

CONTACT INFORMATION	<p><i>Affiliation:</i> Assistant Professor of Computer Science, Purdue University, West Lafayette, Indiana, USA</p> <p><i>Address:</i> Mathias Payer LWSN 3154M, 305 N. University Street West Lafayette, IN 47907, USA</p> <p><i>Phone:</i> +1-919-628-4427</p> <p><i>E-mail:</i> mathias.payer@nebelwelt.net</p> <p><i>WWW:</i> http://www.nebelwelt.net/</p> <p><i>Group:</i> http://hexhive.github.io/</p>
RESEARCH INTERESTS	<p>Protecting systems in the presence of vulnerabilities: <i>system security</i> (binary and compiler-based hardening, dynamic enforcement of security policies, language-based security, binary exploitation), <i>virtualization</i> (binary translation, fault isolation, and secure hypervisors), <i>adaptive optimizations</i> (just-in-time compilation, adaptive feedback, scaling symbolic execution to large workloads, system analysis, and using hardware performance monitors to gather runtime information), and <i>software transactional memory</i> (new algorithms for fast/parallel STM systems).</p>
RESEARCH EXPERIENCE	<p>My research focuses on several aspects of systems security and adaptive optimizations. At its core my group focuses on making programs more resilient against attacks in the presence of vulnerabilities.</p> <p>Security projects: (i) adoption factors and weaknesses of protection mechanisms [J1, C5, TR1, TR2, W3, C15, TR3, M1, TR11, W6, C26, TR13], (ii) hardening techniques to protect binaries [C13, C18, TR6, C22, W5, C24, T1, C27–C29, TR14] and source code [C1–C3, C7, C8, J2, C9, C11, C12, C14, W4, C20, TR4], (iii) (non-weaponized) exploit construction [W1, C23, TR8–TR10], (iv) measuring the impact and effects of security vulnerabilities [J3, C19, C21], (v) evaluating human security and privacy factors [C10, J4], and (vi) evading signature-based detection for malware [W2, TR5, TR7].</p> <p>Systems projects: (i) fast binary translation systems [C4, C25, C31, TR16, W8], (ii) using hardware performance counters to reduce cache misses in JVMs [C32, T2], (iii) evaluate self-adaptive software transactional memory systems [C30, TR15], (iv) measuring and improving GC performance for Android devices [C6, C16, C17], and (v) evaluating how position independent code influences performance [TR12].</p>
TOP TIER PUBLICATIONS	<p>CCS'17 [C7]; SEC'17 [C1]; SP'17 [C3]; NDSS'17 [C5]; CCS'16 [C11, C12] (2x), NDSS'16 [C14]; SEC'15 [C15]; SEC'14 [C22], IMC'14 [C19], OSDI'14 [C20]; ATC'13 [C25], SP'13 [C26]; SP'12 [C28]; PLDI'07 [C32].</p>
WORK EXPERIENCE (EXCERPT)	<p>HexHive group, Purdue University, USA. Aug. 2014 – now</p> <p>Assistant Professor of Computer Science at Purdue University.</p> <p>BitBlaze group, UC Berkeley, USA. Sept. 2012 – July 2014</p> <p>Post doctoral scholar in Dawn Song's BitBlaze group.</p> <p>Google Inc., Mountain View, USA. May – July 2010</p> <p>Software engineer in the anti-malware/anti-phishing team.</p> <p>Laboratory for Software Technology, ETH Zurich, Switzerland Oct. 2006 – Aug. 2012</p> <p>Research assistant (supervision of teaching assistants, organizing and teaching assignments and lectures).</p>
EDUCATION	<p>ETH Zurich, Switzerland</p> <p>Doctor of Science ETH in Computer Science Oct. 2006 – May 2012</p> <ul style="list-style-type: none"> • Thesis title: <i>Safe Loading and Efficient Runtime Confinement: A Foundation for Secure Execution</i> [T1] • Advisor: Thomas R. Gross (ETH Zurich) • Co-advisors: Steven Hand (University of Cambridge, UK) and Srdjan Capkun (ETH Zurich) <p>Diploma/Master of Science ETH in Computer Science Oct. 2001 – Feb. 2006</p> <ul style="list-style-type: none"> • Thesis title: <i>Adaptive Optimization using Hardware Performance Monitors</i> [C32, T2] • Area of study: System Software [T4], Software Engineering; Minor: Robotics [T3]
GRANTS	<ul style="list-style-type: none"> • PRF XR: HexType: Effectively Protecting Software From Type Safety Violations. (\$29,526, jointly with Byoungyoung Lee, 2017). • ONR Grant 12338602 Towards Transformation-Based Legacy Software Fitness: Usage-Driven Binary Debloating and Hardening (\$1,049,028, <i>lead PI</i>, jointly with Dongyan Xu, 2017) • Intel SSG gift (\$75,000, <i>sole PI</i>, 2016). • Sponsored supplement to NFS grant CNS-1513783 (\$46,820, <i>sole PI</i>, 2016). • PRF XR: Prog. Analysis for Sec. and Priv. of Embedded Dev's. (\$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 ... (\$175,000, <i>sole PI</i>, 2015). • PRF XR: PrivData: Enforcing Data Confidentiality for C/C++ (\$25,838, <i>sole PI</i>, 2015). • ACM AOSD student travel grant (250 EUR, 2012).

