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.