Maura Pintor, Assistant Professor @ Unica

Qualification	PhD in Electronic and Computer Engineering
Day and Place of Birth	October 20th, 1991, Cagliari (CA), Italy
Nationality	Italian
Affiliation	Department of Electrical and Electronic Engineering (DIEE), University of Cagliari, Piazza d'Armi, 09123, Cagliari Italy

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.*

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).

09/2021 - 11/2021 **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).

Thesis Supervisor

2023 Co-supervision of the student Luca Scionis for his MSc Thesis "Neural Network Pruning for Adversarial Robustness: An Overview and Experimental Analysis" for the MSc course in Computer Engineering, Cybersecurity and Artificial Intelligence.

Co-supervision of the student Giuseppe Floris for his MSc Thesis "Hyperparameter Optimization for Fast Minimum-norm Attacks" for the MSc course in Computer Engineering, Cybersecurity and Artificial Intelligence.

2021 Co-supervision of the student Daniele Angioni for his MSc Thesis "Robust Machine Learning for Malware Detection under Concept Drift" for the MSc course in Electronic Engineering

Co-supervision of the student Giovanni Manca for his MSc Thesis "Understanding Failures of Gradient-based Attacks on Machine Learning" for the MSc course in Computer Engineering, Cybersecurity and Artificial Intelligence.

Teaching (continued)

- Co-supervision of the student Giorgio Piras for his MSc Thesis "On Explainability of Machine Learning DGA detectors from DNS traffic data" for the MSc course in Computer Engineering, Cybersecurity and Artificial Intelligence.

Research Projects

- 10/2023 - ongoing Participation, with the University of Cagliari, in the EU project "Security for AI and AI for Security" (Sec4AI4Sec), Grant Agreement no.: 101120393, funded by the European Union in the programme HORIZON-CL3-2022-CS-01.
- 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 - 04/2023 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 - 10/2023 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 - 10/2023 **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.*

Participation to International Groups and Associations and Service

Participation to International Groups and Associations

- 2018-current Member of the Institute of Electrical and Electronics Engineers (IEEE)
- Member of the Association for Computing Machinery (ACM)
- 2018 - current Member of the Pattern Recognition and Applications (PRA) Laboratory of the University of Cagliari (Italy).
- 03/2020 - 06/2020 Internship at the BethgeLab, University of Tübingen and Max Planck Institute for Int. Systems, Germany.
- 05/2021 - 08/2021 Internship (online) at the Software Competence Center Hagenberg (SCCH) Laboratory, Austria.

Workshop and Conference Track Chair

- 2023 Workshop co-chair at 16th ACM Workshop on Art. Int. and Security (AISec 2023), co-loc. with ACM CCS.
- Track co-chair at ESANN 2023 special session Towards Machine Learning Models that We Can Trust.
- Track co-chair at Safe, Secure and Robust AI Track at the SAC24 Conference.
- 2022 Workshop co-chair at ARES Intl. Workshop on Continuous Software Eval. and Certif. (IWCSEC 2022).
- Workshop co-chair at ITASEC AI for Security and Security of AI Workshop (AISSAI 2022).

Reviewer for Journals

- IEEE Transactions on Information Forensics and Security (IEEE T-IFS)
- IEEE Transactions on Image Processing (IEEE TIP)
- IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)
- IEEE Transactions on Neural Networks and Learning Systems (IEEE-TNNLS)
- ACM Transactions on Privacy and Security (TOPS)
- Journal of Intelligent Information Systems (JIIS)
- Eurasip Journal on Information Security

Participation to International Groups and Associations and Service (continued)

- Machine Vision and Applications (MVAP)

Reviewer for Conferences

- 2024 International Conference on Learning Representations (ICLR 2024)
- 2023 Neural Information Processing Systems (NeurIPS 2023) - **Top Reviewer**
- Annual Computer Security Applications Conference (ACSAC 2023)
- International Conference on Computer Vision(ICCV 2023)
- International Conference on Availability, Reliability and Security (ARES 2023)

Reviewer for Workshops

- PC at AAAI 2023 Workshop on Practical Deep Learning in the Wild.
- PC at Euro S&P 2023 Workshop on Robust Malware Analysis.
- PC at CVPR 2023 Workshop on Generative Models for Computer Vision
- PC at CVPR 2023 Workshop of Adversarial Machine Learning on Computer Vision: Art of Robustness
- 2022 PC at ICML 2022 Workshop Shift happens: Crowdsourcing metrics and test datasets beyond ImageNet.
- PC at 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.
- 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.
- PC at CVPR 2022 Workshop on The Art of Robustness: Devil and Angel in Adversarial Machine Learning.
- PC at ICML 2022 Workshop on Socially Responsible Machine Learning.
- 2021 PC at CCS 2021 Workshop on Artificial Intelligence and Security (AISec).
- PC at CVPR 2021 Workshop on Adv. ML in Real-World Computer Vision Systems and Online Challenges.
- PC at ICML 2021 Workshop on Socially Responsible Machine Learning.
- PC at ICLR 2021 Workshop on Security and Safety in Machine Learning Systems.
- 2020 PC at AAAI 2021 Workshop - Towards Robust, Secure and Efficient Machine Learning.
- PC at ECCV 2020 Workshop on Adversarial Robustness in the Real World.
- PC at CVPR 2020 Workshop on Adversarial Machine Learning in Computer Vision.

Research Publications

Journal Papers

1. Eghbal-zadeh, H., Zellinger, W., **Pintor**, **M.**, Grosse, K., Koutini, K., Moser, B. A., Biggio, B., & Widmer, G. (2024). Rethinking data augmentation for adversarial robustness. *Information Sciences*, *654*, 119838.

2. 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`

3. 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).*

4. **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`

5. **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. Floris, G., Mura, R., Scionis, L., Piras, G., **Pintor**, **M.**, Demontis, A., & Biggio, B. (2023). Improving fast minimum-norm attacks with hyperparameter optimization. *31st European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, ESANN 2023, Bruges, Belgium, October 4-6, 2023.*

2. Giorgio, P., Maura, P., Ambra, D., & Battista, B. (2023). Samples on thin ice: Re-evaluating adversarial pruning of neural networks. *2023 International Conference on Machine Learning and Cybernetics (ICMLC).*

3. **Pintor, M.**, Demetrio, L., Sotgiu, A., Lin, H.-Y., Fang, C., Demontis, A., & Biggio, B. (2023). Detecting attacks against deep reinforcement learning for autonomous driving. *2023 International Conference on Machine Learning and Cybernetics (ICMLC).*

4. Zheng, Y., Feng, X., Xia, Z., Jiang, X., **Pintor, M.**, Demontis, A., Biggio, B., & Roli, F. (2023). Stateful detection of adversarial reprogramming. *Information Sciences (**Q1** Scimago), 642*, 119093.

5. 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`

6. **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`

7. 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`

8. 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`

9. 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`

10. 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`

11. **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`

12. **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`

13. 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`

14. 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`

15. 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`.

16. 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`

17 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`.

18 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*.

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`

Last update: 2023/12/13