GIORGIO SEVERI

severi.xyz
severi.g@northeastern.edu
https://github.com/ClonedOne
https://www.linkedin.com/in/giorgioseveri/

Brookline, MA

Research Interests

Adversarial Machine Learning and Software Security.

Education

Ph.D., Northeastern University, Boston, MA — Fall 2018 - Present
Major: Computer Science.
Advisor: Prof. Alina Oprea.
Research topic: machine learning security and adversarial machine learning.

Master of Science, Sapienza University of Rome, Rome, Italy — 2015 - 2018
Major: Computer Science and Engineering.
Final grade: 110/110 cum Laude.
Thesis: Malwords, Malware classification and clustering based on textual memory content.

Bachelor of Science, Sapienza University of Rome, Rome, Italy — 2011 - 2014
Major: Computer Science and Engineering
Final grade: 107/110
Thesis: FreebleApp, Development of a smart, location based, mobile advertisement platform on Android OS.

Experience

Applied research intern — Summer 2022
Microsoft AI Red Team, Redmond, WA.

- Worked in the machine learning red team.
- Developed attacks to test the robustness of deployed, large scale, machine learning systems.

Applied research intern — Summer 2021
Microsoft Azure Trustworthy Machine Learning, (Remote) Redmond, WA.

- Worked in the machine learning red team.
- Developed attacks to test the robustness of deployed, large scale, machine learning systems.

Data Science Intern — Summer 2019
FireEye, Reston, VA

- Developed techniques to perform backdoor poisoning attacks in the context of malware classification.

Graduate Assistantship — Fall 2018 - Present
Northeastern University, Khoury College of Computer Sciences, Boston, MA.

- Teaching assistant for *CY 7790: Special Topics in Security and Privacy: Machine Learning Security and Privacy* taught by professor Alina Oprea, Fall 2021.
- Graduate Fellowship for academic year 2018-2019.

- Works in the Network and Distributed Systems Security Lab (NDS2) with professor Alina Oprea.

Junior Research Scientist, Summer 2017
New York University, Tandon School of Engineering, New York, NY.

- Conducted research on malware analysis and classification.
- Employed text mining and machine learning techniques to classify and cluster malicious software samples.

Student Internship, Summer 2016
European Space Agency ESA, ESRIN, Earth Observation Directorate, Italy.

- Evaluated usability of satellite image resources for Hackathon participants.
- Developed a mobile application in Java to test a newly deployed web service.

Internal work placement, 2014 - 2015
Sapienza University, Department of Computer, Control, and Management Engineering Antonio Ruberti, Rome, Italy.

Publications and Patents

Severi, Giorgio, Simona Boboila, Alina Oprea, John Holodnak, Kendra Kratkiewicz, and Jason Matterer. "Poisoning Network Flow Classifiers." To appear in Proceedings of the 39th Annual Computer Security Applications Conference 2023.

Di Bartolomeo, Sara, Giorgio Severi, Victor Schetinger, and Cody Dunne. "Ask and you shall receive (a graph drawing): Testing ChatGPT's potential to apply graph layout algorithms." In Proc. EuroVis Conference on Visualization. 2023.

Severi, Giorgio, Will Pearce, and Alina Oprea. "Bad Citrus: Reducing Adversarial Costs with Model Distances." In 2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 307-312. IEEE, 2022.

Coull, Scott Eric, David Krisiloff, and Giorgio Severi. "System and method for heterogeneous transferred learning for enhanced cybersecurity threat detection." U.S. Patent 11,475,128, issued October 18, 2022.

Severi, Giorgio, Matthew Jagielski, Gökberk Yar, Yuxuan Wang, Alina Oprea, and Cristina Nita-Rotaru. "Network-level adversaries in federated learning." In 2022 IEEE Conference on Communications and Network Security (CNS), pp. 19-27. IEEE, 2022.

Jagielski, Matthew, Giorgio Severi, Niklas Pousette Harger, and Alina Oprea. "Subpopulation data poisoning attacks." In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pp. 3104-3122. 2021.

Severi, Giorgio, Jim Meyer, Scott Coull, and Alina Oprea. "Explanation-Guided Backdoor Poisoning Attacks Against Malware Classifiers." In 30th USENIX Security Symposium (USENIX Security 21). 2021.

Severi, Giorgio, Tim Leek, and Brendan Dolan-Gavitt. "Malrec: compact full-trace malware recording for retrospective deep analysis." In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 3-23. Springer, Cham, 2018.

Talks

"Zen and the Art of Adversarial Machine Learning". Will Pearce, Giorgio Severi. Black Hat Europe 2021, London, UK.

"Exploring Backdoor Poisoning Attacks Against Malware Classifiers". Giorgio Severi, Jim Meyer, Scott Coull. Conference on Applied Machine Learning in Information Security, CAMLIS, 2019, Washington, DC.

Academic Service

Program Committee member for the 16th ACM Workshop on Artificial Intelligence and Security 2023.

Program Committee member for the DSN Workshop on Dependable and Secure Machine Learning 2023.

Shadow Program Committee member for the IEEE Symposium on Security and Privacy 2021.

Additional Experience

Staff member at Codemotion Rome, 2017 and 2015.
Mentor at "Tech My Cosplay", Arduino Hackathon Rome, 2017.
Staff member at Data Driven Innovation Rome 2017.
Staff member at Maker Faire Rome 2014.

Languages

Italian, native speaker.
English, European level CEFR C2. IELTS score: 8.5/9. ESOL CPE certificate.

Awards

Winner Accenture Digital Hackathon Rome 2016.
NASA International SpaceApps Challenge 2015.

- Project CROPP, Global winner for category Galactic Impact and Rome local competition.