KEVIN JOSEPH LEACH

kjleach@umich.edu / 703-475-7750
Citizenship: USA
2-body with Yu Huang

SUMMARY

Cross-disciplinary security researcher seeking 2-body resolution. Publications in ICSE, S&P, NDSS, DSN, EMNLP, and UbiComp. Experience with writing and managing funded grants (total $7.4M). Mentored 18 graduate students, 12 undergraduate students, and 7 research engineers.

ACADEMIC PREPARATION

Senior Research Fellow, University of Michigan–Ann Arbor Computer Science and Engineering 09/2017–Present
Mentors: Westley Weimer

Research Scientist, University of Virginia School of Engineering and Applied Science 01/2017–09/2017
Mentor: Benton Calhoun

Ph.D., University of Virginia Computer Engineering 12/2016
Advisor: Westley Weimer
Dissertation: Transparent System Introspection in Support of Analyzing Stealthy Malware

M.S., George Mason University Computer Science 05/2013
Advisor: Angelos Stavrou

B.S. with Distinction, University of Virginia Computer Engineering and Computer Science 05/2011

HIGHLIGHTS

- **Funding**: Wrote, submitted, and/or contributed to 6 funded grants (total $7.4M, our portion $2.3M)
- **Mentorship**: Mentored 3 PhD students, 2 graduate students, and 7 undergraduates at UMich; 13 PhD students and 5 undergraduates at UVA.
- **Scholarship**: Published in ICSE, Oakland, NDSS, DSN, TDSC, EMNLP; 307 citations.
- **Paper Awards**: ACM Distinguished Paper (ICSE2019) and Best Presentation Awards (GI2019).
- **Awards**: Louis T. Rader Outstanding Graduate Research Award, Outstanding Graduate Teaching Award, Mason Fellowship.
- **Teaching**: Taught 3 undergraduate classes (total 809 students) spanning four semesters: Compilers, Computer Organization, and Conversational Artificial Intelligence.
- **Service**: undergraduate advising (150 advisees formally), reviewer for ICSE, ISPASS.

ACCEPTED REFEREED PUBLICATIONS

[1] Lei Zhou, Fengwei Zhang, Jinghui Liao, Zhenyu Ning, Jidong Xiao, Kevin Leach, Westley Weimer, and Guojun Wang. KShot: Live kernel patching with SMM and SGX. In *50th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2020)*, 2020. To appear. Acceptance rate: 16.5%.

[2] Sean Stapleton, Yashmeet Gambhir, Alexander LeClair, Zachary Eberhart, Westley Weimer, Kevin Leach, and Yu Huang. A human study of comprehension and code summarization. In *28th International Conference on Program Comprehension (ICPC 2020)*, 2020.

[3] Stefan Larson, Eric Guldan, and Kevin Leach. Data query language and corpus tools for slot-filling and intent classification data. In *12th International Conference on Language Resources and Evaluation (LREC 2020)*, 2020. To appear.

[4] Yu Huang, Kevin Angstadt, Kevin Leach, and Westley Weimer. Selective symbolic type-guided checkpointing and restoration for autonomous vehicle repair. In *1st International Workshop on Automated Program Repair (APR2020)*, 2020. To appear.

[5] Ryan Krueger, Yu Huang, Xinyu Liu, Tyler Santander, Westley Weimer, and Kevin Leach. Neurological divide: An fmri study of prose and code writing. In *42nd ACM/IEEE International Conference on Software Engineering (ICSE 2020)*, 2020. To appear. Acceptance rate: 20%.

[6] Stefan Larson, Anish Mahendran, Joseph Peper, Christopher Clarke, Andrew Lee, Parker Hill, Jonathan K Kummerfeld, Kevin Leach, Michael Laurenzano, Lingjia Tang, and Jason Mars. An evaluation dataset for intent classification and out-of-scope prediction. In *2019 Conference on Empirical Methods in Natural Language Processing (EMNLP 2019)*, 2019. Acceptance Rate: 23.8%.

[7] Lei Zhou, Jidong Xiao, Kevin Leach, Westley Weimer, Fengwei Zhang, and Guojun Wang. Nighthawk: Transparent system introspection from ring -3. In *2019 Euroean Symposium on Research in Computer Security (ESORICS 2019)*, 2019. Acceptance Rate: 20%.

