**Week 4: C++ In Research (Part B)**

Nate Bachmeier

March 31, 2019

TIM-8101: Principals of Computer Science

Northcentral University

# Examine current research being done with C++

“Coppelia is an end-to-end tool that given a processor design and collection of security critical requirements, can automatically generate exploit code (Zhang, Deutschbein, Huang, & Sturton, 2018).”

The authors acquired a list of 31 known vulnerabilities in two open source processors. Their goal was to reproduce these issues purely through automated discovery technics. The system detected 29 of the 31 issues and found four new issues. After finding an issue, Coppelia will generate a short exploit script to reproduce the issue. This was used to confirm no false positives were reported and provide a mechanism to validate future patches are accurate.

# How did C++ fit into the research?

The first challenge was to get the processor designs into a format which standard tools can consume and manipulate. The researches decided to accomplish this by compiling the Verilog hardware design language into C++. This reduced the time to start collecting results as rich open source tooling already exist for C++.

After they generated the C++ code it was then compiled another level into LLVM Intermediate Representation byte code. This enabled KLEE, to perform symbolic execution over various portions of the processor implementations.

# What were the research questions?

The researchers

# What did the authors find?

# What is some future work which could be built upon this research? Include both what the authors found, and describe things in your own words.

# What are some similar/contrasting works and their findings?