# Maura Pintor, Assistant Professor @ Unica

✉ `maura.pintor@unica.it` 🌐 `https://maurapintor.github.io`
`@maurapintor` `https://www.linkedin.com/in/maura-pintor/`

## Education and Research

03/2023 - ongoing **University of Cagliari (Italy), Assistant Professor (RTDa).** Machine learning security.

10/2021 - 02/2023 **University of Cagliari (Italy), Postdoctoral Researcher.** Machine learning security.

2018 - 2022 **University of Cagliari (Italy) - PhD (with honors) in Electronic and Computer Engineering**
Topic: Adversarial Machine Learning.
Graduation date: 18/02/2022
Thesis: *Towards Debugging and Improving Adversarial Robustness Evaluations.*

05/2021 - 08/2021 **Software Competence Center Hagenberg (Austria), Visiting Student.** Laboratory: SCCH.

03/2020 - 06/2020 **University of Tübingen (Germany) - Max Planck Institute for Intelligent systems, Visiting Student.** Laboratory: Bethgelab.

2016 - 2018 **University of Cagliari (Italy) - Telecommunications Engineering, 1st Level Degree (Master).**
Graduation date: 25/09/2018. Final degree mark: 110/110, magna cum Laude
Thesis: *A novel temporal descriptor for analyzing small and large crowds by computer vision algorithms.*

2010 - 2016 **University of Cagliari (Italy) - Electronic Engineering, 2nd Level Degree (Bachelor).** Graduation date: 22/07/2016. Final degree mark: 104/110
Thesis: *Methods and Algorithms for gender classification through face image acquisition.*

## Research Projects

10/2022 - ongoing Participation, with the University of Cagliari, in the EU project “European Lighthouse on Secure and Safe AI” (ELSA), Grant Agreement no.: 101070617, funded by the European Union in the programme HORIZON-CL4-2021-HUMAN-01.

10/2021 - ongoing Participation, with the University of Cagliari, in the research project “Huawei R&D Agreement: Deep Reinforcement Learning Key Security Technologies”, Grant Agreement n. TC20201118006.

03/2021 - ongoing Scientific Coordinator, with the company Pluribus One, of the WP6 (Impact: Benchmark Datasets and Tool Flow Pilots) of the EU project “Assurance and certification in secure Multi-party Open Software and Services” (AssureMOSS), Grant Agreement no.: 952647, funded by the EU Union in the programme H2020-SU-ICT-2019.

03/2019 - 03/2020 Scientific Coordinator, with the company Pluribus One, in the EU project “Software framework for runtime-Adaptive and secure deep Learning On Heterogeneous Architectures” (ALOHA), Grant Agreement no.: 780788, funded by the EU Union in the programme H2020-ICT-2017-1.

## Employment History

03/2021 - 03/2023 **Pluribus One S.r.l. (Italy), Collaborator.** Automated techniques to assess, manage, and re-certify the security and privacy risks of multi-party open software and services (MOSS). *Project AssureMOSS - EU.*

03/2019 - 03/2020 **Pluribus One S.r.l. (Italy), Collaborator.** Deep Learning systems in low-power heterogeneous platforms. Development of a module for evaluation of security against Adversarial Attacks. *Project ALOHA - EU.*

02/2018 - 07/2018 **Pluribus One S.r.l. (Italy), Software developer.** Systems for Internet traffic security.

07/2017 - 12/2017 **University of Cagliari (Italy), Collaborator.** IoT system for data gathering and visualization. Design, software development, sensor integration, data management and cloud storage. *MIUR - Smart Cities - CagliariPort2020.*

## Teaching

### Teaching Assistant

12/2019 - ongoing **University of Cagliari (Italy), Teaching Assistant.** Industrial Software Development (MSc in Computer Engineering, Cybersecurity and Artificial Intelligence).

05/2019 - ongoing **University of Cagliari (Italy), Teaching Assistant.** Machine Learning (MSc in Computer Engineering, Cybersecurity and Artificial Intelligence).

## Teaching (continued)

09/2021 - ongoing **University of Cagliari (Italy), Teaching Assistant.** Machine Learning Security (PhD course, PhD programme in Information Engineering and Science, Univ. of Siena, PhD programme in Electronic and Computer Engineering, Univ. of Cagliari).

10/2022 - ongoing **University of Cagliari (Italy), Teaching Assistant.** Machine Learning Security (MSc in Computer Engineering, Cybersecurity and Artificial Intelligence).

### Tutor

11/2022 - 02/2023 **University of Cagliari (Italy), Academic Tutor.** Subject: Industrial Software Development.

