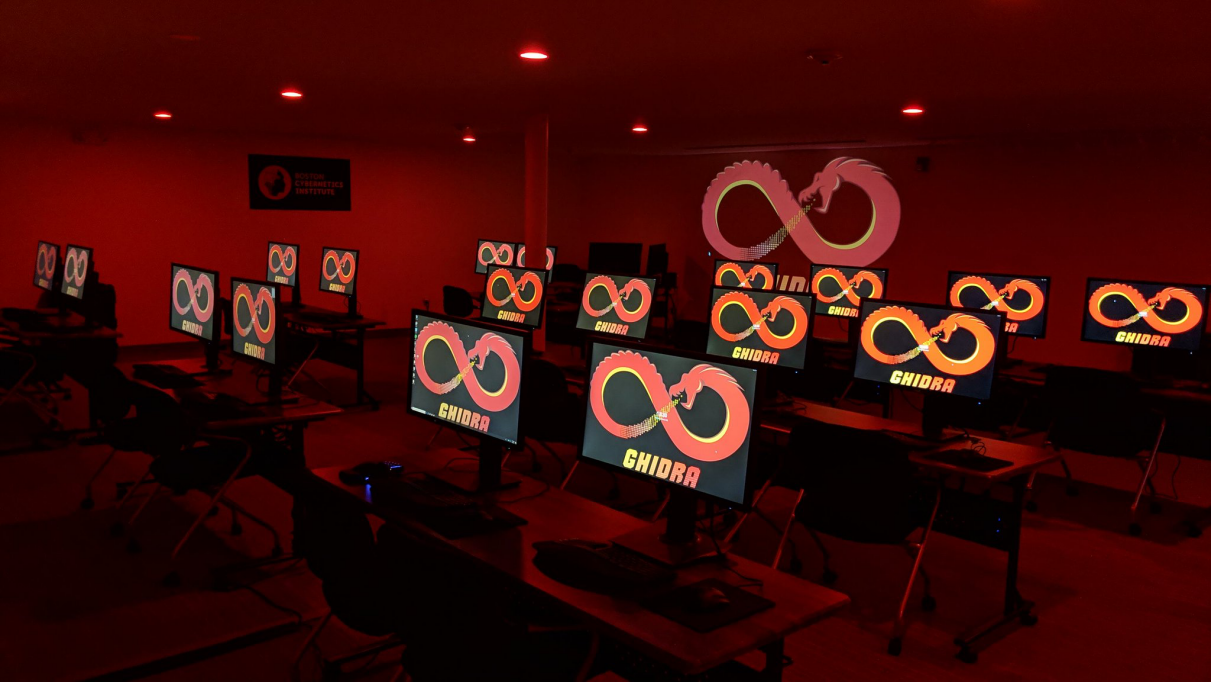
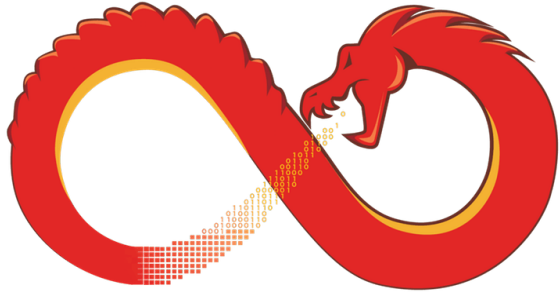

BOSTON CYBERNETICS INSTITUTE
GHIDRA



Reverse Engineering with NSA's Ghidra

COUNTERMEASURE | 2019

Jeremy Blackthorne
Boston Cybernetics Institute

For Audience Members

- All materials are from publicly released tool
- No classified information in this presentation

Jeremy Blackthorne (@0xJeremy)

- **Boston Cybernetics Institute**
  - Co-founder and technical staff
  - Cybersecurity research, consulting, and training
- **Previously at MIT Lincoln Laboratory**
  - Cyber System Assessments Group
  - Researched cyber survivability
- **Education**
  - MS in CS, Rensselaer Polytechnic Institute
  - PhD candidate in CS, Rensselaer Polytechnic Institute
- **United States Marine Corps (2002 – 2006)**
  - 1st Battalion, 7th Marines, 1st MARDIV
  - 3 tours during Operation Iraqi Freedom

Boston Cybernetics Institute (BCI)

- U.S. public benefit corporation founded November 2nd, 2017
- Located next to Harvard University
- Public and private trainings:
  - Reverse-Engineering
  - Malware Analysis
  - Vulnerability Discovery and Exploitation
  - Embedded Systems

Outline

1. Introduction
2. **Ghidra Overview**
3. Ghidra Demo's
4. Management Questions
5. Summary / Questions

What is Ghidra?