[8] Kevin Leach, Ryan Dougherty, Chad Spensky, Stephanie Forrest, and Westley Weimer. Evolutionary computation for improving malware analysis. In *5th Genetic Improvement Workshop (GI 2019)*, 2019. **Best Presentation Award**.

[9] Brandon Carlson, Kevin Leach, Darko Marinov, Meiyappan Nagappan, and Atul Prakash. Open source vulnerability notification. In *15th International Conference on Open Source systems (OSS 2019).* In press.

[10] Yu Huang, Xinyu Liu, Ryan Krueger, Tyler Santander, Xiaosu Hu, Kevin Leach, and Westley Weimer. Distilling neural representations of data structure manipulation using fmri and fnirs. In *41st ACM/IEEE International Conference on Software Engineering (ICSE 2019)*, 2019. **Distinguished Paper Award**.

[11] Fengwei Zhang, Kevin Leach, Angelos Stavrou, and Haining Wang. Towards transparent debugging. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, January 2018. Impact Factor: 6.4.

[12] Jacob Breiholz, Farah Yahya, Christopher J. Lukas, Xing Chen, Kevin Leach, David Wentzloff, and Benton H. Calhoun. A 4.4nw lossless sensor data compression accelerator for 2.9x system power reduction in wireless body sensors. In *IEEE International Midwest Symposium on Circuits and Systems (MWCAS)*, 2017.

[13] Kevin Leach, Fengwei Zhang, and Westley Weimer. Combining secure guard extensions and system management mode to monitor cloud resource usage. In *20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2017)*, 2017. Acceptance rate: 20%.

[14] Yu Huang, Jiaqi Gong, Mark Rucker, Wesley Bonelli, Kevin Leach, Philip Chow, Karl Fua, Matthew Gerber, Bethany Teachman, and Laura Barnes. Towards behavior-aware compting: Understanding behavioral dynamics of social anxiety through smartphone sensors. In *Ubicomp via IMWUT*, 2017.

[15] Yu Huang, Haoyi Xiong, Kevin Leach, Yuyan Zhang, and Laura Barnes. Assessing social anxiety using GPS trajectories and Point-Of-Interest data. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2016)*, Heidelberg, Germany, September 2016. Acceptance rate: 23%.

[16] Kate Highnam, Kevin Angstadt, Kevin Leach, Westley Weimer, Aaron Paulos, and Pat Hurley. An uncrewed aerial vehicle attack scenario and trustworth repair architecture. In *46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2016)*, Toulouse, France, July 2016.

[17] Haoyi Xiong, Jinghe Zhang, Yu Huang, Kevin Leach, and Laura Barnes. DAEHR: A discriminant analysis framework for electronic health record data and an application to early detection of mental health disorders. *Transactions on Intelligent Systems and Technology (TIST)*, December 2015. Under review.

[18] Nicholas J Napoli, Kevin Leach, Laura Barnes, and Westley Weimer. A MapReduce framework to improve template matching uncertainty. In *Proceedings of the 3rd International Conference on Big Data and Smart Computing (BigComp 2016)*, Hong Kong, January 2016. Acceptance rate: 22%.

[19] Kevin Leach, Chad Spensky, Westley Weimer, and Fengwei Zhang. HOPS: Towards transparent introspection. In *Proceedings of the 23rd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER 2016)*, Osaka, Japan, March 2016. Acceptance rate: 37%.

[20] Chad Spensky, Hongyi Hu, and Kevin Leach. LO-PHI: Low observable physical host instrumentation. In *Networks and Distributed Systems Security Symposium 2016 (NDSS 2016)*, San Diego, CA, February 2016. Acceptance rate: 15.8%.

[21] Jinghe Zhang, Haoyi Xiong, Yu Huang, Hao Wu, Kevin Leach, and Laura Barnes. M-SEQ: Early detection of anxiety and depression via temporal orders of diagnoses in electronic health data. In *Proceedings of the 2015 IEEE International Conference on Big Data (BigData 2015)*, September 2015.

