Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
Departamentul Automatica si Informatica Aplicata
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

Centralizator Standarde minimale necesare si obligatorii

1. Structura activitătii candidatului								Activitate candidat		
Nr. crt.	Domeniul activităților			Subcategorii		Indicatori (kpi)	Criterii minime necesare (PROFESOR)	Numar realizat		Suma indicatori realizati
0	1	2	3	4		5	6P	7		8.00
1	Activitatea didacica si profesionala (A1)	Carti si capitole în carti de specialitate in edituri recunoscute	Carti/ monografii/ capitole ca autor	A1.1.1	internationale	25	4 carti/capitole	5	0	0.00
				A1.1.2	nationale	20			5	100.00
		Material didactic / Lucrari didactice	Manuale didactice	A1.2.1		10	2 materiale didactice	2	2	20.00
							Σ kpi ≥ 100			120.00
2	Activitatea de cercetare (A2)	Articole in reviste cotate si in volumele unor manifestari stiintifice indexate ISI proceedings		A2.1		(25+20 * factor impact) / nr.de aut	12 articole	19 articole ISI		373.90
		Factor de impact cumulat pentru publicatii					6	9.135		
		Articole in reviste si volumele unor manifestari stiintifice indexate in alte baze de date internationale (BDI)		A2.2		20 / nr.de autori		25		238.35
		Proprietate intelectuala, brevete de inventie, certificate ORDA		A2.3.1	internationale	35 / nr.de autori		1 patent international		11.67
				A2.3.2	nationale	25 / nr.de autori		0		0.00
		Granturi / proiecte castigate prin competitie	Director/ responsabil	A2.4.1.1	internationale	20 * ani de desfasurare	2 granturi/ proiecte	3 granturi ca director	0	0.00
				A2.4.1.2	nationale	10 * ani de desfasurare			3	30.00
				A2.4.2.1	internationale	4 * ani de desfasurare		2		16.00

			Membru in echipa	A2.4.2.2	nationale	2 * ani de desfasurare		**1**		6.00
							Σ kpi ≥ 500			**675.92**
3	**Recunoasterea si impactul activitatii (A3)**	Citari in carti, reviste si volume ale unor manifestari stiintifice		A3.1.1	carti, ISI	8 / nr aut art.citat	**20 citari**	**116 citari**	**31**	126.00
				A3.1.2	BDI	4 / nr aut art.citat			**85**	160.33
		Prezentari invitate in plenul unor manifestari stiintifice nationale si internationale și Profesor invitat	Punctaj unic pentru fiecare activitate	A3.2.1	internationale	10		**9**		90.00
				A3.2.2	nationale	5		**1**		5.00
		Membru in colectivele de redactie sau comitete stiintifice ale revistelor, organizator de manifestari stiintifice, internationale indexate ISI	Punctaj unic pentru fiecare activitate	A3.3.1	ISI	10		**12**		120.00
				A3.3.2	BDI	6		**17**		96.00
				A3.3.3	nationale si internationale neindexate	3		**2**		6.00
		Premii in domeniu		A3.4.1	Academia Romana, ASTR, academii de ramura, premii internationale	15		**0**		0.00
				A3.4.2	premii nationale in domeniu	5		**5**		25.00
							Σ kpi ≥ 100			**628.33**
Indicatorul de merit (A = A1+A2+A3)						**Σ k1i + Σ k2i + Σ k3i**	700			**1424.25**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A1.1.1 - Carti si capitole în carti de specialitate in edituri recunoscute - internationale

Nr. crt.	Lucrarea publicata	Indicator realizat
1	Frédéric Cuppens, Simon Foley, Bogdan Groza, Marius Minea (Eds.): CRiSIS 2011, Proceedings of the Sixth International Conference on Risks and Security of Internet and Systems, IEEE Catalog Number CFP1161F-ART, ISBN 978-1-4577-1891-5 **(doar merite editoriale, nu se revendica punctaj)**	0
	TOTAL	**0**

A1.1.2 - Carti si capitole în carti de specialitate in edituri recunoscute - nationale

Nr. crt.	Lucrarea publicata	Indicator realizat
1	Groza Bogdan, Constructii criptografice hibride bazate pe tehnici simetrice si asimetrice, aplicatii in sisteme de conducere, Editura Politehnica, Teza de Doctorat, Timisoara, ISBN: 978-973-625-688-2, 131 p., 2008	20
2	Groza Bogdan, Introducere in criptografie: functii criptografice, fundamente matematice si computationale, Editura Politehnica, Timisoara, ISBN 978-606-554-499-4, 200 p., 2012	20
3	Bogdan Groza, Introducere in Sistemele Criptografice cu Cheie Publica, Editura Politehnica Timisoara, ISBN 978-973-625-564-9, 136 p., 2007	20
4	Bogdan Groza, Introducere in Inteligenta Artificiala, Aplicatii cu Strategii de Cautare Neinformate si Informate, Editura PolitehnicaTimisoara, ISBN 978-973-625-779-7, 89 p., 2008	20
5	Bogdan Groza, Editura Politehnica, Cryptography - Application Notes in C, .NET and Java, Editura Politehnica Timisoara, ISBN 978-606-35-0024-4, 84 p., 2015	20
	TOTAL	**100**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A1.2.1 - Material didactic / Lucrari didactice

Nr. crt.	Lucrarea publicata	Indicator realizat
1	Bogdan Groza, Note de curs la criptografie in limba engleza cu titlul "Theoretical Background on Cryptographic Primitives"disponibile la http://www.aut.upt.ro/~bgroza/Books/Crypto_Introduction.pdf	10
2	Stefan Murvay, Horatiu Gurban, Bogdan Groza, Note de laborator in format electronic "A Practical Introduction to Microcontroller Programming with S12", disponibil la http://www.aut.upt.ro/~bgroza/Books/S12Works.pdf	10
	TOTAL	**20**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A2.1 - Articole in reviste cotate si in volumele unor manifestari stiintifice indexate ISI proceedings

Nr. crt.	Lucrarea publicata	Nr. autori	Factor impact	Indicator realizat
1	Cristea, M.; Groza, B., "Fingerprinting Smartphones Remotely via ICMP Timestamps," *Communications Letters, IEEE* , vol.17, no.6, pp.1081,1083, June 2013, ISSN 1089-7798.	2	1.268	25.18
2	Groza, B.; Murvay, S., "Efficient Protocols for Secure Broadcast in Controller Area Networks," *Industrial Informatics, IEEE Transactions on* , vol.9, no.4, pp.2034,2042, Nov. 2013, ISSN 1551-3203.	2	0	12.5
3	Bogdan Groza, Bogdan Warinschi, "Client puzzles and DoS resilience, Revisited", Designs Codes and Cryptography, Springer-Verlag, April 2013. ISSN: 0925-1022	2	0.958	22.08
4	B. Groza, M. Minea, M. Cristea, P.S. Murvay, M. Iacob, "Protocol vulnerabilities in practice: causes, modeling and automatic detection", Proceedings of the Romanian Academy, Series A, Vol. 13, No. 2, April-June, 2012.	5	1.658	11.63
5	Groza, B.; Murvay, S., "Source Identification Using Signal Characteristics in Controller Area Networks" Signal Processing Letters, IEEE, (published Jan. 2014), ISSN 1070-9908	2	1.751	30.01
6	Groza, Bogdan, and Pal-Stefan Murvay. "Broadcast Authentication in a Low Speed Controller Area Network." E-Business and Telecommunications, Springer Berlin Heidelberg, revised post-proceedings version of our article "Higher layer authentication for broadcast in Controller Area Networks" Proc. 6th International Conference on Security and Cryptography (SECRYPT'11), 2012. 330-344.	2	0.25	15
7	Groza, Bogdan, and Marius Minea. "A formal approach for automated reasoning about off-line and undetectable on-line guessing." *Financial Cryptography and Data Security* . Springer Berlin Heidelberg, 2010. 391-399. **(Rank A)**	2	0.25	15
8	Groza, Bogdan, and Marius Minea. "A calculus to detect guessing attacks."*Information Security* . Springer Berlin Heidelberg, 2009. 59-67. **(Rank B)**	2	0.25	15
9	Groza, Bogdan, and Lavinia E. Dragomir. "A multidisciplinary project: How to turn a webcam into a secure-cam." *Applied Computational Intelligence and Informatics, 2009. SACI'09. 5th International Symposium on* . IEEE, 2009.	2	0.25	15
10	Groza, Bogdan. "Analysis of a password strengthening technique and its practical use." *Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on* . IEEE, 2009.	1	0.25	30
11	Groza, Bogdan, and T-L. Dragomir. "Using a cryptographic authentication protocol for the secure control of a robot over TCP/IP." *Automation, Quality and Testing, Robotics, 2008. AQTR 2008. IEEE International Conference on* . Vol. 1. IEEE, 2008.	2	0.25	15
12	Groza, Bogdan, Dragos Pop, and Ioan Silea. "Java implementation of an authentication protocol with application on mobile phones." *Automation, Quality and Testing, Robotics, 2008. AQTR 2008. IEEE International Conference on* . Vol. 1. IEEE, 2008.	3	0.25	10
13	Groza, Bogdan. "Broadcast authentication protocol with time synchronization and quadratic residues chain." *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on* . IEEE, 2007. **(Rank B)**	1	0.25	30
14	Groza, Bogdan. "An Extension of the RSA Trapdoor in a KEM/DEM Framework." *Symbolic and Numeric Algorithms for Scientific Computing, 2007. SYNASC. International Symposium on* . IEEE, 2007.	1	0.25	30

