Presentation Outline

1. Intro
   1. My programs
      1. Verifier\_Round\_3
      2. Random Program Generator
   2. What problem is it attempting to solve
      1. Taking a valid eBPF program, run it through a FOL translator to see if the output matches what eBPF Verifer says it should be. If there is a mismatch, it can indicate a bug in the eBPF Verifier, or a bug in the FOL Verifier
      2. How do you automate program generation to test a wide range of different programs to see the depths of both the eBPF Verifier and the FOL Verifier
   3. What are its limitations
      1. FOL Verifier
         1. Small subset of eBPF instructions supported
      2. Random Program Generation
         1. Unknown chance to produce viable programs for testing due to current random nature
2. Specifics about Verifier\_Round\_3
   1. Internal Logic for Naming Scheme
      1. SSA Naming for every instance a register has a value changed
      2. Required for z3
      3. Initialized by create\_register\_list, which creates a 2D List containing placeholders for the number of registers allowed in the program
      4. Updated by appending a new Register\_Info object to the end of a specific registers sublist
      5. Stored in register\_state\_helper.register\_history
   2. Valid input checking and extension
      1. Any time a function is called, there are three options for getting a value
      2. Imm4, imm8, register
      3. Imm4 would be using a value that, bit wise, is half the size of the regular register
      4. Need to extend the size of the value to not have sign problems
      5. Use extend\_the\_number function to encapsulate both the sign extension, or zero extension needs
   3. Supported eBPF Functions
      1. All functions are generic calls, which can be made to do specific (imm4, imm8, or reg) versions of the call by using the source\_reg and extension\_length parameters
         1. Source\_reg is a Boolean stating whether the input\_value parameter should be treated as a register number or an outside integer
         2. Extension\_length is used to tell extend\_the\_number how many bits a specific imm4 number needs to be lengthened to fit in the register
      2. Add
         1. Three main features
         2. Add two values and create a new instance of the destination register for ssa
         3. Prevent overflow
         4. Prevent underflow
      3. Mov
         1. Sets a new instance of the destination register equal to whatever the incoming value is
      4. Jne
         1. The wonky one
         2. Current attempt (as of Thursday 7/30)
            1. Get the names (ie reference points) for all registers before the jump instruction
            2. Execute the code that would be taken without the jump
            3. Get the names of all registers after the non jump execution
            4. Set a new layer of registers across all initialized registers using an if, then, else z3 function
            5. Return a problem flag that is larger than the instruction counter to tell the main program to skip all instructions until the offset, since this will return a z3 function containing their constraints
         3. Seems to have a large number of bugs
            1. If a nested jump ends at the same location as another jump
            2. If one jump occurs and a nested jump has an offset that’s outside it’s range
   4. Execution of a specific program
3. Specifics about Random Program Generator