Shouhuai Xu

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/1453438/publications.pdf

Version: 2024-02-01

106	2,685	218381	243296
papers	citations	26 h-index	44 g-index

106	106	106	1320
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	A Survey on Ethereum Systems Security. ACM Computing Surveys, 2021, 53, 1-43.	16.1	213
2	A Survey on Systems Security Metrics. ACM Computing Surveys, 2017, 49, 1-35.	16.1	171
3	SySeVR: A Framework for Using Deep Learning to Detect Software Vulnerabilities. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2244-2258.	3.7	165
4	Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach. , 0, , .		114
5	Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study. IEEE Transactions on Information Forensics and Security, 2013, 8, 1775-1789.	4.5	91
6	Modeling and Predicting Cyber Hacking Breaches. IEEE Transactions on Information Forensics and Security, 2018, 13, 2856-2871.	4.5	79
7	A Stochastic Model of Multivirus Dynamics. IEEE Transactions on Dependable and Secure Computing, 2012, 9, 30-45.	3.7	77
8	Predicting Cyber Attack Rates With Extreme Values. IEEE Transactions on Information Forensics and Security, 2015, 10, 1666-1677.	4.5	77
9	Adaptive Epidemic Dynamics in Networks. ACM Transactions on Autonomous and Adaptive Systems, 2014, 8, 1-19.	0.4	70
10	Î¼VulDeePecker: A Deep Learning-Based System for Multiclass Vulnerability Detection. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	3.7	65
11	VulDeeLocator: A Deep Learning-Based Fine-Grained Vulnerability Detector. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2821-2837.	3.7	60
12	Cross-layer detection of malicious websites. , 2013, , .		59
13	STRAM. ACM Computing Surveys, 2019, 51, 1-47.	16.1	55
14	Push- and pull-based epidemic spreading in networks. ACM Transactions on Autonomous and Adaptive Systems, 2012, 7, 1-26.	0.4	53
15	A Stochastic Model of Active Cyber Defense Dynamics. Internet Mathematics, 2015, 11, 23-61.	0.7	46
16	Preventive and Reactive Cyber Defense Dynamics Is Globally Stable. IEEE Transactions on Network Science and Engineering, 2018, 5, 156-170.	4.1	42
17	Cyber Epidemic Models with Dependences. Internet Mathematics, 2015, 11, 62-92.	0.7	40
18	Modeling and predicting extreme cyber attack rates via marked point processes. Journal of Applied Statistics, 2017, 44, 2534-2563.	0.6	40

#	Article	IF	Citations
19	A Vine Copula Model for Predicting the Effectiveness of Cyber Defense Early-Warning. Technometrics, 2017, 59, 508-520.	1.3	40
20	Protecting Cryptographic Keys from Memory Disclosure Attacks. , 2007, , .		39
21	Characterizing the power of moving target defense via cyber epidemic dynamics. , 2014, , .		38
22	A deep learning framework for predicting cyber attacks rates. Eurasip Journal on Information Security, 2019, 2019, .	2.4	38
23	Spatiotemporal Patterns and Predictability of Cyberattacks. PLoS ONE, 2015, 10, e0124472.	1.1	37
24	A Stochastic Model for Quantitative Security Analyses of Networked Systems. IEEE Transactions on Dependable and Secure Computing, 2011, 8, 28-43.	3.7	36
25	Cybersecurity dynamics. , 2014, , .		36
26	Modeling multivariate cybersecurity risks. Journal of Applied Statistics, 2018, 45, 2718-2740.	0.6	36
27	LHAP: A lightweight network access control protocol for ad hoc networks. Ad Hoc Networks, 2006, 4, 567-585.	3.4	35
28	Verifiable Delegated Set Intersection Operations on Outsourced Encrypted Data. , 2015, , .		32
29	Human Cognition Through the Lens of Social Engineering Cyberattacks. Frontiers in Psychology, 2020, 11, 1755.	1.1	32
30	An Extended Stochastic Model for Quantitative Security Analysis of Networked Systems. Internet Mathematics, 2012, 8, 288-320.	0.7	31
31	An evasion and counter-evasion study in malicious websites detection. , 2014, , .		30
32	A roadmap for privacy-enhanced secure data provenance. Journal of Intelligent Information Systems, 2014, 43, 481-501.	2.8	29
33	Metrics Towards Measuring Cyber Agility. IEEE Transactions on Information Forensics and Security, 2019, 14, 3217-3232.	4.5	29
34	A Framework for Enhancing Deep Neural Networks Against Adversarial Malware. IEEE Transactions on Network Science and Engineering, 2021, 8, 736-750.	4.1	29
35	A Framework for Understanding Botnets. , 2009, , .		28
36	Optimizing Active Cyber Defense. Lecture Notes in Computer Science, 2013, , 206-225.	1.0	28

