

Prashanth Krishnamurthy

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/1564103/publications.pdf>

Version: 2024-02-01

33
papers

548
citations

1040056

9
h-index

794594

19
g-index

33
all docs

33
docs citations

33
times ranked

313
citing authors

#	ARTICLE	IF	CITATIONS
1	Towards a New Thermal Monitoring Based Framework for Embedded CPS Device Security. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 524-536.	5.4	15
2	Overriding Autonomous Driving Systems Using Adaptive Adversarial Billboards. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 11386-11396.	8.0	5
3	A Feature-Based On-Line Detector to Remove Adversarial-Backdoors by Iterative Demarcation. IEEE Access, 2022, 10, 5545-5558.	4.2	6
4	Trojan Detection in Embedded Systems With FinFET Technology. IEEE Transactions on Computers, 2022, 71, 3061-3071.	3.4	4
5	HPC-Based Malware Detectors Actually Work: Transition to Practice After a Decade of Research. IEEE Design and Test, 2022, 39, 23-32.	1.2	1
6	Detecting Hardware Trojans in PCBs Using Side Channel Loopbacks. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2022, 30, 926-937.	3.1	9
7	Adaptive output feedback stabilization in prescribed time for nonlinear systems with unknown parameters coupled with unmeasured states. International Journal of Adaptive Control and Signal Processing, 2021, 35, 184-202.	4.1	38
8	Special Session: Machine Learning for Semiconductor Test and Reliability. , 2021, , .		6
9	State Constrained Stochastic Optimal Control Using LSTMs. , 2021, , .		6
10	Machine Learning for NetFlow Anomaly Detection With Human-Readable Annotations. IEEE Transactions on Network and Service Management, 2021, 18, 1885-1898.	4.9	9
11	Overriding Learning-based Perception Systems for Control of Autonomous Unmanned Aerial Vehicles. , 2021, , .		2
12	Resilient redundancy-based control of cyber-physical systems through adaptive randomized switching. Systems and Control Letters, 2021, 158, 105066.	2.3	4
13	Anomaly Detection in Real-Time Multi-Threaded Processes Using Hardware Performance Counters. IEEE Transactions on Information Forensics and Security, 2020, 15, 666-680.	6.9	44
14	A Theoretical Study of Hardware Performance Counters-Based Malware Detection. IEEE Transactions on Information Forensics and Security, 2020, 15, 512-525.	6.9	40
15	Learning-Based Real-Time Process-Aware Anomaly Monitoring for Assured Autonomy. IEEE Transactions on Intelligent Vehicles, 2020, 5, 659-669.	12.7	7
16	Exposing Hardware Trojans in Embedded Platforms via Short-Term Aging. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 3519-3530.	2.7	9
17	Anomaly Detection in Embedded Systems Using Power and Memory Side Channels. , 2020, , .		4
18	Functional Replicas of Proprietary Three-Axis Attitude Sensors via LSTM Neural Networks. , 2020, , .		4

#	ARTICLE	IF	CITATIONS
19	Hardware Trojan Detection Using Controlled Circuit Aging. IEEE Access, 2020, 8, 77415-77434.	4.2	19
20	Sliding-Window Temporal Attention Based Deep Learning System for Robust Sensor Modality Fusion for UGV Navigation. IEEE Robotics and Automation Letters, 2019, 4, 4216-4223.	5.1	9
21	A deep learning gated architecture for UGV navigation robust to sensor failures. Robotics and Autonomous Systems, 2019, 116, 80-97.	5.1	21
22	Adaptive Adversarial Videos on Roadside Billboards: Dynamically Modifying Trajectories of Autonomous Vehicles. , 2019, , .		15
23	Tightly Coupled Semantic RGB-D Inertial Odometry for Accurate Long-Term Localization and Mapping. , 2019, , .		4
24	Stealthy Rootkits in Smart Grid Controllers. , 2019, , .		7
25	Adversarial Learning-Based On-Line Anomaly Monitoring for Assured Autonomy. , 2018, , .		18
26	Process-Aware Covert Channels Using Physical Instrumentation in Cyber-Physical Systems. IEEE Transactions on Information Forensics and Security, 2018, 13, 2761-2771.	6.9	27
27	Reducing Operator Workload for Indoor Navigation of Autonomous Robots via Multimodal Sensor Fusion. , 2017, , .		4
28	Process-aware side channel monitoring for embedded control system security. , 2017, , .		6
29	Emerging (un-)reliability based security threats and mitigations for embedded systems. , 2017, , .		17
30	Sensor modality fusion with CNNs for UGV autonomous driving in indoor environments. , 2017, , .		35
31	Machine learning-based defense against process-aware attacks on Industrial Control Systems. , 2016, , .		48
32	Cybersecurity for Control Systems: A Process-Aware Perspective. IEEE Design and Test, 2016, 33, 75-83.	1.2	72
33	A Singular Perturbation Based Global Dynamic High Gain Scaling Control Design for Systems With Nonlinear Input Uncertainties. IEEE Transactions on Automatic Control, 2013, 58, 2686-2692.	5.7	33