Eric Kilmer

Boston, MA 02129

Education

The Pennsylvania State University **University Park, PA**
Schreyer Honors College, B.S. Computer Engineering *Fall 2011 – Summer 2017*
Schreyer Honors College, M.S. Computer Science and Engineering *Fall 2014 – Summer 2017*

Research and Development

Trail of Bits (New York, NY) **Remote–Boston, MA**
Full-time Employment *Feb. 2019 – Present*

- Contributed various fixes and features to our Manticore symbolic execution engine
- Developed supporting research tools and experiments for the DARPA LADS (Leveraging the Analog Domain for Security) program
  - Analyzed and automated Javascript object memory layout extraction from Google's V8 engine
  - Developed Binary Ninja plugin to perform static analysis for backwards dataflow and memory accesses
  - Ported and retrofitted old QEMU fork to run the open source Solokey MFA device firmware (STM32L432) on QEMU v5
- Developed supporting research tools and experiments for the DARPA CHESS (Computers and Humans Exploring Software Security) program
  - Implemented new and fixed existing system call models in Manticore for network and file handling
  - Developed Manticore plugin to utilize DWARF debug information for more verbose function tracing and execution progress
  - Developed Manticore plugin to utilize DWARF debug information for detection of symbolic out-of-bound memory accesses of local variables
- Contributed in writing various DARPA and government SBIR proposals

MIT Lincoln Laboratory **Lexington, MA**
Full-time Employment *Jul. 2017 – Feb. 2019*

- Developed simple source-level compiler transformations for the C programming language
- Developed a test harness to perform black-box testing and evaluation of resource-adaptive systems.
  - Programmed in Haskell using light formal methods for type-safety and compile-time confidence
  - Supported Amazon AWS ECS deployment and scaling
- Researched and composed new, modern, cyber security guidelines for government systems

Master's Thesis **University Park, PA**
Extending Vulnerability Discovery with Fuzzing and Symbolic Execution to Realistic Applications *2017*

- Contributed features to open-source Cyber Grand Challenge solution, `angr`, written in Python
- Successfully reproduced CGC results on Ubuntu with real `libc` calls
- Performed experiments, collected results, and documented outcomes, shortcomings, and future work

Symantec **Los Angeles, CA**
Summer Internship: STAR Response Team *2016*

- Reverse-engineered malware samples using binary analysis techniques
- Developed tool to extract features from binaries to assist in program author attribution (Python)

Army Research Lab **Adelphi, MD**
Summer Research Internship *2014, 2015*

- Developed network decoders and detectors for an Army Research Lab's network analysis tool (Python)
- Reverse-engineered a Linux XOR-encoded DDoS malware with IDA Pro to write decoders for detection
- Conducted web application security analysis of machines on live networks

Publications

- N. Lageman, E. Kilmer, R. Walls, and P. McDaniel, "BinDNN: Resilient Function Matching Using Deep Learning," in *SECURECOMM*, Guangzhou, China, Oct. 2016.
- R. Walls, E. Kilmer, N. Lageman, and P. McDaniel, "Measuring the Impact and Perception of Acceptable Advertisements," in *ACM 2015 Internet Measurement Conference* (*IMC*), Tokyo, Japan, Oct. 2015.

Core Technical Skills

Languages: Python, Haskell, C, Assembly (x86(-64)), Java, LaTeX, some C++
Technology/Tools: Docker, Vim, Git, Binary Ninja, `man`, IDA Pro