Mourad Debbabi

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/8624527/publications.pdf

Version: 2024-02-01

111 papers	2,554 citations	201674 27 h-index	223800 46 g-index
111 all docs	111 docs citations	111 times ranked	1962 citing authors

#	Article	IF	Citations
1	Inferring and Investigating IoT-Generated Scanning Campaigns Targeting a Large Network Telescope. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 402-418.	5.4	20
2	ProSAS: Proactive Security Auditing System for Clouds. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2517-2534.	5.4	5
3	Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management. IEEE Transactions on Industrial Informatics, 2022, 18, 1641-1653.	11.3	9
4	Chameleon: Optimized feature selection using particle swarm optimization and ensemble methods for network anomaly detection. Computers and Security, 2022, 117, 102684.	6.0	20
5	Security enhancement of time synchronization and fault identification in WAMS using a two-layer blockchain framework. Applied Energy, 2022, 315, 118955.	10.1	3
6	Threat Intelligence Generation Using Network Telescope Data for Industrial Control Systems. IEEE Transactions on Information Forensics and Security, 2021, 16, 3355-3370.	6.9	8
7	A Strings-Based Similarity Analysis Approach for Characterizing IoT Malware and Inferring Their Underlying Relationships. IEEE Networking Letters, 2021, 3, 161-165.	1.9	16
8	Multi-depot vehicle routing problem with risk mitigation: Model and solution algorithm. Expert Systems With Applications, 2020, 145, 113099.	7.6	18
9	Stochastic Modeling, Analysis and Investigation of IoT-Generated Internet Scanning Activities. IEEE Networking Letters, 2020, 2, 159-163.	1.9	8
10	A Scalable Platform for Enabling the Forensic Investigation of Exploited IoT Devices and Their Generated Unsolicited Activities. Forensic Science International: Digital Investigation, 2020, 32, 300922.	1.7	2
11	Scalable and robust unsupervised Android malware fingerprinting using community-based network partitioning. Computers and Security, 2020, 96, 101932.	6.0	5
12	CPA: Accurate Cross-Platform Binary Authorship Characterization Using LDA. IEEE Transactions on Information Forensics and Security, 2020, 15, 3051-3066.	6.9	8
13	Detection and Mitigation of Cyber Attacks on Voltage Stability Monitoring of Smart Grids. IEEE Transactions on Smart Grid, 2020, 11, 5227-5238.	9.0	28
14	NFVGuard: Verifying the Security of Multilevel Network Functions Virtualization (NFV) Stack. , 2020, , .		3
15	Evolutionary learning algorithm for reliable facility location under disruption. Expert Systems With Applications, 2019, 115, 223-244.	7.6	31
16	Wordnet-Based Criminal Networks Mining for Cybercrime Investigation. IEEE Access, 2019, 7, 22740-22755.	4.2	31
17	Learning probabilistic dependencies among events for proactive security auditing in clouds. Journal of Computer Security, 2019, 27, 165-202.	0.8	8
18	On the feasibility of binary authorship characterization. Digital Investigation, 2019, 28, S3-S11.	3.2	17

#	Article	IF	Citations
19	MalDy: Portable, data-driven malware detection using natural language processing and machine learning techniques on behavioralÂanalysis reports. Digital Investigation, 2019, 28, S77-S87.	3.2	47
20	Automated Post-Failure Service Restoration in Smart Grid Through Network Reconfiguration in the Presence of Energy Storage Systems. IEEE Systems Journal, 2019, 13, 3358-3367.	4.6	23
21	Multi-Level Proactive Security Auditing for Clouds. , 2019, , .		1
22	Decoupling coding habits from functionality for effective binary authorship attribution. Journal of Computer Security, 2019, 27, 613-648.	0.8	6
23	Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management1. , 2019, , .		5
24	User-Level Runtime Security Auditing for the Cloud. IEEE Transactions on Information Forensics and Security, 2018, 13, 1185-1199.	6.9	24
25	Data-driven approach for automatic telephony threat analysis and campaign detection. Digital Investigation, 2018, 24, S131-S141.	3.2	5
26	MalDozer: Automatic framework for android malware detection using deep learning. Digital Investigation, 2018, 24, S48-S59.	3.2	273
27	CSC-Detector: A System to Infer Large-Scale Probing Campaigns. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 364-377.	5.4	7
28	OpenStack-Based Evaluation Framework for Smart Grid Cyber Security. , 2018, , .		18
29	Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys and Tutorials, 2018, 20, 3389-3415.	39.4	31
30	Inferring, Characterizing, and Investigating Internet-Scale Malicious IoT Device Activities: A Network Telescope Perspective. , 2018, , .		17
31	PERMON: An OpenStack Middleware for Runtime Security Policy Enforcement in Clouds. , 2018, , .		10
32	Efficient sensor network management for asset localization. Computers and Operations Research, 2018, 99, 148-165.	4.0	8
33	BinGold: Towards robust binary analysis by extracting the semantics of binary code as semantic flow graphs (SFGs). Digital Investigation, 2016, 18, S11-S22.	3.2	32
34	Fingerprinting Android packaging: Generating DNAs for malware detection. Digital Investigation, 2016, 18, S33-S45.	3.2	28
35	Security Assessment of Time Synchronization Mechanisms for the Smart Grid. IEEE Communications Surveys and Tutorials, 2016, 18, 1952-1973.	39.4	32
36	Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. IEEE Communications Surveys and Tutorials, 2016, 18, 1197-1227.	39.4	84

