My research focuses on software security and system security. Systems continue to have exploitable bugs. On one hand, we discover and remove bugs. On the other hand, we make systems resilient against the exploitation of unknown or unpatched vulnerabilities. To discover bugs we propose (i) sanitization techniques that enforce a security property such as memory, type safety, or API flow safety; given concrete program input, our sanitizers flag property violations and (ii) fuzzing techniques that leverage static and dynamic analysis to create program inputs to explore program areas that are not yet covered through existing test cases. To mitigate exploitable vulnerabilities, we focus on control-flow integrity using specific language semantics, enforcing type integrity, and protecting selective data.

Our research builds on and expands binary and compiler-based hardening, dynamic enforcement of security policies, language-based security, fault isolation, and binary analysis. All research prototypes are released as open-source.

**Top Tier Publications**

SEC’23 (2x) [C77, C78], SP’23 [C76]; CCS’22 (2x) [C69, C70], FSE’22 [C75], NDSS’22 (2x) [C68, C71], SEC’22 (2x) [C66, C74]; ASPLOS’21 [C57], CCS’21 [C61], ICSE’21 [C53], ISCA’21 [C58], ISSTA’21 (2x) [C60, C63], NDSS’21 [C55], MICRO’21 [C54], SIGMETRICS’21 [C59], SEC’21 [C64], ATC’20 [C50], NDSS’20 [C45], SEC’20 (3x) [C47, C49, C51], SP’20 [C48]; CCS’19 [C40], SEC’19 [C44], SP’19 [C41], RTSS’19 [C43]; CCS’18 [C36, C38] (2x), NDSS’18 [C33], SEC’18 [C35], SP’18 [C37]; CCS’17 [C31], NDSS’17 [C29], SEC’17 [C25], SP’17 [C27]; CCS’16 [C21, C22] (2x), NDSS’16 [C24]; SEC’15 [C15]; SEC’14 [C14], IMC’14 [C11], OSDI’14 [C12]; ATC’13 [C9], SP’13 [C10]; SP’12 [C6]; PLDI’07 [C1].
• We are incredibly grateful for the generous support from our sponsors.
• Total funding: $15,711,781, 1,499,970 €, 6,430,179 CHF (≈ $23,641,930).
• My group’s share: $3,608,777, 1,499,970 €, 2,692,963 CHF (≈ $7,801,710).
• Intel TSA: Virtual Memory for Post-Moore Servers ($1,187,310.00, co-PI jointly with Babak Falsafi, David Atienza, Abhishek Bhattacharjee, and Boris Grot, my share is $237,400.00, 2021).
• Oracle: Triangle Fuzzing (CHF 70,000, sole PI, 2021).
• Oracle: Automatic generation of deserialisation gadgets via fuzzing (CHF 70,500, sole PI, 2021).
• CYD Fellowship (CHF 12,000, sole PI, 2021).
• IBM Fellowship ($40,000, supporting Atri Bhattacharyya, 2020).
• Botnar Foundation: COVID-19 Real Time Epidemiology I-DAIR Pathfinder (CHF 4,997,768.00, co-PI, jointly with Carmela Troncoso, Jim Larus, Edouard Bugnion, Marcel Salathé, Martin Jaggi, Srdjan Capkun, Seda Gürses, Michael Veale, Klaus Schönenberger, and Boris Danev, my share is CHF 575,634, 2020).
• Facebook AI infrastructure gift (61,000 CHF, sole PI, 2020).
• DARPA AMP DICER: Directed Compilation for Assured Patching ($3,869,729, co-PI at EPFL, jointly with Antonio Bianchi, Giovanni Vigna, Chris Kruegel, Machiry Kumar, my share is $684,918, 2020).
• ONR Grant 12523149 IoT-D: Towards Internets of Dialect-Speaking Things ($976,000 sub contract at EPFL, 2020).
• SNFS Eccellenza MultiSan: Software Security through Multi-dimensional, Input-guided Sanitization (1’024’572 CHF, acceptance rate: 45/229, sole PI, 2019).
• ERC H2020 Starting Grant 850868 CodeSan: Code Sanitization for Vulnerability Pruning and Exploitation Mitigation (1,499,970 €, acceptance rate 178/1363, sole PI, 2019).
• NSF CNS-1801601 SaTC: CORE: Medium: Collaborative: Threat-Aware Defense: Evaluating Threats for Continuous Improvement ($1,199,849, lead PI, jointly with Trent Jaeger and Gang Tan at PSU, my share is $399,849, 2018)
• ONR Grant 12523149 IoT-D: Towards Internets of Dialect-Speaking Things ($6,000,000, jointly with Dongyan Xu, Xiangyu Zhang, Byoungyoung Lee, and Jason Li (IAI), my share is $1,250,000, 2018)
• PRF XR Research Grant: Effective Protection From Type Safety Violations. ($29,526, jointly with Byoungyoung Lee, 2017).
• Purdue CS Corp. Partners Funding Program: Compiler-based Control-Flow Safety (1 RA, about $30,000, 2017).
• ONR Grant 12338602 Towards Transformation-Based Legacy Software Fitness: Usage-Driven Binary Debloating and Hardening ($1,049,028, lead PI, jointly with Dongyan Xu, 2017)
• Intel CERIAS grant (1 50% RA, about $15,000), 2017.
• Purdue CERIAS seed grant, (2 RA for 1 semester, about $30,000), 2017.
• Intel SSG gift ($75,000, sole PI, 2016).
• NSF CNS-1513783: SaTC: ENCORE ENhanced program protection through COmpiler- REwriter cooperation ($1,199,953, jointly with Michael Franz, UC Irvine and Kevin Hamlen, UT Dallas, my share is $404,000, 2015).
• NSF CNS-1464155: CISE CRII: SaTC: Lockdown: Guarded Control-Flow and Data Privacy for Sensitive Data ($175,000, sole PI, 2015).
**AWARDS**  
Best paper awards and prestigious grants
- **ISOC NDSS’22** distinguished paper award [C71], 2022.
- **Usenix WOOT’20** best paper award [W12], 2020.
- **SNFS Eccellenza Grant** MultiSan, 2019.
- **ERC H2020 Starting Grant 850868** CodeSan, 2019.
- **IEEE LangSec’15** best paper award [W6], 2015.
- **ACM IMC’14** best paper award [C11], 2014.
- **IEEE PST’13** best paper award [C8], 2013.

