PERSONAL INFORMATION

Sebastian Banescu

Hochbrücker Weg 2, 85396 Eching, Germany

(+49) 176 4152 5239

banescusebi@gmail.com

de.linkedin.com/in/sebastianbanescu

EDUCATION AND TRAINING

Dates	October 2014 - April 2017
Title of qualification awarded	**Dr. rer. nat.** *"summa cum laude"*
Name of organization	**Technical University of Munich, Germany**, Center for Doctoral Studies in Informatics and its Applications (CeDoSIA) Graduate School, Faculty of Informatics
PhD Thesis Title	Characterizing the Strength of Software Obfuscation Against Automated Attacks

Dates	September 2010 - August 2012
Title of qualification awarded	**MSc.Information Security Technologies** *"cum laude"* (GPA: 8.5 of 10, Thesis: 9 of 10)
Scholarship	Talent Scholarship Program, currently Amandus H. Lundqvist Scholarship Program
Name of organization	**Technical University of Eindhoven, The Netherlands**, Faculty of Computer Science
MSc. Thesis Title	Decision Support for Privacy Auditing

Dates	October 2006 - July 2010
Title of qualification awarded	**BSc. Computer Science and Engineering** (GPA: 9.5 of 10, Thesis: 10 of 10)
Scholarship	Merit-based and Performance-based scholarships due to academic results
Name of organization	**Technical University of Cluj-Napoca, Romania**, Faculty of Computer Science
BSc. Thesis Title	Unpredictable Random Number Generator Applied in Hardware Resource Allocation

WORK EXPERIENCE

Dates	May 2017 - onward
Position	**IT Security Specialist** - member of Connected Car Security Team
Employer	**BMW AG, Germany** - Connected Drive Department
Responsibilities	Developing IT security defenses against car hackers, for the BMW fleet.

Dates	April 2013 - April 2017
Position	**Researcher** / **Teaching Assistant** - member of Software Engineering Chair
Employer	**Technical University of Munich, Germany** - Faculty of Informatics
Responsibilities	Collaborated with Google Chrome security team to develop solutions against browser hijacking malware. Teaching assistance for MSc. and BSc. level courses. Co-developed "Secure Coding" lecture, which was awarded the TUM prize for teaching excellence.

Dates	September 2012 - March 2013
Position	**Security Engineer** - member of Digital Video Broadcast team
Employer	**TP Vision, The Netherlands** - Innovation Site Eindhoven
Responsibilities	Secure design, integration and testing of key management, DRM, copy and content protection systems. Mainly used C/C++. Assessed compliance and robustness rules for new systems.

Dates	February 2012 - August 2012
Position	**Master Thesis Intern** - member of the T-Clouds project team
Employer	**Philips Research, The Netherlands** - Healthcare Information Management, Security Cluster
Responsibilities	Developed secure logging and log aggregation module for the TClouds project co-financed under EU FP7 and obtained **patent US20160134495** for it. Developed a privacy infringement detection and quantification tool and published 2 peer-reviewed papers about it. Mainly used Java.

Dates	July 2011 - November 2011
Position	**Intern Student** - member of Security & Privacy team
Employer	**Deloitte, The Netherlands** - Enterprise Risk Services
Responsibilities	Manual and (semi-)automated penetration testing of web-applications. Developed a privacy escalation testing tool as a script for OWASP WebScarab. Developed a password brute-forcing script for iMacros FF and IE plug-in. Mainly used PHP.

SELECTED PROJECTS

2017-onward	Bilateral Project between BMW and TU Munich: *Intrusion Detection for Connected Cars*
2015-2016	Bilateral Project between Google Canada and TU Munich: *Software Protection for Chrome Against Memory Tampering*
2014	Bilateral Project between Siemens and TU Munich: *Detecting Bugs in Native Software Using Symbolic Execution*
2013-2014	Bilateral Project between Google Germany and TU Munich: *Software Protection for Chrome Against Browser Hijacking Attacks*
2012	EU FP7 Project: *Trustworthy Clouds – Privacy and Resilience for Internet-scale Critical Infrastructure* (TClouds) http://cordis.europa.eu/project/rcn/97862_en.html
2011-2012	Dutch Government Project: *Trusted HEalthCare Services* (COMMIT/THECS) http://www.commit-nl.nl/projects/trusted-healthcare-services
2008-2010	Romanian Government Project: *A High Performance System for Generation and Testing of Random Number Sequences for Cryptographic Applications* (CryptoRand) http://cryptorand.utcluj.ro/

