Antonio Ken Iannillo, Ph.D.

Contact Information

29 Av. John F. Kennedy
1855 Luxembourg
Luxembourg

cell: +352 46 66 44 5482
mail: antonioken.iannillo@uni.lu
website: akiannillo.github.io/

Research Interests

Cybersecurity and Secure System Design (focus on blockchain, advanced encryption methods, and trusted execution environments), AI-Driven Security Technologies (focus on logistics and DeFi), Technology Transfer and Innovation (experience in the e-health industry).

Education

Università degli Studi di Napoli Federico II, Naples, Italy

PhD in Computer Engineering **November 2014 – October 2017**

- Thesis: *Dependability assessment of Android OS*
- Topics: Fault Injection, Fault Modeling, System Security Analysis and Design
- Advisors: Prof. Domenico Cotroneo and Prof. Roberto Natella

Università degli Studi di Napoli Federico II, Naples, Italy

M.Sc., Computer Engineering **November 2011 – January 2014**

- GPA: 3.91
- Thesis: *A Fault injection tool for Java software applications*
- Final grade: 110/110 cum laude

Università degli Studi di Napoli Federico II, Naples, Italy

B.Sc., Computer Engineering **October 2008 – October 2011**

- GPA: 3.88
- Thesis: *Comparison between programming models in Facebook and Google Plus*
- Final grade: 110/110 cum laude

Professional Experience

University of Luxembourg, Luxembourg City, Luxembourg **November 2018 – present**

Interdisciplinary Centre for Security, Reliability and Trust
Research Associate - since November 2018
Research Scientist - since February 2020

- Research group: SEDAN headed by prof. Radu State.
- Ph.D. students support: Dedicated to the mentorship and support of SEDAN Ph.D. students, my role involves providing guidance and assistance to the next generation of researchers. This includes sharing expertise, facilitating research discussions, and fostering a collaborative and productive research environment within the group. I worked with the following students:
  - Sean Rivera (November 2018 - January 2021): Securing robots, an integrated approach for security challenges and monitoring for the robotic operating system.
  - Christof Ferreira Torres (November 2018 - March 2022): From smart to secure contracts, automated security assessment and improvement of Ethereum smart contracts.
  - Bahareh Parhizkari (October 2022 - ongoing): Security of decentralized finance (DeFi) protocols.
  - Prateek Gupta (September 2023 - ongoing): Neural combinatorial optimization for logistic problems.
  - Khetag Albenov (October 2024 - ongoing): Formal Verification Frameworks for Privacy-Compliant Blockchain Finance.
  - Francisco Javier Becerra Sanchez (March 2025 - ongoing): Privacy-Preserving Cryptographic Protocols for Decentralized and Blockchain-Based Systems
- Master's students support: In addition to working with Ph.D. students, I actively supervise and support master's students from the Faculty of Science, Technology and Medicine (FSTM) in preparing their final thesis projects, providing guidance on research methodology, technical execution, and professional development.

- **Luxembourgish R&D fund (partner: GULLIVER)**:
  On-going project. Acquired budget: 800,000 euros. Total project budget: 3,000,000 euros.
  I acquired a partnership with Gulliver Luxembourg S.à r.l., securing a budget of 800,000 million euros for SnT in a granted project from the Ministry of Economy using the Luxembourgish R&D fund. As the Project Manager and Scientist, I am actively involved among SnT (project partner) and Gulliver Luxembourg S.à r.l. (project leader). The primary objective is to enhance software used in transport and logistic services through the incorporation of novel AI technologies, thereby improving efficiency and reliability in the industry.
- **Industrial partnership (partner: QUANTSTAMP)**:
  On-going project. Acquired budget: 260,000 euros.
  I successfully acquired a partnership with Quantstamp, securing a budget of 260,000 euros. Leading the SnT team in collaboration with Quantstamp, spearheading initiatives to advance the security of decentralized finance (DeFi) on the blockchain. This industrial project plays a crucial role in addressing emerging challenges in the blockchain space, contributing to the secure and reliable implementation of DeFi systems.
- **CONCORDIA - EU H2020:**
  Project ended in December 2023. Managed budget: 465,000 euros. Total project budget: 23,000,000 euros.
  I was the leader for liaisons with stakeholders. CONCORDIA was a cybersecurity competence network with leading research, technology, industrial, and public competences. I was actively involved in organizing annual events and several cybersecurity workshops to foster collaboration and knowledge exchange among experts in the field. More information about the project can be found at `https://www.concordia-h2020`.
- **OWL - FNR JUMP project**:
  Project ended in June 2023. Acquired budget: 250,000 euros.
  Served as the Principal Investigator for the "Online Workout Platform" (OWL) project, acquiring a budget of 250,000 euros funded by the FNR. The role involved steering the project towards its goal of establishing a startup company dedicated to commercializing a tele-rehabilitation platform designed for cardiac patients. This initiative not only contributes to scientific research but also has the potential to make a positive impact on healthcare by providing innovative solutions for rehabilitation.
- **STARTS - FNR Junior Core:**
  Project ended in December 2020. Acquired budget: 550,000 euros.
  As the Principal Investigator of the "SecuriTy Assessment of tRusTzone-m based Software" (STARTS) project, successfully acquired a budget of 550,000 euros. The focus was on developing a comprehensive methodology for the security assessment of software based on TrustZone-M technology. Additionally, working on a novel verification and validation framework to implement this methodology effectively. This project represents a significant contribution to advancing the field of software security.
- **Cybersecurity in Robotic Systems (partner: Ministry of Defence)**:
  Project ended in June 2020.
  I internally led a project focusing on the cybersecurity assessment and enforcement in a Robotic Operating System (ROS) for military and defense applications. Utilized Trusted Execution Environments to enhance security measures. Project ended in June 2020.