02/2021 - 07/2021 **University of Cagliari (Italy), Academic Tutor.** Subject: Machine Learning.

02/2017 - 06/2018 **University of Cagliari (Italy), Academic Tutor.** Subject: Computer Science (Python).

## Research Publications

### Journal Papers

1. Mirsky, Y., Demontis, A., Kotak, J., Shankar, R., Gelei, D., Yang, L., Zhang, X., **Pintor, M.**, Lee, W., Elovici, Y., & Biggio, B. (2023). The Threat of Offensive AI to Organizations. *Computers & Security* (**Q1** *Scimago*), *124*, 103006. https://doi.org/https://doi.org/10.1016/j.cose.2022.103006

2. Zheng, Y., Feng, X., Xia, Z., Jiang, X., Demontis, A., **Pintor, M.**, Biggio, B., & Roli, F. (2023). Why adversarial reprogramming works, when it fails, and how to tell the difference. *Information Sciences (**Q1** Scimago).*

3. **Pintor, M.**, Angioni, D., Sotgiu, A., Demetrio, L., Demontis, A., Biggio, B., & Roli, F. (2022). ImageNet-Patch: A Dataset for Benchmarking Machine Learning Robustness against Adversarial Patches. *Pattern Recognition (**Q1** Scimago), abs/2203.04412.* https://arxiv.org/abs/2203.04412

4. **Pintor, M.**, Demetrio, L., Sotgiu, A., Melis, M., Demontis, A., & Biggio, B. (2022). secml: Secure and explainable machine learning in Python. *SoftwareX* (**Q2** *Scimago*), *18*, 101095. https://doi.org/https://doi.org/10.1016/j.softx.2022.101095

### Conference Papers

1. Angioni, D., Demetrio, L., **Pintor, M.**, & Biggio, B. (2022). Robust machine learning for malware detection over time. In C. Demetrescu & A. Mei (Eds.), *Proceedings of the italian conference on cybersecurity (ITASEC 2022), rome, italy, june 20-23, 2022* (pp. 169–180). CEUR-WS.org. http://ceur-ws.org/Vol-3260/paper12.pdf

2. **Pintor, M.**, Demetrio, L., Sotgiu, A., Demontis, A., Carlini, N., Biggio, B., & Roli, F. (2022). Indicators of Attack Failure: Debugging and Improving Optimization of Adversarial Examples. *Advances in Neural Information Processing Systems **(Acceptance rate: 25.6 %)**.* https://arxiv.org/abs/2106.09947

3. Piras, G., **Pintor, M.**, Demetrio, L., & Biggio, B. (2022). Explaining machine learning DGA detectors from DNS traffic data. In C. Demetrescu & A. Mei (Eds.), *Proceedings of the italian conference on cybersecurity (ITASEC 2022), rome, italy, june 20-23, 2022* (pp. 150–168). CEUR-WS.org. http://ceur-ws.org/Vol-3260/paper11.pdf

4. Sotgiu, A., **Pintor, M.**, & Biggio, B. (2022). Explainability-based debugging of machine learning for vulnerability discovery. *ARES 2022: The 17th International Conference on Availability, Reliability and Security, Vienna,Austria, August 23 - 26, 2022*, 113:1–113:8. https://doi.org/10.1145/3538969.3543809

5. Buchgeher, G., Czech, G., Ribeiro, A. S., Kloihofer, W., Meloni, P., Busia, P., Deriu, G., **Pintor, M.**, Biggio, B., Chesta, C., Rinelli, L., Solans, D., & Portela, M. (2021). Task-specific automation in deep learning processes. In G. Kotsis, A. M. Tjoa, I. Khalil, B. Moser, A. Mashkoor, J. Sametinger, A. Fensel, J. Martinez-Gil, L. Fischer, G. Czech, F. Sobieczky, & S. Khan (Eds.), *Database and expert systems applications - dexa 2021 workshops* (pp. 159–169). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-87101-7_16

6. Ozbulak, U., Pintor, M., Van Messem, A., & De Neve, W. (2021). Evaluating adversarial attacks on imagenet: A reality check on misclassification classes. *NeurIPS2021, 35th Conference on Neural Information Processing Systems (NeurIPS 2021), Workshop on ImageNet: Past, Present, and Future*, 1–9. https://openreview.net/pdf?id=oWk2dULs1x

