Stefano Zanero

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/9436436/publications.pdf

Version: 2024-02-01

90 papers	2,342 citations	361045 20 h-index	344852 36 g-index
92 all docs	92 docs citations	92 times ranked	1716 citing authors

#	Article	IF	Citations
1	Unsupervised learning techniques for an intrusion detection system. , 2004, , .		166
2	BitIodine: Extracting Intelligence from the Bitcoin Network. Lecture Notes in Computer Science, 2014, , 457-468.	1.0	150
3	ShieldFS. , 2016, , .		147
4	HelDroid: Dissecting and Detecting Mobile Ransomware. Lecture Notes in Computer Science, 2015, , 382-404.	1.0	140
5	Phoenix: DGA-Based Botnet Tracking and Intelligence. Lecture Notes in Computer Science, 2014, , 192-211.	1.0	97
6	An Experimental Security Analysis of an Industrial Robot Controller. , 2017, , .		94
7	Detecting Intrusions through System Call Sequence and Argument Analysis. IEEE Transactions on Dependable and Secure Computing, 2010, 7, 381-395.	3.7	92
8	Identifying Dormant Functionality in Malware Programs. , 2010, , .		74
9	Cyber-Physical Systems. Computer, 2017, 50, 14-16.	1.2	74
10	A Stealth, Selective, Link-Layer Denial-of-Service Attack Against Automotive Networks. Lecture Notes in Computer Science, 2017, , 185-206.	1.0	74
11	BankSealer: A decision support system for online banking fraud analysis and investigation. Computers and Security, 2015, 53, 175-186.	4.0	60
12	Computer Virus Propagation Models. Lecture Notes in Computer Science, 2004, , 26-50.	1.0	54
13	CANnolo: An Anomaly Detection System Based on LSTM Autoencoders for Controller Area Network. IEEE Transactions on Network and Service Management, 2021, 18, 1913-1924.	3.2	48
14	Studying Bluetooth Malware Propagation: The BlueBag Project. IEEE Security and Privacy, 2007, 5, 17-25.	1.5	45
15	Lines of malicious code. , 2012, , .		45
16	A fast eavesdropping attack against touchscreens. , 2011, , .		39
17	Stranger danger. , 2014, , .		39
18	Reducing false positives in anomaly detectors through fuzzy alert aggregation. Information Fusion, 2009, 10, 300-311.	11.7	38

#	Article	IF	Citations
19	AndroTotal. , 2013, , .		32
20	Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles - ESC Regulatory Affairs Committee/EHRA joint task force report. Europace, 2020, 22, 1742-1758.	0.7	32
21	Two years of short URLs internet measurement. , 2013, , .		31
22	Measuring and Defeating Anti-Instrumentation-Equipped Malware. Lecture Notes in Computer Science, 2017, , 73-96.	1.0	31
23	Open Problems in Computer Virology. Journal in Computer Virology, 2006, 1, 55-66.	1.9	30
24	AndRadar: Fast Discovery of Android Applications in Alternative Markets. Lecture Notes in Computer Science, 2014, , 51-71.	1.0	30
25	All your face are belong to us. , 2012, , .		29
26	Constrained Concealment Attacks against Reconstruction-based Anomaly Detectors in Industrial Control Systems. , 2020, , .		28
27	Analyzing TCP Traffic Patterns Using Self Organizing Maps. Lecture Notes in Computer Science, 2005, , 83-90.	1.0	26
28	Selecting and Improving System Call Models for Anomaly Detection. Lecture Notes in Computer Science, 2009, , 206-223.	1.0	24
29	A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth. IEEE Embedded Systems Letters, 2013, 5, 34-37.	1.3	24
30	Finding Non-trivial Malware Naming Inconsistencies. Lecture Notes in Computer Science, 2011, , 144-159.	1.0	24
31	Security Evaluation of a Banking Fraud Analysis System. ACM Transactions on Privacy and Security, 2018, 21, 1-31.	2.2	23
32	Unsupervised learning algorithms for intrusion detection. , 2008, , .		22
33	A Systematical and longitudinal study of evasive behaviors in windows malware. Computers and Security, 2022, 113, 102550.	4.0	22
34	Security of controlled manufacturing systems in the connected factory: the case of industrial robots. Journal of Computer Virology and Hacking Techniques, 2019, 15, 161-175.	1.6	21
35	Behavioral Intrusion Detection. Lecture Notes in Computer Science, 2004, , 657-666.	1.0	20
36	Seeing the invisible. Operating Systems Review (ACM), 2008, 42, 51-58.	1.5	19

