

Working on the intersection of Security and ML, seeking security and privacy solutions that transcend trust, ideal assumptions, and optimistic threat models (*although, in practice, I end up spending most of my day either breaking AI models or building AI models to break stuff*).

## Interested in:

- ▲ Security in LLMs/agents [[AISeC'24](#), [USENIX'25](#), [ArXiv24](#), [ArXiv25](#)]
- ▼ Security & Privacy in Collaborative Machine Learning [[S&P'23](#), [CCS'21](#), [CCS'22](#)]
- ▼ Password Security [[S&P'24a](#), [S&P'21](#), [USENIX'21](#)]
- ▲ Leakage in Cryptosystems [[S&P'24b](#), [CCS'22](#)]
- ▲ Differential Privacy [[S&P'24a](#)]
- ▼ HPC; GPGPU, Multi-GPU [[ParComp](#)]

## Work experience:

### [ 11/2024 - Now ] Principal Researcher:

*RSAC Labs*  
Switzerland

### [ 04/2024 - 10/2024 ] Visiting Faculty:

*George Mason University, Cybersecurity department*  
Virginia, USA

### [ 10/2021 - 03/2024 ] Postdoctoral Researcher:

*École Polytechnique Fédérale de Lausanne (EPFL)*  
Security and Privacy Engineering Laboratory (SPRING)  
Switzerland

### [ 05/2020 - 9/2021 ] Research Fellow:

*National Research Council (CNR), Institute for applied mathematics “Mauro Picone” (IAC)*  
Italy

### [ 04/2019 - 04/2020 ] Visiting Researcher:

*Stevens Institute of Technology, Computer Science department*  
New Jersey, USA

## Contract & Consulting work:

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

[ 04/2024 ] **Machine Learning Expert** (Security Auditing of Authentication Systems)  
Detack GmbH, Germany

## Education:

### [ 2018 - 2021 ] **Ph.D. in Computer Science** (fellowship winner):

*Sapienza University of Rome, Italy*  
Advisor: *Prof. Massimo Bernaschi* ([massimo.bernaschi@cnr.it](mailto: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:

- **Machine Learning:**

- TensorFlow (e.g., [UniversalNeuralCrackingMachines](#), [ADAMS](#))
- PyTorch (e.g., [NeuralExec](#), [LLMmap](#))

**General purpose languages & libs:**

- Python (e.g., [project\\_mantis](#))
  - MPI, CUDA (e.g., [BootCMatchG](#))
  - C / C++
- 

## Academic service:

- **Program committees:**

- ACM CCS 2023, 2025, 2026
- USENIX Sec. 2023, 2025
- IEEE S&P 2026
- IEEE SaTML 2024, 2025, 2026
- PETs 2025.

- **Workshops:** CRYPTO PPML 2024

- **Teaching:** 2022/2023 “*Privacy Preserving Machine Learning*” in master course: “*Advanced topics on privacy enhancing technologies*” (EPFL).

## Real-world skills:

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

## Publications:

### Preprints:

[ArXiv25] **Dario Pasquini**, Evgenios M. Kornaropoulos, Giuseppe Ateniese, Omer Akgul, Athanasios Theodoridis and Petros Efthathopoulos. *When AIOps Become “AI Oops”: Subverting LLM-driven IT Operations via Telemetry Manipulation* <https://arxiv.org/abs/2508.06394>

[ArXiv24] **Dario Pasquini**, Evgenios M. Kornaropoulos, Giuseppe Ateniese. *Hacking Back the AI-Hacker: Prompt Injection as a Defense Against LLM-driven Cyberattacks* (Finalist in the “Epic Achievement” Category PwnieAwards 2025) <https://arxiv.org/pdf/2410.20911.pdf>

## Top-tier publications:

[USENIX'25] **Dario Pasquini**, Evgenios M. Kornaropoulos, Giuseppe Ateniese. *LLMmap: Fingerprinting For Large Language Models*. 34th USENIX Security Symposium (USENIX Sec'25), August 2025, Seattle, WA, USA <https://arxiv.org/pdf/2407.15847>

[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. (Finalist for the Best Crypto Attack at PwnieAwards 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:

[AISeC'24] **Dario Pasquini**, Martin Strohmeier, Carmela Troncoso. *Neural Exec: Learning (and Learning from) Execution Triggers for Prompt Injection Attacks*. 17'Th ACM Workshop On Artificial Intelligence And Security (Spotlight) <https://arxiv.org/pdf/2403.03792.pdf>.

[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