Other awards, patents, and CVEs
- **5th place at DefCon 30 CTF** (team Organizers), 2022.
- **10th place at DefCon 29 CTF** (team Organizers), 2021.
- **DINAcon’20** Open Government Award for DP3T [TR25], 2020.
- **CSAW MENA ’20** Best Applied Research Award for uRAI [C45], 2020.
- **IEEE SSP’19** Distinguished PC Reviewer Award, 2019.
- **IEEE SSP’19** Distinguished Service Award, 2019.
- **Purdue College of Science Team Award** for work on the information security master program, 2016.
- **Finalist for the Cor Baayen PhD award**, 2013.
- **European patent application 12003967.2/GP161299CH00 Safe Loading - A Foundation for Secure Execution of Untrusted Programs**, May 2013.

**SERVICE**  
Program Committee chair and General chair
- **Program committee chair:** **ISOC NDSS’23** (co-chair with Wenyuan Xu); WOOT’21 (co-chair with Fangfei Liu); WoSSCA’18 (co-chair with Eric Jul and Jan Vitek; ECOOP/ISSTA workshop on speculative side channel analysis); ESSoS’18 (co-chair with Awais Rashid); IEEE ICDCS’18 (co-chair of security track with Herbert Bos); Usenix CSET’17 (co-chair with José Fernandez); ESSoS’17 (co-chair with Eric Bodden); Usenix CSET’16 (co-chair with Eric Eide).
- **Steering committee:** RAID’17 — now.
- **Other committees:** Usenix Security’22 awards committee, Software Security Summer School (SSSS’21) organization, Software Security Summer School (SSSS’20) organization, IEEE SP’19 40 celebration chair, ACM CCS’19 publicity co-chair with Emiliano de Cristofaro, ISOC NDSS’19 workshops co-chair with Giulia Fanti, ISOC NDSS’18 workshops co-chair with Matthew Smith, CM CCS’16 workshops co-chair with Stefan Mangard.
- **Program committee member**
Panelist, reviewer, and external reviewer 2006 – now


