

Maria Papadaki

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/7572218/publications.pdf>

Version: 2024-02-01

41
papers

592
citations

759233

12
h-index

677142

22
g-index

41
all docs

41
docs citations

41
times ranked

526
citing authors

#	ARTICLE	IF	CITATIONS
1	Towards a cross-cultural education framework for online safety awareness. Information and Computer Security, 2021, 29, 664-679.	2.2	3
2	A collaborative approach for national cybersecurity incident management. Information and Computer Security, 2021, 29, 457-484.	2.2	2
3	An empirical analysis of the information security culture key factors framework. Computers and Security, 2021, 108, 102354.	6.0	14
4	Towards a Cross-Cultural Education Framework for Online Safety Awareness. IFIP Advances in Information and Communication Technology, 2020, , 47-57.	0.7	1
5	Fifteen years of phishing: can technology save us?. Computer Fraud and Security, 2019, 2019, 11-16.	1.6	7
6	A Comprehensive Framework for Understanding Security Culture in Organizations. IFIP Advances in Information and Communication Technology, 2019, , 143-156.	0.7	2
7	Towards a maturity model for health-care cloud security (M ² HCS). Information and Computer Security, 2019, 28, 321-345.	2.2	11
8	Factors Limiting the Adoption of Cloud Computing in Teleradiology. International Journal for Information Security Research, 2019, 9, 854-861.	0.3	1
9	Agent-based Vs Agent-less Sandbox for Dynamic Behavioral Analysis. , 2018, , .		7
10	The impact of security and its antecedents in behaviour intention of using e-government services. Behaviour and Information Technology, 2017, 36, 620-636.	4.0	37
11	A survey of cyber-security awareness in Saudi Arabia. , 2016, , .		23
12	Graphical One-Time Password (GOTPass): A usability evaluation. Information Security Journal, 2016, 25, 94-108.	1.9	5
13	The challenge of measuring cyber-dependent crimes. Computer Fraud and Security, 2015, 2015, 5-12.	1.6	25
14	FHSD: An Improved IP Spoof Detection Method for Web DDoS Attacks. Computer Journal, 2015, 58, 892-903.	2.4	14
15	A response selection model for intrusion response systems: Response Strategy Model (RSM). Security and Communication Networks, 2014, 7, 1831-1848.	1.5	2
16	Security challenges of E-government adoption based on end users' perspective. , 2014, , .		1
17	Vulnerability of opportunistic parking assistance systems to vehicular node selfishness. Computer Communications, 2014, 48, 159-170.	5.1	8
18	Active authentication for mobile devices utilising behaviour profiling. International Journal of Information Security, 2014, 13, 229-244.	3.4	64

#	ARTICLE	IF	CITATIONS
19	Security Factors Influencing End Users'™ Adoption of E-Government. Journal of Internet Technology and Secured Transaction, 2014, 3, 320-328.	0.2	7
20	Improving Awareness of Social Engineering Attacks. IFIP Advances in Information and Communication Technology, 2013, , 249-256.	0.7	16
21	Opportunistically-assisted parking search: A story of free riders, selfish liars and bona fide mules. , 2013, , .		4
22	IT Application Outsourcing in Europe: Long-Term Outcomes, Success Factors and Implications for ITO Maturity. , 2013, , .		6
23	Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM). Security and Communication Networks, 2013, 6, 1087-1116.	1.5	19
24	Evaluation of anomaly-based IDS for mobile devices using machine learning classifiers. Security and Communication Networks, 2012, 5, 3-14.	1.5	66
25	A Response Strategy Model for Intrusion Response Systems. International Federation for Information Processing, 2012, , 573-578.	0.4	4
26	Misuse Detection for Mobile Devices Using Behaviour Profiling. International Journal of Cyber Warfare and Terrorism, 2011, 1, 41-53.	0.5	11
27	A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm. Computers and Security, 2010, 29, 712-723.	6.0	69
28	Vulnerability management: an attitude of mind?. Network Security, 2010, 2010, 4-8.	0.8	5
29	Online addiction. , 2010, , .		8
30	An investigation and survey of response options for Intrusion Response Systems (IRs). , 2010, , .		19
31	Behaviour Profiling on Mobile Devices. , 2010, , .		21
32	Assessing the Usability of End-User Security Software. Lecture Notes in Computer Science, 2010, , 177-189.	1.3	14
33	Social engineering: assessing vulnerabilities in practice. Information Management and Computer Security, 2009, 17, 53-63.	1.2	22
34	Scare tactics " A viable weapon in the security war?. Computer Fraud and Security, 2009, 2009, 6-10.	1.6	4
35	Testing our defences or defending our tests: the obstacles to performing security assessment references. Computer Fraud and Security, 2008, 2008, 8-12.	1.6	4
36	The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset. Lecture Notes in Computer Science, 2008, , 139-150.	1.3	20

#	ARTICLE	IF	CITATIONS
37	Considering the potential of criminal profiling to combat hacking. Journal in Computer Virology, 2007, 3, 135-141.	1.9	13
38	Achieving automated intrusion response: a prototype implementation. Information Management and Computer Security, 2006, 14, 235-251.	1.2	13
39	Informing the decision process in an automated intrusion response system. Information Security Technical Report, 2005, 10, 150-161.	1.3	7
40	IDS or IPS: what is best?. Network Security, 2004, 2004, 15-19.	0.8	11
41	Operational Characteristics of an Automated Intrusion Response System. Lecture Notes in Computer Science, 2003, , 65-75.	1.3	2