Prof. Dr. sc. Mathias Payer Revision: September 2026

CONTACT INFORMATION

Affiliation: Professor in Computer Science, École Polytechnique Fédérale de Lausanne (EPFL)

Address: Mathias Payer
BC 160, Station 14
1015 Lausanne, Switzerland

Phone: +4121-693-2708
E-mail: mathias.payer@nebelwelt.net
WWW: https://www.nebelwelt.net/
Group: https://hexhive.epfl.ch/

RESEARCH INTERESTS

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 security properties 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 broadly and thoroughly explore the reachable program state space. To mitigate exploitable vulnerabilities, we focus on control-flow integrity using specific language semantics, enforcing type integrity, and protecting selective data. We open-source all research prototypes.

AFFILIATION

HexHive group, EPFL, Switzerland. **Sep. 2018 – now**
Full Professor in Computer Science (since March 2026).
Associate Professor in Computer Science (until March 2026).
Tenure Track Assistant Professor in Computer Science (until May 2021).

HexHive group, Purdue University, USA. **Aug. 2014 – Aug. 2018**
Adjunct Associate Professor in Computer Science (from Nov. 2019 to June 2023).
Tenure Track Assistant Professor in Computer Science.

BitBlaze group, UC Berkeley, USA. **Sept. 2012 – July 2014**
Postdoctoral scholar in Dawn Song's BitBlaze group.

Google Inc., Mountain View, USA. **May – July 2010**
Software engineer in the anti-malware/anti-phishing team.

Laboratory for Software Technology, ETH Zurich, Switzerland **Oct. 2006 – Aug. 2012**
Research assistant and PhD student.

EDUCATION

ETH Zurich, Switzerland

Doctor of Science ETH in Computer Science **Oct. 2006 – May 2012**
- Thesis title: *Safe Loading and Efficient Runtime Confinement: A Foundation for Secure Execution* [T4]
- Advisor: Thomas R. Gross (ETH Zurich)
- Co-advisors: Steven Hand (Google) and Srđan Čapkun (ETH Zurich)

Diploma/Master of Science ETH in Computer Science **Oct. 2001 – Feb. 2006**
- Thesis title: *Adaptive Optimization using Hardware Performance Monitors* [T3, C1]
- Area of study: System Software [T1], Software Engineering; Minor: Robotics [T2]

ADVISING

Currently advised Ph.D. students:

Two-phased testing, Zhiyao Feng [C126, C99, C85] **Adviser: 2021 – now**
Filesystem testing, Tao Lyu [C109, C99] **Co-advised with Sanidhya Kashyap: 2021 – now**
Abstraction testing, Chibin Zhang [C135, C130, C119, C117] **Adviser: 2022 – now**
Mobile testing, Philipp Mao [C134, C133, C121, C111, C105, C92, C93, C100] **Adviser: 2022 – now**
Automated Testing, Han Zheng [C131, C126, C118, W19, C89] **Adviser: 2023 – now**
Supply chain testing, Rafaila Galanopoulou **Adviser: 2024 – now**
Next gen mobile security, Eduard Vlad **Co-advised with Haitham Al Hassanieh: 2025 – now**
Container security, Sofia Saltovskaia **Adviser: 2025 – now**
Code compartmentalization, Yiwen Xu **Adviser: 2025 – now**
Kernel hardening, Claudio Migliorelli **Co-advised with IBM Research: 2025 – now**
Compartmentalization for code, Shibo Ai **Adviser: 2026 – now**

Postdoctoral scholars (publications during their time in the lab):

Qinying Wang [C135, C128, C126, C101, W18] **Oct. 2024 – now**
Qiang Liu [C130, C131, C117, C110, C94, C91, C82] **2023 – 2026**
Marcel Busch [C126, C111, C105, C92, C93, C98, W18, C78] **2021 – 2025**
Flavio Toffalini [C114, C118, C115, C116, C103, W19, C86, C89, C82, C87, C73, C69] **2021 – 2024**
Gwangmu Lee [C117, C97] **2022 – 2024**
Daniele Antonioli [C67, W13, C65, C64, J7, J8, TR23, TR25] **2020 – 2021**

Graduated Ph.D. students (publications during their PhDs):

Luca Di Bartolomeo, EPFL PhD [C133, C105, C76, C87] **Advisor: 2021 – 2026**
Analyzing and securing the Android App ecosystem.
Florian Hofhammer, EPFL PhD [C122, W18, TR26, C77] **Adviser: 2021 – 2026**
Finding the correct level of abstraction to rehost embedded systems.
Nicolas Badoux, EPFL PhD [C114, C104, C103] **Advisor: 2020 – 2025**
Language dialects to enforce strong (type) safety properties.
Adrian Herrera, ANU PhD [J12, C69, C60, C59] **Co-advised by Tony Hosking: 2018 – 2024**
Leveraging data flow as coverage feedback in fuzzing for bug discovery.
Atri Bhattacharyya, EPFL PhD [C108, C77, C66, C58, C46, C40] **Co-advisor B. Falsafi: 2018 – 2024**
Secure Interface Design Leveraging Hardware/Software Support.
Ahmad Hazimeh, EPFL PhD [C94, C61, C59] **Advisor: 2019 – 2024**
Fuzz testing in practice by drilling down into abstractions and metrics.
Prashast Srivastava, Purdue PhD [C86, C72, C63, W11, C27] **Advisor: 2016 – 2023**
Leveraging abstraction awareness to increase the quality of auto-generated test inputs.
Derrick McKee, Purdue PhD [W17, C71, C62, C34, C33] **Advisor: 2015 – 2022**
Establishing a baseline for efficient compartmentalization mechanisms and policies.
Hui Peng, Purdue PhD [C83, C51, W11, C37, C21, W7] **Advisor: 2015 – 2021**
Customizing coverage exploration to improve fuzzing for "hard to fuzz targets".
Priyam Biswas, Purdue PhD [C56, C31, C25] **Advisor: 2015 – 2020**
Novel mitigations that enforce type-aware control-flow integrity, guarding against attacks.
Yuseok Jeon, Purdue PhD [C103, C50, C42, C31, C21] **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 by Saurabh Bagchi: 2016–2020**
Protecting embedded systems against control-flow hijacking and assessing the impact of mitigations.
Kyriakos Ispoglou, Purdue PhD [C49, C36, W8, W7] **Advisor: 2015–2019**
Analyzing vulnerability threat surface discovered through fuzzing and synthesizing data-flow attacks.
Abe Clements (ECE), Purdue PhD [C45, C47, C35, C39, C27] **Co-advised by S. Bagchi: 2015–2019**
Defending IoT devices against advanced threats by enforcing strong mitigations at low overhead.
Nathan Burow, Purdue PhD [C56, C50, C41, C34, C33, J5] **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 by Patrick Eugster: 2016–2018**
Development of memory abstractions for security, performance, and large data.
Scott A. Carr, Purdue PhD [C34, C33, C31, C25, C26, J5, C24] **Advisor: 2014–2017**
Enforcing confidentiality and integrity of sensitive data to mitigate attacks.
Ahmed Hussein, Purdue PhD [C30, C16, C17] **Co-advised by Tony Hosking: 2014–2016**
Development and optimization of garbage collection strategies for Android mobile systems.

GRANTS

We are incredibly grateful for the generous support from our sponsors.

- CYD Fellowship: Securing Next Generation Cellular Networks (304,984.00, *supporting Eduard Vlad*, 2026).
- ArmaSuisse: Hardening Commercial UAV Firmware (60,000.00, *sole PI*, 2026).
- SEAL: Lambda Health Systems Plateforme de Protection (100,000.00, co-PI with LHS and HEIG-VD, my share is 13,300.00, 2026).
- SBB: Continuous Cyber Assessment for Embedded Systems (120'000.00, *sole PI*, 2026).
- Google Inc.: ML-based patch creation for fuzzing crashes ($30,000.00, *sole PI*, 2025).
- **ERC Horizon Advanced Grant 101201184** LEAPS: Least Privilege Compartments (2,498,320 €, acceptance rate 281/2,467, *sole PI*, 2025)
- SNSF Project: LinSpecteur (CHF 1'481'446, *lead PI*, jointly with Anil Kurmus, Andrea Mambretti, and Alessandro Sorniotti at IBM Research, 2025, my share is CHF 740'726).
- CYD fellowship: IoTSec: Transforming IoT Security (*supporting Marcel Busch*, CHF 128'715).
- Huawei: TEETime: Extensive Fuzzer-Induced TEE Hardening (EUR 90,000, *sole PI*, 2024).
- Armasuisse: Automated Vulnerability Discovery and Prioritization (CHF 136'776, *sole PI*, 2024).
- Qualcomm Innovation Fellowship (*supporting Atri Bhattacharyya*, $40,000.00, 2023).
- 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 deserialization 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).
- Huawei: ProtoFuzz (CHF 94,371.20, *sole PI*, 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).
- **US Air Force Research Lab**: Cross-Abstraction Analysis for Complex Embedded Systems ($735,436, co-PI, jointly with Aurélien Francillon and Davide Balzarotti, my share is $322,538, 2020).
- Facebook AI infrastructure gift (61,000 CHF, *sole PI*, 2020).
- **DARPA AMP** DICER: Directed Compilation for Assured Patching ($3,869,729, co-PI, 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).
- Huawei Shield Lab gift (99,968 CHF, *sole PI*, 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: 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).
- Sponsored supplement to NFS grant CNS-1513783 ($46,820, *sole PI*, 2016).
- PRF XR Research Grant: Program Analysis for Security and Privacy of Embedded Devices. ($29,130, jointly with Patrick Eugster, 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).
- PRF XR: PrivData: Enforcing Data Confidentiality for C/C++ ($25,838, *sole PI*, 2015).