AWARDS	<p>Best paper awards</p> <ul style="list-style-type: none"> • IEEE LangSec'15 [W4], San Jose, California, 2015. • ACM IMC'14 [C19], Vancouver, Canada, 2014. • IEEE PST'13 [C24], Tarragona, Spain, June 2013. <p>Other awards, patents, and CVEs</p> <ul style="list-style-type: none"> • CVE-2015-2877 / Cross-VM Address-Space Layout INtrospection (CAIN). • Purdue College of Science Team Award for work towards a professional information security master, 2016. • Finalist for the Cor Baayen PhD award, 2013. • European patent application 12003967.2/GP161299CH00 <i>Safe Loading - A Foundation for Secure Execution of Untrusted Programs</i>, May 2013.
SERVICE	<p><i>General chair and Program Committee chair</i> 2015 – now</p> <p>General chair: NDSS'18 workshops (co-chair with Matthew Smith), ACM CCS'16 workshops (co-chair with Stefan Mangard).</p> <p>Program committee chair: 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).</p> <p><i>Program committee member</i> 2012 – now</p> <p>2018: AsiaCCS'18, EuroSYS'18 (heavy PC), NDSS'18;</p> <p>2017: ACISP'17, ACSAC'17, AsiaCCS'17, CCS'17, DSN'17, EuroSec'17, NSS'17, SEC'17, SecDev'17;</p> <p>2016: ACISP'16, CCS'16, DSN'16, ESSoS'16, EuroSec'16, NSS'16, SEC'16, SSPREW'16, TRUST'16, WIFS'16, WWW'16;</p> <p>2015: ACNS'15, AsiaCCS'15, CCS'15, EuroSYS'15, PLDI'15 (ERC), PPREW'15;</p> <p>2014: AsiaCCS'14, PPREW'14, PPREW'14b, VEE'14; SyStor'13</p> <p><i>Panelist, reviewer, and external reviewer</i> 2006 – now</p> <p>Poster reviewer for Usenix SEC, 2016.</p> <p>NSF review panelist for SaTC '16, CPS '16, SaTC '17.</p> <p>NWO (Netherlands Organisation for Scientific Research) reviewer, 2015.</p> <p>Journal reviewer for ACM TACO, ACM TOPS, Elsevier COSE, IEEE TDSC, IEEE TPDS.</p> <p>Conference reviewer for CAV, CCS, CGO, HiPeak, PACT, PLDI, PPOPP.</p> <p><i>Service at Purdue</i> 2014 – now</p> <p>ACM student mentor (fall '15); CS graduate admission committee (fall '14, spring '15, fall '15, spring '16); Graduate study committee (fall '16, spring '17); I3P consortium representative (fall '14, spring '16, fall '16).</p> <p><i>Service at ETH Zurich</i> 2008 – 2012</p> <p>PhD representative on recruiting committees for six tenure track positions in CS (May 2011 and Mar. 2012); President of the VMI (association of scientific staff in CS Zurich, Nov. 2010 – Nov. 2011); Member and president of the tuition committee (Sept. 2009 – Mar. 2012); and Member of the departmental conference (Sept. 2008 – Aug. 2012).</p>
INVITED TALKS	<p>CERIAS Symposium, West Lafayette, USA, May 2017; AsiaCCS, Abu Dhabi, UAE, Apr. 2017; IBM Research, Zurich, Switzerland, Jan. 2017; East China Normal University, Shanghai, China, June 2016; Midwest PL summit, West Lafayette, USA, December 2015; CS seminar, Northeastern University, Boston, USA, Oct. 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 Corp., Melbourne, Florida, USA, Feb. 2015; SSP'14 workshop, Phoenix, Arizona, USA, Nov. 2014; Google Security, San Francisco, CA, USA, June 2014; ECE seminar, Virginia Tech, Blacksburg, VA, Mar. 2014; CS seminar, University of Utah, Salt Lake City, UT, USA, Feb. 2014; CS seminar, Purdue University, West Lafayette, IN, USA, Jan. 2014; TRUST, UC Berkeley, Berkeley, CA, USA, Dec. 2013; EPFL, Lausanne, Switzerland, June 2013; SoCal PLS, Santa Barbara, CA, USA, May 2013; UC Irvine, Irvine, CA, USA, May 2013; Intel, Santa Clara, CA, USA, Apr. 2013, Adobe, San Francisco, CA, USA, Jan. 2013; UC Berkeley, Berkeley, CA, USA, May 2012; UC Irvine, CA, USA, May 2012; IBM Research ARL, Austin, TX, USA, Apr. 2011; Swiss Cyber Storm Security Conference, Rapperswil, Switzerland, Mar. 2011; UC Irvine, CA, USA, Mar. 2011; Google TechTalk, Mountain View, CA, USA, June 2010.</p>
ADVISING	<p>Graduate student advising at Purdue</p> <p><i>Fast Memory Safety</i>, Nathan Burow [J1, TR1] Advisor: 2015 – now</p> <p><i>Security for IoT</i>, Abe Clements [C3] (ECE) Co-advised with Saurabh Bagchi: 2015 – now</p> <p><i>Security Evaluation</i>, Hui Peng [W1, C11] Advisor: 2015 – now</p> <p><i>Data-Flow Attack Inference</i>, Priyam Biswas [C1, C7] Advisor: 2015 – now</p> <p><i>Modern Memory Safety</i>, Derrick McKee Advisor: 2015 – now</p> <p><i>Type Safety for C/C++</i>, Yuseok Jeon [C7, C11]. Co-advised with Byoungyoung Lee: 2015 – now</p> <p><i>Binary Hardening</i>, Kyriakos Ispoglou [W1, W2]. Advisor: 2015 – now</p> <p><i>System Security</i>, Terry Ching-Hsiang Hsu [C12] Co-advised with Patrick Eugster: 2016 – now</p> <p><i>Embedded Security</i>, Prashast Srivastava [C3] Advisor: 2016 – now</p>

