Nicola Bena
CURRICULUM VITAE

Indice

1 Informazioni Personali

Cognome: Bena
Nome: Nicola
Data di nascita: 16 febbraio 1996

2 Breve Biografia

2.1 Posizione attuale

Dottorando (XXXVI ciclo) Dipartimento di Informatica "Giovanni degli Antoni"
Università degli Studi di Milano

2.2 Breve storia scolastica e scientifica

- Da *Maggio 2022* è cultore della materia in Reti di calcolatori.
- Da *Novembre 2020* frequenta il Dottorato di Ricerca in Informatica (XXXVI Ciclo) presso l'Università degli Studi di Milano.
- Da *Giugno 2020* ha lavorato come assegnista di ricerca presso il Dipartimento di Informatica (DI), Università degli Studi di Milano.
- Nell'*Aprile 2020* si è Laureato in Sicurezza Informatica presso l'Università degli Studi di Milano con la votazione di 110/110 e Lode.
  Tesi discussa: "Verifiche di Assurance in Architetture di Nuova Generazione: Uno Schema di Certificazione per Sistemi Basati su DevOps". Relatore: Prof. Claudio A. Ardagna.
- Da *Novembre 2019* collabora con Moon Cloud srl, startup innovativa e spin-off dell'Università degli Studi di Milano per la valutazione e il monitoraggio della sicurezza dei sistemi IT.
- Da *Ottobre 2019* a *Gennaio 2020* ha ottenuto un incarico di collaborazione esterna nell'ambito del progetto EU Horizon 2020 *Cyber security cOmpeteNce fOr Research anD Innovation* (CONCORDIA), Dipartimento di Informatica (DI), Università degli Studi di Milano.
- Da *Febbraio 2019* a *Maggio 2019* ha ottenuto un incarico di collaborazione esterna, Dipartimento di Informatica (DI), Università degli Studi di Milano.
- Da *Ottobre 2018* collabora alle attività del laboratorio *SEcure Service-oriented Architectures Research Lab* (SESAR Lab), Dipartimento di Informatica (DI), Università degli Studi di Milano.
- Nell'*Ottobre 2018* si è Laureato in Sicurezza dei Sistemi e delle Reti Informatiche presso l'Università degli Studi di Milano con la votazione di 110/110 e Lode.
  Tesi discussa: "Studio ed implementazione di una architettura avanzata basata su VPN per Security Assessment". Relatore: Prof. Marco Anisetti.

3 Attività di Ricerca e Pubblicazioni Scientifiche

3.1 Partecipazione a progetti di ricerca

Ha partecipato/partecipa ai seguenti progetti di ricerca:

- Piano Nazionale di Ripresa e Resilienza (PNRR)
  Titolo progetto: MUSA: Multilayered Urban Sustainability Action (MUSA), Spoke 2 Big Data-Open Data in Life Sciences
  Periodo: Settembre 2022 – Agosto 2025
  Unità operativa: Università degli Studi di Milano
  Attività: Design e sviluppo di un'innovativa architettura digitale olistica per lo storage e lo scambio sicuro di big data per scienze della vita.

- Grandi Sfide di Ricerca (GSA) – Strategic Line 4: Sicurezza informatica/Cloud
  Titolo progetto: Sovereign Edge-Hub: Un'Architettura Cloud-Edge per la Sovranità Digitale nelle Scienze della Vita (SOV-EDGE-HUB)
  Periodo: Gennaio 2022 – Dicembre 2022
  Unità operativa: Università degli Studi di Milano
  Attività: Progettazione e implementazione di una infrastruttura cloud-edge per Università degli Studi di Milano.