AWARDS

Distinctions and best paper awards
- ***Usenix WOOT'26*** best paper award [C131], 2024.
- ***NDSS'25*** distinguished paper award [C103], 2025.
- ***NDSS'25*** distinguished paper award [C116], 2025.
- ***RAID'24*** best paper award [C94], 2024.
- ***Usenix Security'24*** distinguished paper award [C91], 2024.
- ***Usenix WOOT'24*** best paper award [C100], 2024.
- ***ISOC BAR'24*** distinguished paper award [W18], 2024.
- ***ACM Distinguished Member*** for protecting systems in the presence of vulnerabilities, 2024.
- ***IEEE Senior Member***, 2023.
- ***ACM SIGSOFT FSE'22*** distinguished paper award [C75], 2022.
- ***ISOC NDSS'22*** distinguished paper award [C71], 2022.
- ***Usenix WOOT'20*** best paper award [W12], 2020.
- ***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
- ***Usenix SEC'25*** notable PC Reviewer Award, 2025.
- ***ACM CCS'24*** distinguished PC Reviewer Award, 2024.
- **7th place at DefCon 33 CTF** (team Organizers), 2025.
- **10th place at DefCon 32 CTF** (team Organizers), 2024.
- **9th place at DefCon 31 CTF** (team OrgaKraut), 2023.
- **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.
- ***CSAW US '20*** best Applied Research Runner Up for BLESA [W12], 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*, May 2013.

SERVICE

Program Committee chair and General chair **2015 – now**

ISOC NDSS'27 associate chair; **ISOC NDSS'24** (co-chair with Christina Pöpper); **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). Other committees: Steering committees of RAID (17-now) and WOOT (21-now). DIMVA'24 general chair, U.S. Open-Source Software Security Initiative'22 (NSF/NIST/White House) organization, Usenix Security'22 awards committee, Software Security Summer School (SSSS'21 and SSSS'20) organization, IEEE SP'19 40-year 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, ACM CCS'16 workshops co-chair with Stefan Mangard.

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).

Program committee member **2012 – now**

2027: **Oakland'27**, **SEC'27**
2026: **CCS'26**, FUZZING'26, **SEC'26**, WOOT'26
2025: EuroSP'25, **CCS'25**, **NDSS'25**, **SEC'25**, WOOT'25
2024: **CCS'24**, **SEC'24**, WOOT'24
2023: **CCS'23**, **EuroSYS'23**, FUZZING'23, **Oakland'23**, WOOT'23
2022: **CCS'22**, LangSec'22, **NDSS'22**, **SEC'22**, WiSec'22
2021: LangSec'21, **NDSS'21**, **Oakland'21**, **SEC'21**, WiSec'21;
2020: **NDSS'20**, **Oakland'20**, **SEC'20**, WOOT'20;
2019: **CCS'19**, **EuroSYS'19**, **NDSS'19**, **Oakland'19**, PRiSC'19, **SEC'19**, WOOT'19;
2018: AsiaCCS'18, **CCS'18**, **EuroSYS'18** (PC, awards), **NDSS'18**, **SEC'18** (PC, awards), WOOT'18;
2017: ACISP'17, ACSAC'17, AsiaCCS'17, **CCS'17**, DSN'17, EuroSec'17, NSS'17, **SEC'17**, SecDev'17;
2016: ACISP'16, **CCS'16**, DSN'16, ESSoS'16, EuroSec'16, NSS'16, **SEC'16**, SSPPREW'16, TRUST'16, WIFS'16, **WWW'16**;
2015: ACNS'15, AsiaCCS'15, **CCS'15**, **EuroSYS'15**, **PLDI'15** (ERC), PPREW'15;
2014: AsiaCCS'14, PPREW'14, PPREW'14b, VEE'14; SyStor'13

Panelist, reviewer, and external reviewer **2006 – now**
RVO reviewer, 2021. ERC H2020 reviewer, 2020. Poster reviewer for Usenix SEC, 2016. NSF review panelist for SaTC '16, CPS '16, SaTC '17, CPS '17, SaTC '18, '24. NWO (Netherlands Organisation for Scientific Research) reviewer, 2015, 2023. Journal reviewer for ACM TACO, ACM TOPS, Elsevier COSE, IEEE TDSC, IEEE TPDS. Conference reviewer for CAV, CGO, HiPeak, PACT, PLDI, PPoPP.

INVITED TALKS

Invited Talk, Geneva Cyber Week: Peak Incident Response, Geneva, CH **May 2026**
Keynote, Fuzzing Workshop, NDSS, San Diego, USA **February 2026**
Invited Talk, MPI Bochum, Germany **January 2026**
Invited Talk, INRIA, IRISA, Rennes, France **December 2025**
AISec, Tsinghua, Beijing, China **November 2025**
Invited Talk, IFI, Zürich, Switzerland **November 2025**
Intel Security, Intel, Portland, USA **September 2025**
Keynote, THCon, Toulouse, France **April 2025**
Keynote, EuroSec Workshop, Rotterdam, Netherlands **March 2025**
Keynote, InsomniHack, Lausanne, Switzerland **March 2025**
Invited Talk, AMSec Workshop, Amsterdam, Netherlands **January 2025**
Invited Talk, CYD Campus Conference, Zurich, Switzerland **December 2024**
Invited Talk, Cybersecurity-Konferenz by Digital Liechtenstein, Bendern, FL **November 2024**
Invited Talk, University of Utah, USA **October 2024**
Security Seminar, Stony Brooke University, USA **August 2024**
Huawei Laps Seminar, Singapore **May 2024**

ETH Zurich Seminar, Zürich, Switzerland **May 2024**
DARPA HARDEN Keynote, Online **October 2023**
ESORICS Keynote, Den Haag, Netherlands **October 2023**
GoGE Seminar, SNU, South Korea, Online **May 2023**
QIF Invited Talk, Qualcomm, Online **May 2023**
CERIAS Security Seminar, Purdue University, USA **April 2023**
Security Seminar, KAIST, South Korea **March 2023**
Security Seminar, DSO National Laboratories, Singapore **November 2022**
CS Colloquium Talk, UC Irvine, USA **November 2022**
CS Colloquium Talk, UC Santa Barbara, USA **November 2022**
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 FI_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 **October 2017**
Internet2 Workshop, Indianapolis, USA **October 2017**
WTB Cybersecurity: System Security, Online **October 2017**
ICARS Symposium, Washington DC, USA **September 2017**
GA Tech Cyber Seminar, Atlanta, USA **September 2017**
Science on Tap, Lafayette Brewing Company, Lafayette, USA **September 2017**
KIT, Karlsruhe, Germany **June 2017**
CERIAS Symposium, West Lafayette, USA **May 2017**

AsiaCCS invited talk, Abu Dhabi, UAE **April 2017**
IBM Research Seminar, Zurich, Switzerland **January 2017**
TU Darmstadt, Darmstadt, Germany **December 2016**
TU Wien, Wien, Austria **June 2016**
East China Normal University Colloquium, Shanghai, China **June 2016**
Midwest PL summit, West Lafayette, USA **December 2015**
CS seminar, Northeastern University, Boston, USA **October 2015**
Dagstuhl seminar 15294, Dagstuhl, Germany **July 2015**
CS seminar, ETH Zurich, Zurich, Switzerland **July 2015**
Greater Chicago Area Systems Research Workshop, Chicago, USA **April 2015**
Harris Corporation, Melbourne, Florida, USA **February 2015**
SSP'14 workshop, invited talk, Phoenix, Arizona, USA **November 2014**
Google Security seminar, San Francisco, CA, USA **June 2014**
ECE seminar, Virginia Tech, Blacksburg, VA **March 2014**
CS seminar, University of Utah, Salt Lake City, UT, USA **February 2014**
CS seminar, Purdue University, West Lafayette, IN, USA **January 2014**
TRUST seminar, UC Berkeley, Berkeley, CA, USA **December 2013**
EPFL invited talk, Lausanne, Switzerland **June 2013**
SoCal PLS invited talk, Santa Barbara, CA, USA **May 2013**
UC Irvine seminar, Irvine, CA, USA **May 2013**
Intel invited talk, Santa Clara, CA, USA **April 2013**
Adobe security invited talk, San Francisco, CA, USA **January 2013**
UC Berkeley invited talk, Berkeley, CA, USA **May 2012**
UC Irvine invited talk, CA, USA **May 2012**
IBM Research ARL invited talk, Austin, TX, USA **April 2011**
Swiss Cyber Storm Security Conference, Rapperswil, Switzerland **March 2011**
UC Irvine invited talk, CA, USA **March 2011**
Google TechTalk, Mountain View, CA, USA **June 2010**

TEACHING Lectures and classes prepared and taught

- *Software Security*, CS-412, 6 ECTS, 185 students **Spring 2026**
- *Information Security and Privacy*, COM-402, 8 ECTS, 273 students **Fall 2025**
- *Software Security*, CS-412, 6 ECTS, 142 students **Spring 2025**
- *Information Security and Privacy*, COM-402, 8 ECTS, 228 students **Fall 2024**
- *Topics in Software Security*, CS-510, 3 ECTS, 32 students **Fall 2024**
- *Software Security*, CS-412, 6 ECTS, 96 students **Spring 2024**
- *Information Security and Privacy*, COM-402, 8 ECTS, 246 students **Fall 2023**
- *Topics in Software Security*, CS-510, 2 ECTS, 27 students **Fall 2023**
- *Software Security*, CS-412, 6 ECTS, 130 students **Spring 2023**
- *Software Security*, CS-412, 6 ECTS, 131 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, 77 students **Spring 2020**
- *Operating Systems*, CS-323, 6 ECTS, 81 students (newly designed) **Fall 2019**
- *Software Security*, CS-412, 6 ECTS, 42 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 **Fall 2016**
- *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**

JOURNAL ARTICLES

[J1] Mathias Payer, Ling Huang, Neil Zhenqiang Gong, Kevin Borgolte, and Mario Frank. "What You Submit is Who You Are: A Multi-Modal Approach for Deanonymizing Scientific Publications". In: *IEEE Transactions on Information Forensics and Security*. 2014. DOI: 10.1109/TIFS.2013.2286268.

[J2] Laszlo Szekeres, Mathias Payer, Tao Wei, and R. Sekar. "Eternal War in Memory". In: *IEEE Security and Privacy Magazine*. 2014. DOI: 10.1109/MSP.2013.47.

