COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

Dissertation Defense

Misiker Tadesse Aga

Thwarting Advanced Code-reuse Attacks

Monday, December 9, 2019
2:30 pm – 4:30 pm 3941 Beyster Bldg.

ABSTRACT: Code-reuse attack remains one of the prevailing attack vectors to infiltrate systems. Various mitigation techniques have been proposed to counter this attack vector. However, recent works have shown that code-reuse attacks can circumvent proposed defenses and continue to be a prominent threat. In this thesis, we present low overhead techniques to mitigate advanced code-reuse attacks.

First, this thesis presents a novel approach to thwart advanced control flow attacks called ProxyCFI. ProxyCFI replaces all code pointers in a program with a less powerful construct: pointer proxies. Pointer proxies are random identifiers associated with legitimate control flow edges in the program. Pointer proxy values are defined per function and are re-randomized at program load time. To ensure that the approach covers the entire control flow of the program, we developed a load-time verifier embedded in the ProxyCFI program loader, which performs reachability analyses of the program and verifies that there is no vulnerable control flow transfer.

The second proposed technique to mitigate code-reuse attacks is Smokestack, a runtime stack-layout randomization technique that addresses problems with prior stack randomization approaches. Smokestack instruments programs to randomize their stack layout at runtime for each invocation of a function. In doing so, Smokestack minimizes the utility of information gained by runtime probes of chained code-reuse attacks.

Our final technique randomizes heap allocations to prevent advanced code-reuse attacks orchestrated through heap-resident variables. To this end, we propose the use of multi-variant execution (MVX) to randomize heap allocations in order to ultimately thwart attacks that perform runtime probes to discover allocations.

In all, this thesis presents novel techniques that carve out a new space in advanced code-reuse attack protections, offering a strong protection, while incurring minimal performance overheads.

Chair: Prof. Todd Austin