Dario Pasquini, Ph.D.

19/09/1991, Rome, Italy.

Contact   Personal Page   GitHub   Google Scholar

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

———————————

What I do:

- Security, Privacy, and Machine Learning:
    - [**current focus**] Security and Large Language Models
    - Security & Privacy in Collaborative Learning [S&P'23, CCS'22, CCS'21]
- Password Security (via ML) [S&P'24b, S&P'24a, S&P'21, USENIX'21]
- [inactive] HPC; GPGPU, Multi-GPU [ParComp]

———————————

Where I do it:

[2021 - Now] Postdoctoral Researcher:
École Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland
Security and Privacy Engineering Laboratory (SPRING)
Lab chief: *Prof. Carmela Troncoso* (*carmela.troncoso@epfl.ch*)

[2020 - 2021] Research Fellow:
National Research Council (CNR)
Institute for applied mathematics "Mauro Picone" (IAC), Italy, Rome/Naples
Lab chief: *Prof. Massimo Bernaschi* (*massimo.bernaschi@cnr.it*)

[2019 - 2020] Visiting Researcher:
Stevens Institute of Technology, New Jersey, USA
Host: *Prof. Giuseppe Ateniese* (*ateniese@gmu.edu*).

———————————

Education:

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

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

Tools (I enjoy using):

- **ML/Deep Learning:** TensorFlow, PyTorch, and surrounding ecosystem.

- **HPC/Scripting:** C, CUDA C++, MPI, Python, Perl.

Service:

- **Program committees:** CCS'23, USENIX'23, SaTML 2024.

Publications:

Top-tier Conferences (acceptance rate ∼15%):

[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

[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

[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

[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

[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

[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

[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.

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