15	Groza, Bogdan. "On the use of the discrete power function for building public-key cryptosystems." International Conference on Applied Informatics and Communications, 2007	1	0.25	30
16	Groza, Bogdan, Simona Barbu, Mariana Bilanin, Dorina Petrica, "Implementation of an Authentication Protocol for Sending Audio-Video Information in Java." *Applied Computational Intelligence and Informatics, 2007. SACI'07. 4th International Symposium on* . IEEE, 2007.	4	0.25	7.5
17	Groza, Bogdan, and Toma-Leonida Dragomir. "On the use of one-way chain based authentication protocols in secure control systems." *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on* . IEEE, 2007. **(Rank B)**	2	0.25	15
18	Groza, Bogdan. "Using one-way chains to provide message authentication without shared secrets." *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on* . IEEE, 2006.	1	0.25	30
19	Groza, Bogdan, and Dorina Petrica. "Cryptanalysis of an authentication protocol." *Symbolic and Numeric Algorithms for Scientific Computing, 2005. SYNASC 2005. Seventh International Symposium on* . IEEE, 2005.	2	0.25	15
	TOTAL		**9.135**	**373.9**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A2.2 - Articole in reviste si volumele unor manifestari stiintifice indexate in alte baze de date internationale (BDI)

Nr. crt.	Lucrarea publicata	Baza de date	Nr. autori	Indicator realizat
1	Bogdan Groza, Rene Mayrhofer, SAPHE - Simple Accelerometer based wireless Pairing with HEuristic trees, Proc. 10th International Conference on Advances in Mobile Computing and Multimedia (MoMM'12), ACM, 2012. **(Rank B)**	BDI (DBLP, etc.)	2	10
2	Paula Vasile, Bogdan Groza, Stefan Murvay, Performance analysis of broadcast authentication protocols on CAN-FD and FlexRay, 10th Workshop on Embedded Systems Security (affiliated to ESWEEK'15), 2015.	ACM	3	6.67
3	Cristina Solomon, Bogdan Groza, LiMon - lightweight authentication for tire pressure monitoring sensors, 1st Workshop on the Security of Cyber-Physical Systems (affiliated to ESORICS'15), 2015.	Google Scholar	2	10
4	*Bogdan Groza, Stefan Murvay, Anthony van Herrewege, Ingrid Verbauwhede, LiBrA-CAN: a Lightweight Broadcast Authentication protocol for Controller Area Networks, Proc. 11th International Conference on Cryptology and Network Security (CANS'12), Springer-Verlag, LNCS, 2012.* ***(Rank B)***	BDI (DBLP, etc.)	4	5
5	*Bogdan Groza, Bogdan Warinschi, Revisiting difficulty notions for client puzzles and DoS resilience, Proc. 15th Information Security Conference (ISC'12), Springer-Verlag, LNCS vol. 7483, pp. 39-54, 2012.* ***(Rank B)***	BDI (DBLP, etc.)	2	10
6	*Bogdan Groza, Marius Cristea, Mihai Iacob, Some Security Issues In SCALANCE Wireless Industrial Networks. Proc. 6th International Conference on Availability, Reliability and Security (ARES'11), IEEE Comp. Soc., pp. 493 - 498, 2011.* ***(Rank B)***	BDI (DBLP, etc.)	3	6.67
7	*Bogdan Groza, Marius Minea, Formal modelling and automatic detection of resource exhaustion attacks. Proc. 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS'11), pp. 326-333, ACM, 2011.* ***(Rank B)***	BDI (DBLP, etc.)	2	10
8	*Bogdan Groza, Marius Minea, Customizing protocol specifications for detecting resource exhaustion and guessing attacks. Proc. 9th International Symposium on Formal Methods for Components and Objects (FMCO'10), Springer-Verlag, LNCS vol. 6957, pp. 45-60, 2010.*	BDI (DBLP, etc.)	2	10
9	S. Murvay, B. Groza, Performance improvements for SHA-3 finalists by exploiting microcontroller on-chip parallelism. Proceedings of International Conference on Risks and Security of Internet and Systems (CRiSIS'11), IEEE Comp. Soc., 2011.	BDI (DBLP, etc.)	2	10
10	B. Groza, S. Murvay, Secure Broadcast with One-time Sigantures in Controller Area Networks. Proceedings of International Conference on Availability, Reliability and Security (ARES'11), IEEE Comp. Soc., 2011. **(Rank B)**	BDI (DBLP, etc.)	2	10
11	M. Cristea, B. Groza, Augmenting a webmail application with cryptographic puzzles to deflect spam, IFIP International Conference on New Technologies, Mobility and Security (NTMS'11), IEEE Comp. Soc., 2011.	BDI (DBLP, etc.)	2	10
12	B. Groza, D. Pop, I. Silea, V. Patriciu, Towards Developing Secure Video Surveillance Systems over IP, 4th International Conference on Internet Monitoring and Protection, ICIMP'09, pp.27-33, IEEE Comp. Soc., 2009.	BDI (IEEE)	4	5

13	B. Groza , P.S. Murvay, I. Silea, T. Ionica, Cryptographic authentication on a 8051 based development board, The Third International Conference on Internet Monitoring and Protection, ICIMP'08, IEEE Comp. Soc., 2008	BDI (IEEE)	4	5
14	Bogdan Groza and Toma-Leonida Dragomir. Experimenting with the secure control of a robot over tcp/ip. Automation Computers, Applied Mathematics Journal (ACAM), 2008.	BDI (Google Scholar)	2	10
15	B. Groza, Broadcast authentication with practically unbounded one-way chains, JOURNAL OF SOFTWARE (JSW), Volume 3, Issue 2, ISSN: 1796-217X, Academy Publishers, 2008.	BDI (DBLP, etc.)	1	20
16	B. Groza, D. Petrica, T.L. Dragomir, Using the Discrete Squaring Function in the Delayed Message Authentication Protocol, Proceedings of International Conference on Internet Surveillance and Protection, ICISP'06, Cap-Esterel, France, IEEE Comp. Soc., 2006.	BDI (IEEE)	3	6.67
17	B. Groza, D. Petrica, T.L. Dragomir, A time-memory trade to generate one-time passwords using quadratic residues over Zn, Studies in Informatics and Control vol. 14 no. 3, 2005.	BDI (INSPEC, etc.)	3	6.67
18	Bogdan Groza and Stefan Murvay. Secure broadcast with one-time signatures in controller area networks. International Journal of Mobile Computing and Multimedia Communications (IJMCMC) IJMCMC, pages 1{18, 2013.	BDI (INSPEC, etc.)	2	10
19	Stefan Murvay and Bogdan Groza. Performance evaluation of sha-2 standard vs. sha-3 finalists on two Freescale platforms. International Journal of Secure Software Engineering IJSSE, 2013.	BDI (INSPEC, etc.)	2	10
20	Bogdan Groza and Marius Minea. Bridging dolev-yao adversaries and control systems with time-sensitive channels. In Conference on Critical Information Infrastructures Security (CRITIS). Springer, 2013.	BDI (DBLP, etc.)	2	10
21	Construction techniques for one-way chains and their use in authentication B Groza - Journal of Control Engineering and Applied Informatics, 2006	BDI (Google Scholar	1	20
22	Marius Cristea and Bogdan Groza. Provable synthetic coordinates for increasing pows effectiveness against dos andspam. In International Confernece on Privacy, Security, Risk and Trust (PASSAT), pages 809{810. IEEE, 2012.	BDI (DBLP, etc.)	2	10
23	Bogdan Groza and Dorina Petrica. On chained cryptographic puzzles. In 3rd Romanian-Hungarian Joint Symposium on Applied Computational Intelligence (SACI), pages 25{26. Citeseer, 2006.	BDI (Google Scholar, CiteSeer)	2	10
24	Groza, Bogdan, and Dorina Petrica. "One-time passwords for uncertain number of authentications." Proceedings of CSCS15 (2005).	BDI (Google Scholar	2	10
25	Groza, Bogdan, Dorina Petrica, and Toma-Leonida Dragomir. "SECURITY BASED ON CRYPTOGRAPHIC TECHNIQUES FOR REMOTE CONTROL SYSTEMS." SINTES 12, 20-22.	BDI (Google Scholar	3	6.67
	TOTAL			**238.35**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A2.3.1 - Proprietate intelectuala, brevete de inventie, certificate ORDA - Internationale

