Nuno Ferreira Neves

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/7377677/publications.pdf

Version: 2024-02-01

87	1,801	489802 18	445137 33
papers	citations	h-index	g-index

87	87	87	974
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Statically Detecting Vulnerabilities by Processing Programming Languages as Natural Languages. IEEE Transactions on Reliability, 2022, 71, 1033-1056.	3.5	3
2	Charon: A Secure Cloud-of-Clouds System for Storing and Sharing Big Data. IEEE Transactions on Cloud Computing, 2021, 9, 1349-1361.	3.1	20
3	Elastic Network Virtualization. , 2020, , .		3
4	Towards a Deep Learning Model for Vulnerability Detection on Web Application Variants. , 2020, , .		9
5	Secure multi-cloud virtual network embedding. Computer Communications, 2020, 155, 252-265.	3.1	9
6	Effect of Coding Styles in Detection of Web Application Vulnerabilities. , 2020, , .		3
7	Secure Multi-Cloud Network Virtualization. Computer Networks, 2019, 161, 45-60.	3.2	13
8	SEPTIC: Detecting Injection Attacks and Vulnerabilities Inside the DBMS. IEEE Transactions on Reliability, 2019, 68, 1168-1188.	3.5	16
9	Using Blockchains to Implement Distributed Measuring Systems. IEEE Transactions on Instrumentation and Measurement, 2019, 68, 1503-1514.	2.4	24
10	An empirical study on combining diverse static analysis tools for web security vulnerabilities based on development scenarios. Computing (Vienna/New York), 2019, 101, 161-185.	3.2	16
11	Lazarus. , 2019, , .		11
12	Benchmarking Static Analysis Tools for Web Security. IEEE Transactions on Reliability, 2018, 67, 1159-1175.	3.5	40
13	How blockchains can improve measuring instruments regulation and control. , 2018, , .		12
14	Validating and Securing DLMS/COSEM Implementations with the ValiDLMS Framework. , 2018, , .		6
15	Secure and Dependable Multi-Cloud Network Virtualization. , 2017, , .		0
16	Secure network monitoring using programmable data planes. , 2017, , .		5
17	Demonstrating a Tool for Injection Attack Prevention in MySQL. , 2017, , .		2
18	On Combining Diverse Static Analysis Tools for Web Security: An Empirical Study. , 2017, , .		13

#	Article	IF	Citations
19	Secure Tera-scale Data Crunching with a Small TCB. , 2017, , .		1
20	Secure Identification of Actively Executed Code on a Generic Trusted Component. , 2016, , .		1
21	JITeR: Just-in-time application-layer routing. Computer Networks, 2016, 104, 122-136.	3.2	5
22	Hacking the DBMS to Prevent Injection Attacks. , 2016, , .		4
23	Equipping WAP with WEAPONS to Detect Vulnerabilities: Practical Experience Report. , 2016, , .		6
24	(Literally) Above the clouds: Virtualizing the network over multiple clouds. , 2016, , .		4
25	DEKANT: a static analysis tool that learns to detect web application vulnerabilities. , 2016, , .		46
26	User-Centric Security and Dependability in the Clouds-of-Clouds. IEEE Cloud Computing, 2016, 3, 64-75.	5.3	13
27	Detecting and Removing Web Application Vulnerabilities with Static Analysis and Data Mining. IEEE Transactions on Reliability, 2016, 65, 54-69.	3.5	94
28	Securing Passive Replication through Verification. , 2015, , .		4
29	Stopping a Rapid Tornado with a Puff. , 2014, , .		3
30	Automatic detection and correction of web application vulnerabilities using data mining to predict false positives. , 2014, , .		57
31	Analysis of operating system diversity for intrusion tolerance. Software - Practice and Experience, 2014, 44, 735-770.	2.5	53
32	An intrusion-tolerant firewall design for protecting SIEM systems. , 2013, , .		3
33	Securing energy metering software with automatic source code correction. , 2013, , .		3
34	Byzantine Fault-Tolerant Consensus in Wireless Ad Hoc Networks. IEEE Transactions on Mobile Computing, 2013, 12, 2441-2454.	3.9	29
35	PACE your network: Fair and controllable multi-tenant data center networks. , 2013, , .		0
36	BFT-TO: Intrusion Tolerance with Less Replicas. Computer Journal, 2013, 56, 693-715.	1.5	11

