Simone Aonzo

Curriculum Vitae (Updated to: 2019/08/08)

✉ *simone.aonzo@gmail.com*
🖱 *https://packmad.github.io/*
⊘ *packmad*
🐦 *packm4d*
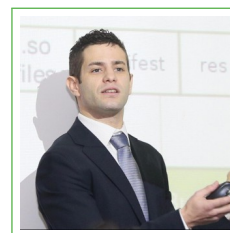
Education

2017–now	**Ph.D. student in Computer Science and Systems Engineering**, *University of Genoa (Italy) (DIBRIS)*.
2010-2015	**Master of Computer Science**, *University of Genoa (Italy), 110/110 cum laude*.

Master Thesis

Title	*"A new permission handling in Android"* [1]
Supervisor	Prof. Giovanni Lagorio

Certifications

2019-03-05	GIAC Reverse Engineering Malware

Work Experience

2015-2017	**Android pentester and developer**, *Talos*, Genoa/Italy.
	I have pentested several Android apps, especially banking ones, according to the Mobile Application Security Verification Standard (MASVS);
	I developed the back end (based on a microservices architecture) of Approver, a commercial analysis service for Android apps.
2007-2010	**Network and Computer Systems Administrators**, *Teknoos*, Savona/Italy.
	Upkeep and configuration of IT infrastructure for small/medium business companies.

Teaching Activity

2017-now	Android Malware Analysis	*for Talos in private companies*
2017-now	Android Mobile Programming	*B.Sc. Computer Engineering*
2017-now	Operating System	*B.Sc. Computer Engineering*
2017-now	Mobile Security	*Master in Cybersecurity*

Natural Languages

Italian	Native speaker
English	CEFR C1

Computer Languages

Programming	C, Python, Java, C#, C++, PHP, Javascript	*sorted by profiency*
Assembly	ARM, x86	

Technical Experience

- To support the experimental evidence of my publications I developed two Android apps ApkMuzzle [1] and Baddroids [2], both of them analyze the apps installed on your Android device: the former removes permissions and advertising, the latter uses an energy saver static analysis technique to extract features for a machine learning model in order to detect malicious apps.
- I teach (see "Teaching Activity") the state-of-the-art techniques and processes to analyze Android malware, starting from the basic concepts of the Android ecosystem.
- Capture-The-Flag player and co-founder of Zenhack team, my favorite categories are reversing and exploitation.

Research Topics by Keywords

- reverse engineering [1, 4]
- phishing [3]
- program analysis [1, 2, 4]
- machine learning [2]

Publications

[1] S. Aonzo, G. Lagorio, and A. Merlo, "Rmperm: A tool for android permissions removal.," in *SECRYPT*, pp. 319–326, 2017.

[2] S. Aonzo, A. Merlo, M. Migliardi, L. Oneto, and F. Palmieri, "Low-resource footprint, data-driven malware detection on android," *IEEE Transactions on Sustainable Computing*, 2017.

[3] S. Aonzo, A. Merlo, G. Tavella, and Y. Fratantonio, "Phishing Attacks on Modern Android," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, (Toronto, Canada), October 2018.

[4] D. Caputo, L. Verderame, S. Aonzo, and A. Merlo, "Droids in disarray: Detecting frame confusion in hybrid android apps," in *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 121–139, Springer, 2019.

References

Prof.	Alessandro Armando	*Research manager*
Prof.	Yanick Fratantonio	
Prof.	Giovanni Lagorio	*Master thesis supervisor*
Prof.	Alessio Merlo	*PhD advisor*
Ph.D.	Luca Verderame	*Talos srls. CEO*