CURRICULUM VITAE

PERSONAL INFORMATION

Name	**Cristian-Alexandru STAICU**
Nationality	Romanian, German
Address	Stuhlsatzenhaus 5, 66123 Saarbrücken, Germany
Telephone	+40767273885 / +4915780213641
E-mail	cris.staicu@gmail.com
Date of Birth	22nd of June 1988
Research Page	https://www.staicu.org

WORK AND RESEARCH EXPERIENCE

CISPA – Helmholtz Center for Information Security, Germany

Tenure-Track Faculty — **October 2020 - present**

My core research interest is in system security, at the intersection of software/web security, software engineering and programming languages. I am leading a research group consisting of three full-time PhD students, one student helper, and multiple thesis students, all performing cutting-edge research in system security. My group's goal is to directly contribute to the open-source ecosystem: either by building tools that can be used by practitioners or by uncovering security vulnerabilities in real systems/projects. I am often a program committee member or author at top-tier security conferences like ACM CCS, USENIX Security, or IEEE S&P. Moreover, I regularly teach and supervise theses at Saarland University.

Technical University of Darmstadt, Germany

Research Assistant — **October 2014 - July 2020**

I was a member of the Software Lab group, performing cross-disciplinary research. My main interest during this time was in analyzing the security and privacy of JavaScript code, mostly using language-based techniques, e.g., static and dynamic program analysis, test generation. In particular, I investigated novel ways of finding and preventing vulnerabilities specific to server-side JavaScript programs and libraries. My research uncovered tens of previously unknown vulnerabilities in server-side libraries, i.e., npm modules.

Semmle Inc Oxford (now GitHub), United Kingdom

Intern — **May 2018 - August 2018**

My internship project was to improve a JavaScript static taint analysis by considering the semantics of third-party libraries. I reported multiple vulnerabilities as a result of my internship (see hackerone profile: cris_semmle).

Philips Research Eindhoven, Netherlands

Intern — **January 2014 - July 2014**

My responsibilities included understanding HIMMO, an identity-based key agreement scheme developed by Philips, implementing two variations of the scheme and analyzing the impact of these modifications both from a security perspective and also from a resource consumption point of view.

acp-IT AG Timişoara, Romania

Software Developer — **October 2010 - July 2012**

I was part of a team that developed an airport passenger flow simulation tool for an important European airport. My contribution to this project was to implement a state-of-the-art algorithm (Social Force Model) as well as to optimize, parallelize and adapt it to the project's needs.

Alcatel-Lucent Timişoara, Romania
Junior Developer **January 2010 - October 2010**
My main contribution was to automatize the existing testing infrastructure by developing a Java tool for creating bootable USB devices.

Continental Automotive Timişoara, Romania
Intern **July 2009 - October 2009**
I designed and implemented a Java / Swing application which manipulates C source code. It is used internally as an easy way to modify huge source code files and keep them consistent.

Dream Production Timişoara, Romania
Programmer **August 2008 - March 2009**
I was part of a team that implemented web applications in PHP, JavaScript, and Flex. I mainly contributed to the development of a platform where people can take actions against day-to-day issues.

EDUCATION

Technical University Darmstadt, Germany
Department of Computer Science
Doctoral Degree **October 2014 - March 2020**
I completed my PhD under the supervision of Prof. Dr. Michael Pradel. My doctoral thesis with the title *Enhancing the Security and Privacy of Full-Stack JavaScript Web Applications* argues for a holistic approach to hardening an important, emerging class of web applications, which use JavaScript both on the server-side and on the client-side. The thesis consists of several peer-reviewed papers, published at top-tier academic conferences, mainly in the areas of security and privacy, software engineering and programming languages.

EIT Digital Master School - Double Degree Program
University of Trento, Italy / University of Twente, Netherlands
Master Degree, Major in Computer Security and Privacy **September 2012 - August 2014**

March 2013 - July 2013	I worked with Dr. Mariano Ceccato on a project within the FBK research center. We investigated ways of selecting a high diversity subset from a large population of obfuscated versions of a program. My contribution was to study the existing search-based techniques and to apply them to our problem.
October 2012 - February 2013	I worked in Prof. Dr. Massimiliano Sala's team to develop a double authentication prototype for a banking service provider company. My contribution was to implement the server-side logic of the application using JEE technologies and cryptographic primitives like RSA, AES, PKCS12.

