UNIVERSITÀ DEGLI STUDI DI MILANO

Curriculum vitae

AL MAGNIFICO RETTORE
DELL'UNIVERSITA' DEGLI STUDI DI MILANO **COD. ID: 5702**

Il sottoscritto chiede di essere ammesso a partecipare alla selezione pubblica, per titoli ed esami, per il conferimento di un assegno di ricerca presso il Dipartimento di __Informatica__

Responsabile scientifico: _Ernesto Damiani_____

Nicola Bena

CURRICULUM VITAE

INFORMAZIONI PERSONALI

Cognome	Bena
Nome	Nicola

OCCUPAZIONE ATTUALE

Incarico	**Struttura**
Assegnista di ricerca	Dipartimento di Informatica, Università degli Studi di Milano
Dottorando	Dipartimento di Informatica, Università degli Studi di Milano

ISTRUZIONE E FORMAZIONE

Titolo	**Corso di studi**	**Università**	**anno conseguimento titolo**
Laurea Magistrale o equivalente	Sicurezza informatica	Università degli Studi di Milano	2020
Specializzazione			
Dottorato Di Ricerca			
Master			
Diploma Di Specializzazione Medica			
Diploma Di Specializzazione Europea			
Altro	Certificato EUCIP – IT Administrator (modulo sicurezza informatica)		2015

ISCRIZIONE AD ORDINI PROFESSIONALI

Data iscrizione	**Ordine**	**Città**

LINGUE STRANIERE CONOSCIUTE

lingue	livello di conoscenza
Inglese	B2

PREMI, RICONOSCIMENTI E BORSE DI STUDIO

anno	Descrizione premio
2020	"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

ATTIVITÀ DI FORMAZIONE O DI RICERCA

L'attività di ricerca si è principalmente collocata nell'ambito della verifica non funzionale di sistemi distribuiti moderni basati su servizi cloud-edge. In particolare, sono state definite e sviluppate diverse tecniche di assurance basate su certificazione per la valutazione della compliance di sistemi distribuiti moderni a requisiti di sicurezza. Inoltre, tali tecniche sono state adattate e applicate alla valutazione di proprietà non funzionali (robustezza) di modelli di machine learning. Nello specifico, l'attività di ricerca si è occupata delle seguenti tematiche.

- *Definizione di nuove tecniche di assurance basate su certificazione* volte a i) migliorare la qualità della valutazione di compliance di sistemi distribuiti moderni a proprietà non funzionali, ii) migliorare la gestione del ciclo di vita di sistemi distribuiti, iii) certificare il processo di sviluppo di un sistema distribuito. **Pubblicazioni rilevanti: RI-1, CI-7.**
- *Design e sviluppo di una piattaforma di assurance a supporto di verifiche in sistemi pubblici, privati, ed ibridi*. Tale piattaforma è stata poi estesa per soddisfare i requisiti posti da sistemi distribuiti cloud-edge-IoT e valutarne la compliance a proprietà non-funzionali (ad es., confidenzialità). **Pubblicazioni rilevanti: CI-1, CI-2, CI-4, CI-5.**
- *Integrazione di tecniche di assurance all'interno del ciclo di vita dei sistemi distribuiti*. Tali tecniche sono state integrate all'interno di framework per la gestione del rischio e hanno esteso pipeline Big Data, permettendo di definire, sviluppare, e implementare pipeline con un livello di fiducia (*trust*) lungo l'intero ciclo di vita. **Pubblicazioni rilevanti: RI-1, RI-3, CI-3, CI-6, CI-7.**
- *Definizione di metodologie per incrementare la robustezza di modelli di machine learning ad attacchi di poisoning*. L'attività di ricerca mira, da un lato, a valutare la robustezza empirica di modelli di machine learning tradizionali (ad es., random forest) in relazione ad attacchi di poisoning e, dall'altro, a definire tecniche basate su ensemble che rafforzino la robustezza dei modelli stessi. **Pubblicazioni rilevanti: RI-2.**

