Bogdan Groza, PhD. Eng.
Associate Professor
Faculty of Automatics and Computers
Politehnica University of Timişoara
Bd. V. Parvan, nr. 10
Timişoara, Romania
www.aut.upt.ro/~bgroza
bogdan.groza@aut.upt.ro

Personal Details

Date of birth: May, 1981
Place of birth: Timişoara, Romania
Present Citizenship: Romanian

Professional Interests

Cryptography and systems security

Academic Degrees

2004-2008	PhD Degree (Magna cum Laude), Subject Area: Cryptography and Systems Security, Politehnica University of Timişoara, Romania
1999-2004	Engineering Degree, Faculty of Automatics and Computers, Politehnica University of Timişoara, Romania

Trainings

Oct. 2014	School on Cryptographic Attacks Porto, Portugal
Jul. 2011	ACM/DAPA International Summer School on Information Security and Protection, University of Ghent, Belgium
Sept. 2009	Summer School On Provable Security (inside ECRYPT-II) Barcelona, Spain
Jul. 2008	Summer school on Cryptography crypt@b-it Bonn-Aachen International Center for Information Technology, Germany
Sept. 2007	Summer school on Cryptography crypt@b-it Bonn-Aachen International Center for Information Technology, Germany

Employment History

2014-present

Associate Professor,
Politehnica University of Timişoara, Romania

- Assigned Courses: Information Security, Advanced Cryptography and Systems Security, Embedded Systems Security, Networks for Embedded Systems
- Director of national research grant PN-II-RU-TE-2014-4-1501, cSeAmaN - Cryptographic Security for Automotive Embedded Devices and Networks (2015-2017)
- National Management Committee (MC) COST Action IC1306 Cryptography for Secure Digital Interaction, http://www.cost.eu/domains_actions/ict/Actions/IC1306?management

2009-2014

Lecturer,
Politehnica University of Timişoara, Romania

- Assigned Courses: Advanced Cryptography and Systems Security, Embedded Systems Security, Data Communications and Applications to Automotives
- Member of national research grant DISSIS PN2/2008-2011, responsible with the design of authentication protocols for industrial systems (e.g., CAN networks)
- Responsible with the development of the ContiLab learning and research platform in cooperation with Continental Corporation at the Department of Automatics and Applied Informatics

2004-2008

PhD Student,
Politehnica University of Timişoara, Romania

- Director of national research grants PN-II-RU-TD-2007-2 nr. 122/2007 (1 year) and CNCSIS-TD-90/2006 (1 year) focused on the design of cryptographic protocols
- Various teaching activities: C/C++ programming, assembly languages, artificial intelligence, etc.

2012
2008-2011

Researcher,
Institute e-Austria Timişoara, Romania

- Member of AVANTSSAR (Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures) FP7 research project
- Member of SPaCIoS (SPaCIoS: Secure Provision and Consumption in the Internet of Services) FP7 research project

Research Presentations (by invitation)

May 2015
In-vehicle security, bridging between academic research and industry requirements
Vector Congress, Vienna, Austria

Mar. 2014
Experiences in bridging academic research in information security with intellectual property and industry requirements
West University Timişoara, Workshop on Intellectual Properties in ICT, Romania

Dec. 2013
Security for Vehicular Buses: from Cryptography to Physically Unclonable Characteristics
Budapest University (BME), Budapest, Hungary

Nov. 2013
Current trends and challenges in cryptography
National Hacking Event Defcamp, Timişoara, Romania

Jul. 2013
LiBrA-CAN and beyond: Physically Unforgeable CAN (PSI-CAN) and Secure Automotive CAN (SeA-CAN)
KU Leuven, COSIC, Leuven, Belgium

Jul. 2013
Client Puzzles, DoS Resilience, Multi-instance (Mi) Security - Revisiting Difficulty Notions
KU Leuven, COSIC, Leuven, Belgium

May 2012
Resource exhaustion attacks: formal verification and cryptographic countermeasures
Upper Austria University of Applied Sciences, FH Oberösterreich in Hagenberg, Linz, Austria

Nov. 2011
Modelling of guessing and resource exhaustion attacks
University of Bristol, Cryptography & Security Group, Bristol, UK

Sept. 2011
Protocol vulnerabilities in practice: causes, modeling and automatic detection
Romanian Cryptology Days, Bucharest, Romania

Program Committees (conferences)

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	1st International Conference on Cryptography and Information security (BalkanCryptSec) (Steering Committee) 9th International Conference on Availability, Reliability and Security (ARES) 1st International Workshop on Secure Internet of Things (SIoT)
2013	8th International Conference on Availability, Reliability and Security (ARES)
2012	7th International Conference on Availability, Reliability and Security (ARES) 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)
2011	6th International Conference on Risks and Security of Internet and Systems (CRiSIS) (Publication Chair)
2010	5th International Conference on Risks and Security of Internet and Systems (CRiSIS) 4th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE) 5th International Conference on Internet Monitoring and Protection (ICIMP)
2009	4th International Conference on Internet Monitoring and Protection (ICIMP)
2007	1st International Workshop on Security and Privacy in Spontaneous Interactions (IWSSI) 2007

Reviewer (journals)

*	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

Selected Publications

[1] Bogdan Groza and Bogdan Warinschi. Cryptographic puzzles and DoS resilience, revisited. *Designs Codes and Cryptography, Springer*, 73(1):177–207, April 2013.

[2] Bogdan Groza and Stefan Murvay. Efficient protocols for secure broadcast in controller area networks. *Transactions on Industrial Informatics, IEEE*, 9(4):2034–2042, November 2013.

[3] Bogdan Groza and Marius Minea. Bridging Dolev-Yao adversaries and control systems with time-sensitive channels. In *8th International Conference on Critical Information Infrastructures Security (CRITIS)*, pages 167–178. Springer, 2013.

[4] Bogdan Groza, Stefan Murvay, Anthony Van Herrewege, and Ingrid Verbauwhede. LiBrA-CAN: a lightweight broadcast authentication protocol for controller area networks. In *11th International Conference on Cryptology and Network Security (CANS)*, pages 185–200. Springer, LNCS, 2012.

[5] Bogdan Groza and Rene Mayrhofer. Saphe: simple accelerometer based wireless pairing with heuristic trees. In *10th International Conference on Advances in Mobile Computing & Multimedia (MoMM)*, pages 161–168. ACM, 2012.

[6] Bogdan Groza and Marius Minea. Formal modelling and automatic detection of resource exhaustion attacks. In *6th ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, pages 326–333. ACM, 2011.

[7] Bogdan Groza and Marius Minea. A formal approach for automated reasoning about off-line and undetectable on-line guessing. In *14th International Conference on Financial Cryptography and Data Security (FC)*, pages 391–399. Springer, LNCS, 2010.

[8] Bogdan Groza and Marius Minea. Customizing protocol specifications for detecting resource exhaustion and guessing attacks. In *9th International Symposium on Formal Methods for Components and Objects (FMCO)*, pages 45–60. Springer, LNCS, 2010.

[9] Bogdan Groza and Marius Minea. A calculus to detect guessing attacks. In *12th Information Security Conference (ISC)*, pages 59–67. Springer, LNCS, 2009.

[10] Bogdan Groza. Broadcast authentication protocol with time synchronization and quadratic residues chain. In *2nd International Conference on Availability, Reliability and Security (ARES)*, pages 550–557. IEEE, 2007.

Timişoara,
December, 2015