- Program EU Horizon 2020 (SU-INFRA02-2019 Security for smart and safe cities, including for public spaces)
  Titolo progetto: Intelligent Management of Processes, Ethics and Technology for Urban Safety (IMPETUS)
  Periodo: Settembre 2020 – Agosto 2022
  Unità operativa: Università degli Studi di Milano
  Attività: Progettazione e implementazione di un'approccio di data governance a tempo di ingestione basato sul controllo dell'accesso, il quale media l'accesso e l'utilizzo di dati in una smart city per cybersecurity.

- Technology Innovation Institute (TII) Funded Research Projects
  Titolo progetto: Prevention and detection of poisoning and adversarial Attacks on Machine Learning Models (PALM)
  Periodo: Novembre 2020 – Aprile 2023
  Unità operativa: Università degli Studi di Milano
  Attività: Definizione di una metodologia per la prevenzione di attacchi di poisoning mediante l'irrobustimento del training di modelli di machine learning.

- Programma EU Horizon 2020 (SU-ICT - Boosting the effectiveness of the Security Union)
  Titolo progetto: Cyber security cOmpeteNce fOr Research anD Innovation (CONCORDIA)
  Periodo: Gennaio 2019 – Dicembre 2023
  Unità operativa: Università degli Studi di Milano
  Attività: Definizione di una serie di threat report che analizzano l'evoluzione delle minacce e vulnerabilità di sicurezza IT, gap e challenge che accompagneranno il futuro prossimo della ricerca sulla sicurezza IT, e le contromisure di sicurezza attualmente disponibili.

3.2 Soggiorni presso centri di ricerca e partecipazione a centri o gruppi di ricerca nazionali e internazionali

- *Giugno – Agosto 2023*: ha visitato LIRIS Lab, INSA Lyon, Lione, Francia (come visiting scholar). L'attività di ricerca, in collaborazione con la Prof.ssa Chirine Guedira, Prof.ssa Nadia Bennani, Dr.ssa Genoveva Vargas-Solar, è stata rivolta alla definizione di nuove metodologie per il trust management in sistemi distribuiti moderni.
- *Febbraio – Aprile 2023*: ha visitato la Khalifa University (come visiting scholar), Abu Dhabi, UAE. L'attività di ricerca, in collaborazione con il Prof. Chan Yeob Yeun, è stata rivolta alla definizione di nuove metodologie per irrobustire modelli di machine learning da attacchi di poisoning.

3.3 Organizzazione di/partecipazione a conferenze internazionali

Program Chair delle seguenti conferenze:

- *3rd Italian Conference on Big Data and Data Science (ITADATA 2024)*, Pisa, Italia, Settembre 2024.
- *2nd Italian Conference on Big Data and Data Science (ITADATA 2023)*, Napoli, Italia, Settembre 2023.

Membro del Comitato di Programma delle seguenti conferenze:

