Vasilios Katos

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/541862/publications.pdf

Version: 2024-02-01

77	914	567247 15	552766 26
papers	citations	h-index	g-index

79	79	79	801
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Vulnerability Exposure Driven Intelligence in Smart, Circular Cities. Digital Threats Research and Practice, 2022, 3, 1-18.	2.4	3
2	Loneliness, life satisfaction, problematic internet use and security behaviours: re-examining the relationships when working from home during COVID-19. Behaviour and Information Technology, 2022, 41, 3161-3175.	4.0	24
3	The Relationships between Gender, Life Satisfaction, Loneliness and Problematic Internet Use during COVID-19: Does the Lockdown Matter?. International Journal of Environmental Research and Public Health, 2022, 19, 1325.	2.6	11
4	A dynamic spatialâ€“temporal deep learning framework for traffic speed prediction on large-scale road networks. Expert Systems With Applications, 2022, 195, 116585.	7.6	16
5	WARDOG: Awareness Detection Watchdog for Botnet Infection on the Host Device. IEEE Transactions on Sustainable Computing, 2021, 6, 4-18.	3.1	7
6	Resurrecting anti-virtualization and anti-debugging: Unhooking your hooks. Future Generation Computer Systems, 2021, 116, 393-405.	7.5	14
7	User Attribution Through Keystroke Dynamics-Based Author Age Estimation. Lecture Notes in Networks and Systems, 2021, , 47-61.	0.7	5
8	Privacy in Data-Driven Circular Economy. , 2021, , 1-3.		0
9	Age and Gender as Cyber Attribution Features in Keystroke Dynamic-Based User Classification Processes. Electronics (Switzerland), 2021, 10, 835.	3.1	11
10	Detection of Advanced Web Bots by Combining Web Logs with Mouse Behavioural Biometrics. Digital Threats Research and Practice, 2021, 2, 1-26.	2.4	9
11	A joint temporal-spatial ensemble model for short-term traffic prediction. Neurocomputing, 2021, 457, 26-39.	5.9	14
12	Unearthing malicious campaigns and actors from the blockchain DNS ecosystem. Computer Communications, 2021, 179, 217-230.	5.1	5
13	R²BN: An Adaptive Model for Keystroke-Dynamics-Based Educational Level Classification. IEEE Transactions on Cybernetics, 2020, 50, 525-535.	9.5	15
14	Encrypted and covert DNS queries for botnets: Challenges and countermeasures. Computers and Security, 2020, 88, 101614.	6.0	30
15	Unravelling Ariadneâ€™s Thread: Exploring the Threats of Decentralised DNS. IEEE Access, 2020, 8, 118559-118571.	4.2	16
16	Pairing a Circular Economy and the 5G-Enabled Internet of Things: Creating a Class of ?Looping Smart Assets?. IEEE Vehicular Technology Magazine, 2020, 15, 20-31.	3.4	11
17	An architecture for resilient intrusion detection in ad-hoc networks. Journal of Information Security and Applications, 2020, 53, 102530.	2.5	4
18	Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. Computers, 2020, 9, 18.	3.3	28

#	Article	IF	Citations
19	A Revised Forensic Process for Aligning the Investigation Process with the Design of Forensic-Enabled Cloud Services. Communications in Computer and Information Science, 2020, , 161-177.	0.5	0
20	A Socio-Technical Perspective on Threat Intelligence Informed Digital Forensic Readiness. , 2020, , 173-184.		0
21	A Socio-Technical Perspective on Threat Intelligence Informed Digital Forensic Readiness. , 2020, , 1201-1212.		0
22	Improving Forensic Triage Efficiency through Cyber Threat Intelligence. Future Internet, 2019, 11, 162.	3.8	13
23	Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments. Ad Hoc Networks, 2019, 95, 101988.	5.5	35
24	Towards a framework for detecting advanced Web bots. , 2019, , .		13
25	IEEE 802.11ax Spatial Reuse Improvement: An Interference-Based Channel-Access Algorithm. IEEE Vehicular Technology Magazine, 2019, 14, 78-84.	3.4	22
26	Actionable threat intelligence for digital forensics readiness. Information and Computer Security, 2019, 27, 273-291.	2.2	11
27	A framework for designing cloud forensic-enabled services (CFeS). Requirements Engineering, 2019, 24, 403-430.	3.1	11
28	From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods. IEEE Communications Surveys and Tutorials, 2018, 20, 3369-3388.	39.4	121
29	Exploring the protection of private browsing in desktop browsers. Computers and Security, 2017, 67, 181-197.	6.0	16
30	You can run but you cannot hide from memory: Extracting IM evidence of Android apps. , 2017, , .		5
31	Cryptographic Key Management in Delay Tolerant Networks: A Survey. Future Internet, 2017, 9, 26.	3.8	14
32	Age Detection Through Keystroke Dynamics from User Authentication Failures. International Journal of Digital Crime and Forensics, 2017, 9, 1-16.	0.7	20
33	A Socio-Technical Perspective on Threat Intelligence Informed Digital Forensic Readiness. International Journal of Systems and Society, 2017, 4, 57-68.	0.1	3
34	Opportunistic key management in delay tolerant networks. International Journal of Information and Computer Security, 2017, 9, 212.	0.2	0
35	Malevolent app pairs. , 2016, , .		6
36	Automated key exchange protocol evaluation in delay tolerant networks. Computers and Security, 2016, 59, 1-8.	6.0	2

