Luis Muoz-Gonzlez

List of Publications by Citations

14 papers	198 citations	7 h-index	14 g-index
15 ext. papers	311 ext. citations	1.9 avg, IF	3.41 L-index

#	Paper	IF	Citations
14	Towards Poisoning of Deep Learning Algorithms with Back-gradient Optimization **2017**,		98
13	Procedural Noise Adversarial Examples for Black-Box Attacks on Deep Convolutional Networks **2019**,		20
12	Exact Inference Techniques for the Analysis of Bayesian Attack Graphs. *IEEE Transactions on Dependable and Secure Computing*, **2019**, 16, 231-244	3.9	18
11	Label Sanitization Against Label Flipping Poisoning Attacks. *Lecture Notes in Computer Science*, **2019**, 5-15	0.9	16
10	Efficient Attack Graph Analysis through Approximate Inference. *ACM Transactions on Privacy and Security*, **2017**, 20, 1-30	2.9	11
9	Dondt fool Me!: Detection, Characterisation and Diagnosis of Spoofed and Masked Events in Wireless Sensor Networks. *IEEE Transactions on Dependable and Secure Computing*, **2017**, 14, 279-293	3.9	11
8	Determining Resilience Gains From Anomaly Detection for Event Integrity in Wireless Sensor Networks. *ACM Transactions on Sensor Networks*, **2018**, 14, 1-35	2.9	7
7	Non-IID data re-balancing at IoT edge with peer-to-peer federated learning for anomaly detection **2021**,		4
6	The Security of Machine Learning Systems. *Intelligent Systems Reference Library*, **2019**, 47-79	0.8	4
5	Efficient Attack Countermeasure Selection Accounting for Recovery and Action Costs **2019**,		3
4	The Secret of Machine Learning. *Itnow*, **2018**, 60, 38-39	0.4	3
3	Shadow-Catcher: Looking into Shadows to Detect Ghost Objects in Autonomous Vehicle 3D Sensing. *Lecture Notes in Computer Science*, **2021**, 691-711	0.9	2
2	Redundancy Planning for Cost Efficient Resilience to Cyber Attacks. *IEEE Transactions on Dependable and Secure Computing*, **2022**, 1-1	3.9	
1	Security and Robustness in Federated Learning **2022**, 363-390		