University of Luxembourg, Luxembourg City, Luxembourg **September 2025 – present**
Lecturer

- **Introduction to Generative AI** Winter Semester 2025/2026
  Undergraduate Course, Bachelor in Computer Science / Bachelor in Applied Information Technology
  Designed and delivered a 4 ECTS course providing students with a comprehensive introduction to Generative AI and LLM-based agent systems. The course covers neural networks, transformers, RAG (Retrieval-Augmented Generation) systems, diffusion models, agentic AI, prompt engineering, and responsible AI deployment. The curriculum incorporates hands-on practical sessions with modern AI frameworks (e.g., PyTorch, LangChain, vector databases) and trains students in best practices for designing, building, and evaluating generative AI applications. The course also covers ethical, socio-economic, and security implications of AI technologies.
- **Generative AI and Cybersecurity: Architectures, Threats, and Defenses** Winter Semester 2025/2026
  Graduate Course, Master in Cybersecurity and Systems Defence (MCYSD)
  Developed and taught a 3 ECTS advanced seminar examining security, privacy, and robustness issues in large language models (LLMs) and LLM-based systems. Topics include state-of-the-art attacks (poisoning, backdoors, inference, jailbreaks) and defense strategies (adversarial training, detection, security-by-design), critical paper discussions, and hands-on evaluation. Prepared students for advanced research and professional roles in AI security and responsible deployment of trustworthy AI systems.

WAVY MEET S.à r.l., Luxembourg City, Luxembourg **March 2023 – present**
CEO and Co-Founder

- WAVY MEET platform: Spin-off of the "OWL - FNR JUMP project", it's a medical software platform with a secure and comprehensive approach to remote rehabilitation.
- **FIT4START #13 graduate:**
  Selected in October 2022. Graduated in June 2023. Acquired budget: 150,000 euros.
  One of the 20 selected startups, from a total of 214 applications coming from 42 countries, for specialized coaching organized by LuxInnovation. WAVY MEET graduated from the program FIT4START funded by the Ministry of the Economy as planned.
- *website:* `https://wavymeet.com/`.

UBI Business School, Luxembourg City, Luxembourg **September 2022 – present**
Adjunct Professor

- Teaching the "Web Application for Business" course to year-3 students of the Bacherlor program.

Università degli Studi di Napoli Federico II, Naples, Italy
November 2017 – October 2018
Research Fellow, Dependable Systems and Software Engineering Research Team

- *Automatic Feature Extraction and Analysis of Faulty Code:* Software faults are code imperfections that may lead to the system's eventually failure. A deep understanding of the code developers insert specific software faults into will help several tasks such as bug prevention, bug detection, and software fault injection.
- *Fuzz Testing on Android OS:* Study and research on important challenges for the robustness (security and dependability) of the Android OS. Study and research on evolutionary algorithms and search strategies. Design and development of a smart testing tool on Android.

Critiware s.r.l., Naples, Italy **November 2017 - April 2018**
Research Consultant

- *Python Fault Injection:* Study and research on Python parsing technologies and programming language theory. Design and implementation of a DSL framework for code changes in Python code. Collaboration with Huawei Technologies Co. Lts.

Northeastern University, Boston, MA **September 2016 – April 2017**
Research Assistant (Visitor), Network and Distributed Systems Security Lab

- *Vendor customizations on Android system services:* Study and research on important challenges for the robustness (security and dependability) of the Android OS. Design and development of an innovative testing tool. Robustness and security testing on physical devices. Tutored by Dr. Cristina Nita-Rotaru.

Consorzio Interuniversitario Nazionale Italiano (CINI), Naples, Italy
January 2014 - October 2014
Junior Research Fellow

- *NFVI reliability:* Research of new approach for software reliability evaluation of virtualized environments for Network Function Virtualization (NFV). Design and implementation of a reliability evaluation tool for VMWare ESXi. Collaboration with Huawei Technologies Co. Lts.