[J3] Scott A. Carr, Francesco Logozzo, and Mathias Payer. "Automatic Contract Insertion with CCBot". In: *IEEE Transactions on Software Engineering*. 2016. DOI: 10.1109/TSE.2016.2625248.

[J4] Jack Reilly, Sebastien Martin, Mathias Payer, and Alexandre M. Bayen. "Creating Complex Congestion Patterns via Multi-objective Optimal Freeway Traffic Control with Application to Cyber-Security". In: *Transportation Research Board*. 2016. DOI: 10.1016/j.trb.2016.05.017.

[J5] Nathan Burow, Scott A. Carr, Joseph Nash, Per Larsen, Michael Franz, Stefan Brunthaler, and Mathias Payer. "Control-Flow Integrity: Precision, Security, and Performance". In: *ACM Computing Surveys*. 2017. DOI: 10.1109/TSE.2016.2625248.

[J6] Mathias Payer. "The Fuzzing Hype-Train: How Random Testing Triggers Thousands of Crashes". In: *IEEE Security and Privacy Magazine*. 2019. DOI: 10.1109/MSEC.2018.2889892.

[J7] Marcel Salathe, Christian Althaus, Nanina Anderegg, Daniele Antonioli, Talai Ballouz, Edouard Bugnion, Srdjan Capkun, Dennis Jackson, Sang-Il Kim, James Larus, Nicola Low, Wouter Lueks, Dominik Menges, Cederic Moullet, Mathias Payer, Julien Riou, Theresa Stadler, Carmela Troncoso, Effyj Vayena, and Viktor von Wyl. "Early evidence of effectiveness of digital contact tracing for SARS-CoV-2 in Switzerland". In: *Swiss Medical Weekly*. 2020. DOI: 10.4414/smw.2020.20457.

[J8] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathe, James R. Larus, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth G. Paterson, Srdjan Capkun, David A. Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel P. Smart, Aysajan Abidin, Seda Guerses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, and Jose Pereira. "Decentralized Privacy-Preserving Proximity Tracing". In: *IEEE Data Engineering Bulletin*. 2020.

[J9] David Chisnall, Deepak Garg, Catalin Hritcu, and Mathias Payer. "Secure Compilation (Dagstuhl Seminar 21481)". In: *Dagstuhl Reports*. 2021. DOI: 10.4230/DagRep.11.10.173.

[J10] Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda Guerses, Jean-Pierre Hubaux, Dennis Jackson, James R. Larus, Wouter Lueks, Rui Oliveira, Mathias Payer, Bart Preneel, Apostolos Pyrgelis, Marcel Salathe, Theresa Stadler, and Michael Veale. "Lessons from a Pandemic: Deploying Decentralized Privacy-Preserving Proximity Tracing". In: *Communications of the ACM*. 2022. DOI: 10.1145/3524107.

[J11] Ognjen Glamocanin, Shashwat Shrivastava, Jinwei Yao, Nour Ardo, Mathias Payer, and Mirjana Stojilovic. "Instruction-Level Power Side-Channel Leakage Evaluation of Soft-Core CPUs on Shared FPGAs". In: *Journal of Hardware and Systems Security*. 2023.

[J12] Adrian Herrera, Mathias Payer, and Antony Hosking. "datAFLow: Toward a Data-Flow-Guided Fuzzer". In: *ACM Transactions on Software Engineering and Methodology*. 2023. DOI: 10.1145/3587156.

[J13] Azra Abtahi Fahliani, Mathias Payer, and Amir Aminifar. “DP-ACT: Decentralized Privacy-Preserving Asymmetric Digital Contact Tracing”. In: *Proceedings on Privacy Enhancing Technologies*. 2024, (30% acceptance rate –35/115). DOI: 10.56553/popets-2024-0019.

[J14] Kaiming Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, and Trent Jaeger. “Comprehensive Memory Safety Validation: An Alternative Approach to Memory Safety”. In: *IEEE Security and Privacy Magazine*. 2024. DOI: 10.1109/MSEC.2024.3379947.

[J15] Liliana Pasquale, Antonino Sabetta, Marcelo d’Amorim, Peter Hegedus, Mehdi Tarrit Mirakhorli, Hamed Okrhavi, Mathias Payer, Awais Rashid, Joanna Santos, Jonathan Spring, Lin Tan, and Katja Tuma. “Challenges to Using LLMs in Code Generation and Repair”. In: *IEEE Security and Privacy Magazine*. 2025. DOI: 10.1109/MSEC.2025.3530488.

[J16] Mathias Payer and Candid Wüst. “Subscription Bombing: Email Under Attack”. In: *Communications of the ACM*. 2026. DOI: 10.1145/3797487.

Conference proceedings

[C1] Florian T. Schneider, Mathias Payer, and Thomas R. Gross. “Online optimization driven by hardware performance monitoring”. In: *ACM International Conference on Programming Language Design and Implementation*. 2007, (25% acceptance rate –45/178). DOI: 10.1145/1250734.1250777.

[C2] Mathias Payer and Thomas R. Gross. “Generating low-overhead dynamic binary translators”. In: *ACM International Systems and Storage Conference*. 2010, (58% acceptance rate –18/31). DOI: 10.1145/1815695.1815724.

[C3] Mathias Payer and Thomas R. Gross. “Fine-grained user-space security through virtualization”. In: *ACM International Conference on Virtual Execution Environments*. 2011, (29% acceptance rate –20/68). DOI: 10.1145/1952682.1952703.

[C4] Mathias Payer and Thomas R. Gross. “Performance evaluation of adaptivity in software transactional memory”. In: *International Symposium on Performance Analysis of Systems and Software*. 2011, (30% acceptance rate –20/65). DOI: 10.1109/ISPASS.2011.5762733.

[C5] Mathias Payer and Thomas R. Gross. “Protecting Applications Against TOCTTOU Races by User-Space Caching of File Metadata”. In: *ACM International Conference on Virtual Execution Environments*. 2012, (37% acceptance rate –20/53). DOI: 10.1145/2151024.2151052.

[C6] Mathias Payer, Tobias Hartmann, and Thomas R. Gross. “Safe Loading - A Foundation for Secure Execution of Untrusted Programs”. In: *IEEE International Symposium on Security and Privacy*. 2012, (13% acceptance rate –40/307). DOI: 10.1109/SP.2012.11.

[C7] Dan Caselden, Alex Bazhanyuk, Mathias Payer, Stephen McCamant, and Dawn Song. “HI-CFG: Construction by Binary Analysis, and Application to Attack Polymorphism”. In: *European Symposium on Research in Computer Security*. 2013, (17% acceptance rate –43/242). DOI: 10.1007/978-3-642-40203-6_10.

[C8] Mathias Payer and Thomas R. Gross. “Hot-Patching a Web Server: a Case Study of ASAP Code Repair”. In: *IEEE Conference on Privacy, Security, and Trust*. 2013, (**best paper award**, 29% acceptance rate –43/146). DOI: 10.1109/PST.2013.6596048.

[C9] Mathias Payer, Enrico Kravina, and Thomas R. Gross. “Lightweight Memory Tracing”. In: *Usenix Annual Technical Conference*. 2013, (13% acceptance rate –32/233).

[C10] Laszlo Szekeres, Mathias Payer, Tao Wei, and Dawn Song. “SoK: Eternal war in memory”. In: *IEEE International Symposium on Security and Privacy*. 2013, (12% acceptance rate –38/315). DOI: 10.1109/SP.2013.13.

[C11] Zakir Durumeric, James Kasten, Frank Li, Nicolas Weaver, Vern Paxson, Michael Bailey, J. Alex Halderman, Jethro Beekman, Johanna Amann, Mathias Payer, and David Adrian. “The Matter of Heartbleed”. In: *ACM Internet Measurement Conference*. 2014, (**best paper award**, 22% acceptance rate –43/188). DOI: 10.1145/2663716.2663755.

[C12] Volodymyr Kuznetsov, Laszlo Szekeres, Mathias Payer, George Candea, Dawn Song, and R. Sekar. “Code-Pointer Integrity”. In: *Usenix Symposium on Operating Systems Design and Implementation*. 2014, (18% acceptance rate –42/232).

[C13] Jack Reilly, Sebastien Martin, Mathias Payer, and Alexandre Bayen. “On Cybersecurity of Freeway Control Systems: Analysis of Coordinated Ramp Metering Attacks”. In: *Transportation Research Board*. 2014.

[C14] Hayawardh Vijayakumar, Xinyang Ge, Mathias Payer, and Trent Jaeger. “JIGSAW: Protecting Resource Access by Inferring Programmer Intentions”. In: *Usenix Security Symposium*. 2014, (19% acceptance rate –67/350).

[C15] Nicholas Carlini, Antonio Barresi, Mathias Payer, David Wagner, and Thomas R. Gross. “Control-Flow Bending: On the Effectiveness of Control-Flow Integrity”. In: *Usenix Security Symposium*. 2015, (15% acceptance rate –67/426).

[C16] Ahmed Hussein, Antony L. Hosking, Mathias Payer, and Christopher A. Vick. “Don’t Race the Memory Bus: Taming the GC Leadfoot”. In: *ACM SIGPLAN International Symposium on Memory Management*. 2015, (48% acceptance rate –12/25). DOI: 10.1145/2887746.2754182.

[C17] Ahmed Hussein, Mathias Payer, Antony L. Hosking, and Christopher A. Vick. “Impact of GC Design on Power and Performance for Android”. In: *ACM International Systems and Storage Conference*. 2015, (35% acceptance rate –18/51). DOI: 10.1145/2757667.2757674.

[C18] Mathias Payer, Antonio Barresi, and Thomas R. Gross. “Fine-Grained Control-Flow Integrity through Binary Hardening”. In: *Conference on Detection of Intrusions and Malware and Vulnerability Assessment*. 2015, (22% acceptance rate –17/75). DOI: 10.1007/978-3-319-20550-2_8.

[C19] Xinyang Ge, Nirupama Talele, Mathias Payer, and Trent Jaeger. “Fine-Grained Control-Flow Integrity for Kernel Software”. In: *IEEE European Symposium on Security and Privacy*. 2016, (17% acceptance rate –29/168). DOI: 10.1109/EuroSP.2016.24.