- *2024 5th International Conference on Computing, Networks and Internet of Things (CNIOT 2024)*, Maggio 2024, Tokyo, Giappone.
- *2024 International Conference on Communication, Information and Digital Technologies (ICCIDT 2024)*, Maggio 2024, Wuhan, Cina.
- *14th International Conference on Cloud Computing and Services Science (CLOSER 2024)*, Aprile 2024, Angers, Francia.
- *21th IEEE International Symposium on Parallel and Distributed Processing with Applications (IEEE ISPA 2023)*, Dicembre 2023, Wuhan, Cina.
- *14th IEEE International Conference On Cloud Computing Technology And Science (CloudCom 2023)*, Dicembre 2023, Napoli, Italia.
- *22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2023)*, Exeter, Regno Unito, Novembre 2023.
- *2023 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2023)*, Venezia, Italia, Luglio - Agosto 2023.
- *IEEE Cloud Summit 2023*, Baltimora, MD, USA, Luglio 2023.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2023)*, Chicago, IL, USA, Luglio 2023.
- *7th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2023) During SMARTCOMP 2023, (IEEE BITS 2023)*, workshop parte di SMARTCOMP 2023, Nashville, TN, USA, Giugno 2023.
- *International Workshop on AI-driven Trustworthy, Secure, and Privacy-Preserving Computing (AidTSP 2023)*, workshop parte di IEEE INFOCOM 2023, New York, USA. Maggio 2023.
- *4th International Conference on Computing, Networks and Internet of Things (CNIOT 2023)*, Xiamen, Cina, Maggio 2023.
- *13th International Conference on Cloud Computing and Services Science (CLOSER 2023)*, Praga, Repubblica Ceca, Aprile 2023.
- *IEEE Global Communications Conference (IEEE GLOBECOM 2022)*, Rio de Janeiro, Brasile, Dicembre 2022.
- *5th International Conference on Machine Learning for Networking (MLN2022)*, Parigi, Francia, Novembre 2022.
- *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TRUSTCOM 2022)*, Wuhan, Cina, Ottobre 2022.
- *2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2022)*, Virtuale, Luglio 2022.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2022)*, Barcellona, Spagna, Luglio 2022.
- *6th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2022) During SMARTCOMP 2022, (IEEE BITS 2022)*, workshop parte di SMARTCOMP 2022, Espoo, Finlandia, Giugno 2022.
- *3rd International Conference on Computing, Networks and Internet of Things (CNIOT 2022)*, Qingdao, Cina, Maggio 2022.
- *12th International Conference on Cloud Computing and Services Science (CLOSER 2022)*, Virtuale, Aprile 2022.
- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2021)*, Chicago, IL, USA, Settembre 2021.
- *5th IEEE International Workshop on Big Data And IoT Security in Smart Computing (BITS2021) During SMARTCOMP 2021, (IEEE BITS 2021)*, workshop parte di SMARTCOMP 2021, Irvine, CA, USA, Agosto 2021.

- *2nd International Conference on Computing, Networks and Internet of Things (CNIOT 2021)*, Pechino, Cina, Maggio 2021.
- *3rd International Conference on Machine Learning for Networking (MLN'2020)*, Parigi, Francia, Novembre 2020.

Ha svolto, in qualità di *sub-reviewer*, revisioni di lavori sottomessi alle seguenti conferenze internazionali:

- *18th International Conference on Information Systems Security (ICISS 2022)*, Tirupati, India, Dicembre 2022.
- *37th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2022)*, Copenaghen, Danimarca, Giugno 2022.
- *37th ACM/SIGAPP Symposium on Applied Computing (ACM SAC 2022)*, Brno, Repubblica Ceca, Aprile 2022.
- *14th IEEE/ACM International Conference on Utility and Cloud Computing (IEEE/ACM UCC 2021)*, Leicester, Regno Unito, Dicembre 2021.
- *6th International Conference on Systems, Control and Communications (ICSCC 2021)*, Chongqing, Cina, Ottobre 2021.
- *36th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2021)*, Oslo, Norvegia, Giugno 2021.
- *19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2020)*, Guangzhou, Cina, Dicembre 2020–Gennaio 2021.
- *International Conference on Security and Privacy in Digital Economy (SPDE 2020)*, Quzhou, Cina, Ottobre–Novembre 2020.
- *2020 IEEE International Conference on Cloud Computing (IEEE CLOUD 2020)*, Pechino, Cina, Ottobre 2020.
- *11th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2019)*, Sidney, Australia, Dicembre 2019.

È stato *publication chair* delle seguenti conferenze:

- *1st Italian Conference on Big Data and Data Science (ITADATA 2022)*, Milano, Italia, Settembre 2022.

