

# Julio C Hernandez-Castro

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/5474126/publications.pdf>

Version: 2024-02-01

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	On the Unbearable Lightness of FIPS 140-2 Randomness Tests. IEEE Transactions on Information Forensics and Security, 2022, 17, 3946-3958.	6.9	10
2	Responding to Targeted Stealthy Attacks on Android Using Timely-Captured Memory Dumps. IEEE Access, 2022, 10, 35172-35218.	4.2	2
3	Efficient Detection and Recovery of Malicious PowerShell Scripts Embedded into Digital Images. Security and Communication Networks, 2022, 2022, 1-12.	1.5	0
4	Real-Time Triggering of Android Memory Dumps for Stealthy Attack Investigation. Lecture Notes in Computer Science, 2021, , 20-36.	1.3	2
5	Persistence in Linux-Based IoT Malware. Lecture Notes in Computer Science, 2021, , 3-19.	1.3	5
6	Intercepting Hail Hydra: Real-time detection of Algorithmically Generated Domains. Journal of Network and Computer Applications, 2021, 190, 103135.	9.1	16
7	On the Effectiveness of Ransomware Decryption Tools. Computers and Security, 2021, 111, 102469.	6.0	4
8	Industrialising Blackmail: Privacy Invasion Based IoT Ransomware. Lecture Notes in Computer Science, 2021, , 72-92.	1.3	2
9	Reducing the Forensic Footprint with Android Accessibility Attacks. Lecture Notes in Computer Science, 2020, , 22-38.	1.3	6
10	Why Current Statistical Approaches to Ransomware Detection Fail. Lecture Notes in Computer Science, 2020, , 199-216.	1.3	8
11	A Roadmap for Improving the Impact of Anti-ransomware Research. Lecture Notes in Computer Science, 2019, , 137-154.	1.3	10
12	Dismantling OpenPuff PDF steganography. Digital Investigation, 2018, 25, 90-96.	3.2	9
13	Digital Image Tamper Detection Technique Based on Spectrum Analysis of CFA Artifacts. Sensors, 2018, 18, 2804.	3.8	17
14	Digital Images Authentication Technique Based on DWT, DCT and Local Binary Patterns. Sensors, 2018, 18, 3372.	3.8	17
15	Bycatch and illegal wildlife trade on the dark web. Oryx, 2017, 51, 393-394.	1.0	18
16	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
17	A PRNU-based counter-forensic method to manipulate smartphone image source identification techniques. Future Generation Computer Systems, 2017, 76, 418-427.	7.5	25
18	Detecting discussion communities on vaccination in twitter. Future Generation Computer Systems, 2017, 66, 125-136.	7.5	76

#	ARTICLE	IF	CITATIONS
19	Assessing the extent and nature of wildlife trade on the dark web. Conservation Biology, 2016, 30, 900-904.	4.7	77
20	Theia: a tool for the forensic analysis of mobile devices pictures. Computing (Vienna/New York), 2016, 98, 1251-1286.	4.8	0
21	Steganalysis of OpenPuff through atomic concatenation of AMP4 flags. Digital Investigation, 2015, 13, 15-21.	3.2	11
22	Smartphone image acquisition forensics using sensor fingerprint. IET Computer Vision, 2015, 9, 723-731.	2.0	8
23	Analysis of errors in exif metadata on mobile devices. Multimedia Tools and Applications, 2015, 74, 4735-4763.	3.9	10
24	On the limits of engine analysis for cheating detection in chess. Computers and Security, 2015, 48, 58-73.	6.0	9
25	Source identification for mobile devices, based on wavelet transforms combined with sensor imperfections. Computing (Vienna/New York), 2014, 96, 829-841.	4.8	10
26	A study on the false positive rate of Stegdetect. Digital Investigation, 2013, 9, 235-245.	3.2	6
27	Cryptanalysis of an EPC Class-1 Generation-2 standard compliant authentication protocol. Engineering Applications of Artificial Intelligence, 2011, 24, 1061-1069.	8.1	21
28	Flaws on RFID grouping-proofs. Guidelines for future sound protocols. Journal of Network and Computer Applications, 2011, 34, 833-845.	9.1	80
29	Practical attacks on a mutual authentication scheme under the EPC Class-1 Generation-2 standard. Computer Communications, 2009, 32, 1185-1193.	5.1	24
30	Bayesian rational exchange. International Journal of Information Security, 2008, 7, 85-100.	3.4	4
31	Secure content access and replication in pure P2P networks. Computer Communications, 2008, 31, 266-279.	5.1	14
32	Steganography in games: A general methodology and its application to the game of Go. Computers and Security, 2006, 25, 64-71.	6.0	41
33	Análisis y evaluación experimental del circuito generador de números aleatorios Lampert Circuit. Colección Jornadas Y Congresos, 0, , .	0.0	1