Security Evaluation, Bader AlBassam
Binary-only Memory Safety, Sushant Dinesh
Security for IoT, Naif Almakhdhub [C3], (ECE)

Advisor: 2016 – now
Advisor: 2016 – now
Co-advised with Saurabh Bagchi: 2017 – now

Formerly advised students at Purdue University:

Data Confidentiality and Integrity, Scott A. Carr, Purdue PhD [J1, C1, C2, C7, TR1, C14]. **Advisor: 2014 – 2017**
GC on Android, Ahmed Hussein, Purdue PhD [C6, C16, C17]. **Co-advised with Tony Hosking: 2014 – 2016**
Binary Analysis, Alessandro Di Federico, visiting PhD student [C1, C4]. **Fall 2016**

Member of graduate committee (defense and prelim exams) **2014 – now**
Gregory Essertel, Chung Hwan Kim (2017, 2016), Karthik Kambatla (2016, 2014), Daniele Midi [C8] (2016, 2015), Julian Stephen (2016), Shin-Yeh Tsai (2016), Keith Chapman (2015), John Ross Wallrabenstein (2014).

External member of the thesis committee **2015 – now**
Andreas Follner (TU Darmstadt, advisor: Eric Bodden, defended 2016) [W1], Xinyang Ge (Penn State, advisor: Trent Jaeger, defended 2016) [C5, C9].

