Dr. sc. ETH Mathias Payer

Revision: March 2018

Contact information

Affiliation: Assistant Professor of Computer Science, Purdue University, West Lafayette, Indiana, USA

Address: Mathias Payer
LWSN 3154M, 305 N. University Street
West Lafayette, IN 47907, USA

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

Research interests

Protecting systems in the presence of vulnerabilities: *system security* (binary and compiler-based hardening, dynamic enforcement of security policies, language-based security, binary exploitation), *virtualization* (binary translation, fault isolation, and secure hypervisors), *adaptive optimizations* (just-in-time compilation, adaptive feedback, scaling symbolic execution, system analysis, and using hardware performance monitors).

Research experience

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.

Security projects: (i) adoption factors and weaknesses of protection mechanisms [C3, J1, C8, TR2, W3, C18, TR3, J5, TR11, W6, C29, TR13], (ii) hardening techniques to protect binaries [C16, C21, TR6, C25, W5, C27, TR1, C30–C32, TR14] and source code [C1, C2, C4–C6, C10, C11, TR1, J2, C12, C14, C15, C17, W4, C23, TR4], (iii) (non-weaponized) exploit construction [W1, C26, TR8–TR10], (iv) measuring the impact and effects of security vulnerabilities [J3, C22, C24], (v) evaluating human security and privacy factors [C13, J4], and (vi) evading signature-based detection for malware [W2, TR5, TR7].

Systems projects: (i) fast binary translation systems [C7, C28, C34, TR16, W8], (ii) using hardware performance counters to reduce cache misses in JVMs [C35, TR2], (iii) evaluating self-adaptive software transactional memory systems [C33, TR15], (iv) measuring and improving GC performance for Android devices [C9, C19, C20], and (v) evaluating how position independent code influences performance [TR12].

Top Tier Publications

SP'18 [C3], NDSS'18 [C1]; CCS'17 [C10], SEC'17 [C4], SP'17 [C6], NDSS'17 [C8]; CCS'16 [C14, C15] (2x), NDSS'16 [C17]; SEC'15 [C18]; SEC'14 [C25], IMC'14 [C22], OSDI'14 [C23]: ATC'13 [C28], SP'13 [C29]; SP'12 [C31]; PLDI'07 [C35].

Employment (excerpt)

HexHive group, Purdue University, USA. — **Aug. 2014 – now**
Assistant Professor of Computer Science at Purdue University.

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* [TR1]
- 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* [C35, TR2]
- Area of study: System Software [TR4], Software Engineering; Minor: Robotics [TR3]

GRANTS

- 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 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

- ***IEEE LangSec'15*** [W4], San Jose, California, 2015.
- ***ACM IMC'14*** [C22], Vancouver, Canada, 2014.
- ***IEEE PST'13*** [C27], Tarragona, Spain, June 2013.

Other awards, patents, and CVEs

- 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 *Safe Loading - A Foundation for Secure Execution of Untrusted Programs*, May 2013.

SERVICE

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

General chair: NDSS'18 workshops (co-chair with Matthew Smith), ACM CCS'16 workshops (co-chair with Stefan Mangard).
Steering committee: RAID'17 – now.
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).

Program committee member **2012 – now**

2019: **Oakland '19**
2018: AsiaCCS'18, **CCS'18**, **EuroSYS'18** (heavy PC), **NDSS'18**, **SEC'18**, 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. 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.

Service at Purdue **2014 – now**

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); Strategic planning committee (summer '17, fall '17, spring '18).

Service at ETH Zurich **2008 – 2012**

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).

INVITED TALKS

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**
CERIAS Symposium, West Lafayette, USA	**May 2017**
AsiaCCS invited talk, Abu Dhabi, UAE	**April 2017**
IBM Research Seminar, Zurich, Switzerland	**January 2017**
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

PhD graduate student advising at Purdue

Fast Memory Safety, Nathan Burow [C1, C2, J1]	**Advisor: 2015 – now**
Security for IoT, Abe Clements [C6] (ECE)	**Co-advised with Saurabh Bagchi: 2015 – now**
Fuzzing Evolution, Hui Peng [C3, W1, C14]	**Advisor: 2015 – now**
Control-flow Hijack Protection, Priyam Biswas [C4, C10]	**Advisor: 2015 – now**

