Daniel Socek, Ph.D.

Curriculum Vitae

Email: dsocek@fau.edu URL: http://www.socek.net

---

1. Fields of Specialization and Interest

- Biometrics, Cryptography, Multimedia Security, Information Security and Secure Communications, Image/Video Coding and Analysis, and FPGA-based System Design

2. Educational Background

- 01/2003 to 08/2006 Ph.D. in Computer Science
  Florida Atlantic University, Boca Raton, Florida 33431(USA)
- 01/2001 to 12/2002 M.Sc. in Mathematical Sciences
  Florida Atlantic University, Boca Raton, Florida 33431 (USA)
- 08/1996 to 12/2000 B.Sc. in Computer Science
  University of Nebraska – Lincoln, Lincoln, Nebraska 68588 (USA)

3. Employment History

- 01/2006 to present Director of Research
  CoreTex Systems, LLC, Boca Raton, Florida 33432
- 09/2006 to 12/2007 Post-Doctoral Research Assistant Professor
  Department of Computer Science and Engineering
  Florida Atlantic University, Boca Raton, Florida 33431
- 01/2003 to 08/2006 Research Assistant (Secure Telecommunications)
  Florida Atlantic University, Boca Raton, Florida 33431
- 05/2002 to 08/2002 System and Security Administration (Internship)
  IBM Corporation, IBM Global Services, Phoenix, Arizona 85018
- 07/2001 to 09/2001 Cryptographic Software Developer
  Avaton, Inc., New York City, New York 10150-1243
- 05/2001 to 06/2001 Consultant for NTRU Public-key Cryptosystem Technologies
  Matsushita Electric Industrial, Co. (Panasonic), Japan
- 01/1997 to 08/2000 Research Assistant (Cryptography and Security)
  Department of Computer Science and Engineering
  University of Nebraska – Lincoln, and *Crypton Inc.*, Lincoln, NE 68588

4. Computing Experience

1. **Programming:** C/C++, VB, Java, VHDL, Assembly, JavaScript, XML, XHTML and CSS
2. **Programmable Environments:** MATLAB, Xilinx, MS Visual Studio, Dreamweaver, Maple, APL, MS Office, LaTex

5. Commercial and Research Projects

Client	Project Description	Involvement
Real Networks, Inc.	Research and development of novel methods for coding of binary shapes and shape regions in digital videos	* Led the development and investigation of methods for coding of binary shapes and shape regions in digital videos * Developed C/C++ software-based codec.
US Navy	Investigation of technologies for automated video surveillance including object detection, tracking and classification.	* Researched various algorithms and techniques involved in video surveillance * Developed MATLAB and C/C++ implementation of proposed algorithms
CoreTex Systems, LLC	Development of VHDL-based hardware design of cryptographic IP cores, and research and development of technology for securing biometric templates.	* Implemented compact and fast versions of AES, DES and 3DES symmetric-key cryptosystems and SHA and MD-5 hashing algorithms in VHDL. * Performed research, documented and implemented technology for storing biometric templates securely. Developed C/C++ libraries for Windows and Linux platforms.
BCAC, Corp.	Development of full Web-based database-driven system for medial insurance claims.	* Developed ASP.NET-based system for a large medical insurance company.
Crypton, Inc. and Avaton, Inc.	Development of software packages utilizing a novel symmetric block cipher based of non-Abelian groups.	* Led the commercial software development project. The project involved full GUI deliverables for Windows and Linux platforms.