[C20] Neil Zhenqiang Gong, Mathias Payer, Reza Moazzezi, and Mario Frank. “Forgery-Resistant Touch-based Authentication on Mobile Devices”. In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2016, (20% acceptance rate –73/350). DOI: 10.1145/2897845.2897908.

[C21] Istvan Haller, Yuseok Jeon, Hui Peng, Mathias Payer, Herbert Bos, Cristiano Giuffrida, and Erik van der Kouwe. “TypeSanitizer: Practical Type Confusion Detection”. In: *ACM Conference on Computer and Communication Security*. 2016, (16% acceptance rate –137/831). DOI: 10.1145/2976749.2978405.

[C22] Terry Ching-Hsiang Hsu, Kevin Hoffman, Patrick Eugster, and Mathias Payer. “Enforcing Least Privilege Memory Views for Multithreaded Applications”. In: *ACM Conference on Computer and Communication Security*. 2016, (16% acceptance rate –137/831). DOI: 10.1145/2976749.2978327.

[C23] Mathias Payer. “HexPADS: a platform to detect "stealth" attacks”. In: *Int’l. Symp. on Eng. Secure Software and Systems*. 2016, (**artifact evaluation award**, 30% acceptance rate –15/50). DOI: 10.1007/978-3-319-30806-7_9.

[C24] Chao Zhang, Scott A. Carr, Tongxin Li, Yu Ding, Chengyu Song, Mathias Payer, and Dawn Song. “VTrust: Regaining Trust on Your Virtual Calls”. In: *Network and Distributed System Security Symposium*. 2016, (15% acceptance rate –60/389). DOI: 10.14722/ndss.2016.23164.

[C25] Priyam Biswas, Alessandro Di Federico, Scott A. Carr, Prabhu Rajasekaran, Stijn Volckaert, Yeoul Na, Michael Franz, and Mathias Payer. “Venerable Variadic Vulnerabilities Vanquished”. In: *Usenix Security Symposium*. 2017, (16% acceptance rate –85/522).

[C26] Scott A. Carr and Mathias Payer. “DataShield: Configurable Data Confidentiality and Integrity”. In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2017, (18% acceptance rate –67/359). DOI: 10.1145/3052973.3052983.

[C27] Abraham A. Clements, Naif Saleh Almakhdhub, Khaled Saab, Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, and Mathias Payer. “Protecting Bare-metal Embedded Systems with Privilege Overlays”. In: *IEEE International Symposium on Security and Privacy*. 2017, (13% acceptance rate –60/450). DOI: 10.1109/SP.2017.37.

[C28] Alessandro Di Federico, Mathias Payer, and Giovanni Agosta. “REV.NG: A Unified Binary Analysis Framework for CFG and Function Boundaries Recovery”. In: *International Conference on Compiler Construction*. 2017, (24% acceptance rate –13/53). DOI: 10.1145/3033019.3033028.

[C29] Xinyang Ge, Mathias Payer, and Trent Jaeger. “An Evil Copy: How the Loader Betrays You”. In: *Network and Distributed System Security Symposium*. 2017, (16% acceptance rate –68/423). DOI: 10.14722/ndss.2017.23199.

[C30] Ahmed Hussein, Mathias Payer, Antony L. Hosking, and Christopher A. Vick. “One Process to Reap Them All: Garbage Collection As A Service”. In: *ACM International Conference on Virtual Execution Environments*. 2017, (43% acceptance rate –18/41). DOI: 10.1145/3050748.3050754.

[C31] Yuseok Jeon, Priyam Biswas, Scott A. Carr, Byoungyoung Lee, and Mathias Payer. “HexType: Efficient Detection of Type Confusion Errors for C++”. In: *ACM Conference on Computer and Communication Security*. 2017, (18% acceptance rate –151/836). DOI: 10.1145/3133956.3134062.

[C32] Daniele Midi, Mathias Payer, and Elisa Bertino. “Memory Safety for Embedded Devices with nesCheck”. In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2017, (18% acceptance rate –67/359). DOI: 10.1145/3052973.3053014.

[C33] Nathan Burow, Derrick McKee, Scott A. Carr, and Mathias Payer. “CFIXX: Object Type Integrity for C++ Virtual Dispatch”. In: *Network and Distributed System Security Symposium*. 2018, (21% acceptance rate –71/331). DOI: 10.14722/ndss.2018.23279.

[C34] Nathan Burow, Derrick McKee, Scott A. Carr, and Mathias Payer. “CUP: Comprehensive User-Space Protection for C/C++”. In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2018, (20% acceptance rate –62/310). DOI: 10.1145/3196494.3196540.

[C35] Abraham A. Clements, Naif Saleh Almakhdhub, Saurabh Bagchi, and Mathias Payer. “ACES: Automatic Compartments for Embedded Systems”. In: *Usenix Security Symposium*. 2018, (19% acceptance rate –100/524).

[C36] Kyriakos Ispoglou, Bader AlBassam, Trent Jaeger, and Mathias Payer. “Block Oriented Programming: Automating Data-Only Attacks”. In: *ACM Conference on Computer and Communication Security*. 2018, (16% acceptance rate –134/809). DOI: 10.1145/3243734.3243739.

[C37] Hui Peng, Yan Shoshitaishvili, and Mathias Payer. “T-Fuzz: fuzzing by program transformation”. In: *IEEE International Symposium on Security and Privacy*. 2018, (11% acceptance rate –63/549). DOI: 10.1109/SP.2018.00056.

[C38] Zhihao Yao, Saeed Mirzamohammadi, Ardalan Amiri Sani, and Mathias Payer. “Milkomeda: Safeguarding the Mobile GPU Interface Using WebGL Security Checks”. In: *ACM Conference on Computer and Communication Security*. 2018, (16% acceptance rate –134/809). DOI: 10.1145/3243734.3243772.

[C39] Naif Saleh Almakhdhub, Abraham A. Clements, Mathias Payer, and Saurabh Bagchi. “BenchIoT: A Security Benchmark for the Internet of Things”. In: *IEEE/IFIP International Conference on Dependable Systems and Networks*. 2019, (21% acceptance rate –54/252). DOI: 10.1109/DSN.2019.00035.

[C40] Atri Bhattacharyya, Alexandra Sandulescu, Matthias Neugschwandtner, Alessandro Sorniotti, Babak Falsafi, Mathias Payer, and Anil Kurmus. “SMoTherSpectre: exploiting speculative execution through port contention”. In: *ACM Conference on Computer and Communication Security*. 2019, (15% acceptance rate –149/933). DOI: 10.1145/3319535.3363194.

[C41] Nathan Burow, Xingping Zhang, and Mathias Payer. “SoK: Shining Light on Shadow Stacks”. In: *IEEE International Symposium on Security and Privacy*. 2019, (13% acceptance rate –73/545). DOI: 10.1109/SP.2019.00076.

[C42] Yuseok Jeon, Junghwan Rhee, Chung Hwan Kim, Zhichun Li, Mathias Payer, Byoungyoung Lee, and Zhenyu Wu. “PoLPer: Process-Aware Restriction of Over-Privileged Setuid Calls in Legacy Applications”. In: *ACM Conference on Data and Application Security and Privacy*. 2019, (23% acceptance rate –28/119). DOI: 10.1145/3292006.3300028.

[C43] Rouhollah Mahfouzi, Amir Aminifar, Soheil Samii, Mathias Payer, Petru Eles, and Zebo Peng. “Butterfly Attack: Adversarial Manipulation of Temporal Properties of Cyber-Physical Systems”. In: *Real-Time Systems Symposium*. 2019, (100% acceptance rate –39/39). DOI: 10.1109/RTSS46320.2019.00019.

[C44] Shin-Yeh Tsai, Mathias Payer, and Yiying Zhang. “Pythia: Remote Oracles for the Masses”. In: *Usenix Security Symposium*. 2019, (15% acceptance rate –111/737).

[C45] Naif Saleh Almakhdhub, Abraham A. Clements, Saurabh Bagchi, and Mathias Payer. “uRAI: Securing Embedded Systems with Return Address Integrity”. In: *Network and Distributed System Security Symposium*. 2020, (17% acceptance rate –88/506). DOI: 10.14722/ndss.2020.24016.

[C46] Atri Bhattacharyya, Andres Sanchez, Esmaeil Mohammmadian Koruyeh, Nael Abu-Ghazaleh, Chengyu Song, and Mathias Payer. “SpecROP: Speculative Exploitation of ROP Chains”. In: *Recent Advances in Intrusion Detection*. 2020, (25% acceptance rate –31/121).

[C47] Abraham A. Clements, Eric Gustafson, Tobias Scharnowski, David Fritz, Christopher Kruegel, Giovanni Vigna, Saurabh Bagchi, and Mathias Payer. “HALucinator: Firmware Re-hosting Through Abstraction Layer Emulation”. In: *Usenix Security Symposium*. 2020, (16% acceptance rate –157/977).

[C48] Sushant Dinesh, Nathan Burow, Dongyan Xu, and Mathias Payer. “RetroWrite: Statically Instrumenting COTS Binaries for Fuzzing and Sanitization”. In: *IEEE International Symposium on Security and Privacy*. 2020, (10% acceptance rate –92/841). DOI: 10.1109/SP40000.2020.00009.

[C49] Kyriakos Ispoglou, Daniel Austin, Vishwath Mohan, and Mathias Payer. “FuzzGen: Automatic Fuzzer Generation”. In: *Usenix Security Symposium*. 2020, (16% acceptance rate –157/977).

[C50] Yuseok Jeon, WookHyun Han, Nathan Burow, and Mathias Payer. “FuZZan: Efficient Sanitizer Metadata Design for Fuzzing”. In: *Usenix Annual Technical Conference*. 2020, (18% acceptance rate –65/348).

[C51] Hui Peng and Mathias Payer. “USBFuzz: A Framework for Fuzzing USB Drivers by Device Emulation”. In: *Usenix Security Symposium*. 2020, (16% acceptance rate –157/977).

