Gorka Abad

Curriculum Vitae

✉ *abad.gorka@ru.nl*
gorkaabad.github.io
in *gorka-abad*
@gorkaabad
GorkaAbad
KasGG7wAAAAJ

Education

2020–Today	**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	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 centres 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.

Publications

2023 **Abad, G.**, Paguada, S., Ersoy, O., Picek, S., Ramírez-Durán, V. J., & Urbieta, A. (2023).**Sniper Backdoor: Single Client Targeted Backdoor Attack in Federated Learning**. To be presented in SaTML'23.

2022 **Abad, G.**, Ersoy, O., Picek, S., Ramírez-Durán, V. J., & Urbieta, A. (2022, November). **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).

Preprints

2022 **Abad, G.**, Picek, S., & Urbieta, A. (2022). On the Security & Privacy in Federated Learning. arXiv preprint arXiv:2112.05423.

Talks

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

2022-Today **Master's student supervision** at Mondragón University & Ikerlan.
Working on adversarial examples for face recognition systems.

Languages

Basque	Native
Spanish	Native
English	Advanced