Paul Van Oorschot

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4807798/publications.pdf

Version: 2024-02-01

126 papers	8,610 citations	186265 28 h-index	118850 62 g-index
137 all docs	137 docs citations	137 times ranked	3575 citing authors

#	Article	IF	Citations
1	Authentication and authenticated key exchanges. Designs, Codes, and Cryptography, 1992, 2, 107-125.	1.6	806
2	The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. , 2012, , .		550
3	Parallel Collision Search with Cryptanalytic Applications. Journal of Cryptology, 1999, 12, 1-28.	2.8	401
4	Graphical passwords. ACM Computing Surveys, 2012, 44, 1-41.	23.0	376
5	A methodology for empirical analysis of permission-based security models and its application to android. , 2010, , .		314
6	Passwords and the evolution of imperfect authentication. Communications of the ACM, 2015, 58, 78-87.	4.5	177
7	White-Box Cryptography and an AES Implementation. Lecture Notes in Computer Science, 2003, , 250-270.	1.3	166
8	A Research Agenda Acknowledging the Persistence of Passwords. IEEE Security and Privacy, 2012, 10, 28-36.	1.2	150
9	Graphical Password Authentication Using Cued Click Points. Lecture Notes in Computer Science, 2007, , 359-374.	1.3	143
10	SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements. , 2013, , .		137
11	Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism. IEEE Transactions on Dependable and Secure Computing, 2012, 9, 222-235.	5.4	120
12	A second look at the usability of click-based graphical passwords. , 2007, , .		109
13	Multiple password interference in text passwords and click-based graphical passwords. , 2009, , .		102
14	Improving text passwords through persuasion. , 2008, , .		91
15	Parallel collision search with application to hash functions and discrete logarithms. , 1994, , .		89
16	On Diffie-Hellman Key Agreement with Short Exponents. Lecture Notes in Computer Science, 1996, , 332-343.	1.3	88
17	A Generic Attack on Checksumming-Based Software Tamper Resistance. , 0, , .		83
18	On interdomain routing security and pretty secure BGP (psBGP). ACM Transactions on Information and System Security, 2007, 10, 11.	4.5	72

#	Article	IF	Citations
19	Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer. Lecture Notes in Computer Science, 2007, , 88-103.	1.3	71
20	On the security of iterated message authentication codes. IEEE Transactions on Information Theory, 1999, 45, 188-199.	2.4	70
21	User interface design affects security: patterns in click-based graphical passwords. International Journal of Information Security, 2009, 8, 387-398.	3.4	70
22	Internet geolocation. ACM Computing Surveys, 2009, 42, 1-23.	23.0	69
23	MDx-MAC and Building Fast MACs from Hash Functions. Lecture Notes in Computer Science, 1995, , 1-14.	1.3	69
24	Purely Automated Attacks on PassPoints-Style Graphical Passwords. IEEE Transactions on Information Forensics and Security, 2010, 5, 393-405.	6.9	64
25	Revisiting Defenses against Large-Scale Online Password Guessing Attacks. IEEE Transactions on Dependable and Secure Computing, 2012, 9, 128-141.	5.4	61
26	On predictive models and user-drawn graphical passwords. ACM Transactions on Information and System Security, 2008, 10, 1-33.	4.5	59
27	Device fingerprinting for augmenting web authentication. , 2016, , .		58
28	Passwords: If Weâ€™re So Smart, Why Are We Still Using Them?. Lecture Notes in Computer Science, 2009, , 230-237.	1.3	56
29	Browser interfaces and extended validation SSL certificates. , 2009, , .		53
30	The developer is the enemy. , 2008, , .		52
31	Exploiting predictability in click-based graphical passwords*. Journal of Computer Security, 2011, 19, 669-702.	0.8	50
32	Hardware-Assisted Circumvention of Self-Hashing Software Tamper Resistance. IEEE Transactions on Professional Communication, 2005, 2, 82-92.	0.8	49
33	SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit. , 2017, , .		46
34	Secure Software Installation on Smartphones. IEEE Security and Privacy, 2011, 9, 42-48.	1.2	45
35	Revisiting Software Protection. Lecture Notes in Computer Science, 2003, , 1-13.	1.3	43
36	Usability of anonymous web browsing. , 2007, , .		43