**Panelist, reviewer, and external reviewer**

- **Security Seminar**, Universität Stuttgart, Germany (July 2022)
- **Security Seminar**, WPI, Worcester, USA (April 2022)
- **DSRC-TII Security Seminar**, TII, Dubai (January 2022)
- **NoHat Conference**, Italy (November 2021)
- **RAID Keynote**, Spain (October 2021)
- **Security and Trust Summit**, Huawei, Germany (September 2021)
- **Cyber Alps**, CYD, Switzerland (July 2021)
- **Security Seminar**, Baidu Research, USA (April 2021)
- **CS Colloquium**, Chalmers University, Sweden (March 2021)
- **Huawei Trusted Computing Forum**, Singapore (February 2021)
- **CANS Keynote**, Vienna, Austria (December 2020)
- **CS Colloquium**, Ohio State University, USA (October 2020)
- **Systems Security Summer School**, Zhejiang University, China (August 2020)
- **SSSS20 RetroWrite Tutorial**, Purdue University, USA (August 2020)
- **Huawei Mobile Security Forum**, Munich, Germany (November 2019)
- **CEA/Leti**, Grenoble, France (October 2019)
- **EURECOM**, Nice, France (September 2019)
- **Security/Privacy Week**, TU Graz, Graz, Austria (September 2019)
- **CROSSING**, TU Darmstadt, Darmstadt, Germany (September 2019)
- **DIMVA Keynote**, Gothenburg, Sweden (June 2019)
- **IC Research Day**, EPFL, Lausanne, Switzerland (June 2019)
- **Huawei Research Forum**, Singapore, Singapore (May 2019)
- **CISPA: distinguished lecture**, Saarbrücken, Germany (March 2019)
- **RUB: CASA distinguished lecture**, Bochum, Germany (March 2019)
- **UniBW F1_CODE Seminar**, Munich, Germany (February 2019)
- **Intel ISEC Conference**, Portland, USA (December 2018)
- **ISSISP: Intl. Summer School on Information Security and Protection**, Canberra, Australia (July 2018)
- **AsiaCCS invited talk**, Songdo, Korea (June 2018)
- **EPFL**, Lausanne, Switzerland (March 2018)
- **ETHZ**, Zurich, Switzerland (March 2018)
- **TUG**, Graz, Austria (January 2018)
- **PRiSC keynote** (POPL’18 workshop), Los Angeles, USA (January 2018)
- **ETH Zurich Colloquium**, Zurich, Switzerland (January 2018)
- **UC Irvine Colloquium**, Irvine, California (November 2017)
**MILCON IoT Panel**, Baltimore, USA  
**Internet2 Workshop**, Indianapolis, USA  
**WTB Cybersecurity: System Security**, Online  
**ICARS Symposium**, West Lafayette, USA  
**GA Tech Cyber Seminar**, Atlanta, USA  
**Science on Tap, Lafayette Brewing Company**, Lafayette, USA

**KIT**, Karlsruhe, Germany  
**CERIAS Symposium**, West Lafayette, USA  
**AsiaCCS invited talk**, Abu Dhabi, UAE  
**IBM Research Seminar**, Zurich, Switzerland  
**TU Darmstadt**, Darmstadt, Germany  
**TU Wien**, Wien, Austria  
**East China Normal University Colloquium**, Shanghai, China

**Midwest PL summit**, West Lafayette, USA  
**CS seminar, Northeastern University**, Boston, USA  
**Dagstuhl seminar 15294**, Dagstuhl, Germany  
**CS seminar, ETH Zurich**, Zurich, Switzerland

**Greater Chicago Area Systems Research Workshop**, Chicago, USA  
**Harris Corporation**, Melbourne, Florida, USA  
**SSP’14 workshop, invited talk**, Phoenix, Arizona, USA  
**Google Security seminar**, San Francisco, CA, USA

**ECE seminar, Virginia Tech**, Blacksburg, VA  
**CS seminar, University of Utah**, Salt Lake City, UT, USA  
**CS seminar, Purdue University**, West Lafayette, IN, USA  
**TRUST seminar, UC Berkeley**, Berkeley, CA, USA