[22] Fengwei Zhang, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun. Using hardware features for increased debugging transparency. In *Proceedings of the 36th IEEE Symposium on Security and Privacy (Oakland 2015)*, May 2015. Acceptance rate: 13.5%.

[23] Fengwei Zhang, Kevin Leach, Haining Wang, and Angelos Stavrou. TrustLogin: Securing password-login on commodity operating systems. In *Proceedings of the 10th ACM Symposium on Information, Computer, and Communications Security (ASIACCS 2015)*, Singapore, April 2015. Acceptance rate: 17.8%.

[24] Fengwei Zhang, Haining Wang, Kevin Leach, and Angelos Stavrou. A framework to secure peripherals at runtime. In *Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS 2014)*, Wrocław, Poland, September 2014. Acceptance rate: 24.7%.

[25] Fengwei Zhang, Kevin Leach, Kun Sun, and Angelos Stavrou. SPECTRE: A dependable system introspection framework. In *Proceedings of the 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013)*, Budapest, Hungary, June 2013. Acceptance rate: 19%.

[26] Kevin Leach. Barley: Combining control flow with resource consumption to detect jump-based rop attacks. In *Proceedings of the 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013)*, Budapest, Hungary, June 2013.

PATENTS

1. Fengwei Zhang, Kevin Leach, Angelos Stavrou, and Haining Wang. Using Hardware Features for Increased Debugging Transparency. US Patent No. 10,127,137. November 13, 2018.

2. Joseph Peper, Michael Laurenzano, and Kevin Leach. Technique for Segmenting Complex Utterances. Provisional Patent Application. February 2020.

Experience

University of Michigan—Ann Arbor 09/2017 – Present
Senior Research Fellow

- **Funding**: Wrote, submitted, and contributed to grant proposals to AFRL and DARPA ($4.3M funded, $1.23M our portion). Submitted internal proposals ($30k funded in-kind for fMRI scans). Submissions to NIH and NSF under review.
  - DARPA Assured Micro Patches (AMP). Using binary analysis to lift legacy binaries to intermediate representations to automatically generate assured variants (with Baris Kasicki, Manos Kapritsos, and Westley Weimer; $1.8M funded, $600k our portion)
  - AFRL Foundations of Trusted Computational Information Systems: Improving Search-Based and Semantic Automated Program Repair. Combining generative- and pattern-based automated program repair techniques to improve trustworthiness of safety-critical software (with Westley Weimer, Stephanie Forrest, and Claire LeGoues; $700k funded, $230k our portion)
  - AFRL Trusted and Resilient Mission Operation: Integrating anomaly detection, automated program repair, and binary rewriting techniques to detect, fix, and harden safety-critical flight control software mid-flight (with Westley Weimer, Jack W. Davidson, Claire LeGoues, and Stephanie Forrest; $1.8M funded, $400k our portion)
- **Grant Management and Delivery**: Integrated techniques for securing autonomous vehicle software, culminating in a successful AFRL demonstration. Wrote reports and organized telecons with Red Team and four other institutional collaborators.
- **Scholarship**:
  - Integrated Intel SMM and SGX to deploy kernel patches at runtime with low efficiency and without having to trust kernel patching mechanisms [1].
  - Designed and conducted an IRB-approved human study using functional MRI to understand the neural representation of software engineering tasks, resulting in an ACM/IEEE Distinguished Paper [10]. Designed an fMRI-safe keyboard, enabling studies involving code writing during scans, resulting in an ICSE paper [5].
  - Developed and published a technique based on covering arrays to increase stealthy malware analysis efficiency [8] (Best Presentation).
  - Developed a system for transparently introspecting system behavior using a combination of Intel ME, SGX, and SMM [7].
- **Mentorship**:
  - 3 PhD students mentored in Clarity Lab: Chris Clarke (Combined virtual assistants); Roland Daynauth (FPGA-accelerated autonomous driving); Andrew Lee (relation extraction via deep learning)
  - 2 remote graduate students mentored: Lei Zhou (SMM- and SGX-based security applications); Mohsen Ahmadi (efficient stealthy malware analysis)
  - 6 Undergraduates mentored: Yujun Qin, Sam Gonzalez, Linh Le (architectural side-channel attacks); Ryan Krueger, Xinyu Liu (fMRI and fNIRS); Scott Andersen (summarization of x86 malware).
- **Teaching and service**: Designed and taught a new senior-level undergraduate NLP/AI course for two semesters (enrollment 40; 69). Taught undergraduate compilers (enrollment 59). Taught required undergraduate computer organization (enrollment 550) and managed 18 instructional assistants. Teaching reviews: 4.84/5.0 vs. 4.4/5.0 median across engineering school. Served departmental undergraduate advising office (total 150 formal advisees).