[C52] Jianliang Wu, Yuhong Nan, Vireshwar Kumar, Mathias Payer, and Dongyan Xu. “BlueShield: Detecting Spoofing Attacks in Bluetooth Low Energy Networks”. In: *Recent Advances in Intrusion Detection*. 2020, (25% acceptance rate –31/121).

[C53] Sumaya Almanee, Arda Unal, Mathias Payer, and Joshua Garcia. “Too Quiet in the Library: An Empirical Study of Security Updates in Android Apps’ Native Code”. In: *International Conference on Software Engineering*. 2021, (22% acceptance rate –138/615). DOI: 10.1109/ICSE43902.2021.00122.

[C54] Cesar Avalos Baddouh, Mahmoud Khairy, Roland N. Green, Mathias Payer, and Timothy G. Rogers. “Principal Kernel Analysis: A Tractable Methodology to Simulate Scaled GPU Workloads”. In: *International Symposium on Microarchitecture*. 2021, (21% acceptance rate –94/430). DOI: 10.1145/3466752.3480100.

[C55] Rohit Bhatia, Vireshwar Kumar, Khaled Serag, Z. Berkay Celik, Mathias Payer, and Dongyan Xu. “Evading Voltage-Based Intrusion Detection on Automotive CAN”. In: *Network and Distributed System Security Symposium*. 2021, (15% acceptance rate –87/573). DOI: 10.14722/ndss.2021.23013.

[C56] Priyam Biswas, Nathan Burow, and Mathias Payer. “Code Specialization through Dynamic Feature Observation”. In: *ACM Conference on Data and Application Security and Privacy*. 2021, (22% acceptance rate –24/106). DOI: 10.1145/3422337.3447844.

[C57] Adrien Ghosn, Marios Kogias, Mathias Payer, James R. Larus, and Edouard Bugnion. “Enclosure: language-based restriction of untrusted libraries”. In: *International Conference on Architectural Support for Programming Languages and Operating Systems*. 2021, (18% acceptance rate –75/398). DOI: 10.1145/3445814.3446728.

[C58] Siddharth Gupta, Atri Bhattacharyya, Yunho Oh, Abhishek Bhattacharjee, Babak Falsafi, and Mathias Payer. “Rebooting Virtual Memory with Midgard”. In: *International Symposium on Computer Architecture*. 2021, (18% acceptance rate –76/406). DOI: 10.1109/ISCA52012.2021.00047.

[C59] Ahmad Hazimeh, Adrian Herrera, and Mathias Payer. “MAGMA: A Ground-Truth Fuzzing Benchmark”. In: *ACM SIGMETRICS*. 2021, (12% acceptance rate –38/315). DOI: 10.1145/3428334.

[C60] Adrian Herrera, Hendra Gunadi, Shane Magrath, Michael Norrish, Mathias Payer, and Tony Hosking. “Seed Selection for Successful Fuzzing”. In: *ACM SIGSOFT International Symposium on Software Testing and Analysis*. 2021, (21% acceptance rate –51/233). DOI: 10.1145/3460319.3464795.

[C61] Zhiyuan Jiang, Xiyue Jiang, Ahmad Hazimeh, Chaojing Tang, Chao Zhang, and Mathias Payer. “Igor: Crash Deduplication Through root-Cause Clustering”. In: *ACM Conference on Computer and Communication Security*. 2021, (22% acceptance rate –196/879). DOI: 10.1145/3460120.3485364.

[C62] Nick Roessler, Lucas Atayde, Imani Palmer, Derrick McKee, Jai Pandey, Vasileios P. Kemerlis, Mathias Payer, Adam Bates, Andre DeHon, Jonathan M. Smith, and Nathan Dautenhahn. “uSCOPE: A Methodology for Analyzing Least-Privilege Compartmentalization in Large Software Artifacts”. In: *Recent Advances in Intrusion Detection*. 2021, (23% acceptance rate –33/138).

[C63] Prashast Srivastava and Mathias Payer. “Gramatron: Effective Grammar-aware Fuzzing”. In: *ACM SIGSOFT International Symposium on Software Testing and Analysis*. 2021, (21% acceptance rate –51/233). DOI: 10.1145/3460319.3464814.

[C64] Jianliang Wu, Ruoyu Wu, Daniele Antonioli, Mathias Payer, Nils Ole Tippenhauer, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. “LIGHTBLUE: Automatic Profile-Aware Debloating of Bluetooth”. In: *Usenix Security Symposium*. 2021, (18% acceptance rate –248/1319).

[C65] Daniele Antonioli, Nils Tippenhauer, Kasper Rasmussen, and Mathias Payer. “BLURtooth: Exploiting Cross-Transport Key Derivation in Bluetooth Classic and Bluetooth Low Energy”. In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2022, (18% acceptance rate –85/463). DOI: 10.1145/3488932.3523258.

[C66] Atri Bhattacharyya, Uros Tesic, and Mathias Payer. “Midas: Systematic Kernel TOCTTOU Protection”. In: *Usenix Security Symposium*. 2022, (17% acceptance rate –256/1492).

[C67] Marco Casagrande, Eleonora Losiouk, Mauro Conti, Mathias Payer, and Daniele Antonioli. "BreakMi: Reversing, Exploiting and Fixing Xiaomi Fitness Tracking Ecosystem". In: *IACR Conference on Crypotographic Hardware and Embedded Systems*. 2022, (37% acceptance rate –83/221).

[C68] Kaiming Huang, Yongzhe Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, and Trent Jaeger. "The Taming of the Stack: Isolating Stack Data from Memory Errors". In: *Network and Distributed System Security Symposium*. 2022, (16% acceptance rate –83/513). DOI: 10.14722/NDSS.2022.23060.

[C69] Zhiyuan Jiang, Shuitao Gan, Adrian Herrera, Flavio Toffalini, Lucio Romerio, Chaojing Tang, Manuel Egele, Chao Zhang, and Mathias Payer. "Evocatio: Conjuring Bug Capabilities from a Single PoC". In: *ACM Conference on Computer and Communication Security*. 2022, (22% acceptance rate –218/972). DOI: 10.1145/3548606.3560575.

[C70] Yuan Li, Wende Tan, Zhizheng Lv, Songtao Yang, Mathias Payer, Ying Liu, and Chao Zhang. "PACMem: Enforcing Spatial and Temporal Memory Safety via ARM Pointer Authentication". In: *ACM Conference on Computer and Communication Security*. 2022, (22% acceptance rate –218/972). DOI: 10.1145/3548606.3560598.

[C71] Derrick McKee, Yianni Giannaris, Carolina Ortega Perez, Howard Shrobe, Mathias Payer, Hamed Okhravi, and Nathan Burow. "Preventing Kernel Hacks with HAKCs". In: *Network and Distributed System Security Symposium*. 2022, (**distinguished paper award**, 16% acceptance rate –83/513). DOI: 10.14722/ndss.2022.24026.

[C72] Prashast Srivastava, Stefan Nagy, Matthew Hicks, Antonio Bianchi, and Mathias Payer. "One Fuzz Doesn't Fit All: Optimizing Directed Fuzzing via Target-tailored Program State Restriction". In: *Annual Computer Security Applications Conference*. 2022, (**best poster award**, 24% acceptance rate –73/303). DOI: 10.1145/3564625.3564643.

[C73] Flavio Toffalini, Mathias Payer, Jianying Zhou, and Lorenzo Cavallaro. "Designing a Provenance Analysis for SGX Enclaves". In: *Annual Computer Security Applications Conference*. 2022, (24% acceptance rate –73/303). DOI: 10.1145/3564625.3567994.

[C74] Fei Wang, Jianliang Wu, Yuhong Nan, Yousra Aafer, Xiangyu Zhang, Dongyan Xu, and Mathias Payer. "ProFactory: Improving IoT Security via Formalized Protocol Customization". In: *Usenix Security Symposium*. 2022, (17% acceptance rate –256/1492).

[C75] Chijin Zhou, Quan Zhang, Mingzhe Wang, Lihua Guo, Jie Liang, Zhe Liu, Mathias Payer, and Yu Jiang. "Minerva: Browser API Fuzzing with Dynamic Mod-Ref Analysis". In: *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2022, (**distinguished paper award**, 22% acceptance rate –99/449). DOI: 10.1145/3540250.3549107.

[C76] Luca Di Bartolomeo, Hossein Moghaddas, and Mathias Payer. "ARMore: Pushing Love Back Into Binaries". In: *Usenix Security Symposium*. 2023, (29% acceptance rate –422/1444).

[C77] Atri Bhattacharyya, Florian Hofhammer, Yuanlong Li, Siddharth Gupta, Andres Sanchez, Babak Falsafi, and Mathias Payer. "SecureCells: A Secure Compartmentalized Architecture". In: *IEEE International Symposium on Security and Privacy*. 2023, (17% acceptance rate –196/1147). DOI: 10.1109/SP46215.2023.00125.

[C78] Marcel Busch, Mathias Payer, Aravind Machiry, Christopher Kruegel, Giovanni Vigna, and Chad Spensky. "TEEzz: Fuzzing Trusted Applications on COTS Android Devices". In: *IEEE International Symposium on Security and Privacy*. 2023, (17% acceptance rate –196/1147). DOI: 10.1109/SP46215.2023.00013.

[C79] Marius Fleischer, Dipanjan Das, Priyanka Bose, Weiheng Bai, Kangjie Lu, Mathias Payer, Christopher Kruegel, and Giovanni Vigna. "ACTOR: Action-Guided Kernel Fuzzing". In: *Usenix Security Symposium*. 2023, (29% acceptance rate –422/1444).

[C80] Ognjen Glamocanin, Hajira Bazaz, Mathias Payer, and Mirjana Stojilovic. “Temperature Impact on Remote Power Side-Channel Attacks on Shared FPGAs”. In: *Design, Automation and Test in Europe Conference*. 2023, (25% acceptance rate –205/820).

[C81] Siddharth Gupta, Yuanlong Li, Qingxuan Kang, Abhishek Bhattacharjee, Babak Falsafi, Yunho Oh, and Mathias Payer. “Imprecise Store Exceptions”. In: *International Symposium on Computer Architecture*. 2023, (21% acceptance rate –79/373). DOI: 10.1145/3579371.3589087.

