University of BRISTOL

Ghidra: Binary code Static Analysis tool

Sanjay Rawat

Features that interests us..

Features that interests us..

- It has many interesting and valuable features

Features that interests us..

- It has many interesting and valuable features
- It is free!

Features that interests us..

- It has many interesting and valuable features
- It is free!
- It can analyse Windows and Linux binaries

Features that interests us..

- It has many interesting and valuable features
- It is free!
- It can analyse Windows and Linux binaries
- Works with several ISA (x86 64 included)

Features that interests us..

- It has many interesting and valuable features
- It is free!
- It can analyse Windows and Linux binaries
- Works with several ISA (x86 64 included)
- It also has decompiler built in!

Features that interests us..

- It has many interesting and valuable features
- It is free!
- It can analyse Windows and Linux binaries
- Works with several ISA (x86 64 included)
- It also has decompiler built in!
- It also has its own IR- pcode

Scripting with Ghidra

Scripting with Ghidra

- There are several good sources for understanding Ghidra GUI and working with it.
  - https://ghidra.re/

Scripting with Ghidra

- There are several good sources for understanding Ghidra GUI and working with it.
  - https://ghidra.re/
- We will be covering the scripting aspects of Ghidra (via the associated lecture video)
  - Supported languages- Java and Jython (python)
  - It comes with several examples to start with
  -

Other sources

- We will be talking about Fuzzing (in later sessions) and the example fuzzer (Vuzzer) has Ghidra based static analysis.
  - https://github.com/vusec/vuzzer64/blob/master/fuzzer-code/ghidra_BB_weight.py
  - We will walk over simple examples of CFG and call graph
    - Code is available in our github repo
      - cfg-gen-ghidra.py
      - xref-callgraph-gen-ghidra.py