Supervised graduate research projects at Purdue **2014 – now**
Hrishikesh Arun Deshpande, spring 2017; Yu-Chen Chang, summer 2016; Craig West, 2015–2016; Jacek Rzeniewicz 2015–2016; Daniele Midi, 2014–2016; Dominik Preikschat 2014–2015; Pinar Yanardag 2014–2015.

Supervised undergraduate research at Purdue **2014 – now**
Andrew Barthel, 2017; Ammar Askar, 2016; Luhze Wang, 2014.

Purdue b01lers student Capture-the-Flag security club advisor **2014 – now**
Founder and graduate advisor for the b01lers club (ranked in the top 50 of thousands of teams worldwide).

Supervised students at ETH Zurich **2006 – 2012**
Enrico Kravina [C25], BSc thesis 2012; Jonas Pfefferle, BSc thesis 2012; Boris Bluntschi [W5, W7], MSc thesis 2011; Noah Heusser, MSc thesis 2011; Tobias Hartmann [C28], BSc thesis 2011; Christian Oberholzer, MSc thesis 2010; Antonio Barresi [W3, C29], MSc thesis 2009; Philipp Wolfensperger, MSc thesis 2009; Marcel Wirth [C31], MSc thesis, 2009; Olivier Saurer, BSc thesis 2008; Peter Suter, MSc thesis 2008; Martin Bill, MSc thesis 2008; Ken Lee, MSc thesis 2008; Marcel Wirth, semester project 2007; Georg Schaetti, MSc thesis 2007; Stephan Classen, MSc thesis 2007; Gianmatteo Costanza, MSc thesis 2006.

TEACHING

Seminars and guest lectures at Purdue **2014 – now**
CS197 junior CS honor students (2016), CERIAS seminar (2015), CS591 graduate research seminar (2014), CERIAS seminar (2014), CS397 junior CS honor students (2014).

Lectures and classes prepared and thought

- Lecturer for *Operating Systems*, CS-354, 3 credits, 148 students **Fall 2017**
- Lecturer for *Software Security*, CS-527, 3 credits, 17 students, (reworked) **Spring 2017**
- Lecturer for the *Systems Security Seminar*, CS-590-SYS, 1 credit, 9 students, several auditors **Spring 2017**
- Lecturer for *Operating Systems*, CS-354, 3 credits, 123 students **Fall 2016**
- Lecturer for the *Systems Security Seminar*, CS-590-SYS, 1 credit, 16 students, several auditors **Fall 2016**
- Lecturer for *Software Security*, CS-590-SWS, 3 credits, 18 students, several auditors (new, founded) **Spring 2016**
- Lecturer for the *Systems Security Seminar*, CS-590-SYS, 1 credit, 7 students, several auditors **Spring 2016**
- Lecturer for *Operating Systems*, CS-503, 3 credits, 45 students **Fall 2015**
- Lecturer for the *Informal Systems Seminar*, 15 students **Fall 2015**
- Lecturer for *Software Engineering*, CS-510, 3 credits, 47 students (significantly redesigned) **Spring 2015**
- Lecturer for the *Informal Systems Seminar*, 8 students (new, founded) **Spring 2015**
- Lecturer for *Language-based Systems Security*, CS-590-LBS, 3 credits, 16 students **Fall 2014**
- Lecturer for *Introduction to C Programming*, 6 hrs., ca. 120 students (developed) **Fall 2008 and 2009**
- TA for *Computer Architecture and System Programming*, ca. 120 students **Fall 2007, 2008, and 2009**
- Lecturer of the exam preparation course for *Introduction to Programming*, ca. 40 students **Summer 2008**
- Head TA for *Computer System Laboratory*, ca. 20 students **Spring 2007 and 2008**
- TA for *Introduction to Programming*, ca. 200 students **Fall 2006 and 2007**
- Student TA for *Compiler Design I*, ca. 80 students **Spring 2005**

REFERENCES I asked the following people to provide written letters of recommendation on request:

- Prof. Dr. Thomas R. Gross, thesis advisor, trg@inf.ethz.ch (ETH Zurich, Switzerland).
- Prof. Dr. Antony Hosking, collaborator, antony.hosking@anu.edu.au (Purdue, USA and ANU, Australia)
- Prof. Dr. Dawn Song, post doctoral advisor, dawnsong.letters@gmail.com (UC Berkeley, USA).
- Prof. Dr. Steven Hand, thesis co-advisor, Steven.Hand@cl.cam.ac.uk (Google, USA).
- Prof. Dr. Srdjan Capkun, thesis co-advisor, srdjan.capkun@inf.ethz.ch (ETH Zurich, Switzerland).

