Curriculum vitae Europass

Informaţii personale

Nume / Prenume	**Bogdan Groza**
Adresă(e)	Universitatea Politehnica Timisoara, Bd. V. Parvan, nr. 10, Timisoara, Romania
Telefon(oane)	0256-403242
E-mail(uri)	bogdan.groza@aut.upt.ro
Naţionalitate(-tăţi)	roman
Data naşterii	Mai 1981

Locul de muncă vizat / Domeniul ocupaţional

Profesor universitar

Experienţa profesională

- Sumar publicaţii: >50 lucrări ştiinţifice, >80% ca prim autor
- Cele mai relevante 5 articole
  - B. Groza, S. Murvay, A. van Herrewege, I. Verbauwhede, LiBrA-CAN: a Lightweight Broadcast Authentication protocol for Controller Area Networks, in *ACM Transactions on Embedded Computing Systems*, accepted November, 2016.
  - B. Groza, B. Warinschi, "Client puzzles and DoS resilience, Revisited", in *Designs Codes and Cryptography*, Springer-Verlag, 73.1, pp. 177-207. 2014.
  - B. Groza, S. Murvay, "Efficient Protocols for Secure Broadcast in Controller Area Networks," *IEEE Transactions on Industrial Informatics*, vol.9, no.4, pp.2034-2042, Nov. 2013.
  - B. Groza, M. Minea, Formal modelling and automatic detection of resource exhaustion attacks. in Proc. 6th ACM Symposium on Information, *Computer and Communications Security (ASIACCS'11)*, pp. 326-333, ACM, 2011. (Rank B)
  - B. Groza, M. Minea. "A formal approach for automated reasoning about off-line and undetectable on-line guessing." In Proc. *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, LNCS, 2010. 391-399. (Rank A)

Perioada	2014-prezent
Funcţia sau postul ocupat	**Conferenţiar universitar**
Activităţi şi responsabilităţi principale	Activitati didactice si de cercetare.

- Cursuri: Embedded Systems Security, Networks for Embedded Systems, Tehnici Avansate pentru Securitatea Informatiei, Inteligenta Artificiala si Sisteme Autonome, Securitatea Informaţiei
- Director al proiectului de cercetare CSEAMAN (Cryptographic Security for Automotive Embedded Devices and Networks) PN-II-RU-TE-2014-4-1501, 2015-2017, 550.000 lei, http://www.aut.upt.ro/~bgroza/Projects/cSEAMAN/cseaman.html, lucrări relevante publicate în cadrul proiectului:
  - B. Groza, S. Murvay, T. Andreica, Evaluating SRAM as Source for Fingerprints and Randomness on Automotive Grade Controllers, 13th International Conference on Security and Cryptography (SECRYPT 2016), full paper, 2016 (Rank B).
  - B. Groza, H. Gurban, S. Murvay, Designing security for in-vehicle networks: a Body Control Module (BCM) centered viewpoint, The 2nd International Workshop on Safety and Security of Intelligent Vehicles (SSIV 2016, affiliated to DSN 2016), full paper, 2016.

- S. Murvay, A. Matei, C. Solomon, B. Groza, Development of an AUTOSAR Compliant Cryptographic Library on State-of-the-Art Automotive Grade Controllers, The 11th International Conference on Availability, Reliability and Security (ARES), full paper, 2016 (Rank B).

- Comitet management retea COST (2013-2017): Action IC1306 Cryptography for Secure Digital Interaction, http://www.cost.eu/domains actions/ict/Actions/IC1306?management

Perioada	2009-2014
Funcţia sau postul ocupat	**Şef de lucrări**
Activităţi şi responsabilităţi principale	Activitati didactice si de cercetare. ▪ Cursuri: Data Security for Embedded Systems, Data Communications and Applications to Automotives, Tehnici Avansate pentru Securitatea Informatiei, Inteligenta Artificiala si Sisteme Autonome ▪ Membru in proiectul de cercetare: DISSIS PN2/2008-2011 proiect destinat dezvoltarii protocoalelor de autentificare cu aplicatie in sisteme industriale, lucrări relevante publicate în cadrul proiectului: o B. Groza, S. Murvay. "Broadcast Authentication in a Low Speed Controller Area Network." E-Business and Telecommunications. Springer Berlin Heidelberg, 2012. 330-344. o B. 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) o 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. o 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) o 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.
Numele şi adresa angajatorului	**Universitatea Politehnica Timisoara**, Blvd. V. Parvan, nr. 10, room A304, Timisoara, Romania
Tipul activităţii sau sectorul de activitate	Invatamant