7. **Pintor, M.**, Demetrio, L., Manca, G., Biggio, B., & Roli, F. Slope: A first-order approach for measuring gradient obfuscation. In: *Esann 2021 - european symposium on artificial neural networks, computational intelligence and machine learning*. 2021. https://www.esann.org/sites/default/files/proceedings/2021/ES2021-99.pdf

8. **Pintor, M.**, Roli, F., Brendel, W., & Biggio, B. (2021). Fast minimum-norm adversarial attacks through adaptive norm constraints (M. Ranzato, A. Beygelzimer, Y. Dauphin, P. Liang, & J. W. Vaughan, Eds.). *Advances in Neural Information Processing Systems* ***(Acceptance rate: 25.7 %)***, *34*, 20052–20062.
   🔗 `https://proceedings.neurips.cc/paper/2021/hash/a709909b1ea5c2bee24248203b1728a5-Abstract.html`

9. Orrù, G., Ghiani, D., **Pintor, M.**, Marcialis, G. L., & Roli, F. Detecting anomalies from video-sequences: A novel descriptor. In: *25th international conference on pattern recognition (icpr 2020)*. 2020. 🔗 `https://arxiv.org/pdf/2010.06407.pdf`

10. Demontis, A., Melis, M., **Pintor, M.**, Jagielski, M., Biggio, B., Oprea, A., Nita-Rotaru, C., & Roli, F. Why do adversarial attacks transfer? explaining transferability of evasion and poisoning attacks. In: *28th usenix security symposium (usenix security 19)* ***(Acceptance Rate: 18.9%)***. 2019, 321–338.
    🔗 `https://www.usenix.org/system/files/sec19-demontis.pdf`

11. Meloni, P., Loi, D., Busia, P., Deriu, G., Pimentel, A. D., Sapra, D., Stefanov, T., Minakova, S., Conti, F., Benini, L., **Pintor, M.**, Biggio, B., Moser, B., Shepeleva, N., Fragoulis, N., Theodorakopoulos, I., Masin, M., & Palumbo, F. Optimization and deployment of cnns at the edge: The aloha experience. In: *Proceedings of the 16th acm international conference on computing frontiers*. CF '19. Alghero, Italy: Association for Computing Machinery, 2019, 326–332. ISBN: 9781450366854. 🔗 `https://doi.org/10.1145/3310273.3323435`.

12. Girau, R., Ferrara, E., **Pintor, M.**, Sole, M., & Giusto, D. Be right beach: A social iot system for sustainable tourism based on beach overcrowding avoidance. In: *2018 ieee international conference on internet of things (ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata)*. IEEE. 2018, 9–14.
    🔗 `https://www.researchgate.net/profile/Roberto_Girau/publication/332179808_Be_Right_Beach_A_Social_IoT_System_for_Sustainable_Tourism_Based_on_Beach_Overcrowding_Avoidance/links/5ca4bb2ca6fdcc12ee8fcc07/Be-Right-Beach-A-Social-IoT-System-for-Sustainable-Tourism-Based-on-Beach-Overcrowding-Avoidance.pdf`

13. Meloni, P., Loi, D., Deriu, G., Pimentel, A. D., Sapra, D., Moser, B., Shepeleva, N., Conti, F., Benini, L., Ripolles, O., Solans, D., **Pintor, M.**, Biggio, B., Stefanov, T., Minakova, S., Fragoulis, N., Theodorakopoulos, I., Masin, M., & Palumbo, F. Aloha: An architectural-aware framework for deep learning at the edge. In: *Proceedings of the workshop on intelligent embedded systems architectures and applications*. INTESA '18. Turin, Italy: Association for Computing Machinery, 2018, 19–26. ISBN: 9781450365987. 🔗 `https://doi.org/10.1145/3285017.3285019`.

14. Meloni, P., Loi, D., Deriu, G., Pimentel, A. D., Sapra, D., **Pintor, M.**, Biggio, B., Ripolles, O., Solans, D., Conti, F., Benini, L., Stefanov, T., Minakova, S., Moser, B., Shepeleva, N., Masin, M., Palumbo, F., Fragoulis, N., & Theodorakopoulos, I. Architecture-aware design and implementation of cnn algorithms for embedded inference: The aloha project. In: *2018 30th international conference on microelectronics (icm)*. 2018, 52–55. 🔗 `https://doi.org/10.1109/ICM.2018.8704093`.

### Preprints

1. Demontis, A., **Pintor, M.**, Demetrio, L., Grosse, K., Lin, H.-Y., Fang, C., Biggio, B., & Roli, F. (2022). A survey on reinforcement learning security with application to autonomous driving. *arXiv preprint arXiv:2212.06123*.

