Julio C Hernandez-Castro

List of Publications by Year
in descending order

33 papers	670 citations	687363 13 h-index	580821 25 g-index
33 all docs	33 docs citations	33 times ranked	598 citing authors

#	Article	IF	Citations
1	No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial Examples, With Applications to CAPTCHA Generation. IEEE Transactions on Information Forensics and Security, 2017, 12, 2640-2653.	6.9	127
2	Flaws on RFID grouping-proofs. Guidelines for future sound protocols. Journal of Network and Computer Applications, 2011, 34, 833-845.	9.1	80
3	Assessing the extent and nature of wildlife trade on the dark web. Conservation Biology, 2016, 30, 900-904.	4.7	77
4	Detecting discussion communities on vaccination in twitter. Future Generation Computer Systems, 2017, 66, 125-136.	7.5	76
5	Steganography in games: A general methodology and its application to the game of Go. Computers and Security, 2006, 25, 64-71.	6.0	41
6	A PRNU-based counter-forensic method to manipulate smartphone image source identification techniques. Future Generation Computer Systems, 2017, 76, 418-427.	7.5	25
7	Practical attacks on a mutual authentication scheme under the EPC Class-1 Generation-2 standard. Computer Communications, 2009, 32, 1185-1193.	5.1	24
8	Cryptanalysis of an EPC Class-1 Generation-2 standard compliant authentication protocol. Engineering Applications of Artificial Intelligence, 2011, 24, 1061-1069.	8.1	21
9	Bycatch and illegal wildlife trade on the dark web. Oryx, 2017, 51, 393-394.	1.0	18
10	Digital Image Tamper Detection Technique Based on Spectrum Analysis of CFA Artifacts. Sensors, 2018, 18, 2804.	3.8	17
11	Digital Images Authentication Technique Based on DWT, DCT and Local Binary Patterns. Sensors, 2018, 18, 3372.	3.8	17
12	Intercepting Hail Hydra: Real-time detection of Algorithmically Generated Domains. Journal of Network and Computer Applications, 2021, 190, 103135.	9.1	16
13	Secure content access and replication in pure P2P networks. Computer Communications, 2008, 31, 266-279.	5.1	14
14	Steganalysis of OpenPuff through atomic concatenation ofÂMP4 flags. Digital Investigation, 2015, 13, 15-21.	3.2	11
15	Source identification for mobile devices, based on wavelet transforms combined with sensor imperfections. Computing (Vienna/New York), 2014, 96, 829-841.	4.8	10
16	Analysis of errors in exif metadata on mobile devices. Multimedia Tools and Applications, 2015, 74, 4735-4763.	3.9	10
17	On the Unbearable Lightness of FIPS 140â€“2 Randomness Tests. IEEE Transactions on Information Forensics and Security, 2022, 17, 3946-3958.	6.9	10
18	A Roadmap for Improving the Impact of Anti-ransomware Research. Lecture Notes in Computer Science, 2019, , 137-154.	1.3	10

#	Article	IF	Citations
19	On the limits of engine analysis for cheating detection in chess. Computers and Security, 2015, 48, 58-73.	6.0	9
20	Dismantling OpenPuff PDF steganography. Digital Investigation, 2018, 25, 90-96.	3.2	9
21	Smartphone image acquisition forensics using sensor fingerprint. IET Computer Vision, 2015, 9, 723-731.	2.0	8
22	Why Current Statistical Approaches to Ransomware Detection Fail. Lecture Notes in Computer Science, 2020, , 199-216.	1.3	8
23	A study on the false positive rate of Stegdetect. Digital Investigation, 2013, 9, 235-245.	3.2	6
24	Reducing the Forensic Footprint with Android Accessibility Attacks. Lecture Notes in Computer Science, 2020, , 22-38.	1.3	6
25	Persistence in Linux-Based IoT Malware. Lecture Notes in Computer Science, 2021, , 3-19.	1.3	5
26	Bayesian rational exchange. International Journal of Information Security, 2008, 7, 85-100.	3.4	4
27	On the Effectiveness of Ransomware Decryption Tools. Computers and Security, 2021, 111, 102469.	6.0	4
28	Real-Time Triggering of Android Memory Dumps for Stealthy Attack Investigation. Lecture Notes in Computer Science, 2021, , 20-36.	1.3	2
29	Industrialising Blackmail: Privacy Invasion Based IoT Ransomware. Lecture Notes in Computer Science, 2021, , 72-92.	1.3	2
30	Responding to Targeted Stealthy Attacks on Android Using Timely-Captured Memory Dumps. IEEE Access, 2022, 10, 35172-35218.	4.2	2
31	AnÃ¡lisis y evaluaciÃ³n experimental del circuito generador de nÃºmeros aleatorios Lampert Circuit. ColecciÃ³n Jornadas Y Congresos, 0, , .	0.0	1
32	Theia: a tool for the forensic analysis of mobile devices pictures. Computing (Vienna/New York), 2016, 98, 1251-1286.	4.8	0
33	Efficient Detection and Recovery of Malicious PowerShell Scripts Embedded into Digital Images. Security and Communication Networks, 2022, 2022, 1-12.	1.5	0