

CIS 751 Project Proposal

Chuck Zumbaugh

November 14, 2025

Proposed Title: Memory corruption vulnerabilities: Modern safeguards and their shortcomings

Overview: Memory corruption vulnerabilities are common and represent a significant portion security bugs. They are relatively easy to introduce, particularly in memory unsafe languages such as C/C++, and allow for arbitrary code execution when exploited. Significant work has been done to improve the security of modern systems through hardware and OS-level protections. Nevertheless, these bugs remain exploitable and many zero-days are the result of memory corruption. The objective of this review will be to explore the following strategies to protect against memory corruption vulnerabilities, including how they function, the problem they solve, and current methods attackers can use to circumvent them.

1. Overview of memory corruption vulnerabilities
2. Modern safeguards and strategies to circumvent them
 - (a) Address space layout randomization (ASLR)
 - (b) Executable-space protection
 - (c) Pointer authentication codes
 - (d) Memory tagging extension