2. Zheng, Y., Feng, X., Xia, Z., Jiang, X., **Pintor, M.**, Demontis, A., Biggio, B., & Roli, F. (2022). Stateful detection of adversarial reprogramming. *CoRR*, *abs/2211.02885*. 🔗 `https://doi.org/10.48550/arXiv.2211.02885`

### Thesis

1. **Pintor, M.** (2022). Towards debugging and improving adversarial robustness evaluations. *UNICA*.
   🔗 `https://iris.unica.it/bitstream/11584/328882/2/PhD_Thesis_Maura_Pintor.pdf`

## Miscellaneous Experience

### Awards and Achievements

2018 **Top Students Fellowship from University of Cagliari**. Merit Scholarship for enrolled graduate students.

2017 **Best IoT - Week Hackathon Project - Siemens Award, 1st place**, Project: Be Right Beach Design and implementation of a system for real-time analysis of beach crowdedness for sustainable tourism, safety improvement, environment preservation and economic growth.

### Chair

08/2022 **Workshop chair at ARES International Workshop on Continuous Software Evaluation and Certification (IWCSEC 2022).**

## Miscellaneous Experience (continued)

- 06/2022 **Workshop chair at ITASEC AI for Security and Security of AI Workshop (AISSAI 2022).**

### Reviewer

- 03/2023 **PC at AAAI Workshop on Practical Deep Learning in the Wild.**
- **PC at Euro S&P Workshop on Robust Malware Analysis.**
- 02/2023 **PC at CVPR Workshop on Generative Models for Computer Vision**
- **PC at CVPR Workshop of Adversarial Machine Learning on Computer Vision: Art of Robustness**
- 04/2022 **PC at ICML 2022 Workshop Shift happens: Crowdsourcing metrics and test datasets beyond ImageNet.**
- 08/2022 **PC at 15th ACM CCS 2022 Workshop on Artificial Intelligence and Security (AISec).**
- **PC at ECCV 2022 Workshop on Out Of Distribution Generalization in Computer Vision.**
- **PC at ECCV 2022 Workshop on Adversarial Robustness in the Real World.**
- 05/2022 **PC at ICML 2022 Workshop New Frontiers in Adversarial Machine Learning.**
- **PC at ICML 2022 Workshop Shift happens: Crowdsourcing metrics and test datasets beyond ImageNet.**
- 03/2022 **PC at CVPR 2022 Workshop on The Art of Robustness: Devil and Angel in Adversarial Machine Learning.**
- 02/2022 **PC at ICML 2022 Workshop on Socially Responsible Machine Learning.**
- 08/2021 **PC at 14th ACM CCS 2021 Workshop on Artificial Intelligence and Security (AISec).**
- 07/2021 **PC at CCS 2021 ACM Workshop on Artificial Intelligence and Security.**
- **PC at CVPR 2021 Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems and Online Challenges.**
- 06/2021 **PC at ICML 2021 Workshop on Socially Responsible Machine Learning.**
- 03/2021 **PC at ICLR 2021 Workshop on Security and Safety in Machine Learning Systems.**
- 11/2020 **PC at AAAI 2021 Workshop - Towards Robust, Secure and Efficient Machine Learning.**
- 08/2020 **PC at ECCV 2020 Workshop on Adversarial Robustness in the Real World.**
- 06/2020 **PC at CVPR 2020 Workshop on Adversarial Machine Learning in Computer Vision.**

### Summer Schools

- 06/2021 **Regularization Methods for Machine Learning (RegML 2021).**
- 07/2020 **Machine Learning Summer School (MLSS 2020).**
- 07/2019 **International Computer Vision Summer School (ICVSS 2019).**

### Posters and Presentations

- 06/2022 **Poster presentation at ICML 2022 Workshop Shift Happens.**
- 11/2021 **Poster presentation at Cybersec&AI Connected.**
- 08/2021 **Poster Session at ICML 2021 Workshop A Blessing in Disguise: The Prospects and Perils of Adversarial Machine Learning.**
- 07/2021 **Oral talk at ICML 2021 Workshop A Blessing in Disguise: The Prospects and Perils of Adversarial Machine Learning.**
- 06/2021 **Poster Session at Microsoft Security Data Science Colloqium.**
- 10/2019 **Poster Session at Cybersec&AI Prague.**

### Open-Source Projects and Other Projects

- **SecML.**Secure and Explainable Machine Learning in Python.
- **PandaVision.** Security evaluation module with onnx, pytorch, and SecML.
- **ML Sec Seminar Series.** Seminars on Machine Learning Security.