Dr. sc. ETH Mathias Payer Revision: January 2020

CONTACT INFORMATION

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

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

Phone: +1-919-628-4427
E-mail: mathias.payer@nebelwelt.net
WWW: https://www.nebelwelt.net/
Group: https://hexhive.github.io/

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 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 against 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'20 (2x) [C46, C48], SP'20 [C47], NDSS'20 [C45]; RTSS'19 [C43], CCS'19 [C40], SEC'19 [C44], SP'19 [C41]; CCS'18 [C36, C38] (2x), SEC'18 [C35], SP'18 [C37], NDSS'18 [C33]; CCS'17 [C31], SEC'17 [C25], SP'17 [C27], NDSS'17 [C29]; 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].

EMPLOYMENT (EXCERPT)

HexHive group, EPFL, Switzerland. **Sep. 2018 – now**
Tenure Track Assistant Professor in Computer Science.

HexHive group, Purdue University, USA. **Aug. 2014 – Aug. 2018**
Assistant Professor in Computer Science.

BitBlaze group, UC Berkeley, USA. **Sept. 2012 – July 2014**
Post doctoral 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 (supervision of teaching assistants, organizing and teaching assignments and lectures).

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]
- Thesis statement: *A secure, dynamic execution platform that combines dynamic control flow integrity, a trusted loader mechanism, and a sandbox to run untrusted code enables full protection from code-oriented exploits.*
- Advisor: Thomas R. Gross (ETH Zurich)
- Co-advisors: Steven Hand (Google) and Srdjan Capkun (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]

Base studies in Computer Science **Oct. 2001 – Oct. 2003**
- Foundations in computer science and electrical engineering (comparable to a bachelor's degree).

GRANTS

- Total funding: $9,804,306, 1,499,970 €, 1,124,540 CHF (≈ **$12,640,071**).
- My own share: $2,933,839, 1,499,970 €, 1,124,540 CHF (≈ **$5,769,604**).
- **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: 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).
- 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

Best paper awards and prestigious grants

- **SNFS Eccellenza Grant** MultiSan, 2019
- **ERC H2020 Starting Grant 850868** CodeSan, 2019
- ***IEEE LangSec'15*** [W6], San Jose, California, 2015.
- ***ACM IMC'14*** [C11], Vancouver, Canada, 2014.
- ***IEEE PST'13*** [C8], Tarragona, Spain, June 2013.

Other awards, patents, and CVEs

- CVE-2018-20169, CVE-2018-19824, CVE-2019-15098, CVE-2019-15098, CVE-2018-19985, CVE-2019-15117, CVE-2019-15118, CVE-2019-15504, CVE-2019-15505, CVE-2015-2877.
- ***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 **2015 – now**

Program committee chair: 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 organizational committees: 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, ACM CCS'16 workshops co-chair with Stefan Mangard.

Program committee member **2012 – now**

2020: **NDSS'20**, **Oakland'20**, **SEC'20**, WOOT'20;
2019: **CCS'19**, **EuroSYS'19** (heavy PC), **NDSS'19**, **Oakland'19**, PRiSC'19, **SEC'19**, WOOT'19;
2018: AsiaCCS'18, **CCS'18**, **EuroSYS'18** (heavy 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**

Poster reviewer for Usenix SEC, 2016. NSF review panelist for SaTC '16, CPS '16, SaTC '17, CPS '17, SaTC '18. NWO (Netherlands Organisation for Scientific Research) reviewer, 2015. Journal reviewer for ACM TACO, ACM TOPS, Elsevier COSE, IEEE TDSC, IEEE TPDS. Conference reviewer for CAV, CCS, CGO, HiPeak, PACT, PLDI, PPoPP.

INVITED TALKS

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**

ADVISING

Currently advised PhD students:

Fuzzing Evolution, Hui Peng [W7, C21, C37, W11], PhD candidate **Advisor: 2015 – now**
Control-flow Hijack Protection, Priyam Biswas [C25, C31], PhD candidate **Advisor: 2015 – now**
Type Safety for C/C++, Yuseok Jeon [C21, C31, C42], PhD candidate **Advisor: 2015 – now**
Kernel Safety, Derrick McKee [C33, C34] **Advisor: 2015 – now**
IoT Security, Naif Almakhdhub [C45, C39, C27], PhD cand. **Co-advised with Saurabh Bagchi: 2016 – now**
Embedded Security Testing, Prashast Srivastava [C27, W11] **Advisor: 2016 – now**
Security Evaluation, Bader AlBassam [C36] **Advisor: 2016 – now**
Data-flow-based testing, Adrian Herrara **Co-advised with Tony Hosking: 2018 – now**
Micro-architectural defenses, Atri Bhattacharyya [C40] **Co-advised with Babak Falsafi: 2018 – now**
Dynamic security testing, Ahmad Hazimeh **Advisor: 2019 – now**
Code-based sanitization, Nicolas Badoux **Advisor: 2020 – now**
Kernel protection, Uroš Tešić **Advisor: 2020 – now**

Currently advised post docs:

Daniele Antonioli **Advisor: 2020 – now**

Formerly advised students:

Kyriakos Ispoglou, Purdue PhD [W7, C36, C48, W8] **Advisor: 2015 – 2019**
Analyzing vulnerability threat surface discovered through fuzzing and synthesizing data-flow attacks.

Sushant Dinesh, Purdue MSc [C47] **Advisor: 2016 – 2019**
Recovering data structures through binary analysis and enabling efficient binary rewriting.

Abe Clements (ECE), Purdue PhD [C35, C27, C46] **Co-advised with Saurabh Bagchi: 2015 – 2019**
Defending IoT devices against advanced threats by enforcing strong mitigations at low overhead.

Nathan Burow, Purdue PhD [J5, C33, C34, C41] **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] **Co-advised with Tony Hosking: 2014 – 2016**
Development and optimization of garbage collection strategies for Android mobile systems.

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

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 thought

- *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 **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**
- *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

[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.

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**, 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**, 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, (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.

[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: Return Address Integrity for Embedded Systems”. In: *Network and Distributed System Security Symposium*. 2020.

[C46] 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.

[C47] 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.

[C48] Kyriakos Ispoglou, Daniel Austin, Vishwath Mohan, and Mathias Payer. “FuzzGen: Automatic Fuzzer Generation”. In: *Usenix Security Symposium*. 2020.

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, (**best workshop paper**). 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.

TECHNICAL REPORTS AND HACKER CONFERENCES

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

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.