- https://www.nsa.gov/ghidra
- "A software reverse engineering (SRE) suite of tools…"
  - https://ghidra-sre.org/
- Free and Open Source Software (FOSS) Apache 2.0 License
- https://github.com/NationalSecurityAgency/ghidra
- Written in Java
  - Requires JDK 11+
  - Runs well on Windows, Linux, and Mac

Ghidra Release

- March 5th, 2019
- RSA Conference
  - **Title:** Come Get Your Free NSA Reverse Engineering Tool!
  - **Author:** Rob Joyce, Senior Advisor, National Security Agency
  - https://www.rsaconference.com/events/us19/agenda/sessions/16608-come-get-your-free-nsa-reverse-engineering-tool

Ghidra Releases

Version	Date
9.0	2019-02-28
9.0.1	2019-03-25
9.0.2	2019-04-03
9.0.4	2019-05-16
9.1	2019-10-23

https://ghidra-sre.org/releaseNotes_9.1_final.html

Ghidra History?

```
user@gunmetal ~/D/ghidra-Ghidra_9.0.2_build> grep -r 199[0-9] * --include "*.java"
Ghidra/Framework/SoftwareModeling/src/main/java/ghidra/program/model/address/AddressOutOfBoundsException.java: * @version 1999-0
Ghidra/Framework/SoftwareModeling/src/main/java/ghidra/program/model/scalar/ScalarOverflowException.java: * @version 1999-03-31
Ghidra/Framework/SoftwareModeling/src/main/java/ghidra/program/model/scalar/ScalarFormat.java: * @version 1999/02/04
Ghidra/Framework/SoftwareModeling/src/main/java/ghidra/program/model/mem/MemoryAccessException.java: * @version 1999-03-31
Ghidra/Framework/Docking/src/test/java/docking/widgets/table/constrainteditor/DateRangeConstraintEditorTest.java:
Ghidra/Framework/Docking/src/test/java/docking/widgets/table/constrainteditor/DateRangeConstraintEditorTest.java:
Ghidra/Framework/Docking/src/test/java/docking/widgets/table/constrainteditor/DateRangeConstraintEditorTest.java:
).getConstraintValueString());
Ghidra/Framework/Docking/src/test/java/docking/widgets/table/constrainteditor/DateRangeConstraintEditorTest.java:
Ghidra/Framework/Docking/src/test/java/docking/widgets/table/constrainteditor/DateRangeConstraintEditorTest.java:
Ghidra/Framework/Docking/src/test/java/docking/widgets/table/constrainteditor/DateRangeConstraintEditorTest.java:
Ghidra/Framework/Docking/src/test/java/docking/widgets/table/constrainteditor/DateRangeConstraintEditorTest.java:
Ghidra/Framework/Generic/src/main/java/generic/hash/SimpleCRC32.java:          0,1996959894,-301047508,-1727442502,124634137,
Ghidra/Framework/Generic/src/main/java/generic/hash/SimpleCRC32.java:          -522852066,-1747789432,162941995,2125561021,-407
Ghidra/Framework/Generic/src/main/java/generic/hash/SimpleCRC32.java:          795835527,1483230225,-1050600021,-1234817731,199
Ghidra/Framework/Generic/src/main/java/generic/hash/SimpleCRC32.java:          -1950435094,-54949764,1658658271,366619977,-1932
Ghidra/Framework/Generic/src/main/java/ghidra/util/exception/NotYetImplementedException.java: * @version 1999/02/05
Ghidra/Features/MicrosoftCodeAnalyzer/src/main/java/ghidra/app/cmd/data/exceptionhandling/EHFunctionInfoModel.java:     public s
Ghidra/Features/MicrosoftCodeAnalyzer/src/main/java/ghidra/app/cmd/data/exceptionhandling/EHFunctionInfoModel.java:     public s
Ghidra/Features/MicrosoftCodeAnalyzer/src/main/java/ghidra/app/cmd/data/exceptionhandling/EHFunctionInfoModel.java:     public s
Ghidra/Features/Base/src/test.slow/java/ghidra/app/merge/listing/FunctionMergerThunk2Test.java: private final static String OVER
Ghidra/Features/Base/src/test.slow/java/ghidra/app/merge/listing/FunctionMergerThunkTest.java:  private final static String OVER
Ghidra/Features/Base/src/test.slow/java/ghidra/app/merge/listing/FunctionMergerThunkTest.java:          chooseVariousOptions("01
Ghidra/Features/Base/src/test.slow/java/ghidra/app/merge/listing/FunctionMergerThunkTest.java:          chooseVariousOptions("01
Ghidra/Features/Base/src/main/java/ghidra/app/util/bin/format/pe/debug/DebugCodeViewConstants.java:     /**Newer CV info, define
```