Professional experience section continues on next page...

- *PON SVEVIA:* Study and research of usability for fault injection tools. Design and implementation of an integrated fault injection tool (Eclipse plug-in) for the fault injection test design and analysis of results, in Java and C/C++ software.

R&D department, Infosys LTD, Bangalore, India **June 2013 – September 2013**
R&D Intern

- *Java Fault Injection:* Study and research of new approaches for the injection of software defects. Design and development of a tool for fault injection into the Java Bytecode. This thesis work has been conducted in India during the preparation of my MSc. degree thesis. Tutored by Dr. Santonu Sarkar.

Other Honors and Awards

INTSYS 2025 Conference Best Paper Award

ISSRE 2017 Conference Best Paper Award

Netsoft 2015 Conference Best Paper Award

Information Technology and Electrical Engineering PhD 2014-2017 scholarship by Università degli Studi di Napoli Federico II

Academic Services

Program Committee/Research Program Committee Member

- International Workshop on Secure and Dependable Machine Learning (SDML), 2026
- International Conference on Dependable Systems and Networks (DSN, CORE Rank A), 2025–2026
- International Symposium on Software Reliability Engineering (ISSRE, CORE Rank A), 2019–2022, 2025
- International Conference on ICT Systems Security and Privacy Protection (IFIP SEC, CORE Rank B), 2021–2022
- International Workshop on Validation and Verification in Future Cyber-Physical Systems (WAFERS), 2021
- International Workshop on Reliability and Security Data Analysis (RSDA), 2019–2021

Steering Committee

- International Workshop on Blockchain for Decentralized Trust and Digital Identity (B4TI), 2025–2026

Fast Abstract Co-Chair

- International Symposium on Software Reliability Engineering (ISSRE, CORE Rank A), 2022

Reviewer

- IEEE Transactions on Information Forensics and Security (TIFS), 2025–2026

Relevant Skills

AI & Machine Learning: Large Language Models (LLMs), Generative AI, Retrieval-Augmented Generation (RAG), Agentic AI and Tool-Calling Agents, Prompt Engineering, Adversarial Machine Learning, AI Robustness and Security, Explainable AI (XAI), AI for Cybersecurity

AI Tools and Frameworks: PyTorch, TensorFlow, Scikit-learn, LangChain, HuggingFace Transformers, OpenAI API, LlamaIndex

Programming: Python, JavaScript, Bash, Java, C/C++

Development & DevOps Tools: Git, GitHub, GitLab, VS Code, Android Studio, Maven, Gradle, Docker

Cybersecurity: AI Security Audits, Secure LLM Application Design, Threat Modeling for AI Systems, FЯIDA

Project Management: Agile (Scrum), Gantt charts, Risk Management, Software Lifecycle Management, ISO knowledge

Interpersonal Skills: Strong communication, teamwork, leadership, adaptability

LANGUAGES

Italian (C2 - native), English (C2 - proficient), French (B2 - independent), Spanish (A2 - basic), Luxembourgish (A2 - basic)

Publications

Prateek Gupta, Daniel Antunes Pedrozo, Aleksandr Koviazin, Jorge Augusto Meira, and Antonio Ken Iannillo
"**SYNAPSE: Synthesizing Narratives from Agentic Path Spatial Exploration**" [9th EAI International Conference on Intelligent Transport Systems (INTSYS 2025)]

Prateek Gupta, Daniel Antunes Pedrozo, Jorge Augusto Meira, Antonio Ken Iannillo, and Danilo D'Aversa
"**Multimodal Learning for Operational Risk Detection in Delivery Route Planning**" [9th EAI International Conference on Intelligent Transport Systems (INTSYS 2025)]
Best Paper Award

Antonio Ken Iannillo
"**ChaosLLM: A Dependability Testing Approach for Tool-calling Agents**" [Software Reliability Engineering (ISSRE), 2025 IEEE 36th International Symposium on]

Bahareh Parhizkari, Antonio Ken Iannillo, Christof Ferreira Torres, Ed Zulkoski, and Radu State
"**On-Chain Risk Signals: Predicting Security Threats in DeFi Projects**" [International Conference on Trust, Security, and Privacy in Computing and Communication (TrustCom 2025)]

Prateek Gupta, Devanand, Antonio Ken Iannillo, Jorge Augusto Meira, Radu State, and Danilo D'Aversa
"**Modelling Electric Vehicle Routing Problem with Heterogeneous Fleet for Simultaneous Pickup and Delivery**" [Computer Aided Systems Theory – EUROCAST 2024]

Pavel Pantiukhov, Dmitrii Koriakov, Antonio Ken Iannillo, and Radu State
"**Whistleblowers' Protection with XRP Ledger**" [Sixth International Conference on Blockchain Computing and Applications (BCCA 2024)]