AWARDS, GRANTS AND SCHOLARSHIPS

2017	**Jungwissenschaftler 2017** awarded by *Stiftung Werner-von-Siemens-Ring*
2016	**Outstanding paper award** at 32nd Annual Computer Security Applications Conference (ACSAC)
2016	**Best paper award** at 6th Software Security, Protection and Reverse Engineering Workshop (SSPREW)
2015	**Google Grant** for funding a full-time PhD student for one year
2014	**Siemens Grant** for funding a full-time PhD student for one semester
2014	**Best Code Cracker of ISSISP 2014** award at the International Summer School on Information Security and Protection, Verona, Italy
2014	**TU Munich Award for Excellence in Teaching**, awarded for newly developed “Secure Coding” lecture
2013	**Google Grant** for funding a full-time PhD student for one year
2010-2012	**Dutch Talent Scholarship Program**, currently Amandus H. Lundqvist Scholarship Program
2009	**ERASMUS Scholarship** for summer internship at ENS Lyon
2007-2010	Romanian government sponsored merit-based and performance-based scholarships due to outstanding academic results

PEER-REVIEWED PUBLICATIONS

Journals

Banescu, S; de Dinechin, F; Pasca, B; Tudoran R; - *Multipliers for Floating-Point Double Precision and Beyond on FPGAs*. ACM SIGARCH Computer Architecture News 38.4: 73-79, 2010

Conferences

1. **Banescu, S**; Collberg, C; Pretschner, A; *Predicting the Resilience of Obfuscated Code Against Symbolic Execution Attacks via Machine Learning*. In Proc. of the USENIX Security Symposium (USENIX Sec), 2017
2. **Banescu, S**; Ahmadvand, M; Pretschner, A; Shield, R; Hamilton, C; *Detecting Patching of Executables without System Calls*. In Proc. of the 7th ACM Conference on Data and Application Security and Privacy (CODASPY), 2017
3. Ochoa, M; **Banescu, S**; Disenfeld, C; Barthe, G; Ganesh, V; *Reasoning about Probabilistic Defense Mechanisms against Remote Attacks*. In Proc. of 2nd IEEE European Symposium on Security and Privacy (EuroS&P), 2017

4 **Banescu, S**; Collberg, C; Ganesh, V; Newsham, Z; Pretschner, A; *Code Obfuscation Against Symbolic Execution Attacks.* In Proc. of 32nd Annual Computer Security Applications Conference (ACSAC), 2016 **Outstanding Paper Award**

5 **Banescu, S**; Wuechner, T; Salem, A; Guggenmos, M; Ochoa, M; Pretschner, A; *A Framework for Empirical Evaluation of Malware Detection Resilience Against Behaviour Obfuscation*. In Proc. of 10th International Conference on Malicious and Unwandted Software (MALWARE), 2015

6 Fedler, R; **Banescu, S**; Pretschner, A; *ISA2R: Improving Software Attack and Analysis Resilience via Compiler-Level Software Diversity*. In Proc. of 34th International Conference on Safety, Reliability, and Security (SAFECOMP), 2015

7 **Banescu, S**; Pretschner, A; Battre, D; Cazzulani, S; Shield, R; Thompson, G; *Software-Based Protection against "Changeware"*. In Proc. of the 5th ACM Conference on Data and Application Security and Privacy (CODASPY), 2015

8 **Banescu, S**; Ochoa, M; Kunze, N; Pretschner, A; *Idea: Benchmarking indistinguishability obfuscation - A candidate implementation*. In Proc. of the International Symposium on Engineering Secure Software and Systems (ESSoS), 2015

9 **Banescu, S**; Petkovic, M; Zannone, N; *Measuring Privacy Compliance Using Fitness Metrics*. Proc. of the 10th International Conference on Business Process Management (BPM), 2012

10 Suciu, A; **Banescu, S**; Marton, K; *Unpredictable random number generator based on hardware performance counters*. Digital Information Processing and Communications (ICDIPC), 2011

11 Tudoran, R; **Banescu, S**; Cret, O; Suciu, A; - *Implementing True Random Number Generators by Overfilling the FPGA Chip*. Proc. of the FPGA World 2009 International Conference (FPGA World), 2009

12 Colesa, A; Tudoran, R; **Banescu, S** - *Software Random Number Generation Based on Race Conditions*. Proc. of the 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, September (SYNASC), 2008

