

# Gorka Abad

## Curriculum Vitae

✉ [abad.gorka@ru.nl](mailto:abad.gorka@ru.nl)  
🌐 [gorkaabad.github.io](https://gorkaabad.github.io)  
in [gorka-abad](https://www.linkedin.com/in/gorka-abad)  
🐦 [@gorkaabad](https://twitter.com/gorkaabad)  
🔗 [GorkaAbad](https://github.com/GorkaAbad)  
🔑 [KasGG7wAAAAJ](https://www.youtube.com/channel/UCasGG7wAAAAAJ)



### Education

- 2021–now **Ph.D. candidate**, *Radboud University*, Nijmegen, The Netherlands,  
In collaboration with Ikerlan research center in Spain.  
research area Adversarial machine learning, mostly backdoor attacks.  
supervisor Dr. Stjepan Picek
- 2019–2020 **Master's degree in cybersecurity**, *Universidad Internacional de La Rioja (UNIR)*,  
Spain, 8.6/10  
thesis *Enhancing IoT security through DLTs* 9/10  
supervisor Fidel Paniagua
- 2015–2019 **Bachelor's degree in Software Engineering**, *Euskal Herriko Unibertsitatea (EHU)*, Spain,  
thesis *Online penetration testing laboratory* 9/10  
supervisor Juan Antonio Pereira

### Experience

- 2020–2020 **Assistant researcher**, *Euskal Herriko Unibertsitatea (EHU)*, Spain  
Working on the Group for Adaptive Teaching-Learning Environment (Ga-Lan Group), which centers on applying Artificial Intelligence techniques for developing learning systems and tools with dynamic adaptation to the user.
- 2020–2020 **Cybersecurity Engineer**, *Arinn Innovation*, Spain  
Internship working on cloud-based WAF management.
- 2018–2019 **Software developer**, *IDE*, Spain  
Internship working on Java software development.

### Teaching

- 2023 Teaching assistant in master's course *Security and Privacy of Machine Learning* at Radboud University, The Netherlands.

### Service to the Academic Community

- 2023–now Reviewer at *IEEE Transactions on Information Forensics & Security (TIFS)*

2023–now    Artifact evaluator at *Network and Distributed System Security (NDSS)*

## Publications

- 2023    Tajalli, H., Abad, G., & Picek, S. (2023). *Poster: Backdoor Attack on Extreme Learning Machines*. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security
- 2023    Xu, J., Abad, G., & Picek, S. (2023). *Rethinking the Trigger-injecting Position in Graph Backdoor Attack*. In International Joint Conference on Neural Networks (IJCNN)
- 2023    Abad, G., Ersoy, O., Picek, S., & Urbieto, A. (2023). *Sneaky Spikes: Uncovering Stealthy Backdoor Attacks in Spiking Neural Networks with Neuromorphic Data*. arXiv preprint arXiv:2302.06279.
- 2023    Abad, G., Xu, J., Koffas, S., Tajalli, B., & Picek, S. (2023). *A Systematic Evaluation of Backdoor Trigger Characteristics in Image Classification*. arXiv preprint arXiv:2302.01740.
- 2023    Abad, G., Paguada, S., Ersoy, O., Picek, S., Ramírez-Durán, V. J., & Urbieto, A. (2023). *Sniper Backdoor: Single Client Targeted Backdoor Attack in Federated Learning*. In First IEEE Conference on Secure and Trustworthy Machine Learning.
- 2022    Abad, G., Ersoy, O., Picek, S., Ramírez-Durán, V. J., & Urbieto, A. (2022). *Poster: Backdoor Attacks on Spiking NNs and Neuromorphic Datasets*. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 3315-3317).
- 2022    Abad, G., Picek, S., & Urbieto, A. (2022). *On the Security & Privacy in Federated Learning*. arXiv preprint arXiv:2112.05423.

## Talks

- 2023    **Sniper Backdoor: Single Client Targeted Backdoor Attack in Federated Learning**  
At SaTML'23 in Raleigh, NC.
- 2023    **Poster: Backdoor Attacks on Spiking NNs and Neuromorphic Datasets.**  
At Ikerlan research center.
- 2022    **Backdoor Attacks on Spiking NNs and Neuromorphic Datasets.**  
At Radboud University.
- 2022    **Poster: Backdoor Attacks on Spiking NNs and Neuromorphic Datasets.**  
At CCS'22.
- 2022    **On the security and privacy in Federated Learning**  
For VeriDevOps European project.
- 2022    **Sniper Backdoor: Single Client Targeted Backdoor Attack in Federated Learning**  
At Radboud University.

2022 **Sniper Backdoor: Single Client Targeted Backdoor Attack in Federated Learning**

At Ikerlan research center.

---

## Courses

2022 Summer School on real-world crypto and privacy, Šibenik, Croatia

2022 Summer School on Security and Privacy, KU Leuven, Leuven, Belgium

---

## Students Supervision

2023 Feb.– **Bachelor's student supervision**, at *UPV/EHU & Ikerlan*, Working on adversarial  
2023 June examples against autonomous driving systems.

2022 June – **Master's student supervision**, at *Mondragón University & Ikerlan*, Working on  
2023 March adversarial examples against face recognition systems.

---

## Languages

Basque Native

Spanish Native

English Advanced