Thesis Defense

Computer Science Master's Program

"Exploiting Compiler-Introduced Vulnerabilities in C: A Cross-Compiler and Cross-Architecture Analysis of Undefined Behavior"

By **Erik McCutchen**

Abstract:

Compilers are a critical component in generating secure software across engineering disciplines. However, languages like C that permit undefined behavior introduce a fundamental tension between the compiler's interpretation of undefined behavior and the security of the generated code. This tension can result in security vulnerabilities that, from the programmer's perspective, are "created" by the compiler. The widespread use of these languages, combined with the complexity of modern optimizations and limited developer visibility into compiler behavior, makes these vulnerabilities both pervasive and difficult to detect.

Building on prior work, this thesis refines a dataset of C code snippets that exhibit Compiler-Introduced Security Bugs (CISB) to systematically explore how different compilers (Clang and GCC) and different target architectures (x86, ARM) generate security bugs based on undefined behavior. A detailed case study further demonstrates how an adversary could exploit binaries containing CISB depending on what compiler was used. This work provides insight into how compiler and software developers can bridge the security gap by highlighting specific instances and preconditions of undefined behavior where this divide breaks down.

Date: Tuesday, June 10th, 2025
Time: 11:00 AM – 1:00 PM
Location: 14-232b
Committee: Dr. Beard, Dr. DeBruhl, and Dr. Schmitt