Workshops

1 Salem, A; **Banescu, S**. *Metadata Recovery From Obfuscated Programs Using Machine Learning*. In Proc. of the 6th Software Security, Protection and Reverse Engineering Workshop (SSPREW@ACSAC), 2016 **Best Paper Award**

2 **Banescu, S**; Lucaci, C; Krämer, B; Pretschner, A; *VOT4CS: A Virtualization Obfuscation Tool for C#*. In Proc. of 2nd International Workshop on Software Protection (SPRO@CCS), 2016

3 Ibrahim, A; **Banescu, S**; *StIns4CS: A State Inspection Tool for C#*. In Proc. of 2nd International Workshop on Software Protection (SPRO@CCS), 2016

4 Holling, D; **Banescu, S**; Probst, M; Petrovska, A; Pretschner, A; *Nequivack: Assessing mutation score confidence*. In Proc. of 9th International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 2016

5 Ganesh, V; **Banescu, S**; Ochoa, M; *The Meaning of Attack Resistant Systems*. In Proc. of the 10th Workshop on Programming Languages Analysis for Security (PLAS@ECOOP), 2015

6 **Banescu, S**; Ochoa, M; Pretschner, A; *A Framework for Measuring Software Resilience Against Automated Attacks*. In Proc. of the 1st International Workshop on Software Protection (SPRO@ICSE), 2015

7 **Banescu, S**; Zannone, N; *Measuring privacy compliance with process specifications*. Proc. of the 7th International Workshop on Security Measurements and Metrics (MetriSec), 2011

TRAININGS OFFERED

2017 **Invited trainer** at "7th Software Security, Protection and Reverse Engineering Workshop" (SSPREW) http://www.ssprew.org/ collocated with ACSAC 2017, Orlando, Florida, USA

2016 **Invited trainer** at "Industrial Software Protection Workshop" organized by Dolby Germany in collaboration with TU Munich, at Dolby office in Nuremberg, Germany

INVITED TALKS

Jul. 2017 *"Characterizing the Strength of Software Obfuscation Against Automated Attacks"* at Dagstuhl Seminar on "Malware Analysis: From Large-Scale Data Triage to Targeted Attack Recognition", Dagstuhl, Germany

Apr. 2017 *"Characterizing the strength of software obfuscation against symbolic execution attacks"* at Singapore University of Technology and Design (SUTD) by Dr. Martin Ochoa, Singapore

Dec. 2016 *"Analysing (De-)Obfuscation via Machine Learning"* at Itestra GmbH Jour Fixe, Munich, Germany

Sep. 2016 *"Code Obfuscation Against Symbolic Execution Attacks"* at Friedrich-Alexander Universität (FAU) Erlangen by Prof. Dr.-Ing. Felix Freiling, Erlangen, Germany

SCIENTIFIC SERVICE

Program Committee

PC Member of "7th Software Security, Protection and Reverse Engineering Workshop" (SSPREW) collocated with ACSAC 2017, Orlando, Florida, USA

External Reviewer

1. MSCS '17: Journal of Mathematical Structures in Computer Science
2. IFIPSEC '17: International Conference on ICT Systems Security and Privacy Protection
3. DIST '16: Journal of Distributed Computing
4. SACMAT '15, '17: ACM Symposium on Access Control Models and Technologies
5. CloudCom '16: IEEE International Conference on Cloud Computing Technology and Science
6. TDSC '13, '14, '15: Transactions on Dependable and Secure Computing
7. CODASPY '14, '15: ACM Conference on Data and Application Security and Privacy
8. NSS '14, '15: The International Conference on Network and System Security
9. QSIC '13: International Conference on Quality Software
10. ESORICS '13: European Symposium on Security in Computer Security