JOURNAL
ARTICLES

- [J1] 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* 50.1 (2018, preprint: <https://arxiv.org/abs/1602.04056>). DOI: 10.1145/3054924.
- [J2] 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.
- [J3] Jack D. 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: *Elsevier Transportation Research Part B: Methodological* (2016). DOI: 10.1016/j.trb.2016.05.017.
- [J4] 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.

CONFERENCE
PROCEEDINGS

- [C1] Priyam Biswas, Alessandro Di Federico, Scott A. Carr, Prabhu Rajasekaran, Stijn Volckaert, Yeoul Na, Michael Franz, and Mathias Payer. “Venerable Variadic Vulnerabilities Vanquished”. In: *SEC: USENIX Security Symposium*. 2017. (16% acceptance rate – 85/522).
- [C2] Scott A. Carr and Mathias Payer. “DataShield: Configurable Data Confidentiality and Integrity”. In: *AsiaCCS: ACM Symp. on InformAtion, Computer and Communications Security*. 2017. (18.7% acceptance rate – 67/359). DOI: 10.1145/3052973.3052983.
- [C3] Abraham A. Clements, Naif Saleh Almkhdub, Khaled Saab, Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, and Mathias Payer. “Protecting Bare-metal Embedded Systems with Privilege Overlays”. In: *Oakland: IEEE Symp. on Security and Privacy*. 2017. (13% acceptance rate – 60/450).
- [C4] Alessandro Di Federico, Mathias Payer, and Giovanni Agosta. “rev.ng: a unified binary analysis framework for CFG and function boundaries recovery”. In: *CC: Intl. Conf. on Compiler Construction*. 2017. (25% acceptance rate – 13/53). DOI: 10.1145/3033019.3033028.
- [C5] Xinyang Ge, Mathias Payer, and Trent Jaeger. “An Evil Copy: How the Loader Betrays You”. In: *NDSS: Network and Distributed System Security Symposium*. 2017. (16% acceptance rate – 68/423). DOI: 10.14722/ndss.2017.23199.
- [C6] Ahmed Hussein, Antony L. Hosking, Mathias Payer, and Christopher A. Vick. “One Process to Reap Them All: Garbage Collection As A Service”. In: *VEE: Int’l Conf. Virtual Execution Environments*. 2017. (44% acceptance rate – 18/41).
- [C7] Yuseok Jeon, Priyam Biswas, Scott A. Carr, Byoungyoung Lee, and Mathias Payer. “HexType: Efficient Detection of Type Confusion Errors for C++”. In: *CCS: ACM Conf. on Computer and Communication Security*. 2017. (18% acceptance rate – 151/836).
- [C8] Daniele Midi, Mathias Payer, and Elisa Bertino. “Memory Safety for Embedded Devices with nesCheck”. In: *AsiaCCS: ACM Symp. on InformAtion, Computer and Communications Security*. 2017. (18.7% acceptance rate – 67/359). DOI: 10.1145/3052973.3053014.
- [C9] Xinyang Ge, Nirupama Talele, Mathias Payer, and Trent Jaeger. “Fine-Grained Control-Flow Integrity for Kernel Software”. In: *EuroSP: IEEE European Symp. on Security and Privacy*. 2016. (17% acceptance rate – 29/168). DOI: 10.1109/EuroSP.2016.24.
- [C10] Neil Zhenqiang Gong, Mathias Payer, Reza Moazzezi, and Mario Frank. “Forgery-Resistant Touch-based Authentication on Mobile Devices”. In: *AsiaCCS: ACM Symp. on InformAtion, Computer and Communications Security*. 2016. (20.9% acceptance rate – 73/350). DOI: 10.1145/2897845.2897908.
- [C11] Istvan Haller, Yuseok Jeon, Hui Peng, Mathias Payer, Herbert Bos, Cristiano Giuffrida, and Erik van der Kouwe. “TypeSanitizer: Practical Type Confusion Detection”. In: *CCS: ACM Conf. on Computer and Communication Security*. 2016. (16% acceptance rate – 137/831). DOI: 10.1145/2976749.2978405.
- [C12] Terry Ching-Hsiang Hsu, Kevin Hoffman, Patrick Eugster, and Mathias Payer. “Enforcing Least Privilege Memory Views for Multithreaded Applications”. In: *CCS: ACM Conf. on Computer and Communication Security*. 2016. (16% acceptance rate – 137/831). DOI: 10.1145/2976749.2978327.
- [C13] Mathias Payer. “HexPADS: a platform to detect “stealth” attacks”. In: *ESSoS: Intl. Symp. on Engineering Secure Software and Systems*. 2016. (32% acceptance rate – 15/50). DOI: 10.1007/978-3-319-30806-7_9.

