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
Position	**PhD. student**
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. Computer Science and Engineering - Information Security Technology** graduated *"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

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 ELF x86 binaries.
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 ELF x86 binaries.
Name of organization	**University of Waterloo, Canada**, Department of Electrical and Computer Engineering

Dates	June 2009 - September 2009
Position	**ERASMUS Exchange student** worked with Prof. Dr. Florent de Dinechin. Developed a high precision multiplication operators for FPGA chips. Mainly used C/C++ to generate VHDL.
Name of organization	**Ecole Normale Superieure Lyon, France**, Laboratoire de l'Informatique du Parallélisme

WORK EXPERIENCE

Dates	May 2017 - onward
Position	**IT Security Specialist** - member of Connected Security Team
Employer	**BMW AG, Germany** - IT-Zentrum München
Responsibilities	Developing IT defenses against hackers, for the connected BMW cars.

Dates April 2013 - April 2017
Position **Researcher** / **Teaching Assistant** - member of Software Engineering Chair
Employer **Technical University of Munich, Germany** - Faculty of Informatics
Responsibilities Research in the field of software protection, collaborated with Google Chrome security teams, developed solutions against browser hijacking malware in C/C++. Teaching assistance for MSc. and BSc. level courses, for 6 semesters. Co-developed "Secure Coding" lecture, which was awarded the TUM prize for teaching excellence. Advised over 15 MSc. and BSc. theses, many of which concluded with peer-reviewed publications; more details at https://www22.in.tum.de/banescu

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. Developed specifications for ARM TrustZone integration of the afore mentioned 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.

PROJECTS

Title **Symbolic Execution for Software Deobfuscation**
Description Generated a set of over 5000 C program benchmarks and obfuscated them with various techniques, i.e.: self-modifying code, virtualization (emulation/packing), control-flow flattening, opaque predicates, mixed boolean-arithmetic, etc. Compiled programs using LLVM Clang and GCC into ELF binaries. Recovered hidden passwords from obfuscated programs by applying directed dynamic symbolic execution on all obfuscated binaries. Analyzed the effect of different obfuscation techniques on the effort required by the symbolic execution-based attack. Identified major differences between different obfuscation transformations.
Skills Used Dynamic symbolic execution, software obfuscation, statistical analysis.
Technologies Used C, Python, Bash Script, R.
Achievements **Outstanding paper** at 32nd Annual Computer Security Applications Conference (ACSAC), 2016. Released dataset of over 5000 C programs to public to advance state of the art in software deobfuscation.

Title **Machine Learning for Classification of Obfuscated Software**
Description Created a dataset of over 11.000 obfuscated C programs and compiled them to ELF binaries. Extracted term-frequency inverse document-frequency (TF-IDF) features from artifacts resulting from both static and dynamic analysis of obfuscated ELF binaries. Applied naive Bayes and decision tree classifiers to determine the obfuscation transformations applied on the obfuscated binaries. Obtained 99% classification accuracy of obfuscated binaries according to applied obfuscation transformations.
Skills Used Supervised machine learning for multi-level classification, static and dynamic binary analysis.
Technologies Used C, Python, Bash Script.
Achievements **Best paper** at 6th Software Security, Protection and Reverse Engineering Workshop (SSPREW), 2016. **Open source** implementation of binary analysis framework called Oedipus for metadata recovery.

Title **Software-based Integrity Protection for Google Chrome**

Description: Wrote proposals and obtained grants for 2 projects in collaboration with Google Germany and Google Canada for developing software-based solutions for protecting Google Chrome against an instance of potentially unwanted programs called browser hijackers. Developed solutions using white-box cryptography, control-flow integrity and dynamic code checksumming. The solutions are able to protect both static and dynamic memory of Google Chrome against unwanted modifications by browser hijackers.

Skills Used: Software protection techniques, reverse engineering

Technologies Used: C/C++, x86 Assembly

Achievements: **Open source** implementation of software protection for Google Chrome. Two peer-reviewed publications at 5th and 7th ACM Conference on Data and Application Security and Privacy (CODASPY), 2015 and 2017.

PEER-REVIEWED PUBLICATIONS

1 **Banescu, S**; Collberg, C; Pretschner, A; *Predicting the Resilience of Obfuscated Code Against Symbolic Execution Attacks via Machine Learning*. To appear in Proc. of the USENIX Security Symposium (USENIX Sec), 2017

2 **Banescu, S**; Ahmadvand, M; Pretschner, A; *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 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**

6 **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

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

8 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

9 **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

10 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

11 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

12 **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

13 **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

14 **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

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

16 Pieters, W; **Banescu, S**; Posea, S; *Preventing system abuse by service composition*. Proc. of the Third International Engineering Systems Symposium (CESUN), 2012

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

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

19 **Banescu, S**; de Dinechin, F; Pasca, B; Tudoran R; - *Multipliers for Floating-Point Double Precision and Beyond on FPGAs*. Proc. of the 1st International Workshop on Highly Efficient Accelerators and Reconfigurable Technologies (HEART), 2010

20 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, 2009

21 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

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 (B2)	Intermediate (B2)	Intermediate (B1)	Intermediate (B1)	Intermediate (B1)

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

Web Technologies
Intermediate: PHP, HTML, JavaScript, CSS, AJAX, XML

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

Integrated Development Environments
Intermediate: Eclipse, MS Visual Studio
Beginner: vim, Matlab, Xilinx ISE

SCM Tools
Intermediate: Subversion (SVN), Git

DBMS
Intermediate: MySQL, MS SQL Server

Soft Skills
Great Communication Skills, Team Player, Detail Oriented, Public Speaking & Presenting

MISCELLANEOUS

Activities and Achievements

Contributer to **Google Syzygy** open source project https://github.com/banescusebi

- **Outstanding paper award** at 32nd Annual Computer Security Applications Conference (ACSAC), December 2016
- **Best paper award** at 6th Software Security, Protection and Reverse Engineering Workshop (SSPREW), December 2016
- **Invited speaker** at Itestra GmbH Jour Fixe, December 2016, Munich Germany
- **Invited speaker** at Friedrich-Alexander Universität (FAU) Erlangen by Prof. Dr.-Ing. Felix Freiling, September 2016, Erlangen Germany.
- **Invited trainer** at “Software Protection Workshop” organized by Dolby Germany, August 2016
- **Winner of “Best Code Cracker of ISSISP 2014”** award at the International Summer School on Information Security and Protection, July 2014, Verona, Italy
- Participated in various **mathematics and informatics olympiads and contests** at county and national levels. Obtained notable awards including **1st, 2nd and 3rd prizes** (1998-2006)

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

Volunteer in civic cleaning campaigns in my home town (1998-2006)

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

Hobbies
Snowboarding, Football, Hiking, Board games