#	Article	IF	Citations
37	Applications of combinatorial designs in computer science. ACM Computing Surveys, 1989, 21, 223-250.	23.0	42
38	SOMA. , 2008, , .		41
39	On instant messaging worms, analysis and countermeasures. , 2005, , .		40
40	Security and usability. , 2008, , .		40
41	On Purely Automated Attacks and Click-Based Graphical Passwords. , 2008, , .		39
42	A three-way investigation of a game-CAPTCHA. , 2014, , .		36
43	Privacy-enhanced sharing of personal content on the web. , 2008, , .		35
44	Understanding and improving app installation security mechanisms through empirical analysis of android. , 2012, , .		35
45	Tapas. , 2012, , .		34
46	User Study, Analysis, and Usable Security of Passwords Based on Digital Objects. IEEE Transactions on Information Forensics and Security, 2011, 6, 970-979.	6.9	33
47	Persuasion for Stronger Passwords: Motivation and Pilot Study. Lecture Notes in Computer Science, 2008, , 140-150.	1.3	33
48	On countering online dictionary attacks with login histories and humans-in-the-loop. ACM Transactions on Information and System Security, 2006, 9, 235-258.	4.5	31
49	Quantifying the security advantage of password expiration policies. Designs, Codes, and Cryptography, 2015, 77, 401-408.	1.6	31
50	On key distribution via true broadcasting. , 1994, , .		29
51	Exploring usability effects of increasing security in click-based graphical passwords. , 2010, , .		28
52	The Internet of Things: Security Challenges. IEEE Security and Privacy, 2019, 17, 7-9.	1.2	28
53	Modern key agreement techniques. Computer Communications, 1994, 17, 458-465.	5.1	27
54	Markets for zero-day exploits. , 2013, , .		26

#	Article	IF	Citations
55	Key recovery attack on ANSI X9.19 retail MAC. Electronics Letters, 1996, 32, 1568.	1.0	25
56	Leveraging personal devices for stronger password authentication from untrusted computers*. Journal of Computer Security, 2011, 19, 703-750.	0.8	24
57	An Empirical Evaluation of Security Indicators in Mobile Web Browsers. IEEE Transactions on Mobile Computing, 2015, 14, 889-903.	5.8	24
58	CPV: Delay-Based Location Verification for the Internet. IEEE Transactions on Dependable and Secure Computing, 2017, 14, 130-144.	5.4	23
59	Revisiting password rules: facilitating human management of passwords. , 2016, , .		21
60	A geometric approach to root finding in GT(q/sup m/). IEEE Transactions on Information Theory, 1989, 35, 444-453.	2.4	20
61	Pushing on string. Communications of the ACM, 2016, 59, 66-74.	4.5	19
62	Security Analysis and Related Usability of Motion-Based CAPTCHAs: Decoding Codewords in Motion. IEEE Transactions on Dependable and Secure Computing, 2014, 11, 480-493.	5.4	18
63	Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?. Lecture Notes in Computer Science, 2012, , 86-103.	1.3	18
64	What Lies Beneath? Analyzing Automated SSH Bruteforce Attacks. Lecture Notes in Computer Science, 2016, , 72-91.	1.3	17
65	Onboarding and Software Update Architecture for IoT Devices. , 2019, , .		15
66	S-RIP: A Secure Distance Vector Routing Protocol. Lecture Notes in Computer Science, 2004, , 103-119.	1.3	13
67	Countering Identity Theft Through Digital Uniqueness, Location Cross-Checking, and Funneling. Lecture Notes in Computer Science, 2005, , 31-43.	1.3	13
68	A monitoring system for detecting repeated packets with applications to computer worms. International Journal of Information Security, 2006, 5, 186-199.	3.4	13
69	Deadbolt. , 2013, , .		13
70	Accurate One-Way Delay Estimation With Reduced Client Trustworthiness. IEEE Communications Letters, 2015, 19, 735-738.	4.1	13
71	Exploring the Usability of CAPTCHAS on Smartphones: Comparisons and Recommendations. , 2015, , .		13
72	Tracking Darkports for Network Defense. , 2007, , .		12

#	Article	IF	Citations
73	Server Location Verification (SLV) and Server Location Pinning. ACM Transactions on Privacy and Security, 2018, 21, 1-26.	3.0	12
74	A Protocol for Secure Public Instant Messaging. Lecture Notes in Computer Science, 2006, , 20-35.	1.3	12
75	Security analysis of the message authenticator algorithm (MAA). European Transactions on Telecommunications, 1997, 8, 455-470.	1.2	11
76	Accurate Manipulation of Delay-based Internet Geolocation. , 2017, , .		11
77	Network scan detection with LQS. , 2011, , .		10
78	A multi-word password proposal (gridWord) and exploring questions about science in security research and usable security evaluation. , 2011, , .		10
79	Comparative Analysis and Framework Evaluating Web Single Sign-on Systems. ACM Computing Surveys, 2021, 53, 1-34.	23.0	10
80	Improving Security Visualization with Exposure Map Filtering. , 2008, , .		9
81	The Future of Authentication. IEEE Security and Privacy, 2012, 10, 22-27.	1.2	9
82	Science of Security: Combining Theory and Measurement to Reflect the Observable. IEEE Security and Privacy, 2018, 16, 12-22.	1.2	9
83	Addressing Online Dictionary Attacks with Login Histories and Humans-in-the-Loop. Lecture Notes in Computer Science, 2004, , 39-53.	1.3	9
84	Exploration and Field Study of a Password Manager Using Icon-Based Passwords. Lecture Notes in Computer Science, 2012, , 104-118.	1.3	8
85	On the security and usability of dynamic cognitive game CAPTCHAs. Journal of Computer Security, 2017, 25, 205-230.	0.8	8
86	CROO: A Universal Infrastructure and Protocol to Detect Identity Fraud. Lecture Notes in Computer Science, 2008, , 130-145.	1.3	8
87	Subgroup Refinement Algorithms for Root Finding in $GF(q)$. SIAM Journal on Computing, 1992, 21, 228-239.	1.0	7
88	Taxing the Queue: Hindering Middleboxes From Unauthorized Large-Scale Traffic Relaying. IEEE Communications Letters, 2015, 19, 42-45.	4.1	7
89	SoK: Securing Emailâ€"A Stakeholder-Based Analysis. Lecture Notes in Computer Science, 2021, , 360-390.	1.3	7
90	Evaluation in the absence of absolute ground truth: toward reliable evaluation methodology for scan detectors. International Journal of Information Security, 2013, 12, 97-110.	3.4	6