Bahareh Parhizkari, Antonio Ken Iannillo, Christof Ferreira Torres, Sebastian Banescu, Joseph Xu, and Radu State
"**Beyond the Public Mempool: Catching DeFi Attacks before They Happen with Real-Time Smart Contract Analysis**" [20th EAI International Conference on Security and Privacy in Communication Networks (EAI SecureComm 2024)]

Bahareh Parhizkari, Antonio Ken Iannillo, Christof Ferreira Torres, Sebastian Banescu, Joseph Xu
"**Timely Identification of Victim Addresses in DeFi Attacks**" [7th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2023)]

Antonio Ken Iannillo, Sean Rivera, Darius Suciu, Radu Sion, and Radu State
"**An REE-independent Approach to Identify Callers of TEEs in TrustZone-enabled Cortex-M Devices**" [ACM CyberPhysical System Security Workshop (CPSS '22)]

Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, and Radu State
"**ConFuzzius: A Data Dependency-Aware Hybrid Fuzzer for Smart Contracts**" [Security and Privacy (EuroS&P), 2021 IEEE European Symposium on]

Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, and Radu State
"**The Eye of Horus: Spotting and Analyzing Attacks on Ethereum Smart Contracts**" [Financial Cryptography and Data Security (FC), 2021 25th International Conference on]

Sean Rivera, Antonio Ken Iannillo, Sofiana Lagraa, Clement Joly and Radu State
"**ROS-FM: Fast Monitoring for the Robotic Operating System(ROS)**" [Engineering of Complex Computer Systems (ICECCS), 2020 25th International Conference on]

Sean Rivera, Vijay K. Gurbani, Sofiane Lagraa, Antonio Ken Iannillo, and Radu State
"**Leveraging eBPF to preserve user privacy for DNS, DoT, and DoH queries**" [Availability, Reliability, and Security (ARES), 2020 15th International Conference on]

Antonio Ken Iannillo and Radu State
"**A Proposal for Security Assessment of Trustzone-M based Software**" [Software Reliability Engineering (ISSRE), 2019 IEEE 30th International Symposium on]

Domenico Cotroneo, Luigi De Simone, Antonio Ken Iannillo, Roberto Natella, Stefano Rosiello***
"**Analyzing the Context of Bug-Fixing Changes in the OpenStack Cloud Computing Platform**" [Software Reliability Engineering (ISSRE), 2019 IEEE 30th International Symposium on]

Sean Rivera, Sofiane Lagraa, Antonio Ken Iannillo, Radu State
"**Auto-encoding Robot State against Sensor Spoofing Attacks**" [Software Reliability Engineering (ISSRE), 2019 IEEE 30th International Symposium on]

Domenico Cotroneo, Antonio Ken Iannillo, Roberto Natella***
"**Evolutionary Fuzzing of Android OS Vendor System Services**" [Empirical Software Engineering Journal (2019)]

Antonio Ken Iannillo, Roberto Natella, Domenico Cotroneo, Cristina Nita-Rotaru
"**Chizpurfle: A Gray-Box Android Fuzzer for Vendor Service Customizations**" [Software Reliability Engineering (ISSRE), 2017 IEEE 28th International Symposium on]
Conference Best Paper Award

Domenico Cotroneo, Francesco Fucci, Antonio Ken Iannillo, Roberto Natella, Roberto Pietrantuono***
"**Software Aging Analysis of the Android Mobile OS**" [Software Reliability Engineering (ISSRE), 2016 IEEE 27th International Symposium on]

Domenico Cotroneo, Antonio Ken Iannillo, Roberto Natella, Roberto Pietrantuono, Stefano Russo***
"**The Software Aging and Rejuvenation Repository**" [Software Reliability Engineering (ISSRE), 2015 IEEE 26th International Symposium on]

Domenico Cotroneo, Luigi De Simone, Antonio Ken Iannillo, Anna Lanzaro, Roberto Natella***
"**Dependability Evaluation and Benchmarking of Network Function Virtualization Infrastructures**" [Network Softwarization (NetSoft), 2015 IEEE 1st Conference on]
Conference Best Paper Award

Domenico Cotroneo, Luigi De Simone, Antonio Ken Iannillo, Anna Lanzaro, Roberto Natella***
"**Usability of Fault Injection**" [Software Reliability Engineering (ISSRE), 2014 IEEE 25th International Symposium on]

Domenico Cotroneo, Luigi De Simone, Antonio Ken Iannillo, Anna Lanzaro, Roberto Natella, Jian Fan, Wang Ping
"**Network Function Virtualization: Challenges and Directions for Reliability Assurance**" [Software Reliability Engineering (ISSRE), 2014 IEEE 25th International Symposium on]

*** international authorship order does not apply; authors are in an alphabetic order, due to internal policies applied by the authors' research group.