CMSC 426

Gokul Natarajan

5/6/22

Write-Up for Ben’s Presentation

Program analysis is used in compiler optimizations to make programs run faster. It can also find bugs or security vulnerabilities. Started by looking at how we can use mathematical formalisms to reason about how programs execute, then examine how programs are represented within compilers and analysis tools. Symbol stripping is used to remove unnecessary information from an executable to make it faster to run. Static analysis is any debugging before running the code and dynamic analysis is running the code through a debugger. LLVM has now become common use between all platforms to compile all different types of code. LLVM is written in C++ with Ghidra and takes many other languages in and translates the code to a low-level intermediate representation of the code into a language used by the LLVM framework. There are many different uses of the compiler mostly which is bug finding. We explored any projects that used the LLVM framework such as mcsema is an early executable lifter that translates executable binaries from native machine code to LLVM bit code. We also had a cracked password demo in the disassembler.