Kyle Hogan

kylehogan.github.io | klhogan@mit.edu

EDUCATION

MIT
EECS PhD Student

BOSTON UNIVERSITY
BA in Computer Science
Chemistry Minor
September 2016

TEACHING & MENTORING

MIT PRIMES
January 2016 - Present
Mentored two high school students on a project studying network bandwidth as a side channel in the cloud[?]. Currently mentoring students studying privacy for Monero transactions [6].

CS558 NETWORK SECURITY
Fall 2015
Teaching Assistant
Covered SQL injection, CSRF, XSS, cracking WEP, ARP spoofing, and web security topics such as HSTS, certificates, and secure cookies. Taught discussion and lab sections, held regular office hours, and maintained a Piazza forum.

BU CODEBREAKERS
Summer 2016
Summer program introducing high school girls to programming and topics in computer security. Gave a guest lecture on DNS and BGP with a focus on DNSSec and BGPSec.

AWARDS

NSF (GRFP)
2018 Graduate Research Fellowship
Boston University
2016 Excellence in Research Award
2015 Clare Boothe Luce Scholar

ACTIVITIES

- practical security seminar
- cryptography, systems security, and MPC reading groups
- Charles River Crypto Day

RESEARCH

COMPUTATIONAL STRUCTURES GROUP | MIT
PhD Student | July 2017 – Present
PhD student advised by Professor Srini Devadas. Working on reducing leakage in secure enclave environments with a particular focus on leakage free demand paging. [3, 4]

SECURITY GROUP | Akamai
Intern | June 2018 – August 2018
Summer intern designing a key management scheme to be used for disaster recovery of encrypted data backups.

MACS PROJECT | Boston University
Research Assistant | September 2015 – May 2017
Worked to apply the Universal Composability framework to construct a proof of security for OpenStack and the Network Time Protocol [2, 1].

MASSACHUSETTS OPEN CLOUD | Boston University
Research Assistant | January 2016 – May 2017
Core developer on a project designing trustworthy bare metal clouds [5].

SECURE RESILIENT SYSTEMS & TECHNOLOGY | MIT LL
Intern | June 2016 – September 2016
Worked as an intern applying MPC to cybersecurity problems. Implemented protocols in VIFF to allow parties to securely compute a joint IP blacklist or aggregate outputs of vulnerability scanners.

SESA LAB | Boston University
UROP | February 2015 – August 2015
Undergraduate researcher on a project modifying a fetal MRI reconstruction algorithm to run in a distributed manner on the cloud.

NMR GROUP | Missouri University of Science & Technology
Undergraduate Research Assistant | May 2014 – July 2014

NEUROMORPHICS LABORATORY | Boston University
UROP | May 2013 – August 2013

MA BIOCHEM LAB | Missouri University of Science & Technology
Student Researcher | March 2012 – June 2012

PRESENTATIONS & PUBLICATIONS

[1] Ran Canetti, Kyle Hogan, Aanchal Malhotra, and Mayank Varia. A universally composable treatment of network time. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*. IEEE, 2017.

[2] Kyle Hogan, Hoda Maleki, Reza Rahaeimehr, Ran Canetti, Marten van Dijk, Jason Hennessey, Mayank Varia, and Haibin Zhang. On the universally composable security of openstack. SecDev, 2019.

[3] Ilia Lebedev, Kyle Hogan, and Srinivas Devadas. Secure boot and remote attestation in the sanctum processor. In *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*. IEEE, 2018.

[4] Ilia Lebedev, Kyle Hogan, Jules Drean, David Kohlbrenner, Dayeol Lee, Krste Asanović, Dawn Song, and Srinivas Devadas. Sanctorum: A lightweight security monitor for secure enclaves. *DATE*, 2019.

[5] Amin Mosayyebzadeh, Gerardo Ravago, Apoorve Mohan, Ali Raza, Sahil Tikale, Nabil Schear, Trammell Hudson, Jason Hennessey, Naved Ansari, Kyle Hogan, Charles Munson, Larry Rudolph, Gene Cooperman, Peter Desnoyers, and Orran Krieger. A secure cloud with minimal provider trust. In *HotCloud 18*, Boston, MA, 2018. USENIX Association.

[6] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, et al. An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163, 2018.