Kernel Safety, Derrick McKee [C1, C2] **Advisor: 2015 – now**
Type Safety for C/C++, Yuseok Jeon [C10, C14] **Co-advised with Byoungyoung Lee: 2015 – now**
Binary Hardening, Kyriakos Ispoglou [W1, W2] **Advisor: 2015 – now**
Safe Kernel Abstractions, Terry Ching-Hsiang Hsu [C15] **Advisor: 2016 – now**
Embedded Security Testing, Prashast Srivastava [C6] **Advisor: 2016 – now**
Security Evaluation, Bader AlBassam **Advisor: 2016 – now**
Binary-only Memory Safety, Sushant Dinesh **Advisor: 2016 – now**
Security for IoT, Naif Almakhdhub [C6], (ECE) **Co-advised with Saurabh Bagchi: 2017 – now**

Formerly advised students at Purdue University:
Scott A. Carr, Purdue PhD [C1, C2, C4, J1, C5, C10, C17] **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 [C9, C19, C20] **Co-advised with Tony Hosking: 2014 – 2016**
Development and optimization of garbage collection strategies for Android mobile systems.
Alessandro Di Federico, visiting PhD student [C4, C7]. **Fall 2016**
Binary analysis and translation across architectures and operating systems.

Member of graduate committee (defense and prelim exams) **2014 – now**
Gregory Essertel, Chung Hwan Kim (2017, 2016), Karthik Kambatla (2016, 2014), Daniele Midi [C11] (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) [C8, C12].

Supervised graduate research projects at Purdue **2014 – now**
Lovepreet Singh, fall 2017; 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**
Jordan Field, 2017; Zixuan Song, 2017; Brian P. Hays, 2017; Nicholas Nevius, 2017; 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 [C28], BSc thesis 2012; Jonas Pfefferle, BSc thesis 2012; Boris Bluntschi [W5, W7], MSc thesis 2011; Noah Heusser, MSc thesis 2011; Tobias Hartmann [C31], BSc thesis 2011; Christian Oberholzer, MSc thesis 2010; Antonio Barresi [W3, C32], MSc thesis 2009; Philipp Wolfensperger, MSc thesis 2009; Marcel Wirth [C34], 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
- *Software Security*, CS-527, 3 credits, about 40 students (reworked) **Spring 2018**
- *CERIAS Seminar*, CS-591-SEC, 1 credit, about 30 students **Spring 2018**
- *Systems Security Seminar*, CS-590-SYS, 1 credit, about 10 students **Spring 2018**

- *Operating Systems*, CS-354, 3 credits, 148 students **Fall 2017**
- the *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**
- the *Systems Security Seminar*, CS-590-SYS, 1 credit, 9 students, several auditors **Spring 2017**
- *Operating Systems*, CS-354, 3 credits, 123 students **Fall 2016**
- the *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**
- the *Systems Security Seminar*, CS-590-SYS, 1 credit, 7 students, several auditors **Spring 2016**
- *Operating Systems*, CS-503, 3 credits, 45 students **Fall 2015**
- the *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**

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. Trent Jaeger, collaborator, tjaeger@cse.psu.edu (Penn State University, USA).
- 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*. 2017. DOI: 10.1109/TSE.2016.2625248.

[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 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.

[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.

[J5] 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.

CONFERENCE PROCEEDINGS

[C1] 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).

[C2] Nathan Burow, Derrick McKee, Scott A. Carr, and Mathias Payer. "CUP: Comprehensive User-Space Protection for C/C++ (to appear)". In: *ACM Symp. on InformAtion, Computer and Communications Security*. 2018, (20% acceptance rate –62/310).

[C3] Hui Peng, Yan Shoshitaishvili, and Mathias Payer. "T-Fuzz: fuzzing by program mutation (to appear)". In: *IEEE International Symposium on Security and Privacy*. 2018, (11% acceptance rate –63/549).

[C4] 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).

[C5] 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.

[C6] 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: TODO.

[C7] 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.

[C8] 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.

[C9] 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.

[C10] Yuseok Jeon, Priyam Biswas, Scott A. Carr, Byoungyoung Lee, and Mathias Payer. “HexType: Efficient Detection of Type Confusion Errors for C++”. In: *ACM Conf on Computer and Communication Security*. 2017, (18% acceptance rate –151/836).