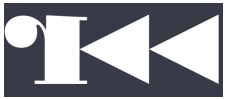
- @0xAlexei first showed me a version of this

Related Tools

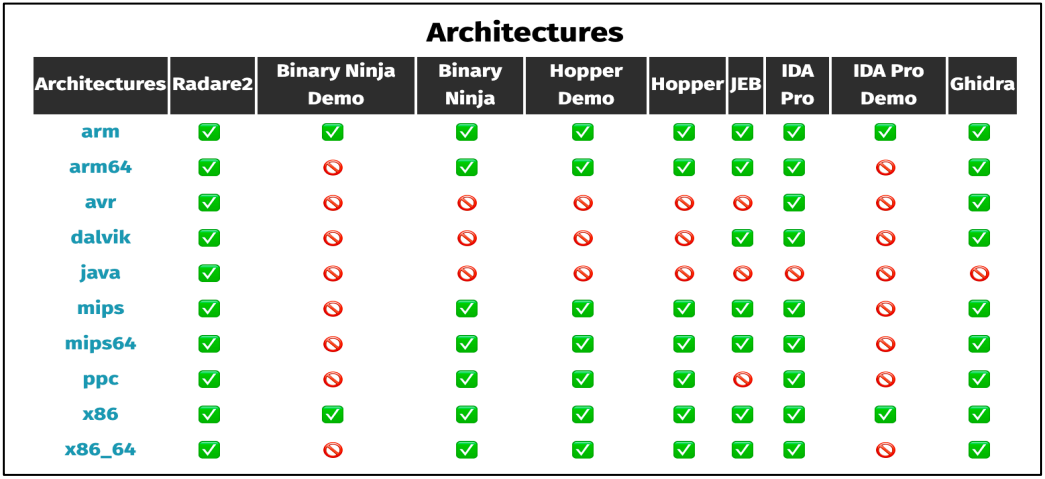
- IDA Pro
  - Free and commercial versions
  - Static and dynamic analysis