Polytechnic University Timişoara, Romania
Faculty of Automation and Computer Science
Bachelor Degree in Computers and Information Technology **October 2007 - July 2011**

2011	I completed my thesis with the title *SherlockJ, Statistical Debugging Tool*, supervised by Prof. Dr. Marius Minea. I designed and implemented an Eclipse plugin which uses existing unit tests and well-known automatic debugging algorithms, i.e., dynamic analysis techniques, to locate bugs inside Java projects.
2009	Won 1st place in "Alexandru Rogojanu" Programming Contest and qualified for "ACM ICPC SouthEastern European Region" representing the university.

PUBLICATIONS LIST

NDSS 2025	A. Alhamdan, **C.-A. Staicu**, *Welcome to Jurassic Park: A Comprehensive Study of Security Risks in Deno and its Ecosystem*, Annual Network and Distributed System Security Symposium (NDSS'25), 2025.
ASE 2024	D. Troppmann, A. Fass, **C.-A. Staicu**, *Typed and Confused: Studying the Unexpected Dangers of Gradual Typing*, International Conference on Automated Software Engineering (ASE'24), 2024.
NAACL 2024	H. Hajipour, N. Yu, **C.-A. Staicu**, M. Fritz, *SimSCOOD: Systematic Analysis of Out-of-Distribution Generalization in Fine-tuned Source Code Models*, Annual Conference of the North American Chapter of the Association for Computational Linguistics (NAACL'24), 2024.
CCS 2023	J. Rack, **C.-A. Staicu**, *Jack-in-the-box: An Empirical Study of JavaScript Bundling on the Web and its Security Implications*, Conference on Computer and Communications Security (CCS'23), 2023.
USENIX SEC 2023	A. Alhamdan, **C.-A. Staicu**, *SandDriller: A Fully-Automated Approach for Testing Language-Based JavaScript Sandboxes*, USENIX Security Symposium, 2023.
USENIX SEC 2023	**C.-A. Staicu**, S. Rahaman, Á. Kiss, M. Backes, *Bilingual Problems: Studying the Security Risks Incurred by Native Extensions in Scripting Languages*, USENIX Security Symposium, 2023.
USENIX SEC 2023	M. Shcherbakov, M. Balliu, **C.-A. Staicu**, *Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js*, USENIX Security Symposium, 2023.
ICSE 2023	M. Bhuiyan, A. Parthasarathy, N. Vasilakis, M. Pradel, **C.-A. Staicu**, *SecBench.js: An Executable Security Benchmark Suite for Server-Side JavaScript*, International Conference on Software Engineering (ICSE'23), 2023.
CCS 2021	N. Vasilakis, **C.-A. Staicu**, N.Ntousakis, K. Kallas, B. Karel, A. DeHon, M. Pradel, *Preventing Dynamic Library Compromise on Node.js via RWX-Based Privilege Reduction*, Conference on Computer and Communications Security (CCS'21), 2021.
ICSE 2020	**C.-A. Staicu**, M. T. Torp, M. Schäfer, A. Møller, M. Pradel, *Extracting Taint Specifications for JavaScript Libraries*, International Conference on Software Engineering (ICSE'20), 2020.
USENIX SEC 2019	**C.-A. Staicu**, M. Pradel, *Leaky Images: Targeted Privacy Attacks in the Web*, USENIX Security Symposium, 2019.
USENIX SEC 2019	M. Zimmermann, **C.-A. Staicu**, C. Tenny, M. Pradel, *Small World with High Risks: A Study of Security Threats in the npm Ecosystem*, USENIX Security Symposium, 2019.
WWW 2019	P. Skolka, **C.-A. Staicu**, M. Pradel, *Anything to Hide? Studying Minified and Obfuscated Code in the Web*, The Web Conference, 2019.
PLAS@CCS 2019	**C.-A. Staicu**, D. Schoepe, M. Balliu, M. Pradel, A. Sabelfeld, *An Empirical Study of Information Flows in Real-World JavaScript*, The Workshop on Programming Languages and Analysis for Security (PLAS'19), 2019.
USENIX SEC 2018	**C.-A. Staicu**, M. Pradel, *Freezing the Web: A Study of ReDoS Vulnerabilities in JavaScript-based Web Servers,* USENIX Security Symposium, 2018.
NDSS 2018	**C.-A. Staicu**, M. Pradel, B. Livshits, *Synode: Understanding and Automatically Preventing Injection Attacks on Node.js,* Annual Network and Distributed System Security Symposium (NDSS'18), 2018.