È stato *publicity chair* delle seguenti conferenze:

- *IEEE International Conference on Cloud Computing (IEEE CLOUD 2024)*, Shenzhen, Cina, Luglio 2024.
- *IEEE International Conference on Web Services (IEEE ICWS 2024)*, Shenzhen, Cina, Luglio 2024.
- *1st Italian Conference on Big Data and Data Science (ITADATA 2022)*, Milano, Italia, Settembre 2022.
- *Big Data and Data Science for Next-Generation Distributed Systems (BDDS 2022)*, workshop parte di *IEEE World Congress on Computational Intelligence (WCCI 2022)*, Padova, Italia, Luglio 2022.
- *IEEE World Congress on Services (IEEE SERVICES 2022)*, Barcellona, Spagna, Luglio 2022.
- *IEEE World Congress on Services (IEEE SERVICES 2021)*, Chicago, IL, USA, Settembre 2021.

Ha presentato i seguenti lavori a conferenze internazionali:

- M. Anisetti, C. A. Ardagna, N. Bena, V. Giandomenico, G. Gianini, "Lightweight Behavior-Based Malware Detection", in *Proc. of 15th International Conference on Management of Digital Systems (MEDES 2023)*, Heraklion, Grecia, Maggio 2023.
- M. Anisetti, C. A. Ardagna, N. Bena, "Certification Meets Modern Service-Based Systems: Connecting Service and Certificate Life Cycle", in *Italian Conference on Cybersecurity (ITASEC 2023)*, Bari, Italia, Maggio 2023.
- C. A. Ardagna, N. Bena, R. M. de Pozuelo, "Bridging the Gap Between Certification and Software Development", in *International Conference on Availability, Reliability and Security (ARES 2022)*, Vienna, Austria, Agosto 2022.
- N. Bena, R. Bondaruc, A. Polimeno, "Security Assurance in Modern IoT Systems", in *4th Workshop on Connected Intelligence for IoT and Industrial IoT Applications (C3IA)*, parte di *IEEE 95th Vehicular Technology Conference (IEEE VTC 2022-Spring)*, Helsinki, Finlandia, Giugno 2022.

- M. Anisetti, C.A. Ardagna, N. Bena, R. Bondaruc, "Towards an Assurance Framework for Edge and IoT Systems", in *IEEE International Conference on Edge Computing (IEEE EDGE 2021)*, Guangzhou, Cina, Dicembre 2021.
- M. Anisetti, C.A. Ardagna, N. Bena, A. Foppiani, "An Assurance-Based Risk Management Framework for Distributed Systems," in *International Conference on Web Services (IEEE ICWS 2021)*, Chicago, IL, USA, Settembre 2021.
- M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, "Stay Thrifty, Stay Secure: A VPN-Based Assurance Framework for Hybrid Systems," in *17th International Conference on Security and Cryptography (SECRYPT 2020)*, Parigi, Francia, Luglio 2020 (vincitore del premio "Best Student Paper Award").

3.4 Attività editoriali

Ha svolto, in qualità di *reviewer*, revisioni di lavori sottomessi alle seguenti riviste internazionali:

- *IEEE Transactions on Artificial Intelligence.*
- *Computers in Biology and Medicine.*
- *SN Computer Science.*
- *IEEE Transactions on Cloud Computing*
- *Computers and Electrical Engineering.*
- *IEEE Transactions on Network and Service Management.*
- *Journal of Reliable Intelligent Environments.*
- *IEEE Transactions on Services Computing.*
- *Computers & Security.*
- *IEEE Access.*
- *Annals of Telecommunications.*
- *Mobile Information Systems.*

Ha svolto attività di revisione per proposte di monografie sottomesse a John Wiley and Sons publisher.

3.5 Premi, riconoscimenti e certificazioni

3.5.1 Premi e riconoscimenti

- Vincitore del premio "Best Student Paper Award" presso la conferenza internazionale "17th International Joint Conference on e-Business and Telecommunications (ICETE)".
  Titolo dell'articolo: "Stay Thrifty, Stay Secure: A VPN-based Assurance Framework for Hybrid Systems".
  Coautori: M. Anisetti, C.A. Ardagna, E. Damiani.