- Binary Ninja
  - Student and commercial versions
  - Static only analysis

- Radare2 (r2)
  - Free and open source
  - Static and dynamic



Detailed Tool Comparison



"Unfair comparison between r2, IDA Pro, and Hopper." -https://rada.re/r/cmp.html

Forward Engineering

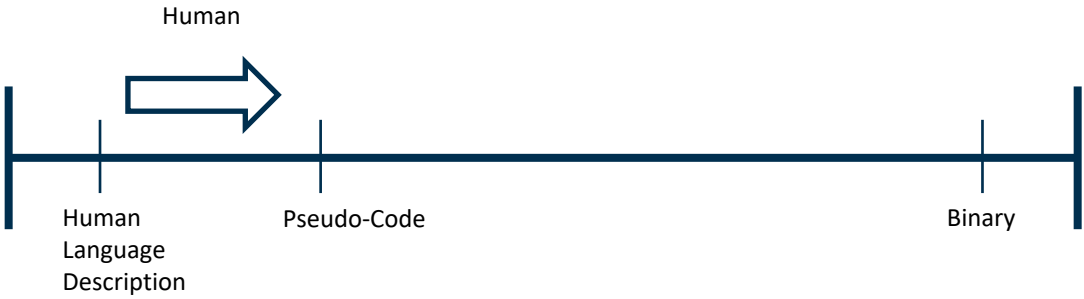
Abstract **Concrete**

Spectrum of Program Abstraction

Forward Engineering

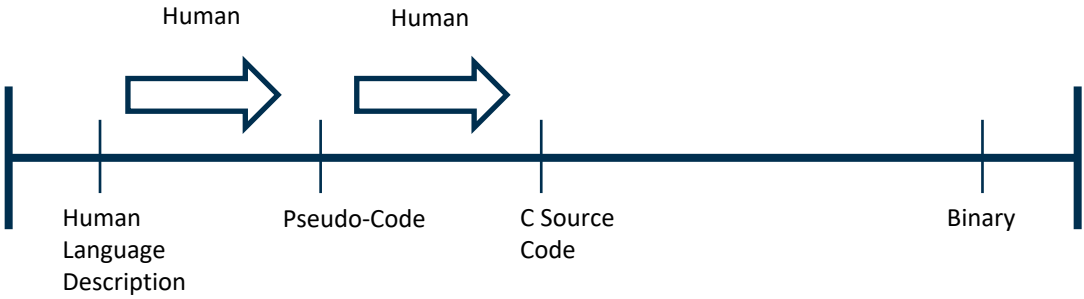
Spectrum of Program Abstraction

Forward Engineering



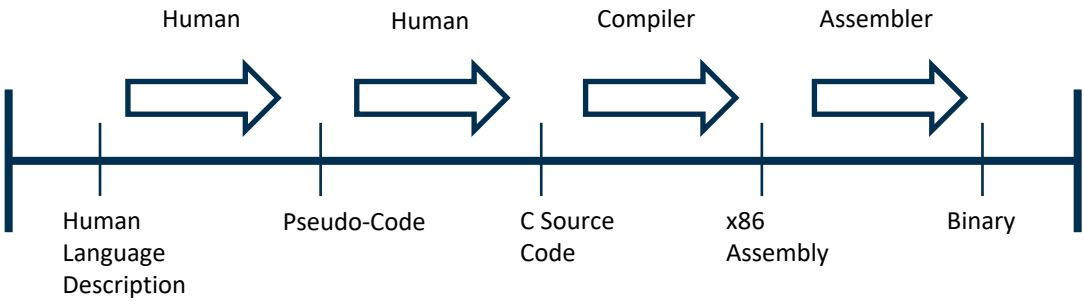
Spectrum of Program Abstraction

Forward Engineering



Spectrum of Program Abstraction

Forward Engineering



Spectrum of Program Abstraction

Reverse Engineering

Abstract **Concrete**

Spectrum of Program Abstraction

Reverse Engineering

Spectrum of Program Abstraction

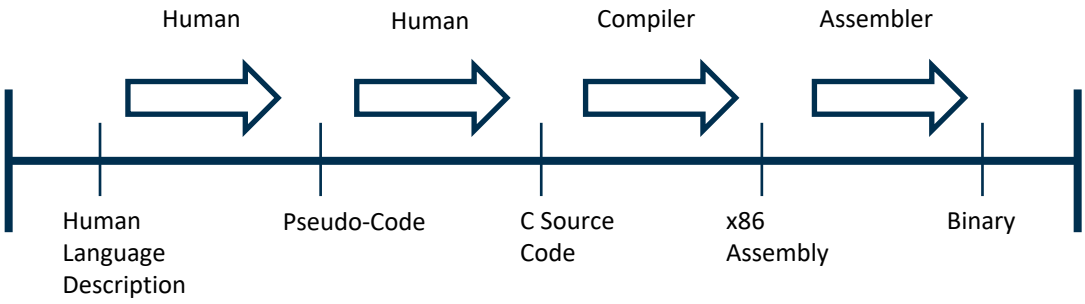
Reverse Engineering

What does this program do?

