SAND2019-8171D

The Center for Cyber Defenders

Expanding computer security knowledge

PIKE: Reverse Engineering and Processor Defining

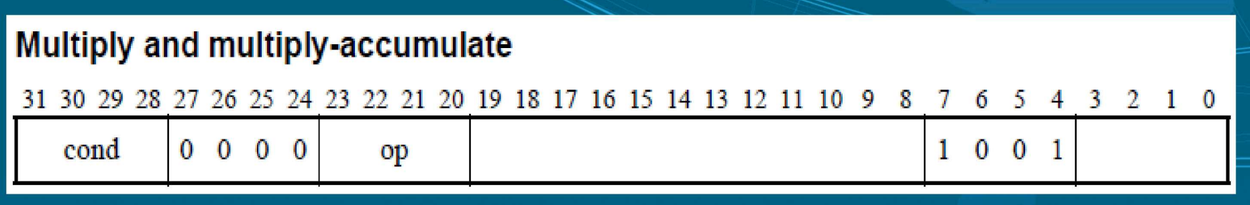
Grant Brown, Tennessee Tech University;

Luke Janik, Northeastern University;

Project Mentor: Josh Templin, 5838

Problem Statement:

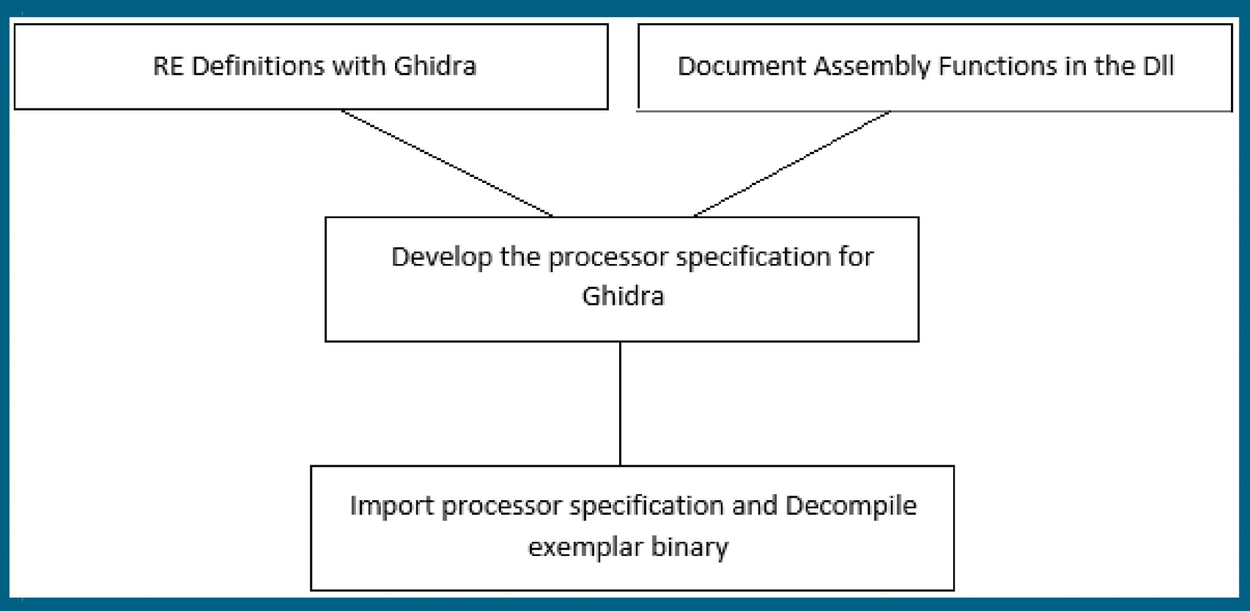
Ghidra is a powerful NSA-developed software reverse engineering tool. It's capabilities are broad, but its disassembly capabilities are limited to those processor architectures which have been specified in Ghidra's database. This task was to explore implementing a Ghidra processor specification for an insufficiently-documented commercial processor. An understanding of how the machine code translates to assembly code must be investigated.



Sample of ARM Instruction Encoded in Bits

Desired Results:

- Gain an understanding of the processor architecture through analysis of available documentation and reverse engineering of an available disassembler.
- Define the assembly instructions in a SLEIGH file for addition to Ghidra's database.
- Define the processor architecture sufficiently to disassemble a binary file assembled for the target processor.



Block Diagram of Objectives

```
:mul^COND^SBIT_ZN rn,rm,rs  is $(AMODE) &  COND & c2527=0
& c2124=0 & SBIT_ZN & rn & c1215=0 & rs & c0407=9 & rm
{
  build COND;
  build rm;
  build rs;
  rn = rm*rs;
  resultflags(rn);
  build SBIT_ZN;
}
```

Example SLEIGH Definition of an Instruction

Objectives and Approach:

Task 1: Extract processor architecture and instruction set architecture from documentation, as available.

Task 2: Reverse Engineering a disassembler .dll file to fill in the gaps, such as the mapping between assembly and machine code.

Task 3: Develop the processor by writing the SLEIGH files necessary for Ghidra to do a complete disassemble.

Task 4: Import the processor specification into Ghidra.

Task 5: Verify by disassembling a candidate binary assembled for that processor.

Impact and Benefits:

- Ghidra has extensive built-in functionalities but there exists a gap in Ghidra's ability to decompile all files. This work will broaden Ghidra's capabilities.