Supervised Students

1. Alexander Ungar (BSc. thesis): *Benchmarking Symbolic Execution Tools on Custom Block Ciphers*, submitted on 15 May 2017
2. Ilya Migal (MSc. thesis): *Prediction of automated deobfuscation & tampering time using machine learning*, submitted on 15 Mar 2017
3. Carlo DiDomenico (MSc. thesis): *iOS Application Hardening via Obfuscation*, submitted on 15 Jan 2017
4. Dennis Fischer (BSc. thesis): *Detecting Process Memory Tampering*, submitted on 15 Feb 2016
5. Amjad Ibrahim (MSc. thesis): *Software Protection by Self-Checking*, submitted on 15 Dec 2015
6. Aleieldin Salem (MSc. thesis): *Metadata Recovery of Transformations from Obfuscated Software via Machine Learning Techniques*, submitted on 21 Oct 2015
7. Renè Milzarek (Guided research): *A Taxonomy of Browser Hijacking Malware*, submitted on 19 Oct 2015
8. Ciprian Lucaci (MSc. thesis): *Software Protection by Virtualization Obfuscation*, submitted on 15 Oct 2015
9. Marco Probst (BSc. thesis): *Checking Non-Equivalence of Software Programs using Symbolic Execution*, submitted on 12 Jun 2015
10. Andreas Geiger (MSc. thesis): *Raising the Bar for Automated Attacks against Web Applications using Software Diversity*, submitted on 15 May 2015
11. Marius Guggenmos (BSc. thesis): *Towards Testing Malware Detection Systems using Behavioral Obfuscation*, submitted on 15 Feb 2015
12. Rafael Fedler (MSc. thesis): *Code Transformations and Software Diversity for Improving Software Attack and Analysis Resilience*, submitted on 15 Nov 2014 **CAST-Förderpreis IT-Sicherheit 2015**
13. Nils Kunze (BSc. thesis): *A Qualitative Study of Indistinguishability Obfuscation*, submitted on 15 Aug 2014
14. Nils Vissman (MSc. thesis): *Software Integrity Protection using White-Box Cryptography*, submitted on 15 May 2014

RESEARCH VISITS

Dates February - March 2016

Position **Visiting Research Scholar** worked with Prof. Dr. Saumya Debray and Prof. Dr. Christian Collberg on characterizing obfuscation strength via case-studies using binary executables.

Name of organization **University of Arizona, Tucson, USA**, Faculty of Computer Science

Dates September 2015

Position **Visiting Research Scholar** worked with Prof. Dr. Vijay Ganesh on employing symbolic execution and SAT/SMT solvers for the purpose of de-obfuscating binary executables.

Name of organization **University of Waterloo, Canada**, Department of Electrical and Computer Engineering

Dates June - September 2009

Position **ERASMUS Exchange student** worked with Prof. Dr. Florent de Dinechin. Developed a C++ tool to generate high precision multiplication operators (as VHDL code) for FPGAs.

Name of organization **Ecole Normale Superieure Lyon, France**, Laboratoire de l'Informatique du Parallélisme

PERSONAL SKILLS AND COMPETENCES

Mother tongue(s) Romanian

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	Advanced (C2)	Advanced (C2)	Advanced (C1)	Advanced (C1)	Advanced (C1)
German	Intermediate (C1)	Intermediate (C1)	Intermediate (B2)	Intermediate (B2)	Intermediate (B2)

Programming and Scripting Languages *Intermediate:* Java, C, R, x86 Assembly, Bash Script, Python
Beginner: C#, VHDL, Matlab, Prolog, Haskel, ML, Lisp

Black-Box Testing Tools *Beginner:* Nessus, Burpsuite, ZAP, Wireshark, Sqlmap, Zenmap

White-Box Testing Tools *Intermediate:* KLEE, S2E
Beginner: Fortify, RIPS, FindBugs

Reverse Engineering *Intermediate:* IDA Pro, GDB, angr, Triton, JavaDecompiler

MISCELLANEOUS

Poster Presentations NOTE: The following posters are not accompanied by proceedings

1. Banescu S. *Raising the Bar for Browser Hijacking*, Google PhD Student Summit on Web Application Security, Google Office, Munich Germany, April 2016
2. Banescu S. *Diverse Software Obfuscation: Attacks and Defenses*, 34th TUM Graduate School Kick-Off Seminar, Frauenchiemsee, Germany, February 2015
3. Banescu S. *Attacks on Software Obfuscation and Diversity*, 5th International Summer School on Information Security and Protection, Verona, Italy, July 2014

Middle-/High-School Participated in various **mathematics and informatics olympiads and contests** at county and national levels. Obtained notable awards including **1st, 2nd and 3rd prizes**

Volunteer Work Volunteer IT Consultant for League of Romanian Students Abroad (2010-2012)

Volunteer in civic cleaning campaigns in my home town

Recommendations Upon request from Prof. Dr. Alexander Pretschner, e-mail: alexander.pretschner@tum.de
Other 10 recommendations already available on Linkedin: de.linkedin.com/in/sebastianbanescu

Research Interests Software Protection, Reverse Engineering, Anomaly Detection