ATTIVITÀ PROGETTUALE

Anno	Progetto
2022-2023	Multilayered Urban Sustainability Action (MUSA), Spoke 2 Big Data-Open Data in Life Sciences; progetto finanziato nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR)
2022	Sovereign Edge-Hub: Un'Architettura Cloud-Edge per la Sovranità Digitale nelle Scienze della Vita (SOV-EDGE-HUB); progetto finanziato nell'ambito del programma Grandi Sfide di Ricerca (GSA) – Strategic Line 4: Sicurezza informatica/Cloud

2020-2022	Intelligent Management of Processes, Ethics and Technology for Urban Safety (IMPETUS); progetto finanziato nell'ambito del programma EU Horizon 2020
2020-2023	Prevention and detection of poisoning and adversarial Attacks on Machine Learning Models (PALM); progetto finanziato da Technology Innovation Institute (UAE)
2019-2023	Cyber security cOmpeteNce fOr Research anD Innovation (CONCORDIA); progetto finanziato nell'ambito del programma EU Horizon 2020

TITOLARITÀ DI BREVETTI

Brevetto

CONFERENZE

Luglio 2020	Speaker: "Stay Thrifty, Stay Secure: A VPN-Based Assurance Framework for Hybrid Systems"	17th International Conference on Security and Cryptography (SECRYPT 2020), Parigi, Francia (Virtuale)
Settembre 2021	Speaker: "An Assurance-Based Risk Management Framework for Distributed Systems"	IEEE International Conference on Web Services (IEEE ICWS 2021), Chicago, IL, USA (Virtuale)
Dicembre 2021	Speaker: "Towards an Assurance Framework for Edge and IoT Systems"	IEEE International Conference on Edge Computing (IEEE EDGE 2021), Guangzhou, Cina (Virtuale)
Giugno 2022	Speaker: "Security Assurance in Modern IoT Systems"	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 (Virtuale)
Luglio 2022	Session chair	IEEE International Conference on Web Services (IEEE ICWS 2022), Barcellona, Spagna
Agosto 2022	Speaker: "Bridging the Gap Between Certification and Software Development"	International Conference on Availability, Reliability and Security (ARES 2022), Vienna, Austria
Novembre 2022	Speaker: "A Multi-Dimensional Certification Scheme for Modern Services"	First Conference on System and Service Quality (QualITA 2022), Milano, Italia

CONVEGNI

Luglio 2021	Speaker: “An Assurance-Based Risk Management Framework for Distributed Systems”	CONCORDIA T1.1 Meeting, Virtuale
Giugno 2022	Speaker: “Bridging the Gap Between Certification and Software Development”	CONCORDIA WP1 Meeting, Monaco, Germania
Ottobre 2022	Speaker: “Security and Privacy of the Data Lake Architecture”	PhD Day Hub, One Health Action Hub: Task Force di ateneo per la resilienza di ecosistemi territoriali, Università degli Studi di Milano, Milano, Italia

SEMINARI

Febbraio 2019	Speaker: “Moon Cloud: Governance di Sicurezza e Verifica di Conformità”	Giornata aperta, Università degli Studi di Milano, Milano, Italia
Marzo 2019	Speaker: “Moon Cloud: Governance di Sicurezza e Verifica di Conformità”	Milano Digital Week, Università degli Studi di Milano, Milano, Italia
Febbraio 2020	Speaker: “Moon Cloud: una Piattaforma per la Cybersecurity”	Giornata aperta, Università degli Studi di Milano, Milano, Italia
Marzo 2023	Speaker: “Distributed Systems Certification: From Services to Machine Learning”	Khalifa University of Science and Technology, Abu Dhabi, UAE
Aprile 2023	Speaker: “Assurance-based Security Governance for ICT systems”	Sapienza Università degli Studi di Roma, Roma, Italia

PUBBLICAZIONI

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

Articoli su riviste
RI-1 M. Anisetti, C. A. Ardagna, N. Bena, “Multi-Dimensional Certification of Modern Distributed Systems”, in IEEE Transactions on Services Computing, 2022
R1-2 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
R1-3 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, 2023