Perioada	2004-2008
Funcţia sau postul ocupat	**Doctorand**
Activităţi şi responsabilităţi principale	Activitati didactice si de cercetare. ▪ Director GRANT TD 122/2007 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, 14490 lei, lucrări relevante publicate: o B. Groza, Broadcast authentication with practically unbounded one-way chains, JOURNAL OF SOFTWARE (JSW), Volume 3, Issue 2, ISSN: 1796-217X, Academy Publishers, 2008. o B. Groza, Broadcast authentication protocol with time synchronization and quadratic residues chains, Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, pp. 550-557, IEEE Comp. Soc., 2007 (Rank B). (extended journal version above) o B. Groza, T.L. Dragomir, On the use of one-way chain based authentication in secure control systems,Second International Conference on Availability, Reliability and Security (ARES'07), International Workshop on Advances in Information Security (WAIS'07), Vienna, Austria, pp. 1214-1221,IEEE Comp. Soc., 2007 (Rank B). o B. Groza, D. Petrica, S. Barbu, M. Bilanin, Implementation of an Authentication Protocol for Sending Audio-Video Information in Java, 4th International Symposium on Applied Computational Intelligence and Informatics, SACI 2007, IEEE Comp. Int. Soc., 2007. o B. Groza, An extension of the RSA trapdoor in a KEM/DEM Framework, Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC'07, IEEE Comp. Soc., 2007

- Director GRANT TD 90/2006 Protocoale de securitate si tehnici criptografice bazate pe functii one-way pentru asigurarea autenticitatii informatiei, 10773 lei, lucrări relevante publicate:
  - B. Groza, Using one-way chains to provide message authentication without shared secrets, 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPeru'06), Lyon, France, pp. 82-87, IEEE Comp. Soc., 2006.
  - 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.
  - B. Groza, The Delayed Message Authentication Protocol with Chains Constructed On the Discrete Power Function, Proceedings of 7th International Conference on Technical Informatics, CONTI'06, pp. 33-36, 2006.
  - B. Groza, Construction techniques for one-way chains and their use in authentication, Control Engineering and Applied Informatics Journal, CEAI, No.1, vol. 8, pp. 42-51, 2006.
  - B. Groza, D. Petrica, On chained cryptographic puzzles, Proceedings of 3rd Romanian-Hungarian Joint Symposium on Applied Computational Intelligence, SACI'06, pp. 182-191, 2006.

Numele şi adresa angajatorului | **Universitatea Politehnica Timisoara**, Blvd. V. Parvan, nr. 10, room A304, Timisoara, Romania

Tipul activităţii sau sectorul de activitate | Invatamant

Perioada | 2008-2011, 2013

Funcţia sau postul ocupat | **Cercetator**

Activităţi şi responsabilităţi principale

- Membru in proiectul AVANTSSAR (Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures) FP7, cercetare in modelarea atacurilor asupra protocoalelor in platforma AVANTSSAR, lucrări relevante publicate în cadrul proiectului:
  - Groza, Bogdan, 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)
  - Groza, Bogdan, and Marius Minea. "A calculus to detect guessing attacks."Information Security. Springer Berlin Heidelberg, LNCS, 2009. 59-67. (Rank B)
  - 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)
  - 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.
- Membru in proiectul SPaCIoS (SPaCIoS: Secure Provision and Consumption in the Internet of Services) FP7 research, extensie a proiectului in modelarea atacurilor asupra sistemelor de conducere industriale, lucrări relevante publicate în cadrul proiectului:
  - Bogdan Groza, Marius Minea. Bridging dolev-yao adversaries and control systems with time-sensitive channels. In Conference on Critical Information Infrastructures Security (CRITIS). Springer, LNCS, 2013.

Numele şi adresa angajatorului | **Institutul e-Austria Timisoara**, Blvd. Vasile Parvan, nr. 4, room 045B

Tipul activităţii sau sectorul de activitate | Cercetare

Perioada | 2007-prezent

Funcţia sau postul ocupat | **Membru** in peste 20 de comitete internationale ale unor conferinte, dintre cere in securitatea informatiei si criptografiei urmatoarele:

- 2016
  - 3rd International Conference on Cryptography and Information security (BalkanCryptSec)
  - 11th International Conference on Risks and Security of Internet and Systems (CRiSIS)
  - 3rd International Workshop on Secure Internet of Things (SIoT)
  - 11th International Conference on Availability, Reliability and Security (ARES)
- 2015
  - 2nd International Conference on Cryptography and Information security (BalkanCryptSec) (Steering Committee)
  - 3rd Romanian Cryptology Days (RCD)
  - 2nd International Workshop on Secure Internet of Things (SIoT)
  - 10th International Conference on Availability, Reliability and Security (ARES)