3.5.2 Certificazioni

- A *Giugno 2015* ha conseguito la certificazione "EUCIP IT Administrator – modulo Sicurezza Informatica"

3.6 Pubblicazioni

Curatele di Volume

CV–1 M. Anisetti, A. Bonifati, N. Bena, C. A. Ardagna, D. Malerba (eds.), "Proceedings of the 1st Italian Conference on Big Data and Data Science (ITADATA2022)", CEUR-Workshop, 2022.

Articoli in Riviste Internazionali

RI–1 M. Anisetti, C. A. Ardagna, N. Bena, E. Damiani, "Rethinking Certification for Trustworthy Machine-Learning-Based Applications", in *IEEE Internet Computing*, vol. 27, no. 6, 2023.

RI–2 M. Anisetti, C. A. Ardagna, A. Balestrucci, N. Bena, E. Damiani, C. Y. Yeun, "On the Robustness of Random Forest Against Untargeted Data Poisoning: An Ensemble-Based Approach", in *IEEE Transactions on Sustainable Computing*, vol. 8, no. 4, 2023.

RI–3 C. A. Ardagna, N. Bena, C. Hebert, M. Krotsiani, C. Kloukinas, and G. Spanoudakis, "Big Data Assurance: An Approach Based on Service-Level Agreements", in *Big Data*, vol. 11, no. 3, 2023.

RI–4 Z. Zhang, S. Umar, Y. Al Hammadi, S. Yoon, E. Damiani, C. A. Ardagna, N. Bena, C. Yeob Yeun, "Explainable Data Poison Attacks on Human Emotion Evaluation Systems based on EEG Signals", in *IEEE ACCESS*, vol. 11, 2023.

RI–5 M. Anisetti, C. A. Ardagna, N. Bena, "Multi-Dimensional Certification of Modern Distributed Systems", in *EEE Transactions on Services Computing*, vol. 16, no. 3, 2023.

Articoli in Atti di Conferenze e Workshop Internazionali

CI–1 M. Anisetti, C. A. Ardagna, N. Bena, "Continuous Certification of Non-Functional Properties Across System Changes", in *Proc. of 21st International Conference on Service-Oriented Computing (ICSOC 2023)*, Roma, Italia, Novembre–Dicembre 2023.

CI–2 C. A. Ardagna, N. Bena, "Non-Functional Certification of Modern Distributed Systems: A Research Manifesto", in *Proc. of IEEE International Conference on Software Services Engineering (IEEE SSE 2023)*, Chicago, IL, USA, Luglio 2023.

CI–3 M. Anisetti, C. A. Ardagna, N. Bena, V. Giandomenico, G. Gianini, "Lightweight Behavior-Based Malware Detection", in *Proc. of 15th International Conference on Management of Digital Systems (MEDES 2023)*, Heraklion, Grecia, Maggio 2023.

CI–4 C.A. Ardagna, N. Bena, R. M. de Pozuelo, "Bridging the Gap Between Certification and Software Development", in *International Conference on Availability, Reliability and Security (ARES 2022)*, Vienna, Austria, Agosto 2022.

CI–5 M. Anisetti, N. Bena, F. Berto, G. Jeon, "A DevSecOps-based Assurance Process for Big Data Analytics", in *IEEE International Conference on Web Services (IEEE ICWS 2022)*, Barcellona, Spagna, Luglio 2022.

CI–6 N. Bena, R. Bondaruc, A. Polimeno, "Security Assurance in Modern IoT Systems", in *Proc. of IEEE 95th Vehicular Technology Conference (IEEE VTC 2022-Spring)*, Helsinki, Finlandia, Giugno 2022.

CI–7 M. Anisetti, C.A. Ardagna, N. Bena, R. Bondaruc, "Towards an Assurance Framework for Edge and IoT Systems", in *IEEE International Conference on Edge Computing (IEEE EDGE 2021)*, Guangzhou, Cina, Dicembre 2021.