#	Article	IF	Citations
37	Hierarchy aware distributed plan execution monitoring. Expert Systems With Applications, 2016, 43, 66-81.	7.6	3
38	Network malware classification comparison using DPI and flow packet headers. Journal of Computer Virology and Hacking Techniques, 2016, 12, 69-100.	2.2	44
39	On the inference and prediction of DDoS campaigns. Wireless Communications and Mobile Computing, 2015, 15, 1066-1078.	1.2	17
40	SIGMA: A Semantic Integrated Graph Matching Approach for identifying reused functions in binary code. Digital Investigation, 2015, 12, S61-S71.	3.2	53
41	BinComp: A stratified approach to compiler provenance Attribution. Digital Investigation, 2015, 14, S146-S155.	3.2	37
42	Security Compliance Auditing of Identity and Access Management in the Cloud: Application to OpenStack. , 2015, , .		27
43	Transportation risk analysis using probabilistic model checking. Expert Systems With Applications, 2015, 42, 4410-4421.	7.6	23
44	Specification, verification, and quantification of security in model-based systems. Computing (Vienna/New York), 2015, 97, 691-711.	4.8	22
45	Spam campaign detection, analysis, and investigation. Digital Investigation, 2015, 12, S12-S21.	3.2	24
46	Towards migrating security policies of virtual machines in Software Defined Networks. , 2015, , .		1
47	Inferring distributed reflection denial of service attacks from darknet. Computer Communications, 2015, 62, 59-71.	5.1	36
48	Scalable code clone search for malware analysis. Digital Investigation, 2015, 15, 46-60.	3.2	19
49	Graph-theoretic characterization of cyber-threat infrastructures. Digital Investigation, 2015, 14, S3-S15.	3.2	19
50	A Visualizable Evidence-Driven Approach for Authorship Attribution. ACM Transactions on Information and System Security, 2015, 17, 1-30.	4.5	29
51	A formal verification framework for SysML activity diagrams. Expert Systems With Applications, 2014, 41, 2713-2728.	7.6	32
52	A Survey and a Layered Taxonomy of Software-Defined Networking. IEEE Communications Surveys and Tutorials, 2014, 16, 1955-1980.	39.4	289
53	PPTP: Privacy-Preserving Traffic Padding in Web-Based Applications. IEEE Transactions on Dependable and Secure Computing, 2014, 11, 538-552.	5.4	13
54	BinClone: Detecting Code Clones in Malware. , 2014, , .		42

#	Article	IF	Citations
55	The multi-depot split-delivery vehicle routing problem: Model and solution algorithm. Knowledge-Based Systems, 2014, 71, 238-265.	7.1	44
56	Multidimensional investigation of source port 0 probing. Digital Investigation, 2014, 11, S114-S123.	3.2	23
57	Quantitative and qualitative analysis of SysML activity diagrams. International Journal on Software Tools for Technology Transfer, 2014, 16, 399-419.	1.9	4
58	On fingerprinting probing activities. Computers and Security, 2014, 43, 35-48.	6.0	31
59	A property-based abstraction framework for SysML activity diagrams. Knowledge-Based Systems, 2014, 56, 328-343.	7.1	9
60	OBA2: An Onion approach to Binary code Authorship Attribution. Digital Investigation, 2014, 11, S94-S103.	3.2	57
61	A secure, efficient, and costâ€effective distributed architecture for spam mitigation on LTE 4G mobile networks. Security and Communication Networks, 2013, 6, 1478-1489.	1.5	4
62	Common weaving approach in mainstream languages for software security hardening. Journal of Systems and Software, 2013, 86, 2654-2674.	4.5	0
63	Towards Fingerprinting Malicious Traffic. Procedia Computer Science, 2013, 19, 548-555.	2.0	13
64	Towards a Distributed Plan Execution Monitoring Framework. Procedia Computer Science, 2013, 19, 1034-1039.	2.0	1
65	Gossiping Based Distributed Plan Monitoring. Procedia Computer Science, 2013, 19, 72-79.	2.0	0
66	Background Knowledge-Resistant Traffic Padding for Preserving User Privacy in Web-Based Applications. , 2013, , .		3
67	Investigating the dark cyberspace: Profiling, threat-based analysis and correlation. , 2012, , .		20
68	On SPIM detection in LTE networks. , 2012, , .		5
69	On the need for data flow graph visualization of Forensic Lucid programs and encoded evidence, and their evaluation by GIPSY. , 2011, , .		2
70	Anonymity meets game theory: secure data integration with malicious participants. VLDB Journal, 2011, 20, 567-588.	4.1	43
71	A game-theoretic framework for specification and verification of cryptographic protocols. Formal Aspects of Computing, 2010, 22, 585-609.	1.8	1
72	Mining writeprints from anonymous e-mails for forensic investigation. Digital Investigation, 2010, 7, 56-64.	3.2	109