- 2014:
  - International Conference on Cryptography and Information security (BalkanCryptSec) (Steering Committee)
  - International Conference on Availability, Reliability and Security (ARES, Rank B)
  - 1st International Workshop on Secure Internet of Things (SIoT)
- 2013
  - International Conference on Availability, Reliability and Security (ARES, Rank B)
- 2012
  - International Conference on Availability, Reliability and Security (ARES, Rank B)
  - International Conference on Risks and Security of Internet and Systems (CRiSIS)
- 2011
  - International Conference on Risks and Security of Internet and Systems (CRiSIS, Rank C) (Publication Chair)
- 2010
  - International Conference on Risks and Security of Internet and Systems (CRiSIS, Rank C)
  - Intl. Conf. on Emerging Security Information, Systems and Technologies (SECURWARE)
  - International Conference on Internet Monitoring and Protection (ICIMP)
- 2009
  - International Conference on Internet Monitoring and Protection (ICIMP)
- 2007
  - International Workshop on Security and Privacy in Spontaneous Interaction (IWSSI)

Perioada | 2011-prezent

Funcţia sau postul ocupat | **Recenzor invitat** la jurnale de top in domeniu

- Designs Codes and Cryptography (Springer)
- Information Security Technical Reports (Elsevier)
- Security and Communication Networks (Wiley)
- Computers & Security (Elsevier)
- Transactions on Information Forensics & Security (IEEE)
- Transactions on Industrial Informatics (IEEE)
- Computer Standards and Interfaces (Elsevier)
- Telecommunication Systems(Springer)
- Wireless Communications (IEEE)
- Journal of Computer and System Sciences (Elsevier)
- Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications
- Journal of Systems and Software (Elsevier)

Perioada | 2011-prezent

Funcţia sau postul ocupat | **Prezentări la universităţi sau evenimente pe bază de invitaţie**

- In-vehicle security, bridging between academic research and industry requirements, **Vector Congress**, Vienna, Austria
- Experiences in bridging academic research in information security with intellectual property and industry requirements, **West University Timisoara**, Workshop on Intellectual Properties in ICT, Romania
- Security for Vehicular Buses: from Cryptography to Physically Unclonable Characteristics, **Budapest University (BME)**, Advances in Telecommunications, Networking and Computing, December 2013
- Current trends and challenges in cryptography, at Hacking Event **Defcamp**, Timisoara, November 2013
- LiBrA-CAN and beyond: Physically Unforgeable CAN (PSI-CAN) and Secure Automotive CAN (SeA-CAN), **KU Leuven**, COSIC, July 2013
- Client Puzzles, DoS Resilience, Multi-instance (Mi) Security - Revisiting Difficulty Notions, **KU Leuven**, COSIC, July 2013
- Resource exhaustion attacks: formal verication and cryptographic countermeasures, Upper Austria University of Applied Sciences, **FH Oberösterreich in Hagenberg, Linz**, Austria, May, 2012
- Modelling of guessing and resource exhaustion attacks, **University of Bristol**, UK, Cryptography & Security Group, November, 2011
- Protocol vulnerabilities in practice: causes, modeling and automatic detection, Romanian Cryptology Days (organizat **Serviciul Informatii Externe**), September, 2011

Educaţie şi formare

Perioada	2016
Diploma obţinută	**Abilitare** în domeniul de doctorat Calculatoare şi Tehnologia Informaţiei
Titlul tezei:	Cryptographic security for automotive systems
Numele şi tipul instituţiei de învăţământ	**Universitatea Politehnica Timişoara**
Perioada	2004-2008
Diploma obţinută	**Doctorat** (Magna Cum Laude)
Titlul tezei:	Constructii criptografice hibride bazate pe tehnici simetrice si asimetrice, aplicatii in sisteme de conducere
Numele şi tipul instituţiei de învăţământ	**Universitatea Politehnica Timişoara**
Perioada	1999-2004
Diploma obţinută	**Inginer**, Facultatea de Automatica si Calculatoare
Numele şi tipul instituţiei de învăţământ	**Universitatea Politehnica Timişoara**
Perioada	1995-1999
Numele şi tipul instituţiei de învăţământ	**Liceul Grigore Moisil Timişoara**
Altele	Participari la diverse cursuri in domeniul criptografiei si securitatii: 24-28 Septembrie 2007, 2nd Cryptography Summer School, Inst. b-it, Bonn, Germany; 28 July – 1 August 2008, 3rd Cryptography Summer School, Inst. b-it, Bonn, Germany; 7-11 September 2009, Summer school on Provable-security, Univ. Barcelona, Spain; 4-8 July 2011, Summer School on Software Security (ACM), Univ. of Ghent, Belgium; 13-17 October 2014, School on Cryptographic Attacks, Porto, Portugal.

Aptitudini şi competenţe personale

Limba maternă	**română**
Limba străină cunoscută	**engleză**

Informaţii suplimentare

http://www.aut.upt.ro/~bgroza/