[C82] Qiang Liu, Flavio Toffalini, Yajin Zhou, and Mathias Payer. “ViDeZZo: Dependency-aware Virtual Device Fuzzing”. In: *IEEE International Symposium on Security and Privacy*. 2023, (17% acceptance rate –196/1147). DOI: 10.1109/SP46215.2023.00136.

[C83] Hui Peng, Zhihao Yao, Ardalan Amiri Sani, Dave (Jing) Tian, and Mathias Payer. “GLeeFuzz: Fuzzing WebGL Through Error-Message-Guided Mutation”. In: *Usenix Security Symposium*. 2023, (29% acceptance rate –422/1444).

[C84] Sirus Shahini, Robert Ricci, Mu Zhang, and Mathias Payer. “Arvin: Greybox Fuzzing Using Approximate Dynamic CFG Analysis”. In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2023, (17% acceptance rate –74/429). DOI: 10.1145/3579856.3582813.

[C85] Ji Shi, Zhun Wang, Zhiyao Feng, Yang Lan, Shisong Qin, Wei You, Wei Zou, Mathias Payer, and Chao Zhang. “AIFORE: Smart Fuzzing Based on Automatic Input Format Reverse Engineering”. In: *Usenix Security Symposium*. 2023, (29% acceptance rate –422/1444).

[C86] Prashast Srivastava, Flavio Toffalini, Kostyantyn Vorobyov, Francois Gauthier, Antonio Bianchi, and Mathias Payer. “Crystallizer: A Hybrid Path Analysis Framework To Aid in Uncovering Deserialization Vulnerabilities”. In: *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2023, (27% acceptance rate –127/465). DOI: 10.1145/3611643.3616313.

[C87] Jianhao Xu, Luca Di Bartolomeo, Flavio Toffalini, Bing Mao, and Mathias Payer. “WarpAttack: Bypassing CFI through Compiler-Introduced Double-Fetches”. In: *IEEE International Symposium on Security and Privacy*. 2023, (17% acceptance rate –196/1147). DOI: 10.1109/SP46215.2023.00176.

[C88] Jianhao Xu, Kangjie Lu, Zhengjie Du, Zhu Ding, Linke Li, Qiushi Wu, Mathias Payer, and Bing Mao. “Silent Bugs Matter: A Study of Compiler-Introduced Security Bugs”. In: *Usenix Security Symposium*. 2023, (29% acceptance rate –422/1444).

[C89] Han Zheng, Jiayuan Zhang, Yuhang Huang, Zezhong Ren, He Wang, Chunjie Cao, Yuqing Zhang, Flavio Toffalini, and Mathias Payer. “FishFuzz: Catch Deeper Bugs by Throwing Larger Nets”. In: *Usenix Security Symposium*. 2023, (29% acceptance rate –422/1444).

[C90] Aleksander Boruch-Gruszecki, Adrien Ghosn, Mathias Payer, and Clément Pit-Claudel. “Gradient: Gradual Compartmentalization via Object Capabilities Tracked in Types”. In: *Object-Oriented Programming, Systems, Languages, and Applications*. 2024, (36% acceptance rate –95/261). DOI: 10.1145/3689751.

[C91] Alexander Bulekov, Qiang Liu, Manuel Egele, and Mathias Payer. “HyperPill: Fuzzing for Hypervisor-bugs by leveraging the Hardware Virtualization Interface”. In: *Usenix Security Symposium*. 2024, (**distinguished paper award**, 18% acceptance rate –417/2276).

[C92] Marcel Busch, Philipp Mao, and Mathias Payer. “GlobalConfusion: TrustZone Trusted Application 0-Days by Design”. In: *Usenix Security Symposium*. 2024, (18% acceptance rate –417/2276).

[C93] Marcel Busch, Philipp Mao, and Mathias Payer. “Spill the TeA: An Empirical Study of Trusted Application Rollback Prevention on Android”. In: *Usenix Security Symposium*. 2024, (18% acceptance rate –417/2276).

[C94] Ahmad Hazimeh, Duo Xu, Qiang Liu, Yan Wang, and Mathias Payer. “Tango: Extracting Higher-Order Feedback through State Inference”. In: *Recent Advances in Intrusion Detection*. 2024, (**best paper award**, 25% acceptance rate –43/172). DOI: 10.1145/3678890.3678908.

[C95] Heqing Huang, Anshunkang Zhou, Mathias Payer, and Charles Zhang. “Everything is Good for Something: Counterexample-Guided Directed Fuzzing via Likely Invariant Inference”. In: *IEEE International Symposium on Security and Privacy*. 2024, (17% acceptance rate –261/1466). DOI: 10.1109/SP54263.2024.00142.

[C96] Kaiming Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, and Trent Jaeger. “Top of the Heap: Efficient Memory Error Protection of Safe Heap Objects”. In: *ACM Conference on Computer and Communication Security*. 2024, (16% acceptance rate –328/1964). DOI: 10.1145/3658644.3690310.

[C97] Gwangmu Lee, Duo Xu, Solmaz Salimi, Byoungyoung Lee, and Mathias Payer. “SyzRisk: A Change-Pattern-Based Continuous Kernel Regression Fuzzer”. In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2024, (21% acceptance rate –129/588). DOI: 10.1145/3634737.3637642.

[C98] Christian Lindenmeier, Mathias Payer, and Marcel Busch. “EL3XIR: Fuzzing COTS Secure Monitors”. In: *Usenix Security Symposium*. 2024, (18% acceptance rate –417/2276).

[C99] Tao Lyu, Liyi Zhang, Zhiyao Feng, Yueyang Pan, Yujie Ren, Meng Xu, Mathias Payer, and Sanidhya Kashyap. “Monarch: A Fuzzing Framework for Distributed File Systems”. In: *Usenix Annual Technical Conference*. 2024, (15% acceptance rate –77/488).

[C100] Philipp Mao, Elias Valentin Boschung, Marcel Busch, and Mathias Payer. “Exploiting Android’s Hardened Memory Allocator”. In: *Usenix Workshop on Offensive Technologies*. 2024, (**best paper award**, 35% acceptance rate –18/51).

[C101] Qinying Wang, Boyu Chang, Shouling Ji, Yuan Tian, Xuhong Zhang, Binbin Zhao, Gaoning Pan, Chenyang Lyu, Mathias Payer, Wenhai Wang, and Raheem Beyah. “SyzTrust: State-aware Fuzzing on Trusted OS Designed for IoT Devices”. In: *IEEE International Symposium on Security and Privacy*. 2024, (17% acceptance rate –261/1466). DOI: 10.1109/SP54263.2024.00070.

[C102] Haoran Xu, Zhiyuan Jiang, Yongjun Wang, Shuhui Fan, Shenglin Xu, Peidai Xie, Shaojing Fu, and Mathias Payer. “Fuzzing JavaScript Engines with a Graph-based IR”. In: *ACM Conference on Computer and Communication Security*. 2024, (16% acceptance rate –328/1964). DOI: 10.1145/3658644.3690336.

[C103] Nicolas Badoux, Flavio Toffalini, Yuseok Jeon, and Mathias Payer. “type++: Prohibiting Type Confusion with Inline Type Information”. In: *Network and Distributed System Security Symposium*. 2025, (**distinguished paper award**, 16% acceptance rate –211/1311). DOI: 10.14722/ndss.2025.230053.

[C104] Nicolas Badoux, Flavio Toffalini, and Mathias Payer. “Sourcerer: channeling the void”. In: *Conference on Detection of Intrusions and Malware and Vulnerability Assessment*. 2025, (24% acceptance rate –25/103). DOI: 10.1007/978-3-031-97620-9_5.

[C105] Luca Di Bartolomeo, Philipp Mao, Yu-Jye Tung, Jessy Ayala, Marcel Busch, Paolo Celada, Samuele Doria, Joshua Garcia, Eleonora Losiouk, and Mathias Payer. “Hercules Droidot and the murder on the JNI Express”. In: *Usenix Security Symposium*. 2025, (17% acceptance rate –407/2385).

[C106] Daniele Cono D’Elia, Thaleia Dimitra Doudali, Cristiano Giuffrida, Miguel Matos, Mathias Payer, Solal Pirelli, Georgios Portokalidis, Valerio Schiavoni, Salvatore Signorello, and Anjo Vahldiek-Oberwagner. “Lessons Learned from Five Years of Artifact Evaluations at EuroSys”. In: *ACM Conference on Reproducibility and Replicability*. 2025. DOI: 10.1145/3736731.3746152.

[C107] Kaiming Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, and Trent Jaeger. "SoK: Challenges and Paths Toward Memory Safety for eBPF". In: *IEEE International Symposium on Security and Privacy*. 2025, (14% acceptance rate –256/1740). DOI: 10.1109/SP61157.2025.00134.

[C108] Yuanlong Li, Atri Bhattacharyya, Madhur Kumar, Abhishek Bhattacharjee, Yoav Etsion, Babak Falsafi, Sanidhya Kashyap, and Mathias Payer. "Single-Address-Space FaaS with Jord". In: *International Symposium on Computer Architecture*. 2025, (**IEEE MICRO Top Picks 2026**, 23% acceptance rate –132/570). DOI: 10.1145/3695053.3731108.

[C109] Tao Lyu, Kumar Kartikeya Dwivedi, Thomas Bourgeat, Mathias Payer, Meng Xu, and Sanidhya Kashyap. "eBPF Misbehavior Detection: Fuzzing with a Specification-Based Oracle". In: *Symposium on Operating Systems Principles*. 2025, (17% acceptance rate –65/370). DOI: 10.1145/3731569.3764797.

[C110] Zheyu Ma, Qiang Liu, Zheming Li, Tingting Yin, Wende Tan, Chao Zhang, and Mathias Payer. "Truman: Constructing Device Behavior Models from OS Drivers to Fuzz Virtual Devices". In: *Network and Distributed System Security Symposium*. 2025, (16% acceptance rate –211/1311). DOI: 10.14722/ndss.2025.240301.