[C11] 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.

[C12] 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.

[C13] 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.

[C14] Istvan Haller, Yuseok Jeon, Hui Peng, Mathias Payer, Herbert Bos, Cristiano Giuffrida, and Erik van der Kouwe. “TypeSanitizer: Practical Type Confusion Detection”. In: *ACM Conf on Computer and Communication Security*. 2016, (16% acceptance rate –137/831). DOI: 10.1145/2976749.2978405.

[C15] Terry Ching-Hsiang Hsu, Kevin Hoffman, Patrick Eugster, and Mathias Payer. “Enforcing Least Privilege Memory Views for Multithreaded Applications”. In: *ACM Conf on Computer and Communication Security*. 2016, (16% acceptance rate –137/831). DOI: 10.1145/2976749.2978327.

[C16] 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.

[C17] 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.

[C18] 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).

[C19] 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.

[C20] 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.

[C21] 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.

[C22] 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.

[C23] 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).

[C24] 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.

[C25] 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).

[C26] 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.

[C27] 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.

[C28] Mathias Payer, Enrico Kravina, and Thomas R. Gross. “Lightweight Memory Tracing”. In: *Usenix Annual Technical Conference*. 2013, (13% acceptance rate –32/233).

[C29] 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.

[C30] 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.

[C31] 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.

[C32] 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.

[C33] 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.

[C34] 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.

[C35] 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.

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: *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: *Usenix Workshop on Offensive Technologies*. 2016, (47% acceptance rate –21/44).

[W3] Antonio Barresi, Kaveh Razavi, Mathias Payer, and Thomas R. Gross. "CAIN: Silently Breaking ASLR in the Cloud". In: *Usenix Workshop on Offensive Technologies*. 2015.

[W4] 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.

[W5] 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.

[W6] 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.

[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: *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: *Workshop on Architectural and Microarchitectural Support for Binary Translation*. 2009.

Technical reports and hacker conferences

[TR1] Mathias Payer. "Type confusion: discovery, abuse, and protection". In: *Chaos Communication Congress*. 2017, (28% acceptance rate –49/170).

[TR2] Mathias Payer. "Memory Corruption: Why We Can't Have Nice Things". In: *Balkan Computer Congress*. 2016.

[TR3] Mathias Payer. "New memory corruption attacks: why can't we have nice things?" In: *Chaos Communication Congress*. 2015.

[TR4] Mathias Payer. "Code-Pointer Integrity". In: *Chaos Communication Congress*. 2014.

[TR5] 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.

[TR6] 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.

[TR7] 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.

[TR8] 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.

[TR9] 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.

[TR10] Mathias Payer. “Triggering Deep Vulnerabilities Using Symbolic Execution”. In: *Chaos Communication Congress*. 2013.

[TR11] Mathias Payer. “WarGames in Memory”. In: *Chaos Communication Congress*. 2013.

[TR12] Mathias Payer. “Too much PIE is bad for performance”. In: *Technical Report* http://nebelwelt.net/publications/files/12TRpie.pdf. 2012.

[TR13] Mathias Payer. “String Oriented Programming - Circumventing ASLR, DEP, and Other Guards”. In: *Chaos Communication Congress* http://nebelwelt.net/publications/files/11CCC.pdf. 2011.

[TR14] 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.

[TR15] 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.

[TR16] Mathias Payer. “secuBT: Hacking the Hackers with User-Space Virtualization”. In: *Chaos Communication Congress* http://nebelwelt.net/publications/files/09CCC.pdf. 2009.

THESES

[TR1] Mathias Payer. “Safe Loading and Efficient Runtime Confinement: A Foundation for Secure Execution”. PhD thesis. 2012.

[TR2] Mathias Payer. “Adaptive Optimization Using Hardware Performance Monitors”. PhD thesis. 2006.

[TR3] Mathias Payer. “Building a client/server multimedia-kiosk using pxe, root-over-nfs, mozilla, and a CMS a.k.a. Multimedia Kiosk revisited”. PhD thesis. 2005.

[TR4] Mathias Payer. “Implementation of a Bluetooth Stack for BTnodes and Nut/OS Version 0.9”. PhD thesis. 2004.