Kevin Joseph Leach

kjleach@umich.edu
Citizenship: USA

Summary

Systems security researcher with significant scientific contributions related to the analysis of advanced stealthy malicious exploits and code. Experience developing software in a startup company. Additional experience applying for and managing research grants, including live demos for Program Managers.

Education

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

M.S., George Mason University Volgenau School of Engineering 05/2013
Master of Science, Computer Science
Advisor: Angelos Stavrou

B.S., University of Virginia School of Engineering and Applied Science 05/2011
Bachelor of Science with Distinction
Majors: Computer Engineering and Computer Science; Minor: Engineering Business

Publications and Technical Reports

[1] 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*, 2019. To appear.

[2] Fengwei Zhang, Kevin Leach, Angelos Stavrou, and Haining Wang. Towards transparent debugging. *IEEE Transactions on Dependable and Secure Computing*, September 2018.

[3] 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 Internaional Midwest Symposium on Circuits and Systems*, 2017.

[4] 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. To appear. Acceptance rate: 20%.

[5] 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)*, Heidelberg, Germany, September 2016. Acceptance rate: 23%.

[6] 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.

[7] 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.

[8] 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%.

[9] 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%.

[10] 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%.

[11] 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.

[12] 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%.

[13] 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%.

[14] 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%.

[15] 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%.

[16] 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.

[17] Fengwei Zhang, Kevin Leach, Angelos Stavrou, and Haining Wang. Using hardware features for increased debugging transparency, November 2018. Patent No. 10,127,137.

Experience

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

- Integrated techniques for securing autonomous vehicle software, culminating in an AFRL demonstration.
- Developed a technique based on covering arrays to increase the efficiency of stealthy malware analysis.
- Developed an approach to securing peripheral IO on IoT and smart devices using ARM TrustZone.
- Developed a system for transparently introspecting system behavior using a combination of Intel ME, SGX, and SMM.
- Advised three undergraduate research students via UROP on a project for efficiently detecting architectural side-channel attacks using in-cache automata.
- Designed and conducted an IRB-approved human study using function MRI to understand the neural representation of software engineering tasks [1].
- Taught undergraduate compilers course with 59 enrolled students. Taught undergraduate computer organization with 550 enrolled students an 18 instructional assistants.
- Performed service obligations for the department (undergraduate advising).

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

- 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 [4].
- 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.
- Managed and advised 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 [3].
- Wrote 3 grant proposals totalling over $2M.

  1. Self-powered systems
     Proposed the development of a model of self-powered Systems-on-Chip for predicting system lifetime based upon workload and environmental conditions.
  2. Robotic localization acceleration via ternary content-addressable memory
     Proposed the development of a TCAM structure for accelerating image processing tasks associated with autonomous vehicular mapping and localization.
  3. A flexible FPGA fabric supporting configurable performance vs. power consumption
     Proposed an FPGA fabric capable of sacrificing performance to lower power consumption for low-utilization tasks.

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.
- Designed and ran experiments to demonstrate an improvement in the quality of predicted vulnerabilities culminating in a Phase II SBIR worth $750k+.

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

- 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 [10].
- Worked with external collaborators on hardware-assisted transparent security research culminating in publications [2, 13, 14] and a patent [18].
- Used Hadoop MapReduce in collaboration with an external department to efficiently fuse sources of information to make robust decisions. Results and findings published [9].
- Collaborated with data scientists to make predictions about mental health outcomes for college students. Results and findings published [12, 8].
- Taught undergraduate compilers course twice. Enrollment over 20. Managed TAs, wrote and graded assignments, gave once-weekly lectures.
- Mentored an undergraduate student on patching embedded software in autonomous aerial vehicles. By combining automated repair techniques with security principles, we seek 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 [7].

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

- Collaborated with a small group of 3 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 situations.

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 [11].

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. Worked closely with my advisor and other students in CSIS group, publishing results and findings along the way [16, 17, 15].
- Awarded the Mason Fellowship to support doctoral research (approx. 5 awards out of 400 applicants).

George Mason University Computer Science Department 08/2011 – 05/2012
Graduate Teaching Assistant

- 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).

Research Projects

Transparent Cloud Resource Monitoring 10/2015 – Present

Designing and developing approaches to transparently monitor resource consumption in cloud scenarios. Exploring Intel SGX as a way to prevent malicious hypervisor guests from consuming too many resources without incurring high overhead.

Automated Quadcopter Repair 08/2015 – Present

Developing techniques to securely and automatically patch security-critical firmware deployed on drones and quadcopters.

LO-PHI 06/2013 – Present

Low-artifact Observable Physical Host Instrumentation
MITLL project focused on developing OS-agnostic and transparent malware analysis tools [11, 10] in the hope of understanding malware that is actively searching for and disabling analysis tools.

MalT: Towards Transparent Debugging 05/2013 – 01/2015

MALT (the Malware Tester) took the first steps towards building a bare-metal, transparent debugging system [13]. MALT uses System Management Mode on Intel platforms to reliably instrument each instruction executed by the system. This fine granularity allows us to detect and correct malicious software that attempts to disable or detect analysis frameworks.

Parallelizing Dempster's Combination Rule with MapReduce 08/2015 – 01/2016

Used Dempster-Shafer Theory to fuse beliefs from multiple information sensors to reduce the effect of noise in these sensors. We leveraged the embarrassingly parallel nature of Dempster's Combination Rule to build a MapReduce framework that efficiently fused thousands of sources together, providing a robust, highly accurate prediction even in the presence of high noise [9].

TrustLogin: Secure Password Login 01/2014 – 04/2015

TrustLogin permits users to input passwords in form fields displayed on the computer while mitigating the risk of keyloggers compromising their account credentials [14]. We use System Management Mode on Intel platforms to store keystrokes in secure memory, and place the password directly into encrypted network packets once the form is submitted. This allows dependable and transparent input of secure account credentials in an environment where a keylogging rootkit may be present.

IOCheck: Transparent Peripheral Firmware Integrity 05/2013 – 05/2014

IOCheck is a framework for verifying the integrity of the firmware in peripheral devices [15]. This tool enables rapid, reliable, and transparent polling-based peripheral firmware integrity checking. By using System Management Mode to regularly inspect firmware integrity, we gain an edge against malicious firmware or peripheral devices that might persist after wiping a system's hard drive.

Spectre: OS-Transparent memory-based attack detection 01/2012 – 05/2013

SPECTRE is a hardware-assisted platform for securely and reliably introspecting a bare-metal system [16]. We

leveraged System Management Mode on Intel platforms to transparently detect memory-based attacks including heap spray, heap overflow, and rootkit attacks.

STONESOUP 05/2011 – 05/2013

Securely **T**aking **O**n **N**ew **E**xecutables in **S**oftware **O**f **U**nknown **P**rovenance
STONESOUP (and our specific implementation, MINESTRONE) is an IARPA-funded project focused on automatically detecting and removing common software vulnerabilities in non-malicious software that includes code from an unknown source. Participated in PM meetings and demos.

Achievements and Honors

Louis T. Rader Graduate Research Award 4 awards out of over 100 graduate students, April 2016.

MIT Lincoln Laboratory Grant PI for $81,000/anum grant. Awarded December 2013.

Outstanding Graduate Teaching Award 5 of 100 engineering GTAs selected, May 2012

Mason Fellowship Roughly 5 awards per year out of over 400 applicants

Engineer in Training Designation towards Virginia Professional Engineer Certification, May 2011

Skills

Programming Languages C/C++, PHP, Java, Python, C#, LaTeX, OCaml, JavaScript, Bash

Numerical Computation Mathematica, MATLAB/Octave, MathCad