ASE 2017	L. Della Toffola, **C.-A. Staicu**, M. Pradel, *Saying "Hi!" Is Not Enough: Mining Inputs for Effective Test Generation*, International Conference on Automated Software Engineering (ASE'17), 2017.
CSUR 2017	E. Andreasen, L. Gong, A. Møller, M. Pradel, M. Selakovic, K. Sen, **C.-A. Staicu**, *A Survey of Dynamic Analysis and Test Generation for JavaScript*, ACM Computing Surveys, 2017.
ICSE 2016	H. Liu, Q. Liu, **C.-A. Staicu**, M. Pradel, Y. Luo, *Nomen est Omen: Exploring and Exploiting Similarities between Argument and Parameter Names*, International Conference on Software Engineering (ICSE'16), 2016.

TALKS AND POSTER SESSIONS

excluding conference talks

2022	CAST/GI Promotionspreis IT-Sicherheit 2022
2021	Daimler AG, *Host: Martin Wittiger*
2020	Blekinge Institute of Technology, *Host: Nurul Momen*
	IMDEA Software Institute *Host: Manuel Carro*
	CISPA – Helmholtz Center for Information Security, *Host: Andreas Zeller*
2019	Katholieke Universiteit Leuven, Belgium, *Host: Wouter Joosen*
	Google Compiler and Programming Language Summit, Germany
	Stanford University, USA, *Host: Giancarlo Pellegrino*
2018	University of Maryland, USA, *Host: Tudor Dumitraş*
	University of Pennsylvania, USA, *Host: Nikos Vasilakis*
	University of California San Diego, USA, *Host: Deian Stefan*
	Karlstad University, Sweden, *Host: Nurul Momen*
	Budapest University of Technology and Economics, Hungary, *Host: Levente Buttyán*

TEACHING, MENTORING AND SERVICE

Courses	*The Web Security Seminar*, seminar at Saarland University, winter semester 2023/2024, with Aurore Fass, Giancarlo Pellegrino, and Ben Stock, *Machine Learning for Program Analysis*, seminar at Saarland University, winter semester 2022/2023, with Giancarlo Pellegrino and Thorsten Holz, *Secure Web Development*, advanced course at Saarland University, summer semester 2022, with Giancarlo Pellegrino, *Program Analysis for Vulnerability Detection*, seminar at Saarland University, winter semester 2020/2021 and 2021/2022, *Joint Advances in Web Security*, seminar at Saarland University, winter semester 2021/2022, with Ben Stock and Giancarlo Pellegrino, *(p)SADWeb: (Pro)Seminar on Attacks & Defense on the Web*, proseminar at Saarland University, summer semester 2021, with Ben Stock and Giancarlo Pellegrino.
Teaching assistant	*Program Testing and Analysis*, course at TU Darmstadt: Fall 2015, Fall 2016, Fall 2017. For 2017, we were awarded the "Feedbackpreis für gute Betreuung" together with my fellow teaching assistants.
Master thesis adviser	**Björn Karthein**, *Exploring the Suitability of Input Invariants for Automated Testing of Web Forms*, Saarland University, 2024, co-supervised with Andreas Zeller **Muhammad Bilal Latif**, *Empirical Study of Full-Stack JavaScript Web Applications*, Saarland University, 2022 **Markus Zimmermann**, *An Empirical Study of the Npm Ecosystem*, Technical University Darmstadt, 2018 (see USENIX 2019) **Philippe Skolka**, *An Empirical Study of Obfuscation and Minification of Client-Side Web Code*, Technical University Darmstadt, 2018 (see WWW 2019)

