Doria Samuele

samueledoria@gmail.com | samudoria.github.io | github.com/samudoria | linkedin.com/in/samueledoria | Google Scholar Profile

Personal Profile

Security Engineer and Researcher specializing in Software and Mobile Security. Focused on engineering practical solutions for vulnerability detection, leveraging advanced static analysis and hybrid techniques. Author of multiple high-impact security tools developed in collaboration with industry leaders like Google. Active participant in the competitive security community with a strong foundation in Reverse Engineering and Binary Exploitation.

Work Experience

EURECOM *Biot, France*

Visiting PhD Researcher *Sep 2025 - Current*

- Architected an **automated binary analysis agent** using the Model Context Protocol (MCP) to orchestrate interaction between Large Language Models (LLMs) and reverse engineering tools.
- Conducted a comparative benchmark between proprietary models, open-source alternatives, and human experts to evaluate automated reverse engineering capabilities.

University of Padua *Padua, Italy*

PhD Security Researcher *Nov 2023 - Current*

- Research on Software Security, with a focus on Android Security.
- Teaching Assistant for the Mobile Security course.
- Anticipated graduation date: November 2026.

École Polytechnique Fédérale de Lausanne (EPFL) *Lausanne, Switzerland*

Research Intern at HexHive *May 2023 - Aug 2023*

- Developed a static analysis tool to create fuzzing harnesses for Android native libraries.

University of Calabria *Cosenza, Italy*

Peer-Tutor for CyberChallenge.it *Feb 2021 - July 2021*

- Peer-tutoring for the *CyberChallenge.it* initiative's participants. I guided them in their first experiences playing CTFs, more specifically in challenges involving Reverse Engineering and Binary Exploitation.

Education

University of Padua *Padua, Italy*

MSc in CyberSecurity *Sept 2021 - Sept 2023*

- Graduation score: 110/110 cum laude
- **Thesis**: *Control-Flow Graph Based Path Reconstruction in Android Applications*

University of Calabria *Cosenza, Italy*

BSc in Computer Engineering *Oct 2018 - Sept 2021*

- Graduation score: 107/110
- **Thesis**: Binary Exploitation on x86-64 and ARM

University of Calabria *Cosenza, Italy*

CyberChallenge.it Participant *Feb 2020 - June 2020*

- Selected among 20 participants to attend lectures and trainings on CyberSecurity and CTF challenges.

Talks & Projects

Project: "SPECK: From Android Textual Guidelines To Automatic Exploitation" *Collaboration with Google*

Funded by the *Google Research Scholar Program* ("Security" category) *November 2022 - Current*

- Engineered **SPECK**, a rule-based static analyzer compliant with Google's official security guidelines to automatically detect vulnerabilities in Android applications.
- Developed **GAPS**, a hybrid analysis tool focusing on code reachability to validate findings and reduce false positives.

Project: "Decompiling the Synergy: Human-LLM Teaming in Reverse Engineering" *San Diego, USA*

Published at NDSS 2026 *February 2026*

- Architected **REaLLM**, a cross-platform AI agent (IDA Pro, Ghidra) that automates artifact recovery for reverse engineers.
- Orchestrated a large-scale empirical study (n=40), demonstrating that AI assistance enables novices to match expert performance in comprehension tasks.
- Quantified the risks of LLM hallucinations, proving that AI-driven vulnerability detection currently yields a negative impact on audit accuracy.

Speaker at DEF CON 33 at the Mobile Hacking Community *Las Vegas, USA*

DEF CON 33 *August 2025*

- Selected to present original research on Android virtualization-based malware.
- Demonstrated practical detection techniques and defense methodologies to industry professionals and security researchers.

Project: "Hercules Droidot and the Murder on the JNI Express" *Seattle, USA*

Published at USENIX Security Symposium *August 2025*

- Co-developed **Poirot**: a fuzzing framework to identify memory corruption vulnerabilities at the Java Native Interface (JNI) boundary.
- Automated the detection of unsafe JNI patterns in large-scale Android applications.

Project: "VirtualPatch: Distributing Android Security Patches through Virtualization"

Published at Computers & Security Journal *August 2025*

- Designed a novel mechanism to hot-patch Android vulnerabilities using virtualization layers, bypassing system-level updates.
- Developed 10 exploits and patches following real-world CVEs to prove **VirtualPatch** effectiveness.

Project: "Matrioska: A User-Centric Defense Against Virtualization-Based Repackaging Malware" *Honolulu, USA*

Published at Annual Computer Security Applications Conference (ACSAC) *December 2023*

- **Matrioska** is a defensive framework to detect virtualization-based repackaging malware on Android.
- Implemented user-centric sandbox to warn users of potential malware.

Honors & Awards

2024	**Winner of 5th best Master thesis on CyberSecurity**, *Clusit*	*Italy*
2023	**"Mille e una lode" Award**, Merit-based scholarship awarded to the top 3% students of each degree.	*Padova, Italy*
2021	**Scholarship**, Awarded for merit during my Master's studies	*Padova, Italy*
2018	**Scholarship**, Awarded for merit during my Bachelor studies	*Cosenza, Italy*

Skills

Security & Analysis	Binary Exploitation (ARM/x64), Reverse Engineering, Fuzzing (AFL++), Static & Dynamic Analysis, Ghidra, IDA Pro, Frida.
Programming	Python, C/C++, Java, SQL, Assembly (ARM/x64), Bash/Zsh.
Tools & Platforms	Linux, Git, Docker, LaTeX, CI/CD Pipelines.

Languages

Italian	Native proficiency
English	C2 level: proficient user