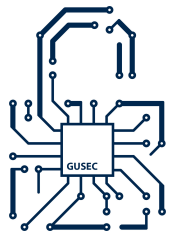
Binary Analysis with Ghidra

Joe Rose

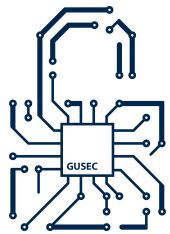
GUSEC

December 11, 2022



Who am I?

- 3rd Year Computer Science
- Secretary of GUSEC
- Massive nerd



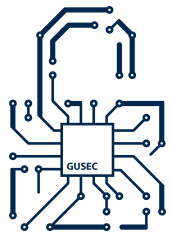
What is Ghidra?

Ghidra is a free and open source reverse engineering tool developed by the National Security Agency (NSA). Ghidra's existence was originally revealed to the public via WikiLeaks in March 2017, but the software itself remained unavailable until its declassification and official release two years later.

Ghidra is written in Java using the Swing framework for the GUI. The decompiler component is written in C++, and is therefore usable in a stand-alone form. Ghidra plug-ins can be developed in Java or Python

Supported Architectures

- Intel x86
- Intel x64
- ARM



What is Binary Analysis?