#	Article	IF	Citations
37	GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks*. Journal of Computer Security, 2006, 14, 301-325.	0.5	26
38	Active cyber defense dynamics exhibiting rich phenomena. , 2015, , .		24
39	Metrics and measurement of trustworthy systems. , 2016, , .		23
40	Statistical Estimation of Malware Detection Metrics in the Absence of Ground Truth. IEEE Transactions on Information Forensics and Security, 2018, 13, 2965-2980.	4.5	23
41	Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity. Advances in Information Security, 2019, , 1-31.	0.9	23
42	A Case Study on using Deep Learning for Network Intrusion Detection. , 2019, , .		21
43	Unified Preventive and Reactive Cyber Defense Dynamics Is Still Globally Convergent. IEEE/ACM Transactions on Networking, 2019, 27, 1098-1111.	2.6	20
44	DroidEye: Fortifying Security of Learning-Based Classifier Against Adversarial Android Malware Attacks. , 2018, , .		19
45	Exploiting Trust-Based Social Networks for Distributed Protection of Sensitive Data. IEEE Transactions on Information Forensics and Security, 2011, 6, 39-52.	4.5	18
46	Multiple cyber attacks against a target with observation errors and dependent outcomes: Characterization and optimization. Reliability Engineering and System Safety, 2017, 159, 119-133.	5.1	18
47	Quantifying the security effectiveness of firewalls and DMZs. , 2018, , .		18
48	A Framework for Predicting Data Breach Risk: Leveraging Dependence to Cope With Sparsity. IEEE Transactions on Information Forensics and Security, 2021, 16, 2186-2201.	4.5	18
49	On the security of group communication schemes. Journal of Computer Security, 2007, 15, 129-169.	0.5	17
50	Emergent behavior in cybersecurity. , 2014, , .		17
51	A new approach to modeling and analyzing security of networked systems. , 2014, , .		16
52	Enhancing Data Trustworthiness via Assured Digital Signing. IEEE Transactions on Dependable and Secure Computing, 2012, 9, 838-851.	3.7	15
53	The Cybersecurity Dynamics Way of Thinking and Landscape. , 2020, , .		15
54	Quantifying the security effectiveness of network diversity. , 2018, , .		14

#	Article	IF	Citations
55	Towards Quantifying the (In)Security of Networked Systems. International Conference on Advanced Networking and Applications, 2007, , .	0.0	12
56	ICSD. , 2018, , .		11
57	A Characterization of Cybersecurity Posture from Network Telescope Data. Lecture Notes in Computer Science, 2015, , 105-126.	1.0	10
58	Extracting attack narratives from traffic datasets. , 2016, , .		10
59	Instructions-Based Detection of Sophisticated Obfuscation and Packing. , 2014, , .		9
60	A dataset generator for next generation system call host intrusion detection systems. , 2017, , .		9
61	Architectural Protection of Application Privacy against Software and Physical Attacks in Untrusted Cloud Environment. IEEE Transactions on Cloud Computing, 2018, 6, 478-491.	3.1	9
62	Non-interactive multisignatures in the plain public-key model with efficient verification. Information Processing Letters, 2010, 111, 82-89.	0.4	8
63	Robustness of non-interdependent and interdependent networks against dependent and adaptive attacks. Physica A: Statistical Mechanics and Its Applications, 2017, 482, 713-727.	1.2	8
64	Blockchain-based automated and robust cyber security management. Journal of Parallel and Distributed Computing, 2022, 163, 62-82.	2.7	8
65	RoPGen. , 2022, , .		8
66	Analyzing DNS activities of bot processes. , 2009, , .		7
67	Optimizing interconnections to maximize the spectral radius of interdependent networks. Physical Review E, 2017, 95, 032308.	0.8	7
68	Measuring Relative Accuracy of Malware Detectors in the Absence of Ground Truth. , 2018, , .		7
69	Cyber-guided Deep Neural Network for Malicious Repository Detection in GitHub. , 2020, , .		7
70	Seeking Foundations for the Science of Cyber Security. Information Systems Frontiers, 2021, 23, 263.	4.1	7
71	SARR: A Cybersecurity Metrics and Quantification Framework (Keynote). Lecture Notes in Computer Science, 2021, , 3-17.	1.0	7
72	Multi-context features for detecting malicious programs. Journal of Computer Virology and Hacking Techniques, 2018, 14, 181-193.	1.6	6