Nr. crt.	Lucrarea certificata	Nr. autori	Indicator realizat
1	G. Tipa (Continental Automotives), B. Groza (UPT), R. Ragobete (Continental Automotives), Schema for generating true random numbers on automotive embedded devices, European Patent Application Number 14465511.5 - 1953/28.05.14., Published as EP2950201 (A1) on 02.12.2015	3	11.67
	TOTAL		**11.67**

A2.3.2 - Proprietate intelectuala, brevete de inventie, certificate ORDA - Nationale

Nr. crt.	Lucrarea certificata	Nr. autori	Indicator realizat
1			
2			
	TOTAL		**0**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A2.4.1.1 - Granturi / proiecte castigate prin competitie - Internationale - ca Director / responsabil

Nr. crt.	Grantul / proiectul	Nr. ani desfasurare	Indicator realizat
1	MC National (Comitet Management National), ICT COST Action IC1306 Cryptography for Secure Digital Interaction (2013-2017), http://www.cost.eu/domains_actions/ict/Actions/IC1306?management **(MC prin aderare - nu se revendica punctaj)**	2	0
	TOTAL		**0**

A2.4.1.2 - Granturi / proiecte castigate prin competitie - Nationale - ca Director / responsabil

Nr. crt.	Grantul / proiectul	Nr. ani desfasurare	Indicator realizat
1	Bogdan Groza, Cryptographic Security for Automotive Embedded Devices and Networks, **PN-II-RU-TE-2014-4-1501**, 2015-2017	1	10
2	Bogdan Groza, Protocoale criptografice de autentificare prin coduri mac cu chei inlantuite si cu sincronizare temporala sau challenge-response si prin semnaturi digitale multiple-time sau one-time in arbori Merkle, **PN-II-RU-TD-2007-2 122/2007**, 2007-2008 (1 an)	1	10
3	Bogdan Groza, Protocoale de securitate si tehnici criptografice bazate pe functii one-way pentru asigurarea autenticitatii informatiei, GRANT **CNCSIS TD 90/2006**, 2006 (1 an)	1	10
	TOTAL		**30**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A2.4.2.1 - Granturi / proiecte castigate prin competitie - Internationale - ca Membru in echipa

Nr. crt.	Grantul / proiectul	Nr. ani desfasurare	Indicator realizat
1	FP7 Automated VAlidatioN of Trust and Security of Service-oriented Architectures AVANTSSAR, FP7-ICT-2007-1 Project no. 216471, 2008-2011 (director Conf.Dr.Ing. Marius Minea)	3	12
2	FP7 SPaCIoS: Secure Provision and Consumption in the Internet of Services Project no. 257876, FP7-ICT-2009-5, ICT-2009.1.4: Trustworthy ICT 01/10/2010 - 30/09/2013 (director Conf.Dr.Ing. Marius Minea)	1	4
	TOTAL		**16**

A2.4.2.2 - Granturi / proiecte castigate prin competitie - Nationale - ca Membru in echipa

Nr. crt.	Grantul / proiectul	Nr. ani desfasurare	Indicator realizat
1	Ioan Silea, Bogdan Groza, Stefan Murvay, Dragos Pop, Raul Robu, Radu Precup, Cercetări în designul şi implementarea unor soluţii moderne pentru securitatea informaţiei în sisteme distribuite, SCADA, DCS şi de control la distanţă cu aplicaţii în distribuţia gazelor, ID_940, PN II - IDEI, 2008-2011, director Prof. Dr. Ing. Ioan Silea.	3	6
	TOTAL		**6**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A3.1.1 - Citari in carti, reviste si volume ale unor manifestari stiintifice indexate ISI

Nr. crt.	Sursa citare	Lucrarea citata	Nr. autori lucrare citata	Indicator realizat
1	Grover, Kanika, Lim, Alvin, A survey of broadcast authentication schemes for wireless networks, AD HOC NETWORKS Volume: 24 Pages: 288-316 DOI: 10.1016/j.adhoc.2014.06.008 Part: A Published: JAN 2015, Accession Number: WOS:000347581200020	Groza, B., Broadcast authentication with practically unbounded one-way chains	1	8.00
2	Zhang, YX (Zhang, Yingxian)[1] ; Liu, AJ (Liu, Aijun)[1] ; Pan, XF (Pan, Xiaofei)[1] ; Ye, Z (Ye, Zhan), A Secure MQAM Scheme Based on Signal Constellation Hopping, KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, 2014	Source Identification Using Signal Characteristics in Controller Area Networks	2	4.00
3	Adao, P (Adao, Pedro)[1,2] ; Mateus, P (Mateus, Paulo)[1,3] ; Vigano, L (Vigano, Luca)[4], Protocol insecurity with a finite number of sessions and a cost-sensitive guessing intruder is NP-complete, THEORETICAL COMPUTER SCIENCE, 2015	Groza, Bogdan, and Marius Minea. "Formal modelling and automatic detection of resource exhaustion attacks." Proceedings of the 6th AsiaCCS. ACM, 2011.	2	4.00
4	Chang, J (Chang, Jing)[1] ; Xue, R (Xue, Rui)[1], A Framework Based on Time and Space for Analyzing Denial of Service Attacks, 4th International Symposium on Information Science and Engineering (ISISE), 2012	ibidem	2	4.00
5	Bruni, A (Bruni, Alessandro)[1] ; Sojka, M (Sojka, Michal); Nielson, F (Nielson, Flemming)[1] ; Nielson, HR (Nielson, Hanne Riis)[1], Formal Security Analysis of the MaCAN Protocol, 11th International Conference on Integrated Formal Methods (IFM), 2014	Groza, Bogdan, et al. "LiBrA-CAN: a Lightweight Broadcast Authentication protocol for Controller Area Networks." Cryptology and Network Security. Springer Berlin Heidelberg, 2012. 185-200.	4	2.00
6	Sikora, A; Berbineau, M; Vinel, A; Jonsson, M; Pirovano, A; Aguado, M, Attack Potential and Efficient Security Enhancement of Automotive Bus Networks Using Short MACs with Rapid Key Change, 6th International Workshop on Communication Technologies for Vehicles (Nets4Cars- Nets4Trains-Nets4Aircraft), 2014	ibidem	4	2.00
7	Lin, CW (Lin, Chung-Wei)[1] ; Zhu, Q (Zhu, Qi); Phung, C (Phung, Calvin); Sangiovanni-Vincentelli, A (Sangiovanni-Vincentelli, Alberto)[1], Security-Aware Mapping for CAN-Based Real-Time Distributed Automotive Systems, 32nd IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2013	ibidem	4	2.00
8	Bittl, S (Bittl, Sebastian), Attack Potential and Efficient Security Enhancement of Automotive Bus Networks Using Short MACs with Rapid Key Change, COMMUNICATION TECHNOLOGIES FOR VEHICLES, NETS4CARS/NETS4TRAINS/NETS4AIRCRAFT 2014 Book Series: Lecture Notes in Computer Science Volume: 8435 Pages: 113-125 Published: 2014, Accession Number: WOS:000342904600011	ibidem	4	2.00
9	Ezaki, Takaya, Tomohiro Date, and Hiroyuki Inoue. "An Analysis Platform for the Information Security of In-Vehicle Networks Connected with External Networks." Advances in Information and Computer Security. Springer International Publishing, 2015. 301-315.	ibidem	4	2
10	Sethi, M (Sethi, Mohit)[1] ; Antikainen, M (Antikainen, Markku); Aura, T (Aura, Tuomas), Commitment-based device pairing with synchronized drawing, 12th IEEE International Conference on Pervasive Computing and Communication (PERCOM) 2014	Groza, Bogdan, and Rene Mayrhofer. "SAPHE: simple accelerometer based wireless pairing with heuristic trees."	2	4.00
11	Antikainen, M (Antikainen, Markku); Sethi, M (Sethi, Mohit); Matetic, S (Matetic, Sinisa); Aura, T (Aura, Tuomas), Commitment-based device-pairing protocol with synchronized drawings and comparison metrics, PERVASIVE AND MOBILE COMPUTING Volume: 16 Special Issue: SI Pages: 205-219 DOI: 10.1016/j.pmcj.2014.10.006 Part: B Published: JAN 2015, Accession Number: WOS:000349759800003	ibidem	2	4.00