**EPFL invited talk**, Lausanne, Switzerland  
**SoCal PLS invited talk**, Santa Barbara, CA, USA  
**UC Irvine seminar**, Irvine, CA, USA  
**Intel invited talk**, Santa Clara, CA, USA

**Adobe security invited talk**, San Francisco, CA, USA  
**UC Berkeley invited talk**, Berkeley, CA, USA  
**UC Irvine invited talk**, CA, USA  
**IBM Research ARL invited talk**, Austin, TX, USA

**Swiss Cyber Storm Security Conference**, Rapperswil, Switzerland  
**UC Irvine invited talk**, CA, USA  
**Google TechTalk**, Mountain View, CA, USA

---

**ADVISING**  
Currently advised PhD students:

*Embedded Security Testing*, Prashast Srivastava [C27, C72, C63, W11], PhD candidate  
**Advisor:** 2016 – now

*Data-flow-based testing*, Adrian Herrera [C59, C60, C69]  
**Co-advised with Tony Hosking:** 2018 – now

*Arch. defenses*, Atri Bhattacharyya [C46, C40, C66, C58]  
**Co-advised with Babak Falsafi:** 2018 – now

*Dynamic security testing*, Ahmad Hazimeh [C59, C61]  
**Advisor:** 2019 – now

*Code-based sanitization*, Nicolas Badoux  
**Advisor:** 2020 – now

*Crash Analysis*, Zhiyuan Jiang [C69, C61]  
**Co-advised at NUDT:** 2020 – now

*Efficient Static Rewriting*, Luca DiBartolomeo  
**Advisor:** 2021 – now

*Architectural Security*, Andrés Sanchez  
**Advisor:** 2021 – now

*OS Security*, Florian Hofhammer  
**Advisor:** 2021 – now

*Two-phased testing*, Zhiyao Feng [C78]  
**Co-advised with Sanidhya Kashyap:** 2021 – now

*Filesystem testing*, Tao Lyu  
**Advised post docs:**  
Gwangmu Lee

**Advisor:** Apr. 2022 – now
Graduated students:

**Derrick McKee**, Purdue PhD [C33, C34, C71, C62]  
Advisor: 2015 – 2022

Establishing a baseline for efficient compartmentalization mechanisms and policies.

**Bader AlBassam**, Purdue (non-thesis) MSc [C36]  
Co-advised with Antonio Bianchi: 2016 – 2022

Analysis of security vulnerabilities.

**Hui Peng**, Purdue PhD [W7, C21, C51, C37, C77, W11]  
Advisor: 2015 – 2021

Customizing coverage exploration to improve fuzzing for “hard to fuzz targets”.

**Priyam Biswas**, Purdue PhD [C56, C25, C31]  
Advisor: 2015 – 2020

Novel mitigations that enforce type-aware control-flow integrity, guarding against attacks.

**Yuseok Jeon**, Purdue PhD [C21, C31, C50, C42]  
Advisor: 2015 – 2020

Development of sanitizers for cast safety for C++ and fast memory safety, eliminating software bugs.

**Naif Almakhdhub**, Purdue PhD [C45, C39, C27]  
Co-advised with Saurabh Bagchi: 2016 – 2020

Protecting embedded systems against control-flow hijacking and assessing the impact of mitigations.

**Kyriakos Ispoglou**, Purdue PhD [W7, C36, C49, W8]  
Advisor: 2015 – 2019

Analyzing vulnerability threat surface discovered through fuzzing and synthesizing data-flow attacks.

**Sushant Dinesh**, Purdue MSc [C48]  
Advisor: 2016 – 2019

Recovering data structures through binary analysis and enabling efficient binary rewriting.

**Abe Clements** (ECE), Purdue PhD [C45, C39, C35, C27, C47]  
Co-advised with S. Bagchi: 2015 – 2019

Defending IoT devices against advanced threats by enforcing strong mitigations at low overhead.

**Nathan Burow**, Purdue PhD [C56, J5, C33, C34, C41, C50]  
Advisor: 2015 – 2018

Enforcement of low overhead memory safety mitigations for C/C++, to protect unsafe code.