[C111] Philipp Mao, Marcel Busch, and Mathias Payer. "NASS: Fuzzing All Native Android System Services with Interface Awareness and Coverage". In: *Usenix Security Symposium*. 2025, (17% acceptance rate –407/2385).

[C112] Matteo Marini, Daniele Cono D'Elia, Mathias Payer, and Leonardo Querzoni. "QMSan: Efficiently Detecting Uninitialized Memory Errors During Fuzzing". In: *Network and Distributed System Security Symposium*. 2025, (16% acceptance rate –211/1311). DOI: 10.14722/ndss.2025.241133.

[C113] CheolJun Park, Marc Egli, BeomSeok Oh, Tuan Dinh Hoang, Suhwan Jeong, Martin Crettol, Insu Yun, Mathias Payer, and Yongdae Kim. "OTABase: Enhancing Over-the-Air Testing to Detect Memory Crashes in Cellular Basebands". In: *Annual Computer Security Applications Conference*. 2025.

[C114] Flavio Toffalini, Nicolas Badoux, Zurab Tsindaze, and Mathias Payer. "Liberating libraries through automated fuzz driver generation: Striking a Balance Without Consumer Code". In: *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2025, (24% acceptance rate –149/612). DOI: 10.1145/3729365.

[C115] Daan Vanoverloop, Andres Sanchez, Flavio Toffalini, Frank Piessens, Mathias Payer, and Jo Van Bulck. "TLBlur: Compiler-Assisted Automated Hardening against Controlled Channels on Off-the-Shelf Intel SGX Platforms". In: *Usenix Security Symposium*. 2025, (17% acceptance rate –407/2385).

[C116] Liam Wachter, Julian Gremminger, Christian Wressnegger, Mathias Payer, and Flavio Toffalini. "DUMPLING: Fine-grained Differential JavaScript Engine Fuzzing". In: *Network and Distributed System Security Symposium*. 2025, (**distinguished paper award**, 16% acceptance rate –211/1311). DOI: 10.14722/ndss.2025.241411.

[C117] Chibin Zhang, Gwangmu Lee, Qiang Liu, and Mathias Payer. "Reflecta: Reflection-based Scalable and Semantic Scripting Language Fuzzing". In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2025. DOI: 10.1145/3708821.3710818.

[C118] Han Zheng, Flavio Toffalini, Marcel Böhme, and Mathias Payer. "MendelFuzz: The Return of the Deterministic Stage". In: *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2025, (24% acceptance rate –149/612). DOI: 10.1145/3715713.

[C119] Bofei Chen, Shuang Liao, Lei Zhang, Chibin Zhang, Mathias Payer, and Yuan Zhang. "Patch-Guided Vulnerability Detection: Extracting Java API Security Rules via Attack–Defense Cross-Analysis". In: *Usenix Security Symposium*. 2026, (13% acceptance rate –362/2750).

[C120] Lukas Dresel, Stijn Pletinckx, Fabio Gritti, Mathias Payer, Giovanni Vigna, and Christopher Kruegel. "It's Not You, It's Me: Reevaluating the Relationship between Concolic Execution and Fuzzing". In: *IEEE European Symposium on Security and Privacy*. 2026, (19% acceptance rate –82/427). DOI: 10.1109/EuroSP68448.2026.00075.

[C121] Rokhaya-Diamil Fall, Philipp Mao, Martin Wagner, and Mathias Payer. "Exploiting Android Apps with Counterfeit Art". In: *Usenix Workshop on Offensive Technologies*. 2026, (40% acceptance rate –26/64).

[C122] Florian Hofhammer, Daniele Antonioli, and Mathias Payer. "PrivacyShield: Relaying BLE Beacons to Counter Unsolicited Tracking". In: *Usenix Security Symposium*. 2026, (13% acceptance rate –362/2750).

[C123] Sungwoo Kim, Hui Peng, Imtiaz Karim, Ruoyu Wu, Jianliang Wu, Elisa Bertino, Mathias Payer, and Dave (Jing) Tian. "FuzzBT: Holistic-State-Guided Fuzzing for Bluetooth Host Stack in Kernels". In: *Usenix Workshop on Offensive Technologies*. 2026, (40% acceptance rate –26/64).

[C124] Philipp Mao, Li Shi, Marcel Busch, and Mathias Payer. "TÄMU: Emulating Trusted Applications at the (GlobalPlatform)-API Layer". In: *IEEE International Symposium on Security and Privacy*. 2026, (12% acceptance rate –254/1995).

[C125] Giacomo Priamo, Daniele Cono D'Elia, Mathias Payer, and Leonardo Querzoni. "Towards Path-aware Coverage-guided Fuzzing". In: *IEEE/ACM International Symposium on Code Generation and Optimization*. 2026. DOI: 10.1109/CGO68049.2026.11395191.

[C126] Zhezhong Ren, Han Zheng, Zhiyao Feng, Qinying Wang, Marcel Busch, Yuqing Zhang, Chao Zhang, and Mathias Payer. "SYSYPHUZZ and the Pressure of More Coverage". In: *Network and Distributed System Security Symposium*. 2026, (17% acceptance rate –265/1481). DOI: 10.14722/ndss.2026.230921.

[C127] Nicolas Szwajcok, Taro Tsuchiya, Enze Liu, Kyle Soska, Mathias Payer, and Nicolas Christin. "Meme Coin Factories: Uncovering Large-Scale Manipulations on pump.fun (to appear)". In: *ACM Conference on Computer and Communication Security*. 2026.

[C128] Qinying Wang, Yong Yang, Yuan Chen, Shouling Ji, and Mathias Payer. "When HTTP 402 Meets the Blockchain: Risks on Emerging x402 Payments". In: *Usenix Security Symposium*. 2026, (13% acceptance rate –362/2750).

[C129] Jianhao Xu, Kunbo Zhang, Mathias Payer, Kangjie Lu, and Bing Mao. "CLower: Detecting Compiler Pessimization Bugs through Redundant Memory Accesses". In: *Object-Oriented Programming, Systems, Languages, and Applications*. 2026. DOI: 10.1145/3798250.

[C130] Chibin Zhang, Qiang Liu, and Mathias Payer. "CrossFit: Demystifying VM Callback Bugs in Interpreters". In: *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2026. DOI: 10.1145/3808111.

[C131] Han Zheng, Flavio Toffalini, Qiang Liu, and Mathias Payer. "Squeezing Juicy Variant Bugs Out of Modern Browsers". In: *Usenix Workshop on Offensive Technologies*. 2026, (**best paper award**, 40% acceptance rate –26/64).

[C132] Cesar Avalos, Mathias Payer, and Tim Rogers. "EoSS: Exploring SASS - A Systematic Framework to Explore NVIDIA's ISA (to appear)". In: *International Conference on Architectural Support for Programming Languages and Operating Systems*. 2027.

[C133] Luca Di Bartolomeo, Philipp Mao, and Mathias Payer. "Forgotten Libraries: Assessing Systemic Android Insecurity (to appear)". In: *Network and Distributed System Security Symposium*. 2027.

[C134] Philipp Mao, Yiwen Xu, Marcel Busch, and Mathias Payer. "Oversharing: Exposing Double Fetch Vulnerabilities in Trusted Applications (to appear)". In: *Network and Distributed System Security Symposium*. 2027.

[C135] Chibin Zhang, Qinying Wang, and Mathias Payer. “All You Wanted to Know About Scripting Language Fuzzing But Were Afraid to Ask (to appear)”. In: *Network and Distributed System Security Symposium*. 2027.

WORKSHOP PROCEEDINGS

[W1] Mathias Payer and Thomas R. Gross. “Requirements for Fast Binary Translation”. In: *Workshop on Architectural and Microarchitectural Support for Binary Translation*. 2009.

[W2] Mathias Payer, Boris Bluntschli, and Thomas R. Gross. “LLDSAL: A Low-Level Domain-Specific Aspect Language for Dynamic Code-Generation and Program Modification”. In: *AOSD workshop on Domain-Specific Aspect Languages*. 2012. DOI: 10.1145/2162037.2162043.

[W3] Mathias Payer, Boris Bluntschli, and Thomas R. Gross. “DynSec: On-the-fly Code Rewriting and Repair”. In: *Usenix Workshop on Hot Topics in Software Upgrades*. 2013.

[W4] Mathias Payer and Thomas R. Gross. “String Oriented Programming: When ASLR is Not Enough”. In: *Program Protection and Reverse Engineering Workshop*. 2013. DOI: 10.1145/2430553.2430555.

[W5] Antonio Barresi, Kaveh Razavi, Mathias Payer, and Thomas R. Gross. “CAIN: Silently Breaking ASLR in the Cloud”. In: *Usenix Workshop on Offensive Technologies*. 2015.

[W6] Vijay D’Silva, Mathias Payer, and Dawn Song. “The Correctness-Security Gap in Compiler Optimization”. In: *Language-theoretic Security IEEE Security and Privacy Workshop*. 2015. DOI: 10.1109/SPW.2015.33.

[W7] Andreas Follner, Alexandre Bartel, Hui Peng, Yu-Chen Chang, Kyriakos Ispoglou, Mathias Payer, and Eric Bodden. “PSHAPE: Automatically Combining Gadgets for Arbitrary Method Execution”. In: *International Workshop on Security and Trust Management*. 2016, (38% acceptance rate –13/34). DOI: 10.1007/978-3-319-46598-2_15.

[W8] Kyriakos Ispoglou and Mathias Payer. “malWASH: Washing malware to evade dynamic analysis”. In: *Usenix Workshop on Offensive Technologies*. 2016, (47% acceptance rate –21/44).

[W9] Mathias Payer. “libdetox: A Framework for Online Program Transformation”. In: *Forming an Ecosystem Around Software Transformation*. 2016.

[W10] Frank Capobianco, Rahul George, Kaiming Huang, Trent Jaeger, Mathias Payer, Srikanth Krishnamurthy, Zhiyun Qian, and Paul Yu. “Employing Attack Graphs for Intrusion Detection”. In: *New Security Paradigms Workshop*. 2019, (41% acceptance rate –10/24).

