Lista Completa de Lucrari

I. Teza de doctorat

[1-TD] *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*

II. Lista lucrari organizate pe structura tipului de activităţi prevăzute în Ordinul ministrului educaţiei, cercetării, tineretului şi sportului nr. 6560 din 20 decembrie 2012

A1.1. Carti si capitole în carti de specialitate in edituri recunoscute

[1-C] *Bogdan Groza, Editura Politehnica, Cryptography - Application Notes in C, .NET and Java, Editura Politehnica Timisoara, ISBN 978-606-35-0024-4, 84 p., 2015.*

[2-C] *Groza Bogdan, Introducere in criptografie: functii criptografice, fundamente matematice si computationale, Editura Politehnica, Timisoara, ISBN 978-606-554-499-4, 200 p., 2012*

[3-C] *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, 2011.*

[4-C] *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*

[5-C] *Bogdan Groza, Introducere in Sistemele Criptografice cu Cheie Publica, Editura Politehnica, Timisoara, ISBN 978-973-625-564-9, 136 p., 2007*

A1.2. Material didactic / Lucrari didactice Manuale didactice

[1-M] *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).*

[2-M] *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*

A1.3. Proprietate intelectuala, brevete de inventie, certificate ORDA – Internationale

[1-PI] *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*

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

[1-ISI-J] Cristea, M.; Groza, B., "Fingerprinting Smartphones Remotely via ICMP Timestamps," Communications Letters, IEEE , vol.17, no.6, pp.1081,1083, June 2013.

[2-ISI-J] 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.

[3-ISI-J] Bogdan Groza, Bogdan Warinschi, "Client puzzles and DoS resilience, Revisited", Designs Codes and Cryptography, Springer-Verlag, April 2013.

[4-ISI-J] 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-ISI-J] Groza, B.; Murvay, S., "Source Identification Using Signal Characteristics in Controller Area Networks" Signal Processing Letters, IEEE, (accepted for publication, January 2014.

*[1-ISI-C] 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-ISI-C] 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, **LNCS**, 2010. 391-399. (Rank A)*

*[3-ISI-C] Groza, Bogdan, and Marius Minea. "A calculus to detect guessing attacks."Information Security. Springer Berlin Heidelberg, **LNCS**, 2009. 59-67. (Rank B)*

*[4-ISI-C] 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.*

*[5-ISI-C] 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.*

*[6-ISI-C] 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.*

*[7-ISI-C] 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.*

*[8-ISI-C] 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)*

*[9-ISI-C] 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.*

[10-ISI-C] Groza, Bogdan. "On the use of the discrete power function for building public-key cryptosystems."

[11-ISI-C] 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.

*[12-ISI-C] 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)*

*[13-ISI-C] 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.*

*[14-ISI-C] 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.*

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

[1-BDI] 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.

[2-BDI] 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.

*[3-BDI] 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)*

*[4-BDI] 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)*

*[5-BDI] 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)*

*[6-BDI] 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)*

*[7-BDI] 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)*

*[8-BDI] 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.*

*[9-BDI] 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.*

*[10-BDI] 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)*

[11-BDI] *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.*

[12-BDI] *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.*

[13-BDI] *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*

[14-BDI] *Bogdan Groza and Toma-Leonida Dragomir. Experimenting with the secure control of a robot over tcp/ip. Automation Computers, Applied Mathematics Journal (ACAM), 2008.*

[15-BDI] *B. Groza, Broadcast authentication with practically unbounded one-way chains, JOURNAL OF SOFTWARE (JSW), Volume 3, Issue 2, ISSN: 1796-217X, Academy Publishers, 2008.*

[16-BDI] *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.*

[17-BDI] *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.*

[18-BDI] *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.*

[19-BDI] *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.*

[20-BDI] *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,* ***LNCS****, 2013.*

[21-BDI] *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.*

[22-BDI] *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.*

Articole in reviste si conferinte nationale fara indexare.

[1-Nat] *Bogdan Groza, Edith Putanu, Toma-Leonida Dragomir, and Dorina Petrica. Development of a client-server platform for simulation of remote control systems. In National Conference of Electrical Drives (CNAE), 2008.*

[2-Nat] *Bogdan Groza, Andrei Alexandroni, and Ioan Silea. An overview of NTLM authentication and its weaknesses in sharepoint solutions. In International Conference on Technical Informatics (CONTI'08), 2008.*

[3-Nat] *Bogdan Groza. The delayed message authentication protocol with chains constructed on the discrete power function. In Proceedings of 7th International Conference on Technical Informatics, pages 33-36, 2006.*

[4-Nat] *Bogdan Groza, Dorina Petrica, and Toma-Leonida Dragomir. Security based on cryptographic techniques for remote control systems. National Symposyum on System Theory, Automation, Robotics, Computers, Informatics, Electronics and Instrumentation (SINTES), 2005.*

[5-Nat] *Bogdan Groza and Dorina Petrica. One-time passwords for uncertain number of authentications. In Proceedings of 15th International Conference on Control Systems and Computer Science (CSCS15), 2005.*

[6-Nat] *Bogdan Groza, Andrei Alexandroni, Ioan Silea, and Victor-Valeriu Patriciu. On the security of some authentication mechanisms from Windows. Scientic Bulletin of Politehnica University of Timisoara (Automatic Control and Computer Science Series), 2008.*

[7-Nat] *Bogdan Groza. Construction techniques for one-way chains and their use in authentication. Journal of Control Engineering and Applied Informatics (CEAI), 8(1):42-51, 2006.*