Abstract **Concrete**

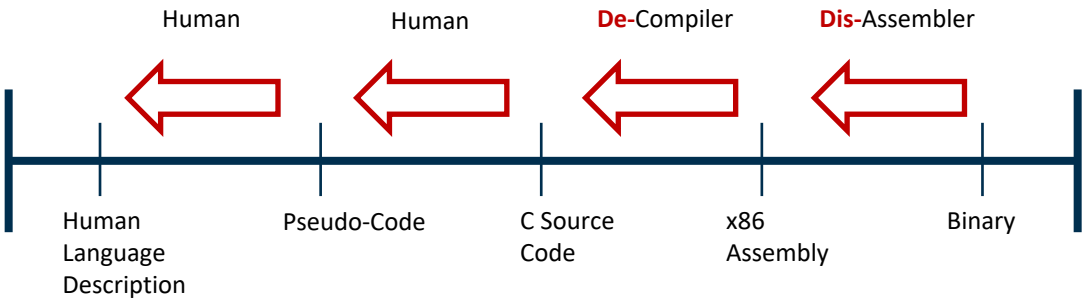
Spectrum of Program Abstraction

Forward Engineering



Spectrum of Program Abstraction

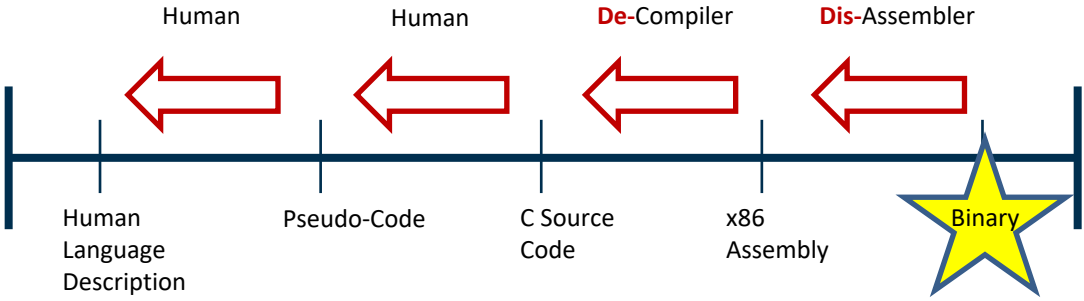
Reverse Engineering



Spectrum of Program Abstraction

Reverse Engineering

What does this program do?



Spectrum of Program Abstraction

Outline

1. Introduction
2. Ghidra Overview
3. **Ghidra Demo's**
4. Management Questions
5. Summary / Questions

Ghidra Demo's!

Outline

1. Introduction
2. Ghidra Overview
3. Ghidra Demo's
4. **Management Questions**
5. Summary / Questions

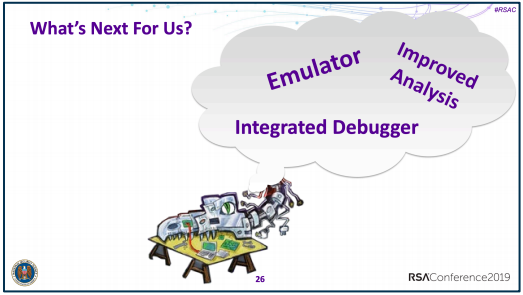
Management Questions

1. Should my team be using this?
2. Will attackers use this against me?
3. If it's free, will this save me money if I switch?

Ghidra Debugger?

1) RSA 2019 Slide by Rob Joyce

2) “Joyce promised, the NSA will release an integrated debugger, a powerful emulator, and improved analysis tools. ”
https://www.theregister.co.uk/2019/03/06/nsa_ghidra_joyce/



3) REcon 2019: Audience member (me) asked:

“When will the debugger be released?”

NSA Presenter: “Probably near the end of summer” (paraphrasing)

Ghidra Debugger Plugin

“not meant to be a full debugger …serves as a small helper tool to assist…

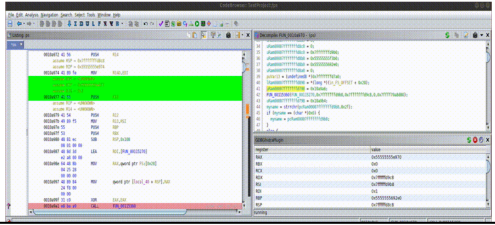
README.md

gdbghidra - a visual bridge between a GDB session and GHIDRA

The purpose of gdbghidra is to provide means during interactive debug sessions in gdb to quickly follow the flow in GHIDRA; similar to our gdbida plugin for IDA Pro. gdbghidra is not meant to be a full debugger. Instead, it merely serves as a small helper tool to assist during interactive debug sessions that make use of a mixture of tools. It provides simple means to quickly follow along a gdb debug session in GHIDRA. Also it does not need any dependencies on the Python side.

