Dario Pasquini, Ph.D.

19/09/1991, Rome, Italy.

email: pasquini.dario.1991@gmail.com
personal page: `https://pasquini-dario.github.io/me/`

Bio:

Security researcher specialized in the intersection of deep learning and cybersecurity. Focused on fortifying digital ecosystems through ML-driven solutions, safeguarding against emerging threats.

Experience:

[**10/2021 - today**] **Postdoctoral Researcher:**
École Polytechnique Fédérale de Lausanne (EPFL), Switzerland
Security and Privacy Engineering Laboratory (SPRING)
Lab lead: *Carmela Troncoso.*

[**02/2021 - 09/2021**] **Research Fellow:**
National Research Council (CNR), Italy.
Institute for applied mathematics “Mauro Picone” (IAC); Rome/Naples.

[**07/2021**] ***Ph.D.*** **in Computer Science:**
Sapienza University of Rome, Italy
Advisor: *Massimo Bernaschi.*
(Fellowship winner).

> [**03/2019 - 03/2020**] **Visiting Researcher**:
> Stevens Institute of Technology, USA
> Advisor: *Giuseppe Ateniese.*

[**2018**] **Master’s degree** in **Computer Science**:
Sapienza University of Rome, Italy
Final Grade: *110/110 cum laude*
Program of Study: *Network and Security*

Research topics and Expertise:

- Security & Privacy in Machine Learning:
  - Collaborative Learning.
  - **(active)** Large Language models.
- Password Security (via ML).
- **(active)** Practical Security & Privacy Crypto-systems (via ML).
- HPC; General-purpose computing on graphics processing units.

Tools:

- **ML/Deep Learning:** TensorFlow, PyTorch, and surrounding ecosystem.
- **HPC/Scripting:** C, CUDA C++, MPI, Python, Perl.

Languages:

- English, Italian (mother tongue).

Publications

Top-Conferences (acceptance rate ∼15%):

[1] **Dario Pasquini**, Giuseppe Ateniese, Carmela Troncoso. *Universal Neural-Cracking-Machines: Self-Configurable Password Models from Auxiliary Data.* 45th IEEE Symposium on Security and Privacy (S&P '24), San Francisco, CA, USA, May 2024

[2] **Dario Pasquini**, Mathilde Raynal, Carmela Troncoso. *On the (In)security of Peer-to-Peer Decentralized Machine Learning.* 44th IEEE Symposium on Security and Privacy (S&P '23), San Francisco, CA, USA, May 2023

[3] **Dario Pasquini**, Danilo Francati, Giuseppe Ateniese. *Eluding Secure Aggregation in Federated Learning via Model Inconsistency.* ACM Conference on Computer and Communications Security (CCS '22), Los Angeles, CA, USA, November 2022

[4] **Dario Pasquini**, Giuseppe Ateniese, Massimo Bernaschi. *Unleashing the Tiger: Inference Attacks on Split Learning.* ACM Conference on Computer and Communications Security (CCS '21), Seul, Republic of Korea, November 2021

[5] **Dario Pasquini**, Marco Cianfriglia, Giuseppe Ateniese, Massimo Bernaschi. *Reducing Bias in Modeling Real-world Password Strength via Deep Learning and Dynamic Dictionaries.* 30th USENIX Security Symposium (USENIX Sec '21), August 2021

[6] **Dario Pasquini**, Ankit Gangwal, Giuseppe Ateniese, Massimo Bernaschi, Mauro Conti. *Improving Password Guessing via Representation Learning.* 42th IEEE Symposium on Security and Privacy (S&P '21), San Francisco, CA, USA, May 2021.

Other:

[7] Etienne Salimbeni, Nina Mainusch, **Dario Pasquini**. *Your Email Address Holds the Key: Understanding the Connection Between Email and Password Security with Deep Learning.* 6th Deep Learning Security and Privacy Workshop, May 2023

[8] **Dario Pasquini**, Giuseppe Ateniese, Massimo Bernaschi. *Interpretable probabilistic password strength meters via deep learning.* 25th European Symposium on Research in Computer Security (ESORICS '20), September 2020.

[9] **Dario Pasquini**, Marco Mingione, Massimo Bernaschi. *Adversarial out-domain examples for generative models.* IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops '19

[10] Massimo Bernaschi, Pasqua D'Ambra, **Dario Pasquini**. *AMG based on compatible weighted matching for GPUs.* Parallel Computing, 2020.

[11] Massimo Bernaschi, Pasqua D'Ambra, **Dario Pasquini**. *BootCMatchG: An adaptive Algebraic MultiGrid linear solver for GPUs.* Software Impacts, 2020.