6. Academic Recognitions, Honors, and Awards

- 2004-2005 The Daniel B. Newell and Aurel B. Newell Doctoral Fellowship ($5,000.00)
- 2003-2004 Graduate Fellowship for Academic Excellence ($5,000.00)

7. Publications

Books

1. Borko Furht, Edin A. Muharemagic and Daniel Socek, "Multimedia Security: Encryption and Watermarking", Springer, 2005. (ISBN: 0387244255)

Book Chapters

1. Daniel Socek, Vladimir Božović and Dubravko Ćulibrk, "Securing Biometric Templates where Similarity is Measured with Set Intersection", CCIS (Communications in Computer and Information Science), Springer, Scheduled for publication in 2008.
2. Borko Furht, Daniel Socek and Ahmet M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques", Multimedia Security Handbook (eds. B. Furht and D. Kirovski), CRC Press, 2005. (ISBN 0849327733)
   * also published in Multimedia Encryption and Authentication Techniques and Applications (eds. B. Furht and D. Kirovski), Auerbach Publications, 2006. (ISBN 0849372127)

Journal Publications

1. Daniel Socek, Vladimir Božović and Dubravko Ćulibrk, "Issues and Challenges in Storing Biometric Templates Securely", Revue de l'Electricité et de l'Electronique (REE), 2008, (accepted).

2. Daniel Socek, Spyros Magliveras, Dubravko Ćulibrk, Oge Marques, Hari Kalva, and Borko Furht, "Digital Video Encryption Algorithms Based on Correlation-Preserving Permutations", EURASIP Journal on Information Security, vol. 2007, Article ID 52965, 15 pages, 2007. doi:10.1155/2007/52965.
3. Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Ćulibrk and Borko Furht, "New approaches to encryption and steganography for digital videos", Multimedia Systems, vol. 13, no. 3, Springer-Verlag, 2007, pp. 191-204.
4. Dubravko Ćulibrk, Daniel Socek and Michal Sramka, "Cryptanalysis of a Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks", Tatra Mountains Mathematical Publications, vol. 37, 2007, pp. 75-91.
5. Dubravko Ćulibrk, Oge Marques, Daniel Socek, Hari Kalva and Borko Furht, "Neural Network Approach to Background Modeling for Video Object Segmentation", IEEE Transactions on Neural Networks, November 2007, pp. 1614-1627.
6. Tanya Seidel, Daniel Socek and Michal Sramka, "Cryptanalysis of Video Encryption Algorithms", Tatra Mountains Mathematical Publications, vol. 29, 2004, pp. 1-9
7. Borko Furht and Daniel Socek, "Multimedia Security: Encryption Techniques", Network Security: Technology Advances, Strategies, and Change Drivers, International Engineering Consortium, 2004, pp. 335-349.
8. Tanya Seidel, Daniel Socek and Michal Sramka, "Parallel Symmetric Attack on NTRU using Non-Deterministic Lattice Reduction", Designs, Codes and Cryptography, Kluwer Academic Publishers, vol. 32, no. 1-3, May 2004, pp. 369-379.

Conference Publications

1. Alvaro Fonseca, Liam M. Mayron, Daniel Socek, and Oge Marques, "Design and Implementation of an Optical Flow-based Autonomus Video Surveillance System", IASTED International Conference on Internet and Multimedia Systems and Applications (EuroIMSA 2008), March 17-19, 2008, Innsbruck, Austria (accepted).
2. Carlos Pertuz, Liam M. Mayron, Daniel Socek, and Oge Marques, "A Model for Detecting and Tracking Humans Using Appearance, Shape, and Motion", IASTED International Conference on Internet and Multimedia Systems and Applications (EuroIMSA 2008), March 17-19, 2008, Innsbruck, Austria (accepted).
3. Daniel Socek, Vladimir Božović and Dubravko Ćulibrk, "Practical Secure Biometrics Using Set Intersection as a Similarity Measure", in International Conference on Security and Cryptography (SECRYPT 2007), July 28-31, 2007, Barcelona, Spain, pp. 25-32.
4. Daniel Socek, Vladimir Božović and Dubravko Ćulibrk, "Issues and Challenges in Storing Biometric Templates Securely", in International Conference on Risks and Security of Internet and Systems (CRiSIS 2007), July 2-5, 2007, Marrakech, Morocco, pp. 75-81.
5. Dubravko Ćulibrk, Vladimir Radenković and Daniel Socek, "Enhancing Video Object Segmentation Results Through Biologically Inspired Postprocessing", in 8th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS 2007), September 26-28, 2007, Niš, Serbia, pp. 329-332.
6. Oge Marques, Liam M. Mayron, Daniel Socek, Gustavo B. Borba and Humberto R. Gamba, "An attention-based method for extracting salient regions of interest from stereo images", in International Conference on Computer Vision Theory and Applications (VISAPP 2007), March 8-11, 2007, Barcelona, Spain, pp. 294-297.
7. Dubravko Ćulibrk, Daniel Socek, Oge Marques, and Borko Furht "Automatic Kernel Width Selection for Neural Network Based Video Object Segmentation", in International Conference on Computer Vision Theory and Applications (VISAPP 2007), March 8-11, 2007, Barcelona, Spain, pp. 472-479.
8. Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Ćulibrk and Borko Furht, "A Permutation-Based Correlation-Preserving Encryption Method for Digital Videos", in International Conference on Image Analysis and Recognition (ICIAR 2006), September 18-20, 2006, Póvoa de Varzim, Portugal, pp. 547-558.
9. Daniel Socek, Michal Sramka, Oge Marques and Dubravko Ćulibrk, "An Improvement to a Biometric-Based Multimedia Content Protection Scheme", in 8th ACM Multimedia and