#	Article	IF	Citations
91	Location verification on the Internet: Towards enforcing location-aware access policies over Internet clients. , 2014, , .		6
92	Baton. , 2014, , .		6
93	Heuristics for the evaluation of captchas on smartphones. , 2015, , .		6
94	A Comparison of Practical Public-Key Cryptosystems based on Integer Factorization and Discrete Logarithms. Lecture Notes in Computer Science, 1991, , 577-581.	1.3	6
95	Security visualization tools and IPv6 addresses. , 2009, , .		5
96	Reducing Unauthorized Modification of Digital Objects. IEEE Transactions on Software Engineering, 2012, 38, 191-204.	5.6	5
97	An Alternate Explanation of two BAN-logic â€œfailuresâ€. Lecture Notes in Computer Science, 1994, , 443-447.	1.3	5
98	Addressing SMTP-Based Mass-Mailing Activity within Enterprise Networks. Proceedings of the Computer Security Applications Conference, 2006, , .	0.0	4
99	A control point for reducing root abuse of file-system privileges. , 2010, , .		4
100	Mercury: Recovering Forgotten Passwords Using Personal Devices. Lecture Notes in Computer Science, 2012, , 315-330.	1.3	4
101	Analysis, Implications, and Challenges of an Evolving Consumer IoT Security Landscape. , 2019, , .		4
102	On splitting sets in block designs and finding roots of polynomials. Discrete Mathematics, 1990, 84, 71-85.	0.7	3
103	Discovering Packet Structure through Lightweight Hierarchical Clustering. , 2008, , .		3
104	Reducing threats from flawed security APIs: The banking PIN case. Computers and Security, 2009, 28, 410-420.	6.0	3
105	Countering unauthorized code execution on commodity kernels: A survey of common interfaces allowing kernel code modification. Computers and Security, 2011, 30, 571-579.	6.0	3
106	System security, platform security and usability. , 2010, , .		3
107	Handbook of Applied Crytography.. American Mathematical Monthly, 1999, 106, 85.	0.3	2
108	VideoTicket. , 2008, , .		2

#	Article	IF	Citations
109	Revisiting network scanning detection using sequential hypothesis testing. Security and Communication Networks, 2012, 5, 1337-1350.	1.5	2
110	Blockchains and Stealth Tactics for Teaching Security. IEEE Security and Privacy, 2020, 18, 3-5.	1.2	2
111	Localization of credential information to address increasingly inevitable data breaches. , 2008, , .		2
112	A View of Security as 20 Subject Areas in Four Themes. IEEE Security and Privacy, 2022, 20, 102-108.	1.2	2
113	Accommodating IPv6 Addresses in Security Visualization Tools. Information Visualization, 2011, 10, 107-116.	1.9	1
114	Location Verification of Wireless Internet Clients: Evaluation and Improvements. IEEE Transactions on Emerging Topics in Computing, 2017, 5, 563-575.	4.6	1
115	Software Security and Systematizing Knowledge. IEEE Security and Privacy, 2019, 17, 4-6.	1.2	1
116	Toward Unseating the Unsafe C Programming Language. IEEE Security and Privacy, 2021, 19, 4-6.	1.2	1
117	Coevolution of Securityâ€™s Body of Knowledge and Curricula. IEEE Security and Privacy, 2021, 19, 83-89.	1.2	1
118	Malicious Software. Information Security and Cryptography, 2021, , 183-211.	0.3	1
119	User Authenticationâ€"Passwords, Biometrics and Alternatives. Information Security and Cryptography, 2021, , 55-90.	0.3	1
120	Software Securityâ€"Exploits and Privilege Escalation. Information Security and Cryptography, 2020, , 155-182.	0.3	1
121	Untangling Security and Privacy. IEEE Security and Privacy, 2020, 18, 4-6.	1.2	0
122	Comparative Analysis and Framework Evaluating Mimicry-Resistant and Invisible Web Authentication Schemes. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 534-549.	5.4	0
123	Public-Key Certificate Management and Use Cases. Information Security and Cryptography, 2021, , 213-244.	0.3	0
124	Cryptographic Building Blocks. Information Security and Cryptography, 2021, , 29-53.	0.3	0
125	Web and Browser Security. Information Security and Cryptography, 2021, , 245-279.	0.3	0
126	Authentication Protocols and Key Establishment. Information Security and Cryptography, 2021, , 91-124.	0.3	0