- [C14] Chao Zhang, Scott A. Carr, Tongxin Li, Yu Ding, Chengyu Song, Mathias Payer, and Dawn Song. "VTrust: Regaining Trust on Virtual Calls". In: *NDSS: Network and Distributed System Security Symposium*. 2016. (15% acceptance rate – 60/389). DOI: 10.14722/ndss.2016.23164.
- [C15] Nicholas Carlini, Antonio Barresi, Mathias Payer, David Wagner, and Thomas R. Gross. "Control-Flow Bending: On the Effectiveness of Control-Flow Integrity". In: *SEC: USENIX Security Symposium*. 2015. (16% 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: *ISMM: Intl. Symp 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: *SYSTOR: 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: *DIMVA: Conf. on Detection of Intrusions and Malware and Vulnerability Assessment*. 2015. (23% acceptance rate – 17/75). DOI: 10.1007/978-3-319-20550-2_8.
- [C19] 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: *IMC: ACM Internet Measurement Conference*. 2014 (**best paper**, 23% acceptance rate – 43/188). DOI: 10.1145/2663716.2663755.
- [C20] Volodymyr Kuznetsov, Mathias Payer, Laszlo Szekeres, George Candea, Dawn Song, and R. Sekar. "Code Pointer Integrity". In: *OSDI: Symp. on Operating Systems Design and Implementation*. 2014. (18% acceptance rate – 42/232).
- [C21] Jack Reilly, Sebastien Martin, Mathias Payer, and Alexandre Bayen. "On Cybersecurity of Freeway Control Systems: Analysis of Coordinated Ramp Metering Attacks". In: *TRB'14: Transportation Research Board*. 2014.
- [C22] Hayawardh Vijayakumar, Xinyang Ge, Mathias Payer, and Trent Jaeger. "JIGSAW: Protecting Resource Access by Inferring Programmer Intentions". In: *SEC: USENIX Security Symposium*. 2014. (19% acceptance rate – 67/350).
- [C23] Dan Caselden, Alex Bazhanyuk, Mathias Payer, Stephen McCamant, and Dawn Song. "HI-CFG: Construction by Binary Analysis, and Application to Attack Polymorphism". In: *ESORICS: European Symp. on Research in Comp. Security*. 2013. (17.8% acceptance rate – 43/242). DOI: 10.1007/978-3-642-40203-6_10.
- [C24] Mathias Payer and Thomas Gross. "Hot-Patching a Web Server: a Case Study of ASAP Code Repair". In: *PST'13: Proc. Conf. on Privacy, Security, and Trust*. 2013. (**best paper**, 29% acceptance rate – 43/146). DOI: 10.1109/PST.2013.6596048.
- [C25] Mathias Payer, Enrico Kravina, and Thomas R. Gross. "Lightweight Memory Tracing". In: *ATC'13: Usenix Annual Technical Conference*. 2013. (14% acceptance rate – 32/233).
- [C26] Laszlo Szekeres, Mathias Payer, Tao Wei, and Dawn Song. "SoK: Eternal war in memory". In: *Oakland: IEEE Symp. on Security and Privacy*. 2013. (12% acceptance rate – 38/315). DOI: 10.1109/SP.2013.13.
- [C27] Mathias Payer and Thomas R. Gross. "Protecting Applications Against TOCTTOU Races by User-Space Caching of File Metadata". In: *VEE: Int'l Conf. Virtual Execution Environments*. 2012. (38% acceptance rate – 20/53). DOI: 10.1145/2151024.2151052.
- [C28] Mathias Payer, Tobias Hartmann, and Thomas R. Gross. "Safe Loading - A Foundation for Secure Execution of Untrusted Programs". In: *S&P'12: Proc. Int'l Symp. on Security and Privacy*. 2012. (13% acceptance rate – 40/307). DOI: 10.1109/SP.2012.11.
- [C29] Mathias Payer and Thomas R. Gross. "Fine-grained user-space security through virtualization". In: *VEE: Int'l Conf. Virtual Execution Environments*. 2011. (29% acceptance rate – 20/68). DOI: 10.1145/1952682.1952703.
- [C30] Mathias Payer and Thomas R. Gross. "Performance evaluation of adaptivity in software transactional memory". In: *ISPASS'11: Proc. IEEE Int'l. Symp. on Perf. Analysis of Systems and Software*. 2011. (31% acceptance rate (20/65)). DOI: 10.1109/ISPASS.2011.5762733.
- [C31] Mathias Payer and Thomas R. Gross. "Generating low-overhead dynamic binary translators". In: *SYSTOR: ACM International Systems and Storage Conference*. 2010. (58% acceptance rate – 18/31). DOI: 10.1145/1815695.1815724.

