Simone Aonzo

Résumé (Updated to: 2020/11/23)

✉ simone.aonzo@gmail.com
🖰 https://simoneaonzo.it/

— Postdoctoral Systems Security Researcher —

Education

2017–2020	**Ph.D. in Computer Science and Systems Engineering**, *DIBRIS*, University of Genoa (Italy).
2010-2015	**Master in Computer Science**, *University of Genoa (Italy)*, *110/110 cum laude*.

Ph.D. Thesis

Title	*"Novel Attacks and Defenses in the Userland of Android"*
Advisor	Prof. Alessio Merlo

Master Thesis

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

Certifications

2019-03-05	GIAC Reverse Engineering Malware

Work Experience

2020-now	**Postdoctoral researcher**, *EURECOM*, Sophia Antipolis/France.
2015-2017	**Android pentester and developer**, *Talos srls*, 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 Administrator**, *Teknoos*, Savona/Italy.
	Maintenance and configuration of IT infrastructure for small/medium business companies.

Teaching

2017-2020	**Android Reverse Engineering**, *for Talos srls in private companies*.
2018-2019	**Mobile Security**, *Master in Cybersecurity*, University of Genoa (Italy).

Teaching Support

2017-2019	**Android Programming**, *B.Sc. Computer Engineering*, University of Genoa (Italy).
2017-2018	**Operating Systems**, *B.Sc. Computer Engineering*, University of Genoa (Italy).

Natural Languages

Italian	Native speaker
English	CEFR C1

Computer Languages

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

Technical Experience

- I have designed and developed (see "Work Experience") the back-end of Approver; it is based on Java Spring and Python Flask frameworks.
- I have developed two Android apps, ApkMuzzle [1] and Baddroids [2], to support the experimental evidence of my publications. Both of them analyze the apps installed on an 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.
- Capture-The-Flag player and co-founder of Zenhack team, my favorite categories are reversing and exploitation.

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] A. Mantovani, S. Aonzo, X. Ugarte-Pedrero, A. Merlo, and D. Balzarotti, "Prevalence and impact of low-entropy packing schemes in the malware ecosystem," in *Network and Distributed System Security (NDSS) Symposium*, February 2020.

[5] 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.

[6] S. Aonzo, G. C. Georgiu, L. Verderame, and A. Merlo, "Obfuscapk: An open-source black-box obfuscation tool for android apps," *SoftwareX*, vol. 11, p. 100403, 2020.

Research Topics by Keywords

- program analysis [1, 2, 5, 6, 4]
- reverse engineering [1, 5, 6, 4]
- machine learning [2, 4]
- phishing [3]

Three most important publications

1. *Phishing Attacks on Modern Android* [3]
2. *Prevalence and impact of low-entropy packing schemes in the malware ecosystem* [4]
3. *Low-resource footprint, data-driven malware detection on Android* [2]

References

Prof. Alessandro Armando	*alessandro.armando@consorzio-cini.it*
Prof. Davide Balzarotti Costa	*davide.balzarotti@eurecom.fr*
Prof. Yanick Fratantonio	*yanick@fratantonio.me*
Prof. Alessio Merlo	*alessio@dibris.unige.it*