12	Han, K (Han, Kyusuk)[1] ; Potluri, SD (Potluri, Swapna Divya)[1] ; Shin, KG (Shin, Kang G.)[1], On Authentication in a Connected Vehicle: Secure Integration of Mobile Devices with Vehicular Networks, 4th IEEE/ACM International Conference on Cyber-Physical Systems (ICCPS) 2013	Groza, Bogdan, and Pal-Stefan Murvay. "Broadcast Authentication in a Low Speed Controller Area Network." E-Business and Telecommunications. Springer Berlin Heidelberg, 2012. 330-344.	2	4.00
13	Fujimoto, Y (Fujimoto, Yasutaka)[1] ; Ohishi, K (Ohishi, Kiyoshi), Newest Developments and Recent Trends in Sensors and Actuators - A Survey, 39th Annual Conference of the IEEE Industrial-Electronics-Society (IECON), 2013	Groza, Bogdan, and Pal-Stefan Murvay. "Efficient Protocols for Secure Broadcast Authentication in a Low Speed Controller Area Network.", 2013. IEEE Trans.	2	4.00
14	A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN, Woo, S (Woo, Samuel); Jo, HJ (Jo, Hyo Jin); Lee, DH (Lee, Dong Hoon) IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS Volume: 16 Issue: 2 Pages: 993-1006 DOI: 10.1109/TITS.2014.2351612, Published: APR 2015	ibidem	2	4.00
15	Wu, JD (Wu, Jiande); Du, J (Du, Jin); Lin, ZY (Lin, Zhengyu); Hu, YH (Hu, Yihua); Zhao, CW (Zhao, Chongwen); He, XM (He, Xiangning) Power Conversion and Signal Transmission Integration Method Based on Dual Modulation of DC-DC Converters, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS Volume: 62 Issue: 2 Pages: 1291-1300 DOI: 10.1109/TIE.2014.2336628 Published: FEB 2015	ibidem	2	4.00
16	Samant, PK (Samant, Pramit Kumar)[1] ; Saini, P (Saini, Poonam)[1] ; Challa, RK (Challa, Rama Krishna)[1], A Combined Request/Response and Time Delay Technique to detect Attacks in a PKI-Based Architecture for M-Commerce, 3rd IEEE International Advance Computing Conference (IACC), 2013	Groza, Bogdan. "Broadcast authentication protocol with time synchronization and quadratic residues chain." Availability, Reliability and Security, 2007. ARES 2007.	1	8.00
17	Horvat, G (Horvat, Goran)[1] ; Zagar, D (Zagar, Drago)[1] ; Martinovic, G (Martinovic, Goran)[1], STFTP: Secure TFTP Protocol for Embedded Multi-Agent Systems Communication, ADVANCES IN ELECTRICAL AND COMPUTER ENGINEERING, ISI, 2013	Groza, Bogdan, et al. "Cryptographic authentication on the communication from an 8051 based development board over UDP." Internet Monitoring and Protection, ICIMP' 2008.	4	2.00
18	Lin, Hsiung-Cheng; Liu, Liang-Yih; Pai, Kuo-Hung, A Microprocessor-Based Monitoring and Control System via Internet in Case Study of Pet Care, Conference: International Conference on Computational Materials Science (CMS 2011)	ibidem	4	2.00
19	Tritilanunt, S (Tritilanunt, Suratose), Performance Evaluation of Non-parallelizable Client Puzzles for Defeating DoS Attacks in Authentication Protocols, 24th Annual Conference on Data and Applications Security and Privacy, 2013	Groza, Bogdan, and Dorina Petrica. "On chained cryptographic puzzles." 3rd Romanian-Hungarian Joint Symposium on Applied Computational Intelligence (SACI), Timisoara, Romania. 2006.	2	4.00
20	Abliz, M (Abliz, Mehmud)[1] ; Znati, T (Znati, Taieb)[1], A Guided Tour Puzzle for Denial of Service Prevention, 25th Annual Computer Security Applications Conference, 2009	ibidem	2	4.00
21	Chen, LQ (Chen, Liqun)[1] ; Morrissey, P (Morrissey, Paul); Smart, NP (Smart, Nigel P.); Warinschi, B (Warinschi, Bogdan), Security Notions and Generic Constructions for Client Puzzles, 15th International Conference on the Theory and Application of Cryptology and Information Security, 2009	ibidem	2	4.00
22	Tritilanunt, S (Tritilanunt, Suratose)[1] ; Boyd, C (Boyd, Colin)[1] ; Foo, E (Foo, Ernest)[1] ; Nieto, JMG (Nieto, Juan Manuel Gonzalez)[1], Toward non-parallelizable client puzzles, 6th International Conference on Cryptology and Network Security, 2009	ibidem	2	4.00
23	Wan, M (Wan, Ming)[1] ; Shang, WL (Shang, Wenli)[1] ; Zhao, JM (Zhao, Jianming)[1] ; Zhang, SS (Zhang, Shengshan)[1], C2Puzzle: A Novel Computational Client Puzzle for Network Security, International Conference on Mechatronics and Semiconductor Materials (ICMSCM 2013)	ibidem	2	4.00
24	*of Service Resilience of Authentication Systems." IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications(2013): 451.* ***(carte)***	ibidem	2	4.00
25	Radu, T (Radu, Tomoiaga)[1] ; Mircea, S (Mircea, Stratulat)[1], The Behaviour of the Cryptographic Primitives in Case of Large Data Volumes, PROCEEDINGS OF THE 2010 8TH INTERNATIONAL CONFERENCE ON COMMUNICATIONS (COMM), 2010	Solga, M., Groza B. , Evaluarea performantelor computationale pentru functii criptografice simetrice si asimetrice, pe platformele Windows si Unix	2	4.00

26	Radu, T (Radu, Tomoiaga)[1] ; Mircea, S (Mircea, Stratulat)[1], The Behaviour of the Cryptographic Primitives in Case of Large Data Volumes, PROCEEDINGS OF THE 2010 8TH INTERNATIONAL CONFERENCE ON COMMUNICATIONS (COMM), 2010	Groza B. , Introducere in Sistemele Criptografice cu Cheie Publica Published: 2007	1	8.00
27	Radu, T (Radu, Tomoiaga)[1] ; Mircea, S (Mircea, Stratulat)[1], The Behaviour of the Cryptographic Primitives in Case of Large Data Volumes, PROCEEDINGS OF THE 2010 8TH INTERNATIONAL CONFERENCE ON COMMUNICATIONS (COMM), 2010	Groza B. , Universitatea Politehncă din Timişoara CONSTRUCŢII CRIPTOGRAFICE HIBRIDE, BAZATE PE TEHNICI SIMETRICE ŞI ASIMETRICE ,Teza de Doctorat, 2008	1	8.00
28	Ordi, Ali, et al. "A Novel WLAN Client Puzzle Against DoS Attack based on Pattern Matching."	Groza, Warinschi, Cryptographic puzzles and DoS resilience, revisited, Designs Codes and Cryptography, Springer, 2014	2	4.00
29	Meadows, Catherine. "Emerging Issues and Trends in Formal Methods in Cryptographic Protocol Analysis: Twelve Years Later." Logic, Rewriting, and Concurrency. Springer International Publishing, 2015. 475-492.	ibidem	2	4.00
30	Oka Saputra, Komang, Wei-Chung Teng, and Tsung-Han Chen. "Hough Transform-Based Clock Skew Measurement Over Network."	Groza, Cristea, Fingerprinting Smartphones Remotely via ICMP Timestamps, Comm. Lett, 2013	2	4.00
31	Khanna, Vimal K., REMOTE FINGERPRINTING OF MOBILE PHONES	ibidem	2	4.00
		TOTAL		**126**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A3.1.2 - Citari in carti, reviste si volume ale unor manifestari stiintifice indexate BDI

