed and the respective real sequences. We experimentally evaluated CANnolo on a set of simulated attacks

applied over a real-world dataset. We show that our approach outperforms the state-of-the-art model by improving the detection rate and precision.

31 JAN 2021 – CURRENT
Research project - Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises (PALANTIR)

https://webs.um.es/mattia.zago/palantir.html
The rapid advances in digital technology necessitate finding ways to ensure digital security and help small and medium-sized enterprises (SMEs) recover from cyberattacks. The EU-funded PALANTIR project aims to implement a framework combining privacy assurance, data protection, incident detection and recovery aspects. The project will also focus on cyber-resilience and ensure the SMEs' compliance with the relevant data privacy and protection regulations. The outcomes of the project will provide those enterprises with security tools that will boost their resilience at a reasonable cost.

2015 – 2018
Research project - Framework for self-organized network management in virtualized and software defined networks (SELFNET)

https://selfnet-5g.eu/
The SELFNET project designed and implemented an autonomic network management framework to achieve self-organizing capabilities in managing network infrastructures by automatically detecting and mitigating a range of common network problems that are currently still being manually addressed by network operators, thereby significantly reducing operational costs and improving user experience. SELFNET explores a smart integration of state-of-the-art technologies in Software-Defined Networks (SDN), Network Function Virtualization (NFV), Self-Organizing Networks (SON), Cloud computing, Artificial intelligence, Quality of Experience (QoE) and Nextgeneration networking to provide a novel intelligent network management framework that is capable of assisting network operators in key management tasks: automated network monitoring by the automatic deployment of NFV applications to facilitate system-wide awareness of Health of Network metrics to have more direct and precise knowledge about the real status of the network; autonomic network maintenance by defining high-level tactical measures and enabling autonomic corrective and preventive actions against existing or potential network problems.

VOLUNTEERING

2016 – 2020
Erasmus Student Network (ESN)

Murcia, Spain
I was part of the Erasmus association which aims to promote international mobility in Europe. I have been the local representative for the federation regarding the Mov'in Europe project. Since 2019, I have been fulfilling the vice-president role with HR and team management functions. I studied, developed and successfully deployed multimedia techniques to achieve nationally-relevant awards for students online engagement within the ESN federation. I've been responsible for securing the digital ecosystem of the association using GSuite, including obtaining the no-profit certification.
www.esnmurcia.org

In compliance with the Italian Legislative Decree no. 196/2003 and 101/2018, and with the art. 13 of the EU GDPR 679/2016, I hereby authorize the recipient of this document to use and process my personal details for the sole purpose of recruiting and selecting staff.

Verona, 26 Sep 2022

Mattia Zago

ZAGO MATTIA
Ordine degli Ingegneri della Provincia di Verona
Ingegnere

F.to digitalmente, originale conservato presso la Segreteria