**Terry Ching-Hsiang Hsu**, Purdue PhD [C22]  
Co-advised with Patrick Eugster: 2016 – 2018

Development of memory abstractions for security, performance, and large data.

**Scott A. Carr**, Purdue PhD [C25, J5, C33, C34, C26, C31, C24]  
Advisor: 2014 – 2017

Development of compiler-based mitigations for vulnerabilities in systems software, focusing on enforcing confidentiality and integrity on sensitive data.

**Ahmed Hussein**, Purdue PhD [C16, C17, C30]  

Development and optimization of garbage collection strategies for Android mobile systems.

Visiting students:

**Han Zheng** visiting PhD student from University of Chinese Academy of Sciences  
Improving targeted fuzzing.  
2022

**Qiang Liu** visiting PhD student from Zhejiang Yuexiu University  
Automated testing of hypervisor components.  
Fall 2021 – Spring 2022

**Majid Salehi** visiting PhD student from KU Leuven  
Efficient testing of embedded systems through cross-ISA-transplantation.  
Fall 2021

**Alessandro Di Federico**, visiting PhD student [C25, C28]  
Binary analysis and translation across architectures and operating systems.  
Fall 2016

**EPFL Polygl0ts student Capture-the-Flag (CTF) team advisor**  
2018 – now

Founder and advisor for the polygl0ts CTF team (ranked in the top 50 of thousands of teams worldwide), founder and former adviser of the Purdue b01lers CTF team (2014–2019).

TEACHING

Lectures and classes prepared and taught

- **Software Security**, CS-412, 6 ECTS, 129 students  
  Spring 2022

- **Operating Systems**, CS-323, 6 ECTS, 151 students (with Sanidhya Kashyap)  
  Fall 2021

- **Software Security**, CS-412, 6 ECTS, 74 students  
  Spring 2021

- **Operating Systems**, CS-323, 6 ECTS, 128 students  
  Fall 2020

- **Software Security**, CS-412, 6 ECTS, 54 students  
  Spring 2020
• Operating Systems, CS-323, 6 ECTS, 81 students (newly designed) Fall 2019
• Software Security, CS-412, 6 ECTS, 47 students Spring 2019
• Topics in Language-based Software Security, CS-725, 2 ECTS, 17 students Fall 2018
• Software Security, CS-527, 3 credits, 25 students (reworked) Spring 2018
• CERIAS Seminar, CS-591-SEC, 1 credit, 11 students Spring 2018
• Systems Security Seminar, CS-590-SYS, 1 credit, 10 students Spring 2018
• Operating Systems, CS-354, 3 credits, 148 students Fall 2017
• Systems Security Seminar, CS-590-SYS, 1 credit, 11 students, several auditors Fall 2017
• Software Security, CS-527, 3 credits, 17 students, (reworked) Spring 2017
• Systems Security Seminar, CS-590-SYS, 1 credit, 9 students, several auditors Spring 2017
• Operating Systems, CS-354, 3 credits, 123 students Spring 2017
• Systems Security Seminar, CS-590-SYS, 1 credit, 16 students, several auditors Fall 2016
• Software Security, CS-590-SWS, 3 credits, 18 students, several auditors (new, founded) Spring 2016
• Systems Security Seminar, CS-590-SYS, 1 credit, 7 students, several auditors Spring 2016
• Operating Systems, CS-503, 3 credits, 45 students Fall 2015
• Informal Systems Seminar, 15 students Fall 2015
• Software Engineering, CS-510, 3 credits, 47 students (significantly redesigned) Spring 2015
• Informal Systems Seminar, 8 students (new, founded) Spring 2015
• Language-based Systems Security, CS-590-LBS, 3 credits, 16 students Fall 2014
• Introduction to C Programming, 6 hrs., ca. 120 students (developed) Fall 2008 and 2009
• Exam preparation courses, Head TA, and TA for a variety of courses at ETH Zurich 2006 – 2012
**JOURNAL ARTICLES**


**CONFERENCE PROCEEDINGS**


**BOOKS AND CHAPTERS**


**THERSES**


