Patrick McDaniel

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/8182367/publications.pdf

Version: 2024-02-01

45 papers	5,873 citations	840776 11 h-index	713466 21 g-index
46 all docs	46 docs citations	46 times ranked	4075 citing authors

#	Article	IF	Citations
1	The Limitations of Deep Learning in Adversarial Settings. , 2016, , .		1,868
2	Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks. , 2016, , .		1,398
3	Security and Privacy Challenges in the Smart Grid. IEEE Security and Privacy, 2009, 7, 75-77.	1.2	902
4	IccTA: Detecting Inter-Component Privacy Leaks in Android Apps. , 2015, , .		258
5	A Survey of BGP Security Issues and Solutions. Proceedings of the IEEE, 2010, 98, 100-122.	21.3	231
6	Semantically Rich Application-Centric Security in Android. , 2009, , .		220
7	IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT. , 2019, , .		125
8	A survey on IoT platforms: Communication, security, and privacy perspectives. Computer Networks, 2021, 192, 108040.	5.1	116
9	IotSan. , 2018, , .		87
10	The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. International Journal of Distributed Sensor Networks, 2006, 2, 267-287.	2.2	85
11	Methods and limitations of security policy reconciliation. ACM Transactions on Information and System Security, 2006, 9, 259-291.	4.5	82
12	Program Analysis of Commodity IoT Applications for Security and Privacy. ACM Computing Surveys, 2020, 52, 1-30.	23.0	76
13	Domain-Z: 28 Registrations Later Measuring the Exploitation of Residual Trust in Domains. , 2016, , .		37
14	Exploiting open functionality in SMS-capable cellular networks. Journal of Computer Security, 2008, 16, 713-742.	0.8	31
15	From Languages to Systems: Understanding Practical Application Development in Security-typed Languages. , 2006, , .		29
16	Kratos. , 2020, , .		29
17	Defending Against Attacks on Main Memory Persistence. , 2008, , .		24
18	Malware traffic detection using tamper resistant features. , 2015, , .		23

#	Article	IF	Citations
19	Privacy Preserving Communication in MANETs. , 2007, , .		22
20	Scalable Web Content Attestation. , 2009, , .		21
21	Verifying Internet of Things Safety and Security in Physical Spaces. IEEE Security and Privacy, 2019, 17, 30-37.	1.2	21
22	Composite Constant Propagation and its Application to Android Program Analysis. IEEE Transactions on Software Engineering, 2016, 42, 999-1014.	5.6	20
23	Real-time Analysis of Privacy-(un)aware IoT Applications. Proceedings on Privacy Enhancing Technologies, 2021, 2021, 145-166.	2.8	18
24	Adversarial Network Forensics in Software Defined Networking. , 2017, , .		17
25	Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks. , 2020, , .		16
26	Justifying Integrity Using a Virtual Machine Verifier. , 2009, , .		15
27	Data Provenance and Security. IEEE Security and Privacy, 2011, 9, 83-85.	1.2	15
28	Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems. , 2007, , .		13
29	Scalable Web Content Attestation. IEEE Transactions on Computers, 2012, 61, 686-699.	3.4	10
30	PinUP: Pinning User Files to Known Applications. , 2008, , .		9
31	<i>MLSNet:</i> A Policy Complying Multilevel Security Framework for Software Defined Networking. IEEE Transactions on Network and Service Management, 2021, 18, 729-744.	4.9	9
32	Guest Editors' Introduction: Special Section on Software Engineering for Secure Systems. IEEE Transactions on Software Engineering, 2008, 34, 3-4.	5.6	6
33	Improving Radioactive Material Localization by Leveraging Cyber-Security Model Optimizations. IEEE Sensors Journal, 2021, 21, 9994-10006.	4.7	6
34	Adversarial examples for network intrusion detection systems. Journal of Computer Security, 2022, 30, 727-752.	0.8	6
35	Whoâ€™s Controlling My Device? Multi-User Multi-Device-Aware Access Control System for Shared Smart Home Environment. ACM Transactions on Internet of Things, 2022, 3, 1-39.	4.6	6
36	IoTRepair: Systematically Addressing Device Faults in Commodity IoT. , 2020, , .		5

#	Article	IF	Citations
37	IoTRepair: Flexible Fault Handling in Diverse IoT Deployments. ACM Transactions on Internet of Things, 2022, 3, 1-33.	4.6	5
38	Enforcing Multilevel Security Policies in Unstable Networks. IEEE Transactions on Network and Service Management, 2022, 19, 2349-2365.	4.9	4
39	Structured security testing in the smart grid. , 2012, , .		2
40	Attack Resilience of Cache Replacement Policies: A Study Based on TTL Approximation. IEEE/ACM Transactions on Networking, 2022, 30, 2433-2447.	3.8	2
41	Experimental tests of Gamma-ray Localization Aided with Machine-learning (GLAM) capabilities. Nuclear Instruments and Methods in Physics Research, Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 2022, 1038, 166905.	1.6	2
42	Enforcing agile access control policies in relational databases using views. , 2015, , .		1
43	Non-Invasive Methods for Host Certification. , 2006, , .		0
44	Adversarial Network Forensics in Software Defined Networking. , 2017, , .		0
45	Exposing Android social applications: linking data leakage to privacy policies. Journal of Cyber Security Technology, 2021, 5, 139-190.	2.9	0