[W11] Prashast Srivastava, Hui Peng, Jiahao Li, Hamed Okhravi, Howard Shrobe, and Mathias Payer. “FirmFuzz: Automated IoT Firmware Introspection and Analysis”. In: *Workshop on the Internet of Things Security and Privacy*. 2019, (40% acceptance rate –8/20). DOI: 10.1145/3338507.3358616.

[W12] Jianliang Wu, Yuhong Nan, Vireshwar Kumar, Dave (Jing) Tian, Antonio Bianchi, Mathias Payer, and Dongyan Xu. “BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy”. In: *Usenix Workshop on Offensive Technologies*. 2020, (**best paper award**, 33% acceptance rate –12/36).

[W13] Daniele Antonioli and Mathias Payer. “On the Insecurity of Vehicles Against Protocol-Level Bluetooth Threats”. In: *Usenix Workshop on Offensive Technologies*. 2022, (38% acceptance rate –10/26).

[W14] Adrian Herrera, Mathias Payer, and Antony L. Hosking. “DatAFLow: Towards a Data-Flow-Guided Fuzzer”. In: *International Fuzzing Workshop*. 2022.

[W15] Khaled Serag, Vireshwar Kumar, Z. Berkay Celik, Rohit Bhatia, Mathias Payer, and Dongyan Xu. “Attacks on CAN Error Handling Mechanism (Demo)”. In: *Automotive and Autonomous Vehicle Security Workshop*. 2022, (88% acceptance rate –15/17). DOI: https://dx.doi.org/10.14722/autosec.2022.23013.

[W16] Charly Castes, Adrien Ghosn, Neelu S. Kalani, Yuchen Qian, Marios Kogias, Mathias Payer, and Edouard Bugnion. “Creating Trust by Abolishing Hierarchies”. In: *Workshop on Hot Topics in Operating Systems*. 2023, (26% acceptance rate –31/117).

[W17] Derrick McKee, Nathan Burow, and Mathias Payer. “Accurate Compiler and Optimization Independent Function Identification Using Program State Transformations”. In: *Workshop on Binary Analysis Research*. 2023, (72% acceptance rate –8/11). DOI: 10.14722/bar.2023.23003.

[W18] Florian Hofhammer, Marcel Busch, Qinying Wang, Manuel Egele, and Mathias Payer. “SURGEON: Performant, Flexible and Accurate Re-Hosting via Transplantation”. In: *Workshop on Binary Analysis Research*. 2024. DOI: 10.14722/bar.2024.23011.

[W19] Han Zheng, Flavio Toffalini, and Mathias Payer. “TuneFuzz: adaptively exploring target programs”. In: *Workshop on Search-Based and Fuzz Testing*. 2024.

[TR1] Mathias Payer. “secuBT: Hacking the Hackers with User-Space Virtualization”. In: *Chaos Communication Congress http://nebelwelt.net/publications/files/09CCC.pdf*. 2009.

[TR2] Mathias Payer. “I Control Your Code - Attack Vectors Through the Exes of Software-based Fault Isolation”. In: *Chaos Communication Congress http://nebelwelt.net/publications/files/10CCC.pdf*. 2010.

[TR3] Mathias Payer and Thomas R. Gross. “adaptSTM - An Online Fine-Grained Adaptive STM System”. In: *Technical Report http://nebelwelt.net/publications/files/10TRadaptstm.pdf*. 2010.

[TR4] Mathias Payer. “String Oriented Programming - Circumventing ASLR, DEP, and Other Guards”. In: *Chaos Communication Congress http://nebelwelt.net/publications/files/11CCC.pdf*. 2011.

[TR5] Mathias Payer. “Too much PIE is bad for performance”. In: *Technical Report http://nebelwelt.net/publications/files/12TRpie.pdf*. 2012.

[TR6] Dan Caselden, Alex Bazhanyuk, Mathias Payer, Stephen McCamant, and Dawn Song. “Transformation-aware Exploit Generation using a HI-CFG”. In: *Technical Report http://nebelwelt.net/publications/files/13TRhicfg.pdf*. 2013.

[TR7] Stephen McCamant, Mathias Payer, Dan Caselden, Alex Bazhanyuk, and Dawn Song. “Transformation-Aware Symbolic Execution for System Test Generation”. In: *Technical Report http://nebelwelt.net/publications/files/13TRhicfg2.pdf*. 2013.

[TR8] Mathias Payer. “Triggering Deep Vulnerabilities Using Symbolic Execution”. In: *Chaos Communication Congress*. 2013.

[TR9] Mathias Payer. “WarGames in Memory”. In: *Chaos Communication Congress*. 2013.

[TR10] Mathias Payer. “Code-Pointer Integrity”. In: *Chaos Communication Congress*. 2014.

[TR11] Mathias Payer. “Embracing the New Threat: Towards Automatically Self-Diversifying Malware”. In: *Symposium on Security for Asia Network + 360 http://nebelwelt.net/publications/files/14SyScan360.pdf*. 2014.

[TR12] Mathias Payer, Antonio Barresi, and Thomas R. Gross. “Lockdown: Dynamic Control-Flow Integrity”. In: *Technical Report http://nebelwelt.net/publications/files/14TRlockdown.pdf*. 2014. DOI: 10.3929/ethz-a-010171214.

[TR13] Mathias Payer, Stephen Crane, Per Larsen, Stefan Brunthaler, Richard Wartell, and Michael Franz. “Similarity-based matching meets Malware Diversity”. In: *arXiv Technical Report http://nebelwelt.net/publications/files/14TRmaldiv.pdf*. 2014.

[TR14] Antonio Barresi, Kaveh Razavi, Mathias Payer, and Thomas R. Gross. “Silently Breaking ASLR in the Cloud”. In: *BlackHat Europe* http://nebelwelt.net/publications/files/15BHEU.pdf. 2015.

[TR15] Mathias Payer. “New memory corruption attacks: why can’t we have nice things?” In: *Chaos Communication Congress*. 2015.

[TR16] Mathias Payer. “Memory Corruption: Why We Can’t Have Nice Things”. In: *Balkan Computer Congress*. 2016.

[TR17] Mathias Payer. “Control-Flow Hijacking: Are We Making Progress?” In: *ACM Symp. on InformAtion, Computer and Communications Security* http://nebelwelt.net/publications/files/17AsiaCCS3.pdf. 2017.

[TR18] Mathias Payer. “Protecting bare-metal smart devices with EPOXY”. In: *Balkan Computer Congress*. 2017.

[TR19] Mathias Payer. “Protecting bare-metal smart devices with EPOXY”. In: *Symposium on Security for Asia Network + 360*. 2017.

[TR20] Mathias Payer. “Type confusion: discovery, abuse, and protection”. In: *Chaos Communication Congress*. 2017, (28% acceptance rate –49/170).

[TR21] Mathias Payer. “Type Confusion: Discovery, Abuse, Protection”. In: *Symposium on Security for Asia Network + 360*. 2018.

[TR22] Matteo Rizzo and Mathias Payer. “No source, no problem! High speed binary fuzzing”. In: *Chaos Communication Congress*. 2019, (20% acceptance rate –39/194).

[TR23] Daniele Antonioli and Mathias Payer. “From the Bluetooth Standard to Standard Compliant 0-days”. In: *Hardwear.IO Hardware Security Conference and Training*. 2020.

[TR24] Atri Bhattacharyya and Mathias Payer. “SMoTherSpectre: Exploiting speculative execution through port contention”. In: *InsomniHack Conference*. 2020.

[TR25] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathe, James R. Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Srdjan Capkun, Kenneth G. Paterson, David A. Basin, Jan Beutel, Dennis Jackson, Bart Preneel, Nigel Smart, Dave Singelee, Aysajan Abidin, Seda Guerses, Michael Veale, Cas Cremers, Michael Backes, Reuben Binns, Ciro Cattuto, Alain Barrat, Giuseppe Persiano, Dario Fiore, Manuel Barbosa, and Dan Boneh. “DP3T - Decentralized Privacy-Preserving Proximity Tracing”. In: *Technical Report* http://nebelwelt.net/publications/files/20TRdp3t.pdf. 2020.

[TR26] Florian Hofhammer, Atri Bhattacharyya, Majid Salehi, Bruno Crispo, Manuel Egele, Mathias Payer, and Marcel Busch. “EmbedFuzz: High Speed Fuzzing Through Transplantation”. In: *arXiv Technical Report* http://nebelwelt.net/publications/files/24arXiv.pdf. 2024. DOI: 10.48550/arXiv.2412.12746.

[TR27] Philipp Mao, Marcel Busch, and Mathias Payer. “Not To Be Trusted - A Fiasco in Android TEEs”. In: *Chaos Communication Congress*. 2025.

[TR28] Mathias Payer. “Advancing from "What the fuzz?" to "All the Fuzz!"”. In: *International Fuzzing Workshop*. 2026.

BOOKS AND CHAPTERS

[B1] Volodymyr Kuznetzov, Laszlo Szekeres, Mathias Payer, George Candea, R. Sekar, and Dawn Song. “Code-pointer Integrity”. In: *The Continuing Arms Race*. 2018. DOI: 10.1145/3129743.3129748.

[B2] Mathias Payer. “How Memory Safety Violations Enable Exploitation of Programs”. In: *The Continuing Arms Race*. 2018. DOI: 10.1145/3129743.3129745.

[B3] Mathias Payer. “Software Security: Principles, Policies, and Protection (SS3P)”. In: *Open Textbook*. 2018.

THESES

[T1] Mathias Payer. “Implementation of a Bluetooth Stack for BTnodes and Nut/OS Version 0.9”. Bachelor Project Thesis. 2004.

[T2] Mathias Payer. “Building a client/server multimedia-kiosk using pxe, root-over-nfs, mozilla, and a CMS a.k.a. Multimedia Kiosk revisited”. Bachelor Project Thesis. 2005.

[T3] Mathias Payer. “Adaptive Optimization Using Hardware Performance Monitors”. Master Thesis. 2006.

[T4] Mathias Payer. “Safe Loading and Efficient Runtime Confinement: A Foundation for Secure Execution”. PhD Thesis. 2012. DOI: 10.3929/ethz-a-007329902.