#	Article	IF	Citations
37	Intercept: Profiling Windows Network Device Drivers. Lecture Notes in Computer Science, 2013, , 61-75.	1.0	0
38	Recycling Test Cases to Detect Security Vulnerabilities. , 2012, , .		5
39	Robust and Speculative Byzantine Randomized Consensus with Constant Time Complexity in Normal Conditions. , 2012, , .		1
40	Using Behavioral Profiles to Detect Software Flaws in Network Servers. , 2011, , .		3
41	DiveInto: Supporting Diversity in Intrusion-Tolerant Systems. , 2011, , .		2
42	Reverse Engineering of Protocols from Network Traces. , 2011, , .		50
43	OS diversity for intrusion tolerance: Myth or reality?. , 2011, , .		59
44	RITAS: Services for Randomized Intrusion Tolerance. IEEE Transactions on Dependable and Secure Computing, 2011, 8, 122-136.	3.7	25
45	Byzantine consensus in asynchronous message-passing systems: a survey. International Journal of Critical Computer-Based Systems, 2011, 2, 141.	0.1	37
46	Randomization can be a healer: consensus with dynamic omission failures. Distributed Computing, 2011, 24, 165-175.	0.7	2
47	Automatically complementing protocol specifications from network traces. , 2011, , .		6
48	Turquois: Byzantine consensus in wireless ad hoc networks. , 2010, , .		12
49	Vulnerability Discovery with Attack Injection. IEEE Transactions on Software Engineering, 2010, 36, 357-370.	4.3	37
50	Highly Available Intrusion-Tolerant Services with Proactive-Reactive Recovery. IEEE Transactions on Parallel and Distributed Systems, 2010, 21, 452-465.	4.0	97
51	Randomized Consensus in Wireless Environments: A Case Where More is Better. , 2010, , .		4
52	A Distributed Systems Approach to Airborne Self-Separation. , 2010, , 215-236.		0
53	Designing Modular and Redundant Cyber Architectures for Process Control: Lessons learned. , 2009, , .		4
54	Intrusion-tolerant self-healing devices for critical infrastructure protection. , 2009, , .		9

#	Article	IF	Citations
55	Randomization Can Be a Healer: Consensus with Dynamic Omission Failures. Lecture Notes in Computer Science, 2009, , 63-77.	1.0	5
56	The Crutial Way of Critical Infrastructure Protection. IEEE Security and Privacy, 2008, 6, 44-51.	1.5	59
57	Detection and Prediction of Resource-Exhaustion Vulnerabilities. , 2008, , .		19
58	Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities. , 2008, , .		9
59	The CRUTIAL reference critical information infrastructure architecture: a blueprint. International Journal of System of Systems Engineering, 2008, 1, 78.	0.4	17
60	The CRUTIAL Architecture for Critical Information Infrastructures. Lecture Notes in Computer Science, 2008, , 1-27.	1.0	15
61	Robustness Testing of the Windows DDK. , 2007, , .		23
62	Resilient Intrusion Tolerance through Proactive and Reactive Recovery. , 2007, , .		39
63	Quantifying Software Maintainability Based on a Fault-Detection/Correction Model. , 2007, , .		17
64	A Low-Power and SEU-Tolerant Switch Architecture for Network on Chips. , 2007, , .		31
65	Intrusion Tolerance in Wireless Environments: An Experimental Evaluation. , 2007, , .		3
66	Worm-IT â€“ A wormhole-based intrusion-tolerant group communication system. Journal of Systems and Software, 2007, 80, 178-197.	3.3	21
67	Experimental Comparison of Local and Shared Coin Randomized Consensus Protocols. Proceedings of the IEEE Symposium on Reliable Distributed Systems, 2006, , .	0.0	17
68	Intrusion-tolerant middleware: the road to automatic security. IEEE Security and Privacy, 2006, 4, 54-62.	1.5	56
69	Proactive Resilience Revisited: The Delicate Balance Between Resisting Intrusions and Remaining Available. , 2006, , .		8
70	Proactive resilience through architectural hybridization. , 2006, , .		22
71	From Consensus to Atomic Broadcast: Time-Free Byzantine-Resistant Protocols without Signatures. Computer Journal, 2006, 49, 82-96.	1.5	85
72	CRUTIAL: The Blueprint of a Reference Critical Information Infrastructure Architecture. Lecture Notes in Computer Science, 2006, , 1-14.	1.0	11

#	Article	IF	Citations
73	Low complexity Byzantine-resilient consensus. Distributed Computing, 2005, 17, 237-249.	0.7	32
74	Solving vector consensus with a wormhole. IEEE Transactions on Parallel and Distributed Systems, 2005, 16, 1120-1131.	4.0	27
75	Intrusion-Tolerant Architectures: Concepts and Design. Lecture Notes in Computer Science, 2003, , 3-36.	1.0	92
76	The Design of a COTS Real-Time Distributed Security Kernel. Lecture Notes in Computer Science, 2002, , 234-252.	1.0	29
77	Adaptive recovery for mobile environments. Communications of the ACM, 1997, 40, 68-74.	3.3	81
78	Lightweight logging for lazy release consistent distributed shared memory. , 1996, , .		35
79	A checkpoint protocol for an entry consistent shared memory system. , 1994, , .		41
80	Orthogonal Persistence in a Heterogeneous Distributed Object-Oriented Environment. Computer Journal, 1994, 37, 531-541.	1.5	1
81	Fault detection using hints from the socket layer. , 0, , .		6
82	The architecture of a secure group communication system based on intrusion tolerance. , 0, , .		1
83	Efficient Byzantine-resilient reliable multicast on a hybrid failure model. , 0, , .		20
84	How Resilient are Distributed f Fault/Intrusion-Tolerant Systems?. , 0, , .		26
85	Resilient State Machine Replication. , 0, , .		3
86	Randomized Intrusion-Tolerant Asynchronous Services. , 0, , .		19
87	Using Attack Injection to Discover New Vulnerabilities. , 0, , .		36