- [C32] Florian T. Schneider, Mathias Payer, and Thomas R. Gross. “Online optimizations driven by hardware performance monitoring”. In: *PLDI: ACM Conf. on Programming Language Design and Implementation*. 2007. (25% acceptance rate – 45/178). DOI: 10.1145/1250734.1250777.

WORKSHOP
PROCEEDINGS

- [W1] 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: *STM’16: 12th International Workshop on Security and Trust Management*. 2016. (38% acceptance rate – 13/34). DOI: 10.1007/978-3-319-46598-2_15.
- [W2] Kyriakos Ispoglou and Mathias Payer. “malWASH: Washing malware to evade dynamic analysis”. In: *WOOT: Usenix Workshop on Offensive Technologies*. 2016. (48% acceptance rate – 21/44).
- [W3] Antonio Barresi, Kaveh Razavi, Mathias Payer, and Thomas R. Gross. “CAIN: Silently Breaking ASLR in the Cloud”. In: *WOOT: Usenix Workshop on Offensive Technologies*. 2015. (35% acceptance rate – 20/57).
- [W4] Vijay D’Silva, Mathias Payer, and Dawn Song. “The Correctness-Security Gap in Compiler Optimization”. In: *LangSec’15: Second Workshop on Language-Theoretic Security*. 2015. (**best workshop paper**). DOI: 10.1109/SPW.2015.33.
- [W5] Mathias Payer, Boris Bluntschli, and Thomas R. Gross. “DynSec: On-the-fly Code Rewriting and Repair”. In: *HotSWUp’13: Workshop on Hot Topics in Software Upgrades*. 2013.
- [W6] Mathias Payer and Thomas R. Gross. “String Oriented Programming: When ASLR is Not Enough”. In: *PPREW’13: Program Protection and Reverse Engineering Workshop*. 2013. DOI: 10.1145/2430553.2430555.
- [W7] Mathias Payer, Boris Bluntschli, and Thomas R. Gross. “LLDSAL: A Low-Level Domain-Specific Aspect Language for Dynamic Code-Generation and Program Modification”. In: *DSAL’12: Proceedings of the 7th AOSD workshop on Domain-Specific Aspect Languages*. 2012. DOI: 10.1145/2162037.2162043.
- [W8] Mathias Payer and Thomas R. Gross. “Requirements for Fast Binary Translation”. In: *AMAS-BT’09: 2nd Workshop on Arch. and Microarch. Support for Binary Translation*. 2009.

MAGAZINE
ARTICLES

- [M1] Laszlo Szekeres, Mathias Payer, Lenx Wei, Dawn Song, and R. Sekar. “Eternal War in Memory”. In: *IEEE Security and Privacy Magazine* (2014). DOI: 10.1109/MSP.2013.47.