Atti di convegni
CI-1 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), Luglio 2020, Parigi, Francia
CI-2 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-3 M. Anisetti, C. A. Ardagna, N. Bena, A. Foppiani, "An Assurance-Based Risk Management Framework for Distributed Systems", in Proc. of IEEE International Conference on Web Services (IEEE ICWS 2021), Settembre 2021, Chicago, IL, USA
CI-4 M. Anisetti, C. A. Ardagna, N. Bena, R. Bondaruc, "Towards an Assurance Framework for Edge and IoT Systems", in Proc. of IEEE International Conference on Edge Computing (IEEE EDGE 2021), Dicembre 2021, Guangzhou, Cina
CI-5 N. Bena, R. Bondaruc, A. Polimeno, "Security Assurance in Modern IoT Systems", in Proc. of 4th Workshop on Connected Intelligence for IoT and Industrial IoT Applications (C3IA), parte di IEEE 95th Vehicular Technology Conference (IEEE VTC 2022-Spring), Giugno 2022, Helsinki, Finlandia
CI-6 M. Anisetti, N. Bena, F. Berto, G. Jeon, "A DevSecOps-based Assurance Process for Big Data Analytics", in Proc. of IEEE International Conference on Web Services (IEEE ICWS 2022), Luglio 2022, Barcellona, Spagna
CI-7 C. A. Ardagna, N. Bena, R. M. de Pozuelo, "Bridging the Gap Between Certification and Software Development", in Proc. of International Conference on Availability, Reliability and Security (ARES 2022), Agosto 2022, Vienna, Austria

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/

ALTRE INFORMAZIONI

Visiting scholar presso Khalifa University of Science and Technology, Abu Dhabi, UAE (febbraio – aprile 2023), attività di ricerca supervisionata dal Prof. Chan Yeob Yeun nell'ambito della definizione di nuove metodologie per irrobustire modelli di machine learning rispetto ad attacchi di poisoning.
Membro del laboratorio SEcure Service-oriented Architectures Research Lab (SESAR Lab), Dipartimento di

Informatica, Università degli Studi di Milano, a partire dal 2018.

Collaboratore del Center for Cyber physical security (C2PS), Khalifa University of Science and Technology, Abu Dhabi, UAE, a partire dal 2023.

Student Member dell'Institute of Electrical and Electronics Engineers (IEEE), a partire dal 2022.

Segretario del Laboratorio CINI Big Data, a partire dal 2022.

Revisore di lavori sottomessi alle seguenti riviste internazionali:

- 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

Membro del comitato di programma delle seguenti conferenze/workshop internazionali:

- 3rd International Conference on Machine Learning for Networking (MLN'2020), Novembre 2020, Parigi, Francia.
- 2nd International Conference on Computing, Networks and Internet of Things (CNIOT 2021), Maggio 2021, Pechino, Cina.
- 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, Agosto 2021, Irvine, CA, USA.
- IEEE International Conference on Cloud Computing (IEEE CLOUD 2021), Settembre 2021, Chicago, IL, USA.
- 12th International Conference on Cloud Computing and Services Science (CLOSER 2022), Aprile 2022, Virtuale.
- 3rd International Conference on Computing, Networks and Internet of Things (CNIOT 2022), Maggio 2022, Qingdao, Cina.
- 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, Giugno 2022, Espoo, Finlandia.
- IEEE International Conference on Cloud Computing (IEEE CLOUD 2022), Luglio 2022, Barcellona, Spagna.
- 2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2022), Luglio 2022, Virtuale.
- IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TRUSTCOM 2022), Ottobre 2022, Wuhan, Cina.
- 5th International Conference on Machine Learning for Networking (MLN2022), Novembre 2022, Parigi, Francia.
- IEEE Global Communications Conference (IEEE GLOBECOM 2022), Dicembre 2022, Rio de Janeiro, Brasile.
- 13th International Conference on Cloud Computing and Services Science (CLOSER 2023), Aprile 2023, Praga, Repubblica Ceca.
- 4th International Conference on Computing, Networks and Internet of Things (CNIOT 2023), Maggio 2023, Xiamen, Cina.
- International Workshop on AI-driven Trustworthy, Secure, and Privacy-Preserving Computing (AidTSP 2023), workshop parte di IEEE INFOCOM 2023, Maggio 2023, New York, USA.

