Dorjan Hitaj

Current position

feb.'22 –	**Postdoctoral Researcher**.
university	*Sapienza University of Rome, Italy*
research area	*Machine Learning and Security*
supervisor	Luigi V. Mancini

Education

nov.'18 – feb.'22	**PhD in Computer Science**.
university	*Sapienza University of Rome, Italy*
thesis title	Hidden between Gradients: Evaluating the Limits of Machine Learning in Cybersecurity Applications
advisor	Luigi V. Mancini
Evaluation	Excellent

sept.'16 – jul.'18	**Master of Science in Computer Science**.
university	*Sapienza University of Rome, Italy*
thesis title	Novel Evasion Attacks against Ownership-Enforcing methods for Neural Network Machine Learning Models
advisor	Luigi V. Mancini
GPA	*30/30*
Final grade	110 cum laude
extra	Honours program *(Percorso di Eccellenza)*

oct.'12 – jul.'15	**Bachelor in Business Informatics**.
university	*Epoka University, Albania*
thesis title	*Towards Indestructible Molecular Robots*
advisor	Ilir Capuni
award	*Ranked 1st among Graduate Class of 2015*
GPA	*4.0/4.0 (High honours)*

Experience

Research Positions

Oct.'20 – **Researcher**.
university *Sapienza University of Rome, Italy*
topic *Task Leader and local coordinator in Gen4Olive EU project (Horizon-2020)*

Jun.'21 – Oct.'21 **Researcher**.
university *Sapienza University of Rome, Italy*
topic *Study of Machine Learning models and data analysis techniques for scoring and evaluation of computer games*
supervisor *Luigi V. Mancini*

mar.'20 – apr.'20 **Researcher**.
university *Sapienza University of Rome, Italy*
topic *Study of Machine Learning models and data analysis techniques for scoring and evaluation of computer games*
supervisor *Luigi V. Mancini*

aug.'18 – oct.'18 **Researcher**.
university *Sapienza University of Rome, Italy*
topic *Study and Design of Novel Defense and Attack methods in Machine Learning systems*
supervisor *Luigi V. Mancini*

Research Projects

Apr.'22 – **Work-Package Leader**.
university *Sapienza University of Rome, Italy*
Project ***Gen4Olive*** *European Union's Horizon 2020 research and innovation programme (Grant Agreement No. 101000427)*
Work-Package *I am currently managing the work package 6 lead by Sapienza University of Rome.*

Oct.'20 – **Task Leader**.
university *Sapienza University of Rome, Italy*
Project ***Gen4Olive*** *European Union's Horizon 2020 research and innovation programme (Grant Agreement No. 101000427)*
Task *T6.2: Design and implementation of a User-Friendly software platform for farmers, nurseries and breeders.*

Teaching Positions

jan.'20 – **Teaching Assistant**, Sapienza University of Rome, Italy.
Data and Network Security, Master Degree course in Computer Science.
professor Luigi V. Mancini

Software Developing Positions

jul.'17 – apr.'18 **Software Developer**, Chainside, Rome, Italy.

jul.'15 – sept.'16 **Software Developer**, Excellence Labs, Tirana, Albania.

Freelance Software Developing

dec.'15 – jun.'16 **Software Developer**, AIAD (Albanian Integrated Agriculture Digitalization), Tirana, Albania.

apr.'15 – apr.'16 **Software Developer**, Okazioni.yt, Albania.

dec.'15 – feb.'16 **Software Developer**, WarshaPlus Company, Saudi Arabia.

Internships

jan.'15 – mar.'15 **Intern**, *Human Resources and Finance Department*, United States Embassy, Tirana, Albania.

Mentoring

oct.'14 – jun.'15 **Object Oriented Programming with JAVA**, *"Programming Club" Epoka University*, Albania.

Extracurricular

jan.'18 – jun.'18 **Honours Program (Percorso di Eccellenza)**.
university *Sapienza University of Rome, Italy*
topic *Secure Machine Learning*
supervisor *Luigi V. Mancini*

Grants and Scholarships

nov.'21 – oct.'22 **Research Fellowship**
funding *Computer Science Department*, Sapienza University of Rome, Italy.

nov.'21 **Student Grant for Research Activity (Avvio alla Ricerca Type II)**
funding *Sapienza University of Rome*, Sapienza University of Rome, Italy.

nov.'18 – oct.'21 **PhD Scholarship**.
funding *Computer Science Department*, Sapienza University of Rome, Italy.

jun.'21 – oct.'21 **Student Grant for Research Activity**
funding *Computer Science Department*, Sapienza University of Rome, Italy.