Bachelor thesis adviser	**Hong-Thai Luu**, *Usages and Misuses of Cryptographic APIs in JavaScript*, Saarland University, 2023
	Jeremy Rack, *Studying the role of JavaScript bundlers in modern web applications*, Saarland University, 2022
	Adithya Srinivas Parthasarathy, *Browser Fingerprinting using SVG Images*, IIITDM-Kancheepuram, 2022
	Raoul Scholtes, *Applying Code Property Graphs for Cross-Language Taint Analysis*, Saarland University, 2022, co-supervised with Giancarlo Pellegrino
	Dominic Troppmann, *On the Prevalence of Native Extensions in Scripting Languages*, Saarland University, 2021
	Paul Szymanski, *A Study of State-of-the-Art Call Graph Creation Approaches for JavaScript*, Saarland University, 2021
	Patrick Mell, *Detecting Parallelization Opportunities in JavaScript Programs*, Technical University Darmstadt, 2016
PC member	ACM Conference on Computer and Communications Security 2024
	IEEE Symposium on Security and Privacy 2024
	ACM International Conference on the Foundations of Software Engineering 2024
	ACM SIGSOFT International Symposium on Software Testing and Analysis 2024
	Workshop of Designing Security for the Web 2024
	IEEE Symposium on Security and Privacy 2023
	ACM Conference on Computer and Communications Security 2023
	ACM ASIA Conference on Computer and Communications Security 2023
	Workshop on Measurements, Attacks, and Defenses for the Web 2023
	IEEE/ACM Automated Software Engineering 2023 - Industry Showcase Track
	ACM Conference on Computer and Communications Security 2022
	ACM ASIA Conference on Computer and Communications Security 2022
	Workshop on Measurements, Attacks, and Defenses for the Web 2022
	Workshop on Privacy in the Electronic Society 2021
	International Working Conference on Source Code Analysis and Manipulation 2021
	International Conference on Availability, Reliability and Security 2021
	International Conference on Security and Privacy in Communication Networks 2021
	European Workshop on Systems Security 2021
	Workshop on Measurements, Attacks, and Defenses for the Web 2021
	International Conference on Cryptology And Network Security 2020
	IEEE Symposium on Security and Privacy 2019 Student PC
Reviewer	Proceedings on Privacy Enhancing Technologies 2023
	ACM Transactions on Software Engineering and Methodology 2023
	IEEE Transactions on Software Engineering 2023
	Dutch Research Council (NWO) Talent Programme 2022
	ACM Transactions on Software Engineering and Methodology 2022
	Empirical Software Engineering Journal 2021
	IEEE Transactions on Software Engineering 2021
	ACM Transactions on Privacy and Security 2020
Session Chair	Workshop on Measurements, Attacks, and Defenses for the Web 2021
Student volunteer	Programming Language Design and Implementation 2015

SKILLS AND INTERESTS

I am a curious person and I enjoy pushing my limits. I love long-distance running, cycling, cooking and reading. In February 2012 I passed the TOEFL iBT exam with a score of 106 points. I am currently working on improving my German (obtained Goethe-Zertifikat B2 in September 2022), and Hungarian (A1 level) language skills.

MEDIA COVERAGE

These are news entries that covered my work, during the years:

The Daily Swig, Prototype pollution project yields another Parse Server RCE, 2022

The Register, Node.js prototype pollution is bad for your app environment, 2022

New Statesman, Software is becoming more interdependent, and that's a big problem, 2022

The Daily Swig, Node.js security: Parse Server remote code execution vulnerability resolved, 2022

Snyk Blog, Safer together: Snyk and CISPA collaborate for the greater good, 2022

The Daily Swig, Node.js sandboxes are open to prototype pollution, 2021

TU Darmstadt website, Einfrieren von Webseiten, 2018

ZDNet, Hacking 20 high-profile dev accounts could compromise half of the npm ecosystem, 2019

Naked Security, Serious Security: How to stop dodgy HTTP headers clogging your website, 2018

Bleeping Computer, JavaScript Web Apps and Servers Vulnerable to ReDoS Attacks, 2018

SECURITY ADVISORIES

Below, there is a list of vulnerabilities I helped uncover. I was also awarded bug bounties by Twitter, Facebook, Dropbox, and Salesforce.

Sandbox breakout	CVE-2021-21413, CVE-2021-23449, CVE-2021-23555, CVE-2021-23594, CVE-2021-23543, CVE-2021-23771, CVE-2022-23923, CVE-2024-21486, CVE-2024- 21487
ReDoS	CVE-2017-15010, CVE-2017-16118, CVE-2017-16119, CVE-2017-16137, CVE-2017-16138, CVE-2017-18214, CVE-2017-16116, CVE-2017-16113, CVE-2017-16099, CVE-2017-16114, CVE-2017-16115, CVE-2017-16116, CVE-2017-16111, CVE-2017-16117, CVE-2017-16098, CVE-2017-16100, CVE-2019-1010266
Injections	CVE-2017-16042, CVE-2017-16020, CVE-2019-5414, CVE-2018-16460, CVE-2018-16461, CVE-2019-5413, CVE-2019-1010174
Prototype pollution	CVE-2018-16472, CVE-2018-16490, CVE-2022-24760, CVE-2021-23518, CVE-2021-23760, CVE-2021-23507, CVE-2021-23497, CVE-2021-23460, CVE-2021-23558, CVE-2022-25354, CVE-2022-25296, CVE-2022-25352, CVE-2022-22143, CVE-2022-24279, CVE-2022-25862, CVE-2021-23470
DoS	CVE-2022-25324, CVE-2022-21144, CVE-2022-21227, CVE-2021-39131
Privacy issue	HackerOne 329957

REFERENCES

Available on request.

Last updated on September 23, 2024.