#	Article	IF	Citations
73	Leak-free mediated group signatures1. Journal of Computer Security, 2009, 17, 489-514.	0.5	5
74	A First Step towards Characterizing Stealthy Botnets. , 2009, , .		5
75	TNGuard: Securing IoT Oriented Tenant Networks Based on SDN. IEEE Internet of Things Journal, 2018, 5, 1411-1423.	5.5	5
76	Node diversification in complex networks by decentralized colouring. Journal of Complex Networks, 2019, 7, 554-563.	1.1	5
77	A Characterization of the problem of secure provenance management. , 2009, , .		4
78	A control flow graph-based signature for packer identification. , 2017, , .		4
79	Can We Leverage Predictive Uncertainty to Detect Dataset Shift and Adversarial Examples in Android Malware Detection?. , 2021, , .		4
80	Social engineering attacks and defenses in the physical world vs. cyberspace: A contrast study. , 2022, , 3-41.		4
81	A Framework for Characterizing the Evolution of Cyber Attacker-Victim Relation Graphs. , 2018, , .		3
82	Analyzing Root Causes of Intrusion Detection False-Negatives: Methodology and Case Study. , 2019, , .		3
83	Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses. , 2020, , .		3
84	Preventive and Reactive Cyber Defense Dynamics With Ergodic Time-Dependent Parameters is Globally Attractive. IEEE Transactions on Network Science and Engineering, 2021, 8, 2517-2532.	4.1	3
85	ExHPD: Exploiting Human, Physical, and Driving Behaviors to Detect Vehicle Cyber Attacks. IEEE Internet of Things Journal, 2021, 8, 14355-14371.	5.5	3
86	Election with Bribe-Effect Uncertainty: A Dichotomy Result. , 2019, , .		3
87	On the properties of cryptographic protocols and the weaknesses of the BAN-like logics. Operating Systems Review (ACM), 1997, 31, 12-23.	1.5	2
88	(How) Can We Manage the Trustworthiness of Security Infrastructures and Services?. , 2008, , .		2
89	State of Science in Alarm System Safety: Implications for Researchers, Vendors, and Clinical Leaders. Biomedical Instrumentation and Technology, 2022, 56, 19-28.	0.2	2
90	A probabilistic characterization of a fault-tolerant gossiping algorithm. Journal of Systems Science and Complexity, 2009, 22, 88-108.	1.6	1

#	Article	IF	Citations
91	ON THE QUASI-STATIONARY DISTRIBUTION OF SIS MODELS. Probability in the Engineering and Informational Sciences, 2016, 30, 622-639.	0.6	1
92	Special issue on social network security and privacy. Concurrency Computation Practice and Experience, 2018, 30, e4414.	1.4	1
93	RollSec: Automatically Secure Software States Against General Rollback. International Journal of Parallel Programming, 2018, 46, 788-805.	1.1	1
94	Statistical modeling of computer malware propagation dynamics in cyberspace. Journal of Applied Statistics, 2022, 49, 858-883.	0.6	1
95	Data-Driven Characterization and Detection of COVID-19 Themed Malicious Websites. , 2020, , .		1
96	Relationships between Driver Errors and Delay Discounting in a Simulated Driving Task. Perspectives on Behavior Science, 2020, 43, 487-500.	1.1	1
97	On the security of three-party cryptographic protocols. Operating Systems Review (ACM), 1998, 32, 7-20.	1.5	1
98	APIN: Automatic Attack Path Identification in Computer Networks. , 2020, , .		1
99	SAND: semi-automated adaptive network defense via programmable rule generation and deployment. Science China Information Sciences, 2022, 65, 1.	2.7	1
100	Enhancing anonymity via market competition. , 2004, , .		0
101	Towards Understanding the (In)security of Networked Systems under Towards Understanding the (In)security of Networked Systems under Topology-Directed Stealthy Attacks. , 2006, , .		0
102	Global stabilization over the network with continuous loss of states. , 2010, , .		0
103	Performance Comparison and Feedback Controller Design of Network Controlled Systems with Continuous Loss of States. , 2011, , .		0
104	Information consensus for multi-agent systems via nonlinear protocols. , 2012, , .		0
105	Programmable decoder and shadow threads: Tolerate remote code injection exploits with diversified redundancy. , 2014, , .		0
106	Programmable decoder and shadow threads: Tolerate remote code injection exploits with diversified redundancy. , 2014, , .		0