Dario Pasquini, Ph.D.
19/09/1991, Rome, Italy.

Contact Personal Page GitHub Google Scholar

Researcher operating at the bleeding edge of the intersection of *Security* and *"AI"*, seeking security and privacy solutions that transcend trust and ideal assumptions (*in reality, I spend most of my day either breaking ML models or building ML models to break stuff*).

Working on:

- Security & Privacy in Machine Learning:
  - Large Language Models [ArXiv24]
  - Private Collaborative Learning [S&P'23, CCS'21, CCS'22]
- Password Security (using ML) [S&P'24a, S&P'21, USENIX'21]
- (Practical) Security Cryptographic Protocols (using ML) [S&P'24b, CCS'22]
- Differential Privacy [S&P'24a]
- [inactive] HPC; GPGPU, Multi-GPU [ParComp]

Experience:

[**04/2024 - Now**] **Visiting Faculty:**
George Mason University, Virginia, USA

[**10/2021 - 03/2024**] **Postdoctoral Researcher:**
École Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland
Security and Privacy Engineering Laboratory (SPRING)

[**05/2020 - 9/2021**] **Research Fellow:**
National Research Council (CNR)
Institute for applied mathematics "Mauro Picone" (IAC), Italy, Rome/Naples

[**04/2019 - 04/2020**] **Visiting Researcher**:
Stevens Institute of Technology, New Jersey, USA

Contract & Consulting work:

[**12/2023 - Now**] **Password Recovery Expert** (Cryptocurrency)
DSEC Labs LLC, Virginia, USA

Education:

[**2018 - 2021**] ***Ph.D.* in Computer Science** (fellowship winner):
Sapienza University of Rome, Italy
Advisor: *Prof. Massimo Bernaschi* (*massimo.bernaschi@cnr.it*)

[**2015 - 2017**] **Master degree** in **Computer Science**:
Sapienza University of Rome, Italy
Final Grade: *110/110 cum laude*
Program of Study: *Network and Security*

Technical Skills (at least, the ones you might want to pay me for):

- **Machine Learning:**
  - TensorFlow (e.g., UniversalNeuralCrackingMachines, ADAMS, SplitNN_FSHA, PLR)
  - PyTorch (e.g., LLM_NeuralExec)
- **HPC**:
  - CUDA (e.g., BootCMatchG)
  - MPI
- **Languages**:
  - Python
  - C / C++

Academic service:

- **Program committees:** · ACM CCS 2023, · USENIX Sec. 2023, · IEEE SaTML 2024.
- **Teaching:** 2022/2023 *"Privacy Preserving Machine Learning"* in master course: *"Advanced topics on privacy enhancing technologies"* (EPFL).

Real skills:

- Open water swimmer
- ex-Triathlete
- ex-MMA practitioner
- Weekend quant

Publications:

Preprints:

[ArXiv24] **Dario Pasquini**, Martin Strohmeier, Carmela Troncoso. *Neural Exec: Learning (and Learning from) Execution Triggers for Prompt Injection Attacks.* https://arxiv.org/pdf/2403.03792.pdf

Top-tier:

[S&P'24b] **Dario Pasquini**, Danilo Francati, Giuseppe Ateniese, Evgenios M. Kornaropoulos. *Breach Extraction Attacks: Exposing and Addressing the Leakage in Second Generation Compromised Credential Checking Services.* 45th IEEE Symposium on Security and Privacy (S&P'24), San Francisco, CA, USA, May 2024. https://eprint.iacr.org/2023/1848.pdf

[S&P'24a] **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. https://arxiv.org/pdf/2301.07628.pdf

[S&P'23] **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 https://arxiv.org/pdf/2205.08443.pdf

[CCS'22] **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. https://arxiv.org/pdf/2111.07380.pdf

[CCS'21] **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. https://arxiv.org/pdf/2012.02670.pdf

[USENIX'21] **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. https://arxiv.org/pdf/2010.12269.pdf

[S&P'21] **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. https://arxiv.org/pdf/1910.04232.pdf

Other Publications:

[S&Pw'23] 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

[ESORICS'20] **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

[EuroS&Pw'19] **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

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

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