

Curriculum Vitæ of David Kohlbrenner

Contact

David Kohlbrenner

david.kohlbrenner@gmail.com
+1-571-236-5681
dkohlbre.com

Academic History

- 8/2018 — Present **University of California, Berkeley**
Postdoc
- 8/2011 — 8/2018 **University of California, San Diego**
Master of Science in Computer Science (*2015*)
Doctor of Philosophy, Computer Science (*2018*)
- 8/2007 — 5/2011 **Carnegie Mellon University**
Bachelor of Science, Computer Science. Minor in Philosophy

Publications

- [1] D. Kohlbrenner and H. Shacham, “On the effectiveness of mitigations against floating-point timing channels,” in *Proceedings of USENIX Security 2017* (E. Kirda and T. Ristenpart, eds.), pp. 69–81, USENIX, Aug. 2017.
- [2] C. Disselkoen, D. Kohlbrenner, L. Porter, and D. Tullsen, “Prime+abort: A timer-free high-precision l3 cache attack using intel tsx,” in *Proceedings of USENIX Security 2017* (E. Kirda and T. Ristenpart, eds.), pp. 51–67, USENIX, Aug. 2017.
- [3] D. Kohlbrenner and H. Shacham, “Trusted browsers for uncertain times,” in *Proceedings of USENIX Security 2016* (T. Holz and S. Savage, eds.), pp. 63–80, USENIX, Aug. 2016.
- [4] M. Andryscio, D. Kohlbrenner, K. Mowery, R. Jhala, S. Lerner, and H. Shacham, “On sub-normal floating point and abnormal timing,” in *Proceedings of IEEE Security and Privacy (“Oakland”) 2015* (L. Bauer and V. Shmatikov, eds.), IEEE Computer Society, May 2015.
- [5] K. Mowery, M. Wei, D. Kohlbrenner, H. Shacham, and S. Swanson, “Welcome to the entropics: Boot-time entropy in embedded devices,” in *Security and Privacy (SP), 2013 IEEE Symposium on*, pp. 589–603, IEEE, 2013.

Teaching experience

- Summer 2017 **Instructor CSE80 - UNIX Lab**
New course developed from scratch
Immersion learning for the terminal and UNIX environment
Open-sourced at <https://bitbucket.com/t4cs/t4cs>
- Spring 2014 **Teaching Assistant CSE127 - Computer Security**
Developed large attack projects for students
Lectured for section, held office hours, grading
200+ students and 2 other TAs
- 2013 — Present **Advisor for UC San Diego SIGINT CTF Team**
Lectured on a variety of security topics
Organized and taught workshops on security topics
Taught reverse engineering skills and tools

Industry Experience

- 6/2015 — 9/2015 **Internship at Qualcomm Technologies Inc.**
Security evaluation of an embedded system product line
Produced 90 page report with recommendations, all were implemented
- 9/2012 — 9/2013 **Co-founder of Somerset Recon**
Embedded systems reverse engineer
Reverse engineered undocumented wire protocols
Developed embedded platforms in C with heavy resource constraints
- Summer 2010 & 2011 **Internships at Sandia National Laboratories**

Service

- External reviewer for USENIX Security 2017
- External reviewer for USENIX Security 2016
- Preliminary Judge for NYU CSAW Applied Research Competition 2017, 2018
- UC San Diego Academic Integrity Review Board 2016—2018

Awards

- UC San Diego CSE Graduate Award for Research 2016
- 2nd place NYU Poly CSAW Applied Research Competition 2016
“Trusted browsers for uncertain times”
- 3rd place NYU Poly CSAW Applied Research Competition 2013
“Welcome to the Entropics: Boot-Time Entropy in Embedded Devices.”

Invited Talks

- 11/2017 **Invited talk at The University of Arizona**
Uncovering and addressing security assumptions about hardware
- 5/2017 **Invited talk at OWASP San Diego**
Timing attacks on web privacy and how to trust the browser again
- 5/2016 **Invited lecture ECE 289 UC San Diego**
Side channel research and attacks
- 6/2015 **Invited talk at University City High School**
The security mindset

Selected Skills

Languages: C, Python, x86/x86_64 Assembly, L^AT_EX

Reverse Engineering: C++, x86/x86_64 binaries, C, embedded systems

Tools: IDA, Wireshark

CTF

2009—2011 Founding member of Carnegie Mellon University's PPP team

2013—Present Founder and advisor for UC San Diego's SIGINT team