University of Virginia 01/2017 – 08/2017
Research Scientist

- **Funding**: Contributed to grant proposals for improving ultra-low-energy circuits ($3M funded, $1M our portion).
- **Scholarship**: Developed a platform for securely measuring resources consumed by virtual machines based on Intel Secure Guard Extensions and System Management Mode, culminating in a publication [13].
- **Grant Management and Delivery**: Developed a large-scale system model of low-power systems-on-chip comprising sensor nodes supporting the Internet-of-Things. Combined low-level circuit simulations from Spectre and SPICE with theoretical circuit models to rapidly simulate system behavior to inform design decisions from the circuit level to the smart city level. Investigated emergent security properties of large-scale IoT deployments.
- **Mentorship**: Managed and mentored the Robust Low-Power VLSI group: 13 PhD students and 4 undergraduate researchers. Collaborated on multiple publications related to low-power SRAMs and body sensor networks [12].

GrammaTech, Inc. 06/2016 – 09/2016
Research Scientist Intern

- Developed a tool for detecting vulnerabilities in a stripped binary by leveraging statistical features in a large corpus of existing binary code by using CodeSurfer, a static analysis tool. Applied machine learning techniques to extract features from binaries and compute a notion of similarity between pairs of binaries (DARPA MUSE).
- Designed and ran experiments to demonstrate an improvement in the quality of predicted vulnerabilities culminating in a Phase II SBIR worth $1M.

University of Virginia 08/2013 – 12/2016
MIT Lincoln Laboratory Research Assistant

- **Funding**: Applied for and won a $81,000/anum research grant. Led UVA's extension of the low-overhead instrumentation project (LO-PHI), collaborating with MIT LL. Findings and results were published [19, 20].
- **Scholarship**:
  - Worked with external collaborators on hardware-assisted transparent security research culminating in publications [11, 22, 23] and a patent.
  - Used Hadoop MapReduce to efficiently use sources of information to make robust decisions. Published [18].
  - Collaborated with data scientists to make predictions about mental health outcomes for college students. Published [21, 17].
- **Mentorship**: Mentored an undergraduate student (Kate Highnam) on patching embedded software in autonomous aerial vehicles. By combining automated repair techniques with security principles, we sought to correct buggy flightplans that might compromise the integrity of a vehicle's mission, ultimately culminating in a demo for AFRL Program Managers and collaborative publications [16].
- **Teaching**: Taught undergraduate compilers course twice. Enrollment over 20. Managed TAs, wrote and graded assignments, gave all lectures.

Kryptowire LLC 01/2013 – 09/2014
Senior Mobile Engineer

- Collaborated with a group of 3 engineers to develop tools for auditing security and protecting intellectual property on mobile platforms for over 1000 different Android apps. This software is used to vet apps on phones in military settings.

MIT Lincoln Laboratory 06/2013 – 08/2013
Summer Research Intern, Group 59

- Worked with the Cyber Systems Assessments group on the low-overhead instrumentation project (LO-PHI) relating to transparent system analysis tools. Our findings and results were published [20].

George Mason University Center for Secure Information Systems 06/2011 – 05/2013
Graduate Research Assistant

- Contributed to an IARPA-funded project related to automatically fixing security bugs in software of unknown provenance (STONESOUP). Worked closely with my advisor and other students in CSIS, publishing results and findings along the way [25, 26, 24].
- Awarded the Mason Fellowship to support doctoral research (approx. 5 awards out of 400 applicants).
- Served as the TA for CS471, Operating Systems, for two semesters. Hosted recitations, taught a lecture, and graded assignments. This course was required by the undergraduate curriculum taken by 80 or more students each semester. Received the Outstanding Graduate Teaching Award issued by GMU's Engineering School (approx. 5 awards out of 100 GTAs).