CI–8 M. Anisetti, C.A. Ardagna, N. Bena, A. Foppiani, "An Assurance-Based Risk Management Framework for Distributed Systems," in *IEEE International Conference on Web Services (IEEE ICWS 2021)*, Chicago, IL, USA, Settembre 2021.

CI–9 M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, "An Assurance Framework and Process for Hybrid Systems", in *E-Business and Telecommunications, ICETE 2020*

CI–10 M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, "Stay Thrifty, Stay Secure: A VPN-Based Assurance Framework for Hybrid Systems," in *Proc. of the 17th International Conference on Security and Cryptography (SECRYPT 2020)*, Parigi, Francia, Luglio 2020.

Capitoli in libri/enciclopedie

CL–1 C.A. Ardagna, N. Bena, "Location Information (privacy of)," in *Encyclopedia of Cryptography, Security and Privacy (3rd Ed.)*, S. Jajodia, P. Samarati and M. Young (eds.), Springer, 2021.

CL–2 C.A. Ardagna, N. Bena, "Privacy-Aware Languages," in *Encyclopedia of Cryptography, Security and Privacy (3rd Ed.)*, S. Jajodia, P. Samarati and M. Young (eds.), Springer, 2021.

CL–3 C.A. Ardagna N. Bena, "XML-Based Access Control Languages," in *Encyclopedia of Cryptography, Security and Privacy (3rd Ed.)*, S. Jajodia, P. Samarati and M. Young (eds.), Springer, 2021.

Altre pubblicazioni

AP–1 M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, J. Sessa, "Threats, Gaps and Challenges in the Era of COVID-19", in *CONCORDIA blog*, 2021. https://www.concordia-h2020.eu/blog-post/threats-gaps-and-challenges-in-the-era-of-covid-19/.

AP–2 M. Anisetti, C.A. Ardagna, N. Bena, E. Damiani, J. Sessa, "Countermeasures and Research Actions", in *CONCORDIA blog*, 2022. https://www.concordia-h2020.eu/blog-post/countermeasures-and-research-actions/.

4 Attività didattiche

4.1 Attività didattiche nell'ambito di scuole di specializzazione post-laurea

Ha tenuto/terrà i seguenti insegnamenti all'interno dei corsi di perfezionamento dell'Università degli Studi di Milano:

- *Novembre 2023*: "AI: poisoning attacks and countermeasure", Corso di Perfezionamento in Criminalità Informatica e Investigazioni Digitali – Intelligenza Artificiale, attacchi, crimini informatici, investigazioni e aspetti etico-sociali (con C. A. Ardagna).
- *Giugno 2022*: "Il metaverso da un punto di vista tecnico e informatico", Corso di perfezionamento in Big Data, Artificial Intelligence e Piattaforme – Aspetti tecnici e giuridici connessi all'utilizzo dei dati e alla loro tutela (con C. A. Ardagna).
- *Dicembre 2021*: "L'idea di anonimato e il presentarsi in rete anonimi", Corso di Perfezionamento Online in Criminalità Informatica e Investigazioni Digitali – Le procedure di investigazione e di rimozione dei contenuti digitali. Pornografia, proprietà intellettuale, odio e terrorismo, oblio, tutela della reputazione (con C.A. Ardagna).
- *Ottobre 2020*: "I filtri e l'utilizzo di strumenti quali VPN e Tor", Corso di Perfezionamento Online in Criminalità Informatica e Investigazioni Digitali – La digital forensics sulle infedeltà del partner, del dipendente, del professionista e sulle frodi nelle piattaforme digitali (con C.A. Ardagna).

Ha tenuto/terrà i seguenti corsi online.

- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtuale), Novembre 2022 (con M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtuale), Maggio 2022 (con M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtuale), Novembre 2021 (con M. Anisetti, A. Polimeno).
- "Cybersecurity Consultant: A security assessment scenario". CONCORDIA Certified Cybersecurity Consultant (Virtuale), Giugno 2021 (con M. Anisetti, A. Polimeno).