TECHNICAL
REPORTS AND
HACKER
CONFERENCES

- [TR1] Nathan Burow, Scott A. Carr, Stefan Brunthaler, Mathias Payer, Joseph Nash, Per Larsen, and Michael Franz. *Control-Flow Integrity: Precision, Security, and Performance*. arXiv’16: <http://arxiv.org/abs/1602.04056>. 2016.
- [TR2] Mathias Payer. *Memory Corruption: Why We Can’t Have Nice Things*. BalCCon’16: <http://nebelwelt.net/publications/files/16BalCCon-presentation.pdf>. 2016.
- [TR3] Mathias Payer and Nicholas Carlini. “New memory corruption attacks: why can’t we have nice things?”. In: *32c3’15: Proc. 32th Chaos Communication Congress*. 2015.
- [TR4] Mathias Payer. “Code-Pointer Integrity”. In: *31c3’14: Proc. 31th Chaos Communication Congress*. 2014.
- [TR5] Mathias Payer. *Embracing the New Threat: Towards Automatically Self-Diversifying Malware*. SyScan’14: <http://nebelwelt.net/publications/files/14SyScan.pdf>. 2014.
- [TR6] Mathias Payer, Antonio Barresi, and Thomas R. Gross. *Lockdown: Dynamic Control-Flow Integrity*. ETH Zurich Technical Report <http://nebelwelt.net/publications/files/14TRlockdown.pdf>. 2014.
- [TR7] Mathias Payer, Stephen Crane, Per Larsen, Stefan Brunthaler, Richard Wartell, and Michael Franz. *Similarity-based matching meets Malware Diversity*. arXiv’14: <http://arxiv.org/abs/1409.7760>. 2014.
- [TR8] Dan Caselden, Alex Bazhanyuk, Mathias Payer, Laszlo Szekeres, Stephen McCamant, and Dawn Song. *Transformation-aware Exploit Generation using a HI-CFG*. Tech. rep. UCB/EECS-2013-85. EECS Department, University of California, Berkeley, 2013.
- [TR9] Stephen McCamant, Mathias Payer, Dan Caselden, Alex Bazhanyuk, and Dawn Song. *Transformation-Aware Symbolic Execution for System Test Generation*. Tech. rep. UCB/EECS-2013-125. EECS Department, University of California, Berkeley, 2013.
- [TR10] Mathias Payer. “Triggering Deep Vulnerabilities Using Symbolic Execution”. In: *30c3’13: Proc. 30th Chaos Communication Congress*. 2013.
- [TR11] Mathias Payer. “WarGames in Memory”. In: *30c3’13: Proc. 30th Chaos Communication Congress*. 2013.

- [TR12] Mathias Payer. *Too much PIE is bad for performance*. ETH Zurich Technical Report <http://nebelwelt.net/publications/files/12TRpie.pdf>. 2012.
- [TR13] Mathias Payer. "String Oriented Programming - Circumventing ASLR, DEP and Other Guards". In: *28c3'11: Proc. 28th Chaos Communication Congress*. 2011.
- [TR14] Mathias Payer. "I control your code - Attack vectors through the eyes of Software-based Fault Isolation". In: *27c3'10: Proc. 27th Chaos Communication Congress*. 2010.
- [TR15] Mathias Payer and Thomas Gross. *adaptSTM - An Online Fine-Grained Adaptive STM System*. 2010.
- [TR16] Mathias Payer. "secuBT: Hacking the Hackers with User-Space Virtualization". In: *26c3'09: Proc. 26th Chaos Communication Congress*. 2009.

THESES

- [T1] Mathias Payer. "Safe Loading and Efficient Runtime Confinement: A Foundation for Secure Execution". PhD thesis. ETH Zurich URL: <http://nebelwelt.net/publications/12PhD>, 2012.
- [T2] Mathias Payer. *Adaptive Optimization Using Hardware Performance Monitors*. Master thesis, ETH Zurich, 2006.
- [T3] Mathias Payer. *Building a client/server multimedia-kiosk system using pxe; root-over-nfs, mozilla and a CMS a.k.a Multimedia Kiosk revisited*. Term project report, ETH Zurich, 2005.
- [T4] Mathias Payer. *Implementation of a Bluetooth Stack for BTnodes and Nut/OS Version 0.9*. Term project report, ETH Zurich, 2004.