- 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, Giugno 2023, Nashville, TN, USA.
- IEEE International Conference on Cloud Computing (IEEE CLOUD 2023), Luglio 2023, Chicago, IL, USA.
- IEEE Cloud Summit 2023, Luglio 2023, Baltimora, MD, USA.
- 2023 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2023), Luglio - Agosto 2023, Venezia, Italia.
- 14th IEEE International Conference On Cloud Computing Technology And Science (CloudCom 2023), Dicembre 2023, Napoli, Italia.

Sub-reviewer di lavori sottomessi alle seguenti conferenze/workshop internazionali:

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

Publication chair delle seguenti conferenze:

- 1st Italian Conference on Big Data and Data Science (ITADATA 2022), Settembre 2022, Milano, Italia.
- 2nd Italian Conference on Big Data and Data Science (ITADATA 2023), Settembre 2023, Napoli, Italia.

Publicity chair delle seguenti conferenze/workshop:

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

Correlatore delle seguenti tesi di laurea 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".
- 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 implementazione 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 Maddè. “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”.
- Christian Vaccarino. “Studio ed implementazione di sonde per la verifica di sicurezza di sistemi Windows”.

Correlatore delle seguenti tesi di laurea 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”.
- Davide Carone. “Un Sistema di Automatizzazione della Scrittura di Controlli di Security Assurance”.
- Andrei Cosmin Cozmei. “Distributed Learning per IoT Security: una Survey”.
- Matteo Cavagnino. “Design and Development of an Assurance Methodology for Security Certifications in IoT Systems”.
- Alex Fortunato. “Studio ed Implementazione di un Sistema per l’Assurance di Firewall e Dispositivi di Sicurezza Perimetrale”.

Co-supervisore dei seguenti visiting student, nell’ambito di diverse tematiche inerenti alla sicurezza, alla valutazione di assurance, 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.

Cultore della materia in Reti di calcolatori, a partire da maggio 2022.

Tutor didattico dell’insegnamento “Reti di calcolatori” 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 partire dall’A.A. 2019-2020.

Tutor dei seguenti corsi nell’ambito del corso di laurea in Sicurezza dei Sistemi e delle Reti Informatiche Dipartimento di Informatica, Università degli Studi di Milano:

- Progettazione di software sicuro (A.A. 2019-2020)
- Progettazione model-driven del software (A.A. 2019-2020)
- Reti di calcolatori, modulo di laboratorio (A.A. 2019-2020, 2021-2022).

Docente dei seguenti insegnamenti nell’ambito dei seguenti corsi di perfezionamento dell’Università degli Studi di Milano:

- 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)
- 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)
- 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)
Docente dei seguenti corsi online nell'ambito del progetto EU Horizon 2020 CONCORDIA: "Cybersecurity Consultant: A security assessment scenario", parte di "CONCORDIA Certified Cybersecurity Consultant" (con M. Anisetti, A. Polimeno; Giugno 2021, Novembre 2021, Maggio 2022, Novembre 2022)

Le dichiarazioni rese nel presente curriculum sono da ritenersi rilasciate ai sensi degli artt. 46 e 47 del DPR n. 445/2000.

Il presente curriculum, non contiene dati sensibili e dati giudiziari di cui all'art. 4, comma 1, lettere d) ed e) del D.Lgs. 30.6.2003 n. 196.

RICORDIAMO che **i curricula SARANNO RESI PUBBLICI sul sito di Ateneo** e pertanto si prega di non inserire dati sensibili e personali. Il presente modello è già precostruito per soddisfare la necessità di pubblicazione senza dati sensibili.

Si prega pertanto di **NON FIRMARE** il presente modello.

Luogo e data: Trescore Balneario (BG), 02-04-2023