4.2 Attività di tutoraggio

Docente tutor per i seguenti corsi della Laurea Triennale in Sicurezza dei Sistemi e delle Reti Informatiche, Dipartimento di Informatica, Università degli Studi di Milano:

- A.A. 2021-22: *Reti di calcolatori (laboratorio)*.
- A.A. 2019-20: *Reti di calcolatori (laboratorio)*.
- A.A. 2019-20: *Progettazione model-driven del software*.
- A.A. 2019-20: *Progettazione di software sicuro*.

Ha svolto/svolge attività di tutor didattico dei seguenti insegnamenti nell'ambito del corso di laurea in Sicurezza dei Sistemi e delle Reti Informatiche (edizione online), Dipartimento di Informatica, Università degli Studi di Milano:

- A.A. 2022-23: *Reti di calcolatori*.
- A.A. 2021-22: *Reti di calcolatori*.
- A.A. 2020-21: *Reti di calcolatori*.
- A.A. 2019-20: *Reti di calcolatori*.

4.3 Relatore/Correlatore di tesi di laurea magistrale e triennale

Ha seguito/segue, in qualità di correlatore, le seguenti tesi triennali, nell'ambito di diverse tematiche inerenti alla sicurezza, alla valutazione di assurance, alla cloud, ai microservizi.

- Marco A. Bonissi. "Studio e realizzazione di uno strumento per il rilevamento di exfiltration di dati".

- Ruslan Bondaruc. "Studio e realizzazione di un IDS di nuova generazione basato su un'architettura edge".
- Ruslan Bondaruc. "An Advanced Security Assurance An Advanced Security Assurance".
- Carlo Civardi. "Implementation of an IoT Environment to Simulate Assurance Activities".
- Simone Corradin. "Design e realizzazione di uno strumento per monitoraggio di VPN".
- Matteo dal Grande. "Studio e implementazione di una pipeline di DevSecOps".
- Ez Eddine Ed Daouy. "Studio ed implementazione di sonde per la collezione di log".
- Yannick Joly. "Studio e implemntazione di un sistema di security assurance basato su monitoraggio: Un caso di studio Campus Scolastico".
- Giovanni Locatelli. "Studio e realizzazione di una soluzione di hardening per Windows".
- Nicola Lopatriello. "Un tool per la gestione del ciclo di vita di controlli di security assurance".
- Stefano Maddé. "Studio e sviluppo di una sonda di rete per rilevazione di allegati e-mail infetti".
- Michele Mastroberti. "I firewall e le minacce criptate".
- Luca Mori. "Design and implementation of a risk management solution for machine learning models".
- Xhanluka Rama. "Design e sviluppo di uno strumento per la generazione automatica di report di sicurezza".
- Luca Ruggeri. "Studio ed implementazione di un sistema per l'automazione di attività di penetration testing".
- Victoria Sheng. "Design, progettazione e sviluppo di una dashboard per l'analisi e la visualizzazione dei risultati di un processo di security assurance".
- Daniel Simonini. "Studio ed implementazione di un sistema di autenticazione con JWT".
- Salvatore Sorvillo. "Data poisoning in federated learning".
- Christian Vaccarino. "Studio ed implementazione di sonde per la verifica di sicurezza di sistemi Windows".

Segue, ha seguito, come co-relatore, le seguenti tesi magistrali, nell'ambito di diverse tematiche inerenti alla sicurezza, alla valutazione di assurance, alla cloud, ai microservizi.

- Ruslan Bondaruc. "An Advanced Security Assurance System for Edge/IoT Environments".
- Matteo Cavagnino. "Design and Development of an Assurance Methodology for Security Certifications in IoT Systems".
- Andrei Cosmin Cozmei. "Studio di soluzioni di sicurezza in ambito IoT basate su Machine Learning".
- Alex Fortunato. "Studio ed Implementazione di un Sistema per l'Assurance di Firewall e Dispositivi di Sicurezza Perimetrale".
- Marco Pedrinazzi. "A Transparent Certification Scheme Based on Blockchain".