#	ARTICLE	IF	CITATIONS
37	There's a Hole in that Bucket!. , 2018, , .		19
38	File Block Classification by Support Vector Machine. , 2011, , .		18
39	Wireless Malware Propagation: A Reality Check. IEEE Security and Privacy, 2009, 7, 70-74.	1.5	17
40	Faces in the Distorting Mirror. , 2014, , .		16
41	BankSealer: An Online Banking Fraud Analysis and Decision Support System. IFIP Advances in Information and Communication Technology, 2014, , 380-394.	0.5	16
42	GroupDroid. , 2017, , .		15
43	Characterizing Background Noise in ICS Traffic Through a Set of Low Interaction Honeypots. , 2019, , .		14
44	Jackdaw: Towards Automatic Reverse Engineering of Large Datasets of Binaries. Lecture Notes in Computer Science, 2015, , 121-143.	1.0	14
45	A comprehensive black-box methodology for testing the forensic characteristics of solid-state drives. , 2013, , .		13
46	Grab 'n Run. , 2015, , .		13
47	A Secure-by-Design Framework for Automotive On-board Network Risk Analysis. , 2019, , .		12
48	CopyCAN. , 2019, , .		12
49	ReCAN â€" Dataset for reverse engineering of Controller Area Networks. Data in Brief, 2020, 29, 105149.	0.5	12
50	Smart Factory Security: A Case Study on a Modular Smart Manufacturing System. Procedia Computer Science, 2021, 180, 666-675.	1.2	12
51	BURN. , 2011, , .		11
52	GreatEatlon: Fast, Static Detection of Mobile Ransomware. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2017, , 617-636.	0.2	11
53	Prometheus: Analyzing WebInject-based information stealers. Journal of Computer Security, 2017, 25, 117-137.	0.5	10
54	ZARATHUSTRA: Extracting WebInject signatures from banking trojans. , 2014, , .		9

#	Article	IF	Citations
55	On the Use of Different Statistical Tests for Alert Correlation â€“ Short Paper. Lecture Notes in Computer Science, 2007, , 167-177.	1.0	9
56	Detecting Insecure Code Patterns in Industrial Robot Programs. , 2020, , .		9
57	Context-Based File Block Classification. International Federation for Information Processing, 2012, , 67-82.	0.4	8
58	Practical Exploit Generation for Intent Message Vulnerabilities in Android. , 2015, , .		8
59	FraudBuster: Temporal Analysis and Detection of Advanced Financial Frauds. Lecture Notes in Computer Science, 2018, , 211-233.	1.0	8
60	Trellis: Privilege Separation for Multi-user Applications Made Easy. Lecture Notes in Computer Science, 2016, , 437-456.	1.0	8
61	Amaretto: An Active Learning Framework for Money Laundering Detection. IEEE Access, 2022, 10, 41720-41739.	2.6	7
62	A methodology for the repeatable forensic analysis of encrypted drives. , 2008, , .		6
63	ULISSE, a network intrusion detection system. , 2008, , .		6
64	When Cyber Got Real: Challenges in Securing Cyber-Physical Systems. , 2018, , .		6
65	A Supervised Auto-Tuning Approach for a Banking Fraud Detection System. Lecture Notes in Computer Science, 2017, , 215-233.	1.0	6
66	GOLIATH: A Decentralized Framework for Data Collection in Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 13372-13385.	4.7	6
67	A social-engineering-centric data collection initiative to study phishing. , 2011, , .		5
68	Black-box forensic and antiforensic characteristics of solid-state drives. Journal of Computer Virology and Hacking Techniques, 2014, 10, 255-271.	1.6	5
69	Extended Abstract: Toward Systematically Exploring Antivirus Engines. Lecture Notes in Computer Science, 2018, , 393-403.	1.0	5
70	A Practical Attack Against a KNX-based Building Automation System. , 2014, , .		5
71	GIVS: Integrity Validation for Grid Security. Lecture Notes in Computer Science, 2005, , 147-154.	1.0	4
72	NoSQL Breakdown: A Large-scale Analysis of Misconfigured NoSQL Services. , 2020, , .		4

#	ARTICLE	IF	CITATIONS
73	Security and Trust in the Italian Legal Digital Signature Framework. Lecture Notes in Computer Science, 2005, , 34-44.	1.0	3
74	Integrating Partial Models of Network Normality via Cooperative Negotiation: An Approach to Development of Multiagent Intrusion Detection Systems. , 2008, , .		3
75	Effective Multimodel Anomaly Detection Using Cooperative Negotiation. Lecture Notes in Computer Science, 2010, , 180-191.	1.0	3
76	XSS PEEKER: Dissecting the XSS Exploitation Techniques and Fuzzing Mechanisms of Blackbox Web Application Scanners. IFIP Advances in Information and Communication Technology, 2016, , 243-258.	0.5	3
77	ELISA: ELiciting ISA of Raw Binaries for Fine-Grained Code and Data Separation. Lecture Notes in Computer Science, 2018, , 351-371.	1.0	3
78	GIVS: integrity validation for grid security. International Journal of Critical Infrastructures, 2008, 4, 319.	0.1	2
79	Observing the Tidal Waves of Malware: Experiences from the WOMBAT Project. , 2010, , .		2
80	Scalable Testing of Mobile Antivirus Applications. Computer, 2015, 48, 60-68.	1.2	2
81	Response to ESMA/2016/773: 'The Distributed Ledger Technology Applied to Securities Markets'. SSRN Electronic Journal, 0, , .	0.4	2
82	Lessons learned from the Italian law on privacy â€" Part I. Computer Law and Security Review, 2004, 20, 310-313.	1.3	1
83	Security and Privacy Measurements in Social Networks: Experiences and Lessons Learned. , 2014, , .		1
84	SysTaint. , 2018, , .		1
85	A Practical Attack Against a KNX-based Building Automation System. , 0, , .		1
86	Quantum matching pursuit: A quantum algorithm for sparse representations. Physical Review A, 2022, 105, .	1.0	1
87	Lessons learned from the Italian law on privacy â€" Part II. Computer Law and Security Review, 2004, 20, 384-389.	1.3	0
88	Systems Security Research at Politecnico di Milano. , 2011, , .		0
89	Integrated detection of anomalous behavior of computer infrastructures. , 2012, , .		0
90	On-chip system call tracing: A feasibility study and open prototype. , 2016, , .		0