Nr. crt.	Sursa citare	Baza de date	Lucrarea citata	Nr. autori lucrare citata	Indicator realizat
1	Abliz, Mehmud, and Taieb Znati. "New Approach to Mitigating Distributed Service Flooding Attacks." ICONS 2012, The Seventh International Conference on Systems. 2012.	BDI (Google Scholar)	Groza, Bogdan, and Dorina Petrica. "On chained cryptographic puzzles." 3rd Romanian-Hungarian Joint Symposium on Applied Computational Intelligence (SACI), Timisoara, Romania. 2006.	2	2.00
2	Tritilanunt, Suratose. Protocol engineering for protection against denial-of-service attacks. Diss. Queensland University of Technology, 2009.	BDI (Google Scholar)	ibidem	2	2.00
3	M. Abliz Internet Denial of Service Attacks and Defense Mechanisms, PhD Thesis, University of Pittsburgh, 2011.	BDI (Google Scholar)	ibidem	2	2.00
4	Abliz, Mehmud, Taieb Znati, and Adam Lee. "Mitigating Distributed Service Flooding Attacks with Guided Tour Puzzles." International Journal On Advances in Security 5.3 and 4 (2012): 121-133.	BDI (Google Scholar)	ibidem	2	2.00
5	Jeckmans, A. J. P. "Practical client puzzle from repeated squaring." (2009), MsC Thesis, Twente University.	BDI (Google Scholar)	ibidem	2	2.00
6	Michalas, Antonis, Nikos Komninos, and Neeli R. Prasad. "Cryptographic Puzzles and Game Theory against DoS and DDoS attacks in Networks." (2008).	BDI (Google Scholar)	ibidem	2	2.00
7	Lin, H. C., et al. "A Remote Microprocessor-Based Monitoring and Control System via Internet in Case Study of Pet Care." Lecture Notes in Engineering and Computer Science 2191 (2011).	BDI (Scopus)	Groza, Bogdan, et al. "Cryptographic authentication on the communication from an 8051 based development board over UDP." Internet Monitoring and Protection, ICIMP' 2008.	4	1.00
8	Callaghan, David Michael. "Embedded database systems and methods in an industrial controller environment." U.S. Patent No. 7,467,018. 16 Dec. 2008.	BDI (Google Patents)	ibidem	4	1.00
9	Callaghan, David M. "Automation device data interface." U.S. Patent No. 7,565,351. 21 Jul. 2009.	BDI (Google Patents)	ibidem	4	1.00
10	Callaghan, David M., and Brian A. Batke. "Application and service management for industrial control devices." U.S. Patent No. 7,693,581. 6 Apr. 2010.	BDI (Google Patents)	ibidem	4	1.00
11	Callaghan, David M. "Reliable messaging instruction." U.S. Patent No. 7,706,895. 27 Apr. 2010.	BDI (Google Patents)	ibidem	4	1.00
12	Higuera Neira, Brayan Steven, and Luis F. Pedraza. "Implementación del algoritmo criptográfico AES (Advanced Encryption Standard) para un controlador de tráfico vehicular." Revista Tecnura 17 (2013): 35-48.	BDI (Google Scholar)	ibidem	4	1.00
13	Krauß, Christoph, Markus Schneider, and Claudia Eckert. "On handling insider attacks in wireless sensor networks." Information Security Technical Report 13.3 (2008): 165-172.	BDI (Google Scholar)	Groza, Bogdan. "Broadcast authentication protocol with time synchronization and quadratic residues chain." Availability, Reliability and Security, 2007. ARES 2007.	1	4.00
14	Krishnakumar S., Srinivasan R., SECURING TESLA BROADCAST PROTOCOL WITH DIFFIE-HELLMAN KEY EXCHANGE, INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET), ISSN 0976 – 6367.	BDI (Google Scholar)	ibidem	1	4.00
15	Vishwakarma, Sandeep, Pramit Kumar Samant, and Amit Sharma. "Attacks in a PKI-Based Architecture for M-commerce." Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on. IEEE, 2015.	BDI (Google Scholar)	ibidem	1	4.00
16	Yue, Qinggang, Feng Liu, and Rui Xue. "Some improvements to the cost-based framework for analyzing denial of service attacks." Trusted Systems (2012): 84-101.	BDI (Scopus)	Groza, Bogdan, and Marius Minea. "Formal modelling and automatic detection of resource exhaustion attacks." Proceedings of the 6th AsiaCCS. ACM, 2011.	2	2.00
17	Meng, Bo, Wei Huang, and Zimao Li. "Automated Proof of Resistance of Denial of Service Attacks Using Event with Theorem Prover." Journal of Computers 8.7 (2013): 1728-1741.	BDI (Scopus)	ibidem	2	2.00

18	Patel, H., Jinwala, D.C. Modeling and analysis of internet key exchange protocolv2 and a proposal for its variant (2013) Compute 2013 - 6th ACM India Computing Convention: Next Generation Computing Paradigms and Technologies	BDI (Scopus)	ibidem	2	2.00
19	Terzi, Ramazan, et al. "An Intelligent Technique for Detecting Malicious Users on Mobile Stores." *Machine Learning and Applications (ICMLA), 2014 13th International Conference on*. IEEE, 2014.	BDI (Google Scholar)	ibidem	2	2.00
20	Garcia-Alfaro, Joaquin, Jordi Herrera-Joancomartí, and Joan Melià-Seguí. "Security and Privacy Concerns About the RFID Layer of EPC Gen2 Networks." Advanced Research in Data Privacy. Springer International Publishing, 2015. 303-324.	BDI (Google Scholar)	ibidem	2	2.00
21	Elsabagh, Mohamed, et al. "Radmin: Early Detection of Application-Level Resource Exhaustion and Starvation Attacks." Research in Attacks, Intrusions, and Defenses. Springer International Publishing, 2015. 515-	BDI (Google Scholar)	ibidem	2	2.00
22	Bellare, Mihir, Thomas Ristenpart, and Stefano Tessaro. "Multi-instance security and its application to password-based cryptography." Advances in Cryptology (CRYPTO'12). Springer Berlin Heidelberg, 2012. 312-329. Revised Version. (Rank A)	BDI (Google Scholar)	Groza, Bogdan, and Bogdan Warinschi. "Revisiting difficulty notions for client puzzles and dos resilience." Information Security. Springer Berlin Heidelberg, 2012. 39-54.	2	2.00
23	Stebila, Douglas, et al. "Stronger difficulty notions for client puzzles and denial-of-service-resistant protocols." Topics in Cryptology (CT-RSA'11). Springer Berlin Heidelberg, 2011. 284-301. Revised Version. (Rank A)	BDI (Google Scholar)	ibidem	2	2.00
24	Kuppusamy, Lakshmi Devi. "Modelling client puzzles and denial-of-service resistant protocols." PhD Thesis, Queensland University (2012).	BDI (Google Scholar)	ibidem	2	2.00
25	Studnia, Ivan, et al. "Survey on security threats and protection mechanisms in embedded automotive networks." Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on. IEEE, 2013. (Rank A)	BDI (Scopus)	Groza, Bogdan, et al. "LiBrA-CAN: a Lightweight Broadcast Authentication protocol for Controller Area Networks." Cryptology and Network Security. Springer Berlin Heidelberg, 2012. 185-200.	4	1.00
26	Studnia, Ivan, et al. "Security of embedded automotive networks: state of the art and a research proposal." Proceedings of Workshop CARS (2nd Workshop on Critical Automotive applications: Robustness & Safety) of the 32nd International Conference on Computer Safety, Reliability and Security. 2013. (Rank B)	BDI (Google Scholar)	ibidem	4	1.00
27	Krishnakumar, S. "An Approach to Security and Performance in a Distributed Wireless Mesh Network." (2013). PhD Thesis, SRM University.	BDI (Google Scholar)	ibidem	4	1.00
28	Bruton, Jennifer Ann. "Securing CAN Bus Communication: An Analysis of Cryptographic Approaches." (2014).	BDI (Google Scholar)	ibidem	4	1.00
29	Han, Kyusuk, André Weimerskirch, and Kang G. Shin. "Automotive Cybersecurity for In-Vehicle Communication."	BDI (Google Scholar)	ibidem	4	1.00
30	Wang, Qiyan, and Sanjay Sawhney. "VeCure: A practical security framework to protect the CAN bus of vehicles." *Internet of Things (IOT), 2014 International Conference on the*. IEEE, 2014.	BDI (Google Scholar)	ibidem	4	1.00
31	Lin, Chung-Wei. "Security Mechanisms and Security-Aware Mapping for Real-Time Distributed Embedded Systems." (2015). PhD Thesis, UC Berkeley	BDI (Google Scholar)	ibidem	4	1.00
32	Lin, Chung-Wei, Qi Zhu, and Alberto Sangiovanni-Vincentelli. "Security-Aware Modeling and Efficient Mapping for CAN-Based Real-Time Distributed Automotive Systems." Embedded Systems Letters, IEEE 7.1 (2015): 11-14.	BDI (Google Scholar)	ibidem	4	1.00
33	Xie, Yong, et al. "Security-aware signal packing algorithm for CAN-based automotive cyber-physical systems." *Automatica Sinica, IEEE/CAA Journal of* 2.4 (2015): 422-430.	BDI (Google Scholar)	ibidem	4	1.00
34	Ribeiro, M. A. "Méthodes formelles pour la vérification probabiliste de propriétés de sécurité de protocoles cryptographiques.", PhD Thesis, 2011	BDI (Google Scholar)	Groza, Bogdan, and Marius Minea. "A calculus to detect guessing attacks."Information Security. Springer Berlin Heidelberg, 2009. 59-67.	2	2.00
35	Li, Zhiwei, and Weichao Wang. "Rethinking about guessing attacks." Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (AsiaCCS'11). ACM, 2011. (Rank B)	BDI (ACM, Scopus)	ibidem	2	2.00