Ha seguito/segue, in qualità di co-supervisore, i seguenti laureandi (visiting student) presso l'Università degli Studi di Milano e Moon Cloud srl nell'ambito di diverse tematiche inerenti alla sicurezza, alla cloud, ai microservizi.

- Nicolas Tourette. "Design and develop probes for host or network scan against malwares or viruses". University of Burgundy School of Materials & Sustainable Development and Computer Science & Electronics Engineering.

4.4 Seminari

- "Anonimato in Rete: Dai Cookie a Tor". Lezione nell'ambito del corso *Reti di Calcolatori*, Laurea triennale in Informatica, Università degli Studi di Napoli "Parthenope", Napoli, Dicembre 2023.
- "Assurance in Modern ICT Systems: From Theory to Practice". Shandong University of Technology, Cina, Agosto 2023 (con M. Anisetti).
- "Distributed Systems Certification: From Services to Machine Learning". INSA Lyon, Francia, Giungo 2023.
- "Moon Cloud: a Distributed System for Security Assurance". Lezione nell'ambito del corso *Cloud Computing Technologies*, Laurea magistrale in Informatica, Università degli Studi di Milano, Milano, Giugno 2023.
- "Multi-Dimensional Certification of Artificial Intelligence". *Building Bridges through Multidisciplinary Cooperation: Perspective Approaches for Inclusive Artificial Intelligence*, Milano, Maggio 2023.

- "Assurance-based Security Governance for ICT systems". Lezione nell'ambito del corso *Cybersecurity Seminars*, Laurea magistrale in Cybersecurity, Sapienza Università di Roma, Roma. Aprile 2023 (con M. Anisetti).
- "Distributed Systems Certification: From Services to Machine Learning". Khalifa University, Abu Dhabi, UAE, Marzo 2023.
- "A Multi-Dimensional Certification Scheme for Modern Services". *First Conference on System and Service Quality (QualITA 2022)*, Politecnico di Milano, Milano, Novembre 2022.
- "Security and Privacy of the Data Lake Architecture". PhD Day Hub, Università degli Studi di Milano, Milano, Ottobre 2022.
- "Bridging the Gap Between Certification and Software Development". CONCORDIA WP1 Meeting, Monaco, Germania, Giugno 2022.
- "An Assurance-Based Risk Management Framework for Distributed Systems". CONCORDIA T1.1 Meeting, Luglio 2021.
- "Moon Cloud: una Piattaforma per la Cybersecurity". Giornata aperta, Dipartimento di Informatica (DI), Università degli Studi di Milano, Milano, Febbraio 2020 (con M. Anisetti, A. Polimeno).
- "Moon Cloud: Governance di Sicurezza e Verifica di Conformità". Milano Digital Week, Dipartimento di Informatica (DI), Università degli Studi di Milano, Milano, Marzo 2019 (con C.A. Ardagna).
- "Moon Cloud: Governance di Sicurezza e Verifica di Conformità". Giornata aperta, Dipartimento di Informatica (DI), Università degli Studi di Milano, Milano, Febbraio 2019 (con P. Ceravolo).

5 Altro

Membro di organizzazioni ed associazioni

- Segretario del Laboratorio Nazionale CINI Data Science
- Student Member IEEE

Competenze linguistiche

- Italiano: madrelingua
- Inglese: B2

Competenze informatiche

- Programmazione: C, Go, Java, Python, Rust, Typescript
- Paradigmi di sviluppo: GraphQL, REST; metodologie di sviluppo: DevOps, DevSecOps
- Sistemi operativi: Linux, MacOS, Windows
- Altro: Docker, HTML, Latex, PostgreSQL

Data: 29 Dicembre 2023 Luogo: Milano