nov.'20 **Student Grant for Research Activity (Avvio alla Ricerca Type I)**
funding *Sapienza University of Rome*, Sapienza University of Rome, Italy.

mar.'20 – apr.'20 **Student Grant for Research Activity**
funding *Computer Science Department*, Sapienza University of Rome, Italy.

aug.'18 – oct.'18 **Student Grant for Research Activity**
funding *Computer Science Department*, Sapienza University of Rome, Italy.

sept.'16 – jul.'18 **Student Scholarship** , *Master of Science in Computer Science*.
funding *LazioDiSCo*, Lazio Region, Italy.

sep.'12 – jun.'15 **Student Scholarship**, *Bachelor in Business Informatics*.
funding Epoka University, Albania

Awards

feb.'20 **Premio di Laurea**, *prize for being among the best graduates of the academic year 2017-2018 in the Lazio region, LazioDiSCO*.

may.'19 **High Academic Honour Certificate *(Laureato Eccellente)***, *for being among the best graduates of the academic year 2017-2018, Sapienza University of Rome*.

jun.'15 **High Academic Honour Certificate**, *for excellent performance during studies of Bachelor in Business Informatics, Epoka University*.

jun.'15 **Certificate of Achievement**, *Ranked 1st in the Graduating Class of 2015, Bachelor Program in Business Informatics, Epoka University*.

mar.'15 **Best Idea**, *Tung Ideve StartUp, Epoka University*.

mar.'14 **First Place (ZeroCool team member)**, *Intelligent Minds online Programming Contest IMoPC-2014, Epoka University*.

Skills

Computer Skills

programming languages	Python, PHP, Java, SQL
markup languages	HTML
style sheet languages	CSS
frameworks and libraries	PyTorch, Tensorflow, Keras, Django, Symphony, Laravel, Flask, Hadoop
utility	Iptables

Languages

native	Albanian
fluent	English (TOEFL IBT, 103)
intermediate	Italian

Publications

[1] Ilir Capuni, Anisa Halimi, and Dorjan Hitaj. **Towards Indestructible Molecular Robots**. In *SOFSEM*, 2015.

[2] Dorjan Hitaj, Briland Hitaj, and Luigi V. Mancini. **Evasion Attacks Against Watermarking Techniques found in MLaaS Systems**. IEEE International Conference on Software Defined Systems, 2019.

[3] Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo DeCarli, and Luigi V. Mancini. **The Naked Sun: Malicious Cooperation Between Benign-Looking Processes** ACNS 2020: 18th International Conference on Applied Cryptography and Network Security.

[4] Dorjan Hitaj, Briland Hitaj, Sushil Jajodia, and Luigi V. Mancini. **Capture the Bot: Using Adversarial Examples to Improve CAPTCHA Robustness to Bot Attacks** IEEE Intelligent Systems, 2021.

[5] Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo DeCarli, and Luigi V. Mancini. **EnCoD: Distinguishing Compressed and Encrypted File Fragments** 14th International Conference on Network and System Security, 2020.

[6] Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo DeCarli, and Luigi V. Mancini. **Evading Behavioral Classifiers: A Comprehensive Analysis on Evading Ransomware Detection Techniques** Neural Computing and Applications, 2022.

[7] Dorjan Hitaj, Giulio Pagnotta, Iacopo Masi, and Luigi V. Mancini. **Evaluating the Robustness of Geometry-Aware Instance-Reweighted Adversarial Training** technical report.

[8] Fabio De Gaspari, Dorjan Hitaj, Giulio Pagnotta, Lorenzo DeCarli, and Luigi V. Mancini. **Reliable Detection of Compressed and Encrypted Data** Neural Computing and Applications, 2022.

[9] Giulio Pagnotta, Dorjan Hitaj, Fabio De Gaspari, and Luigi V. Mancini. **PassFlow: Guessing Passwords with Generative Flows** The 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2022.

[10] Dorjan Hitaj, Giulio Pagnotta, Briland Hitaj, Fernando Perez-Cruz, and Luigi V. Mancini. **FedComm: Federated Learning as a Medium for Stealthy Communication** under submission.

[11] Giulio Pagnotta, Dorjan Hitaj, Briland Hitaj, Fernando Perez-Cruz, and Luigi V. Mancini. **TATTOOED: A Robust Deep Neural Network Watermarking Scheme based on Spread-Spectrum Channel Coding** under submission.

[12] Dorjan Hitaj, Giulio Pagnotta, Briland Hitaj, Luigi V. Mancini, and Fernando Perez-Cruz. **MaleficNet: Hiding Malware into Deep Neural Networks using Spread-Spectrum Channel Coding** 27th European Symposium on Research in Computer Security (ESORICS), 2022.