#	Article	IF	Citations
37	Privacy-preserving, user-centric VoIP CAPTCHA challenges. Information and Computer Security, 2016, 24, 2-19.	2.2	1
38	â€œWater, Water, Every Whereâ€• Nuances for a Water Industry Critical Infrastructure Specification Exemplar. Lecture Notes in Computer Science, 2016, , 243-246.	1.3	3
39	Mitigating Circumstances in Cybercrime: A Position Paper. , 2015, , .		0
40	Language-independent gender identification through keystroke analysis. Information and Computer Security, 2015, 23, 286-301.	2.2	7
41	Reengineering the user: privacy concerns about personal data on smartphones. Information and Computer Security, 2015, 23, 394-405.	2.2	24
42	A novel mechanism for anonymizing Global System for Mobile Communications calls using a resourceâ€based Session Initiation Protocol community network. Security and Communication Networks, 2015, 8, 486-500.	1.5	1
43	Data Recovery Strategies for Cloud Environments. , 2015, , 377-391.		0
44	A method for forensic artefact collection, analysis and incident response in environments running session initiation protocol and session description protocol. International Journal of Electronic Security and Digital Forensics, 2014, 6, 241.	0.2	3
45	On-scene triage open source forensic tool chests: Are they effective?. Digital Investigation, 2013, 10, 99-115.	3.2	10
46	The Sphinx enigma in critical VoIP infrastructures: Human or botnet?. , 2013, , .		6
47	A critical review of 7 years of Mobile Device Forensics. Digital Investigation, 2013, 10, 323-349.	3.2	62
48	Differential malware forensics. Digital Investigation, 2013, 10, 311-322.	3.2	14
49	Macroeconomics of privacy and security for identity management and surveillance. Kybernetes, 2013, 42, 140-163.	2.2	3
50	Keystroke forensics. , 2013, , .		6
51	A framework for password harvesting from volatile memory. International Journal of Electronic Security and Digital Forensics, 2012, 4, 154.	0.2	5
52	An integrated model for online transactions: illuminating the black box. Information Management and Computer Security, 2012, 20, 184-206.	1.2	12
53	Practical Password Harvesting from Volatile Memory. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2012, , 17-22.	0.3	1
54	Real time DDoS detection using fuzzy estimators. Computers and Security, 2012, 31, 782-790.	6.0	69

#	Article	IF	Citations
55	A Framework for Anonymizing GSM Calls over a Smartphone VoIP Network. International Federation for Information Processing, 2012, , 543-548.	0.4	2
56	A Novel Security Architecture for a Space-Data DTN. Lecture Notes in Computer Science, 2012, , 342-349.	1.3	2
57	A Framework for Access Control with Inference Constraints. , 2011, , .		6
58	Surveillance, Privacy and the Law of Requisite Variety. Lecture Notes in Computer Science, 2011, , 123-139.	1.3	3
59	Requirements for a Forensically Ready Cloud Storage Service. International Journal of Digital Crime and Forensics, 2011, 3, 19-36.	0.7	15
60	On the detection of pod slurping attacks. Computers and Security, 2010, 29, 680-685.	6.0	3
61	Economics of Personal Data Management: Fair Personal Information Trades. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 151-160.	0.3	4
62	Information Assurance and Forensic Readiness. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 181-188.	0.3	11
63	Digital Forensic Investigations: A New Frontier for Informing Systems. , 2009, , 361-371.		2
64	From Synergy to Symbiosis. International Journal of Information Technologies and Systems Approach, 2009, 2, 1-14.	1.4	0
65	A cyber-crime investigation framework. Computer Standards and Interfaces, 2008, 30, 223-228.	5.4	19
66	The security and privacy impact of criminalising the distribution of hacking tools. Computer Fraud and Security, 2008, 2008, 9-16.	1.6	4
67	Cyber-Crime Investigations: Complex Collaborative Decision Making. , 2008, , .		2
68	Innovation management through the use of diversity networks. International Journal of Knowledge and Learning, 2008, 4, 357.	0.2	2
69	A partial equilibrium view on security and privacy. Information Management and Computer Security, 2008, 16, 74-83.	1.2	13
70	Exoinformation Space Audits: An Information Richness View of Privacy and Security Obligations. Journal of Information Privacy and Security, 2007, 3, 29-44.	0.4	3
71	Exploring confusion in product ciphers through regression analysis. Information Sciences, 2007, 177, 1789-1795.	6.9	0
72	Network intrusion detection: Evaluating cluster, discriminant, and logit analysis. Information Sciences, 2007, 177, 3060-3073.	6.9	37

#	Article	IF	Citations
73	An Interdisciplinary Approach to Forensic IT and Forensic Psychology Education. IFIP Advances in Information and Communication Technology, 2007, , 65-71.	0.7	3
74	Modelling corporate wireless security and privacy. Journal of Strategic Information Systems, 2005, 14, 307-321.	5.9	14
75	A randomness test for block ciphers. Applied Mathematics and Computation, 2005, 162, 29-35.	2.2	17
76	Data Recovery Strategies for Cloud Environments. , 0, , 251-265.		4
77	Managing IS Security and Privacy. , 0, , 1246-1254.		1