Security Workshop (MM&Sec 2006), September 26-27, 2006, Geneva, Switzerland, pp. 135-139.

10. Daniel Socek, Dubravko Ćulibrk, Hari Kalva, Oge Marques and Borko Furht, "Permutation-Based Low-Complexity Alternate Coding in Multi-View H.264/AVC", in IEEE International Conference on Multimedia & Expo (ICME 2006), July 9-12, 2006, Toronto, ON, Canada, pp. 2141-2144.
11. Dubravko Ćulibrk, Oge Marques, Daniel Socek, Hari Kalva and Borko Furht, "A Neural Network Approach to Bayesian Background Modeling for Video Object Segmentation", in International Conference on Computer Vision Theory and Applications (VISAPP 2006), February 25-28, 2006, Setúbal, Portugal, pp. 474-479.
12. Daniel Socek, Dubravko Ćulibrk, Oge Marques, Hari Kalva and Borko Furht, "A Hybrid Color-Based Foreground Object Detection Method for Automated Marine Surveillance", in Advanced Concepts for Intelligent Vision Systems (ACIVS 2005), September 20-23, 2005, Antwerp, Belgium, pp. 340-347.
13. Daniel Socek, Shujun Li, Spyros S. Magliveras and Borko Furht, "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption", in 1st IEEE/CreateCom International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005), September 5-9, 2005, Athens, Greece, pp. 406-408.
14. Daniel Socek and Dubravko Ćulibrk, "On the Security of a Clipped Hopfield Neural Network Cryptosystem", in 7th ACM Multimedia and Security Workshop (MM&Sec 2005), August 1-2, 2005, New York NY, USA, pp. 71-75.
15. Daniel Socek and Spyros S. Magliveras, "General Access Structures in Audio Cryptography", in IEEE International Conference on Electro Information Technology (EIT 2005), May 22-25, 2005, Lincoln NE, USA.

Technical Reports

1. Daniel Socek and Dubravko Ćulibrk, "Methods for Binary Shape Coding in Digital Videos", Technical Report for Real Networks, Inc, May 2007. *Confidential
2. Spyros S. Magliveras and Daniel Socek, "Evaluation of NTRU cryptosystem", Technical Report for Matsushita Electric Industrial (Panasonic), July 2001. *Confidential

Theses/Dissertations

1. Daniel Socek, "Deterministic and Non-deterministic Basis Reduction Techniques for NTRU Lattices", M.Sc. thesis, Department of Mathematical Sciences, Florida Atlantic University, December 2002.
2. Daniel Socek, "Permutation-Based Transformations for Digital Multimedia Encryption and Steganography", Ph.D. dissertation, Department of Computer Science and Engineering, Florida Atlantic University, August 2006.

8. Patents

Daniel Socek, Hari Kalva and Spyros S. Magliveras, "Methods for encrypting and compressing video", Patent #20070291941