#	Article	IF	Citations
73	PCM: a privacyâ€preserving detection mechanism in mobile ad hoc networks. Security and Communication Networks, 2010, 3, 167-184.	1.5	1
74	A Practical Framework for the Dataflow Pointcut in AspectJ. , 2009, , .		0
75	Synergistic verification and validation of systems and software engineering models. International Journal of General Systems, 2009, 38, 719-746.	2.5	0
76	Interprocedural and Flow-Sensitive Type Analysis for Memory and Type Safety of C Code. Journal of Automated Reasoning, 2009, 42, 265-300.	1.4	2
77	New aspect-oriented constructs for security hardening concerns. Computers and Security, 2009, 28, 341-358.	6.0	3
78	Towards an integrated e-mail forensic analysis framework. Digital Investigation, 2009, 5, 124-137.	3.2	64
79	On the Meaning of SysML Activity Diagrams. , 2009, , .		15
80	QoS-aware middleware for web services composition: a qualitative approach. Enterprise Information Systems, 2009, 3, 449-470.	4.7	17
81	A game-theoretic intrusion detection model for mobile ad hoc networks. Computer Communications, 2008, 31, 708-721.	5.1	61
82	Game theoretic models for detecting network intrusions. Computer Communications, 2008, 31, 1934-1944.	5.1	27
83	A novel approach of mining write-prints for authorship attribution in e-mail forensics. Digital Investigation, 2008, 5, S42-S51.	3.2	95
84	An aspect-oriented approach for the systematic security hardening of code. Computers and Security, 2008, 27, 101-114.	6.0	19
85	Execution monitoring enforcement under memory-limitation constraints. Information and Computation, 2008, 206, 158-184.	0.7	39
86	Cross-Language Weaving Approach Targeting Software Security Hardening. , 2008, , .		1
87	Type and Effect Annotations for Safe Memory Access in C. , 2008, , .		2
88	A Moderate to Robust Game Theoretical Model for Intrusion Detection in MANETs. , 2008, , .		13
89	A High-level Aspect-oriented-based Framework for Software Security Hardening. Information Security Journal, 2008, 17, 56-74.	1.9	15
90	A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in MANET. , 2008, , .		21

#	Article	IF	Citations
91	A novel flow-sensitive type and effect analysis for securing C code. , 2008, , .		1
92	Automated Windows Memory File Extraction for Cyber Forensics Investigation. Journal of Digital Forensic Practice, 2008, 2, 117-131.	0.2	2
93	A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks. , 2007, , .		28
94	Towards an Aspect Oriented Approach for the Security Hardening of Code. , 2007, , .		12
95	An Efficient and Truthful Leader IDS Election Mechanism for MANET. , 2007, , .		4
96	Team Edit Automata for Testing Security Property. , 2007, , .		2
97	Modeling Security Protocols as Games. , 2007, , .		0
98	Modeling Security Protocols as Games. , 2007, , .		1
99	Verifying Security Properties of Cryptoprotocols: A Novel Approach. , 2007, , .		0
100	A Denotational Semantic Model for Validating JVML/CLDC Optimizations under Isabelle/HOL. , 2007, , .		0
101	Team Edit Automata for Testing Security Property. , 2007, , .		3
102	Forensic memory analysis: From stack and code to execution history. Digital Investigation, 2007, 4, 114-125.	3.2	25
103	Analyzing multiple logs for forensic evidence. Digital Investigation, 2007, 4, 82-91.	3.2	52
104	What middleware for network centric operations?. Knowledge-Based Systems, 2007, 20, 255-265.	7.1	8
105	Forensic analysis of logs: Modeling and verification. Knowledge-Based Systems, 2007, 20, 671-682.	7.1	12
106	A Formal Type System for Java.. Journal of Object Technology, 2007, 6, 117.	0.9	6
107	A Game Theoretic Model to Handle Network Intrusions over Multiple Packets. , 2006, , .		7
108	A selective dynamic compiler for embedded Java virtual machines targeting ARM processors. Science of Computer Programming, 2006, 59, 38-63.	1.9	1

#	Article	IF	Citations
109	Security by typing. International Journal on Software Tools for Technology Transfer, 2003, 4, 472-495.	1.9	4
110	Towards the Correctness of Security Protocols. Electronic Notes in Theoretical Computer Science, 2003, 83, 55-98.	0.9	1
111	From CML to a Model-Based Concurrent Specification Language. Concurrent Engineering Research and Applications, 1996, 4, 137-148.	3.2	0