36	Garcia-Alfaro, Joaquin, Jordi Herrera-Joancomartí, and Joan Melià-Seguí. "Security and Privacy Concerns About the RFID Layer of EPC Gen2 Networks." Advanced Research in Data Privacy. Springer International Publishing, 2015. 303-324.	BDI (Google Scholar)	ibidem	2	2.00
37	Szilagyi, Christopher Johnathan. Low cost multicast network authentication for embedded control systems. PhD. Thesis Carnegie Mellon University, 2012.	BDI (Google Scholar)	Groza, Bogdan, and Pal-Stefan Murvay. "Higher Layer Authentication for Broadcast in Controller Area Networks." SECRYPT. 2011.	2	2.00
38	Bruton, Jennifer Ann. "Securing CAN Bus Communication: An Analysis of Cryptographic Approaches." (2014).	BDI (Google Scholar)	ibidem	2	2.00
39	Wang, Qiyan, and Sanjay Sawhney. "VeCure: A practical security framework to protect the CAN bus of vehicles." *Internet of Things (IOT), 2014 International Conference on the*. IEEE, 2014.	BDI (Google Scholar)	ibidem	2	2.00
40	Wasicek, Armin. *Security in Time-Triggered Systems,* Ph. D. thesis, Vienna University of Technology, 2012.	BDI (Google Scholar)	Groza, Bogdan, and T-L. Dragomir. "Using a cryptographic authentication protocol for the secure control of a robot over TCP/IP." AQTR 2008.	2	2.00
41	Zahugi, Emaad Mohamed H., Ahmed M. Shabani, and T. V. Prasad. "Libot: Design of a low cost mobile robot for outdoor swarm robotics." Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on. IEEE, 2012.	BDI (IEEE)	ibidem	2	2.00
42	Radu, T., Mircea, S. Evaluation of DES, 3 DES and AES on windows and unix platforms (2010) ICCC-CONTI 2010 - IEEE International Joint Conferences on Computational Cybernetics and Technical Informatics, Proceedings, art. no. 5491317, pp. 119-123.	BDI (Scopus)	Groza B. , Universitatea Politehncă din Timişoara CONSTRUCŢII CRIPTOGRAFICE HIBRIDE, BAZATE PE TEHNICI SIMETRICE ŞI ASIMETRICE ,Teza de Doctorat, 2008	1	4.00
43	Everett, Christopher E., and Damon McCoy. "OCTANE: Open Car Testbed And Network Experiments Bringing Cyber-Physical Security Research to Researchers and Students", 6th Workshop on Cyber Security Experimentation and Test, part of 22nd USENIX Security Symposium (USENIX Security '13) (Rank A)	BDI (Google Scholar)	Groza, Bogdan, and Stefan Murvay. "Secure Broadcast with One-Time Signatures in Controller Area Networks." Availability, Reliability and Security (ARES), 2011.	2	2.00
44	Szilagyi, Christopher Johnathan. Low cost multicast network authentication for embedded control systems. PhD. Thesis Carnegie Mellon University, 2012.	BDI (Google Scholar)	ibidem	2	2.00
45	Bruton, Jennifer Ann. "Securing CAN Bus Communication: An Analysis of Cryptographic Approaches." (2014).	BDI (Google Scholar)	ibidem	2	2.00
46	Wang, Qiyan, and Sanjay Sawhney. "VeCure: A practical security framework to protect the CAN bus of vehicles." Internet of Things (IOT), 2014 International Conference on the. IEEE, 2014.	BDI (Google Scholar)	ibidem	2	2.00
47	Borazjani, Parnian Najafi, Christopher E. Everett, and Damon McCoy. "OCTANE: An Extensible Open Source Car Security Testbed."	BDI (Google Scholar)	ibidem	2	2.00
48	Tomoiaga, Radu, and Mircea Stratulat. "AES Performance Analysis on Several Programming Environments, Operating Systems or Computational Platforms."Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on. IEEE, 2010.	BDI (Scopus)	Groza, Bogdan, Dragos Pop, and Ioan Silea. "Java implementation of an authentication protocol with application on mobile phones." AQTR 2008.	3	1.33
49	Čiča, Zoran. "FPGA implementacija SHA-3 standarda za heširanje." Proceedings of 57th ETRAN Conference, Zlatibor, Serbia, June 3-6, 2013	BDI (Google Scholar)	Murvay, P-S., and Bogdan Groza. "Performance improvements for SHA-3 finalists by exploiting microcontroller on-chip parallelism." Risk and Security of Internet and Systems (CRiSIS), 2011.	2	2.00
50	Gilbert M. Wolrich et al., Instructions to perform JH cryptographic hashing in a 256 bit data path, http://www.google.com/patents/WO2013112118A2?cl=en	BDI (Google Patents)	ibidem	2	2.00
51	Vaisla, Kunwar Singh, and Rajendra Kumar Bharti. "Modified Authentication Protocol of X. 509–Directory Authentication Services."	BDI (Google Scholar)	Groza, Bogdan, and Toma-Leonida Dragomir. "On the use of one-way chain based authentication protocols in secure control systems." ARES 2007.	2	2.00
52	Vennila, R., and V. Duraisamy. "MULTI-LEVEL GROUP KEY MANAGEMENT TECHNIQUE FOR MULTICAST SECURITY IN MANET." Journal of Theoretical & Applied Information Technology 49.2 (2013).	BDI (Scopus)	ibidem	2	2.00
53	DEEPIKARANI, K., et al. "DATA TRANSMISSION USING TCP, GZIP & TINY ALGORITHMS."	BDI (Google Scholar)	ibidem	2	2.00
54	Bailey, Daniel V., William M. Duane, and Eric Young. "Protected resource access control utilizing intermediate values of a hash chain." U.S. Patent No. 8,990,905. 24 Mar. 2015.	BDI (Google Scholar)	ibidem	2	2.00
55	Bailey, Daniel V., William M. Duane, and Aaron Katz. "Protected resource access control utilizing credentials based on message authentication codes and hash chain values." U.S. Patent No. 8,984,602. 17 Mar. 2015.	BDI (Google Scholar)	ibidem	2	2.00

