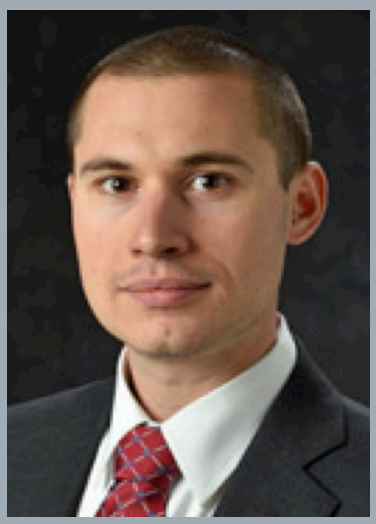
WPI



WPI Alumnus, Dr. Richard Skowyra joined MIT Lincoln Laboratory in 2014 as a technical staff member in the Cyber Analytics and Decision Systems Group. His research is focused on the security applications of software-defined networking, the design and assessment of moving-target defenses, and the application of automated reasoning techniques to cybersecurity modeling and analysis. Dr. Skowyra's research interests also include distributed systems, network security, cyber-physical systems security, software engineering, and artificial intelligence. Dr. Skowyra holds BS and MS degrees from Worcester Polytechnic Institute and a PhD from Boston University, all in computer science.

CyberCorps®: Scholarship for Service

Seminar Series 2016-2017

The Quest for Memory Safety

Dr. Richard W. Skowyra

Cyber Analytics and Decision Systems

MIT Lincoln Laboratory

Date: Tuesday, April 4, 2017
Place: 320 Fuller Labs
Time: 11:00 am – 1:00pm (discussion followed by pizza)

Abstract

Memory corruption is at the heart of almost all malware in the wild, and has fueled an arms race from 1972 to the present. In this talk I will provide a brief history of memory corruption, discuss a bypass attack we developed against a well-known defense, and then present a memory corruption defense we developed at MIT Lincoln Laboratory. The first half of the talk will focus on Control Flow Integrity (CFI), a well-known defensive technique that tries to prevent memory corruption attacks by restricting control flow transfers to only 'valid' targets. I'll discuss a method we developed to bypass this defense by breaking the underlying assumption CFI relies on upon: that an attack must contain invalid control transfers. The second part of the talk will focus on a defense we developed called Timely Address Space Re-Randomization, which seeks to disrupt code reuse attacks via synchronized re-randomizations of memory layout.