gdbghidra consists of the following two parts:

- dist/ghidra_9.0.1_PUBLIC_*_GDBGHIDRA.zip
- data/gdb_ghidra_bridge_client.py : gdb python script



https://github.com/Comsecuris/gdbghidra

Management Questions

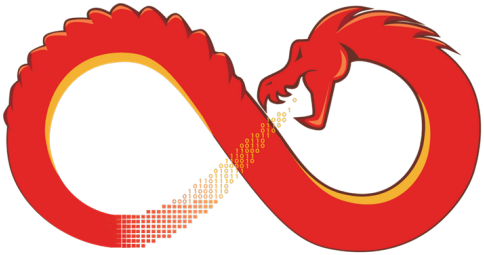
1. Should my team be using this?
2. Will attackers use this against me?
3. If it's free, will this save me money if I switch?

Outline

1. Introduction
2. Ghidra Overview
3. Ghidra Demo's
4. Management Questions
5. **Summary / Questions**

Ghidra Summary

- Free and open source
- Good disassembler
- Good decompiler
- Extendable (Java)
- Scriptable (Python)
- Debugger coming soon(ish)?
- Generally, not a replacement for all other tools
- Avoid learning it at your own peril



Contact Info

- Recent and Upcoming Trainings
  - August 2019: Ringzer0, Las Vegas
  - October 2019: Hack in the Box, Abu Dhabi
  - December 2019: 44Con, London
  - April 2020: Infiltrate, Miami

- Contact
  - Boston-Cyber.Eventbrite.com
  - www.BostonCyber.org
  - info@bostoncyber.org
  - @BosCybernetics
  - @0xJeremy

Appendix

Ghidra Official Materials

- https://www.nsa.gov/ghidra
- https://ghidra-sre.org/
- https://github.com/NationalSecurityAgency/ghidra
- RSA Conference 2019, Get Your Free NSA Reverse Engineering Tool by Rob Joyce, Senior Advisor for Cybersecurity NSA: https://www.rsaconference.com/industry-topics/presentation/come-get-your-free-nsa-reverse-engineering-tool

Ghidra Presentations

INFILTRATE 2019, Three Heads are Better Than One: Mastering Ghidra, Alexei Bulazel and Jeremy Blackthorne
https://vimeo.com/335158460
https://github.com/0xAlexei/INFILTRATE2019/blob/master/INFILTRATE%20Ghidra%20Slides.pdf

Texas Cyber Summit 2019, Ghidra for the begineer reverse engineering
https://texascybersummitii2019.sched.com/event/UQhj/re-1012-ghidra-for-the-begineer-reverse-enginering?iframe=yes&w=100%&sidebar=yes&bg=dark

Texas Cyber Summit 2019, Intro to Reverse Engineering with Ghidra: Taming the Dragon
https://texascybersummitii2019.sched.com/event/UQr0/re-1080-intro-to-reverse-engineering-with-ghidra-taming-the-dragon?iframe=yes&w=100%&sidebar=yes&bg=dark

Ghidra Trainings

- https://ghidra.re/online-courses/
- https://www.blackhat.com/tr-19/training/schedule/index.html#reverse-engineering-firmware-with-ghidra-17037
- https://cyberweek.ae/session/reverse-engineering-with-ghidra/
- https://ringzer0.training/reverse-engineering-with-ghidra.html
- https://44con.com/44con-training/reverse-engineering-with-ghidra/
- https://infiltratecon.com/conference/training/reverse-engineering-with-ghidra.html

Ghidra Interoperability Plugins

- https://github.com/radareorg/r2ghidra-dec
- https://github.com/daenerys-sre/source
- https://github.com/Cisco-Talos/GhIDA
- https://github.com/Comsecuris/gdbghidra