56	Bailey, Daniel V., William M. Duane, and Eric Young. "Protected resource access control utilizing intermediate values of a hash chain." U.S. Patent No. 9,064,094. 23 Jun. 2015.	BDI (Google Scholar)	ibidem	2	2.00
57	Zhang, Xiaodong, Xiujuan Li, and Ke Lu. "Remote video monitoring system based on ARM and Linux." Intelligent Control and Information Processing (ICICIP), 2012 Third International Conference on. IEEE,	BDI (IEEE)	Groza, Bogdan, et al. "Towards developing secure video surveillance systems over IP." Internet Monitoring and Protection, 2009. ICIMP'09. Fourth International Conference on. IEEE, 2009.	4	1.00
58	Chia-Chen Fang, A Secure Scheme of SIP Controlled IP Tele-Camera, MsC Thesis, 2010.	BDI (Google Scholar)	ibidem	4	1.00
59	Xu, Miao, et al. "Lightweight secure communication protocols for in-vehicle sensor networks." Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles, part of ACM-CCS. ACM, 2013. (Rank A)	BDI (ACM, Scopus)	Groza, Bogdan, and Rene Mayrhofer. "SAPHE: simple accelerometer based wireless pairing with heuristic trees."	2	2.00
60	Matetic, Sinisa. "Engineering device pairing with fuzzy cryptography." (2014). MsC Thesis Aalto University	BDI (Google Scholar)	ibidem	2	2.00
61	Krentz, Konrad-Felix, and Gerhard Wunder. "6doku: Towards Secure Over-the-Air Preloading of 6LoWPAN Nodes using PHY Key Generation." ITG-Fachbericht-Smart SysTech 2015 (2015).	BDI (Google Scholar)	ibidem	2	2.00
62	Bedekar N. and Shee C., A novel approach to true random number generation in wearable computing environments using MEMS sensors, 10th International Conference on Information Security and Cryptology, Inscrypt 2014; Beijing; China; 13 December 2014 through 15 December 2014	BDI (Scopus)	ibidem	2	2.00
63	Juels, Ari. "Device pairing using a cryptographic commitment process involving measured motion values." U.S. Patent No. 9,185,100. 10 Nov. 2015.	BDI (Google Scholar)	ibidem	2	2.00
64	Radu, T., Mircea, S. AES behavior on several programming environments and different operating systems or computational platforms (2010) ICCC-CONTI 2010 - IEEE International Joint Conferences on Computational Cybernetics and Technical Informatics, Proceedings, art. no. 5491315, pp. 125-130.	BDI (Scopus)	Solga, M., Groza, B., Evaluarea Performantelor Computaţionale Pentru Funcţii Criptografice Simetrice Şi. Asimetrice pe platformele Windows şi Unix (Raport Cercetare)	2	2.00
65	Tomoiaga, R., Stratulat, M. AES performance analysis on several programming environments, operating systems or computational platforms (2010) Proceedings - 5th International Conference on Systems and Networks Communications, ICSNC 2010, art. no. 5635003, pp. 172-176.	BDI (Scopus)	ibidem	2	2.00
66	Bruton, Jennifer Ann. "Securing CAN Bus Communication: An Analysis of Cryptographic Approaches." (2014).	BDI (Scopus)	Groza, Bogdan, and Pal-Stefan Murvay. "Broadcast Authentication in a Low Speed Controller Area Network." E-Business and Telecommunications. Springer Berlin Heidelberg, 2012. 330-344.	2	2.00
67	Wang, Qiyan, and Sanjay Sawhney. "VeCure: A practical security framework to protect the CAN bus of vehicles." Internet of Things (IOT), 2014 International Conference on the. IEEE, 2014.	BDI (IEEE)	ibidem	2	2.00
68	Bruton, Jennifer Ann. "Securing CAN Bus Communication: An Analysis of Cryptographic Approaches." (2014).	BDI (Google Scholar)	Groza, Bogdan, and Pal-Stefan Murvay. "Efficient Protocols for Secure Broadcast Authentication in Controller Area Network.", 2013. IEEE Trans.	2	2.00
69	Woo, Samuel, Hyo Jin Jo, and Dong Hoon Lee. "A practical wireless attack on the connected car and security protocol for in-vehicle can." (2014).	BDI (Google Scholar)	ibidem	2	2.00
70	Kalintsev, N. , Mikhaylov, D., Hardware-software system for malicious logic detection in hardware infrastructure of carsJournal of Theoretical and Applied Information Technology, Volume 69, Issue 3, 30 November 2014, Pages 589-598	BDI (Scopus)	ibidem	2	2.00
71	Kleberger, Pierre. "On Securing the Connected Car-Methods and Protocols for Secure Vehicle Diagnostics." PhD diss., Chalmers University of Technology, 2015.	BDI (Google Scholar)	ibidem	2	2.00
72	Zou, Xiaofu, et al. "A new approach for data processing in supply chain network based on FPGA." The International Journal of Advanced Manufacturing Technology (2015): 1-12.	BDI (Google Scholar)	ibidem	2	2.00
73	Katz, Jonathan, Andrew Miller, and Elaine Shi. *Pseudonymous Secure Computation from Time-Lock Puzzles*. Vol. 857. Cryptology ePrint Archive, 2014.	BDI (Google Scholar)	Groza, Warinschi, Cryptographic puzzles and DoS resilience, revisited, Designs Codes and Cryptography, Springer, 2014	2	2.00
74	Miller, Andrew, et al. "PREPRINT: Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions."	BDI (Google Scholar)	ibidem	2	2.00

75	Jiang, Linzhi, et al. "Analysis and Comparison of the Network Security Protocol with DoS/DDoS Attack Resistance Performance." High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on. IEEE, 2015.	BDI (Google Scholar)	ibidem	2	2.00
76	Luis da Costa Cordeiro, Weverton, and Luciano Paschoal Gaspary. "Limiting fake accounts in large-scale distributed systems through adaptive identity management." Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE,	BDI (Google Scholar)	ibidem	2	2.00
77	Katz, Jonathan, Andrew Miller, and Elaine Shi. "Pseudonymous Broadcast and Secure Computation from Cryptographic Puzzles."	BDI (Google Scholar)	ibidem	2	2.00
78	Tarwala, Mohammed, et al. "ANDROID MALWARE."	BDI (Google Scholar)	Groza, Cristea, Fingerprinting Smartphones Remotely via ICMP Timestamps, Comm. Lett, 2013	2	2.00
79	Kassem, Mohamed M., Haitham S. Hamza, and Imane A. Saroit. "A Clock Skew Addressing Scheme for Internet of Things."	BDI (Google Scholar)	ibidem	2	2.00
80	Chen, Tsung-Han, A Clock Skew Measuring Method for Networks with Large Delay Jitters, MsC Thesis	BDI (Google Scholar)	ibidem	2	2.00
81	Yang, Yu-Chi. "An Improved Hough Transform-based Clock Skew Measurement." (2015).	BDI (Google Scholar)	ibidem	2	2.00
82	Chen, Tsung-Han. "A Clock Skew Measuring Method for Networks with Large Delay Jitters." (2014).	BDI (Google Scholar)	ibidem	2	2.00
83	Werner, Janis. "Directional Antenna System-Based DoA/RSS Estimation, Localization and Tracking in Future Wireless Networks: Algorithms and Performance Analysis." Tampereen teknillinen yliopisto. Julkaisu-Tampere University of Technology. Publication; 1350 (2015).	BDI (Google Scholar)	ibidem	2	2.00
84	Werner, Janis, et al. "Joint user node positioning and clock offset estimation in 5G ultra-dense networks." IEEE Global Communications Conference (GLOBECOM). 2015.	BDI (Google Scholar)	ibidem	2	2.00
85	Hacha, A., Bah S., Bakkoury Z., A new authentication scheme for sip registration in a manet environment, International Journal of Computer Science and Applications Volume 12, Issue 1, 2015, Pages 134-147	BDI (Scopus)	Groza, Bogdan, and Dorina Petrica. "One-time passwords for uncertain number of authentications." Proceedings of CSCS15 (2005).	2	2.00
			TOTAL		**160.33**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A3.2.1 - Profesor invitat si Prezentari invitate in plenul unor manifestari stiintifice - Internationale

Nr. crt.	Activitatea	Indicator realizat
1	**Invited Presentation:** Protocol vulnerabilities in practice: causes, modeling and automatic detection, **Romanian Cryptology Days 2011**, Bucharest, Romania https://www.sie.ro/rcd2011/En/Programme_e.html	10
2	**Invited Presentation:** Security for Vehicular Buses: from Cryptography to Physically Unclonable Characteristics. **BalkanCrypt 2013**, Sofia, Bulgaria	10
3	**Guest Lecture:** Resource exhaustion attacks: formal verification and cryptographic countermeasures, Upper Austria University of Applied Sciences, FH Oberosterreich in Hagenberg, Linz, Austria May 2012	10
4	**Research Seminar:** Security for Vehicular Buses: from Cryptography to Physically Unclonable Characteristics, **Budapest University (BME)**, Seminar Series on Advances in Telecommunications, Networking and Computing, http://www.hit.bme.hu/~buttyan/atnc/#20131205-Groza	10
5	**Research Seminar:** LiBrA-CAN and beyond: Physically Unforgeable CAN (PSI-CAN) and Secure Automotive CAN (SeA-CAN), **KU Leuven**, COSIC July 2013	10
6	**Research Seminar:** Client Puzzles, DoS Resilience, Multi-instance (Mi) Security - Revisiting Difficulty Notions, **KU Leuven**, COSIC July 2013	10
7	**Research Seminar:** Modelling of guessing and resource exhaustion attacks, **University of Bristol, UK**, Cryptography & Security Seminars, http://www.cs.bris.ac.uk/Research/CryptographySecurity/seminars/abstracts.html	10
8	**Invited Presentation**: Experiences in bridging academic research in information security with intellectual property and industry requirements, West University Timisoara, RO, **Workshop on Intelectual Properties in ICT**, 2014, http://host.hpc.uvt.ro/events/workshop-on-intellectual-properties-in-ict-and-e-infrastructures/	10
9	**Invited Presentation:** In-vehicle security, bridging between academic research and industry requirements, **Vector Congress**, Vienna, May, 2015. https://at.vector.com/portal/medien/cmc/events/commercial_events/VectorAustriaKongress_2015/Vector_Congress_Agenda_2015.pdf	10
	TOTAL	**90**

A3.2.1 - Profesor invitat si Prezentari invitate in plenul unor manifestari stiintifice - nationale

Nr. crt.	Activitatea	Indicator realizat

1	**Invited Presentation:** Current trends and challenges in cryptography, Conferinta Internationala de Hacking Def.Camp 2013, Timisoara, Romania, http://127.0.defcamp.ro/defcamp-timisoara-3-noiembrie/	5
	TOTAL	**5**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A3.3.1 - Membru in colectivele de redactie sau comitete stiintifice ale revistelor, organizator de manifestari stiintifice - indexate ISI

Nr. crt.	Activitatea	Indicator realizat
1	8th International Conference on Availability, Reliability and Security, Conferinta Internationala, Regensburg, Austria, 2013 http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6657199	10
2	Internationala, Prague, Czek Republic, 2012 http://www.ares-conference.eu/ares2012/www.ares-conference.eu/conf/index7692.html?option=com_content&view=article&id=4&Itemid=79	10
3	Recenzor la Designs Codes and Cryptography (Springer)	10
4	Recenzor la Wireless Communications (IEEE)	10
5	Recenzor la Transactions on Industrial Informatics (IEEE)	10
6	Recenzor la Security and Communication Networks (Wiley)	10
7	Recenzor la Computer Standards & Interfaces (Elsevier)	10
8	Recenzor la Telecommunication Systems (Springer)	10
9	Recenzor la Computers & Security (Elsevier)	10
10	Recenzor la Arabian Journal of Science and Engineering (Springer)	10
11	Recenzor la Journal of Computer and System Sciences	10
12	Recenzor la Transactions on Information Forensics & Security (IEEE)	10
	TOTAL	**120**

A3.3.2 - Membru in colectivele de redactie sau comitete stiintifice ale revistelor, organizator de manifestari stiintifice - indexate BDI

Nr. crt.	Activitatea	Indicator realizat
1	1st International Workshop on Secure Internet of Things (SIOT 2014) http://siot-workshop.org/2014/#pc	6
2	2nd International Workshop on Secure Internet of Things (SIOT 2015) http://siot-workshop.org/#pc	6
3	3rd Romanian Cryptology Days RCD'2015 https://www.sie.ro/rcd2015/ProgramCommittee.html	6
4	BalkanCryptSec 2016, Bucharest, Romania https://www.cs.bris.ac.uk/bcs16/programcommittee.html	6
5	2nd International Conference on Cryptography and Information security - BalkanCryptSec 2015, Koper, Croatia https://conferences.matheo.si/event/16/page/0	6
6	BalkanCryptSec 2014, Istabul, Turkey http://www.gstl.itu.edu.tr/BalkanCryptSec/committees.htm	6
7	University of Fribourg, 2015 http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7299869	6
8	9th International Conference on Availability, Reliability and Security, ARES, University of Fribourg, Switzerland, 2014 http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6980239	6
9	7th International Conference on Risks and Security of Internet and Systems, CRiSIS, Cork, Ireland, 2012 http://4c.ucc.ie/crisis2012/committees.html	6
10	6th International Conference on Risks and Security of Internet and Systems, CRiSIS, Timisoara, Romania, 2011 http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6061837	6
11	5th International Conference on Risks and Security of Internet and Systems, CRiSIS, Montreal, Canada, 2010	6

12	4th International Conference on Emerging Security Information, Systems and Technologies, SECURWARE Venice, Italy, 2010 http://www.iaria.org/conferences2010/ComSECURWARE10.html	6
13	5th International Conference on Internet Monitoring and Protection, Conferinta Internationala, Barcelona, Spain, ICIMP 2010 http://www.iaria.org/conferences2010/ComICIMP10.html	6
14	4th International Conference on Internet Monitoring and Protection, Conferinta Internationala, Venice, Italy, ICIMP 2009 http://www.iaria.org/conferences2009/ComICIMP09.html	6
15	Recenzor la Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)	6
16	Recenzor la Information Security Technical Report (Elsevier)	6
	TOTAL	**96**

A3.3.3 - Membru in colectivele de redactie sau comitete stiintifice ale revistelor, organizator de manifestari stiintifice - nationale si internationale neindexate

Nr. crt.	Activitatea	Indicator realizat
1	1st International Workshop on Security for Spontaneous Interaction, Conferinta Internationala, Innsbruck, Austria, 2007 (linkul nu mai este indisponibil)	3
2	Cryptography summer school, http://www.csie.ase.ro/avizier/cryptography-summer-school Bucharest, Romania, 2014	3
	TOTAL	**6**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

TOTAL 222

Universitatea Politehnica Timisoara
Facultatea de Automatica si Calculatoare
RAMURA DE STIINTA: INGINERIA SISTEMELOR, CALCULATOARE SI TEHNOLOGIA INFORMATIEI

Candidat: Conf. Dr. Ing. Bogdan Ioan Groza

A3.4.1 - Premii in domeniu - Academia Romana, ASTR, academii de ramura, premii internationale

Nr. crt.	Premiul decernat	Indicator realizat
	TOTAL	**0**

A3.4.2 - Premii in domeniu - premii nationale

Nr. crt.	Premiul decernat	Indicator realizat
1	Premierea rezultatelor cercetarii, articol ISI "Source Identification Using Signal Characteristics in Controller Area Networks" - PN-II-RU-PRECISI-2015-9-8650	5
2	Premierea rezultatelor cercetarii, articol ISI "Cryptographic puzzles and DoS resilience, revisited", 2014 - PN-II-RU-PRECISI-2014-8-5996	5
3	Premierea rezultatelor cercetarii, articol ISI "Efficient Protocols for Secure Broadcast in Controller Area Networks" - PN-II-RU-PRECISI-2013-7-4156	5
4	Premierea rezultatelor cercetarii, articol ISI "Fingerprinting Smartphones Remotely via ICMP Timestamps" - PN-II-RU-PRECISI-2013-7-3765	5
5	Distinctia Magna cum Laude pentru teza de doctorat	5
	TOTAL	**25**

Candidat,
Conf. Dr. Ing. Bogdan Ioan Groza

TOTAL 25