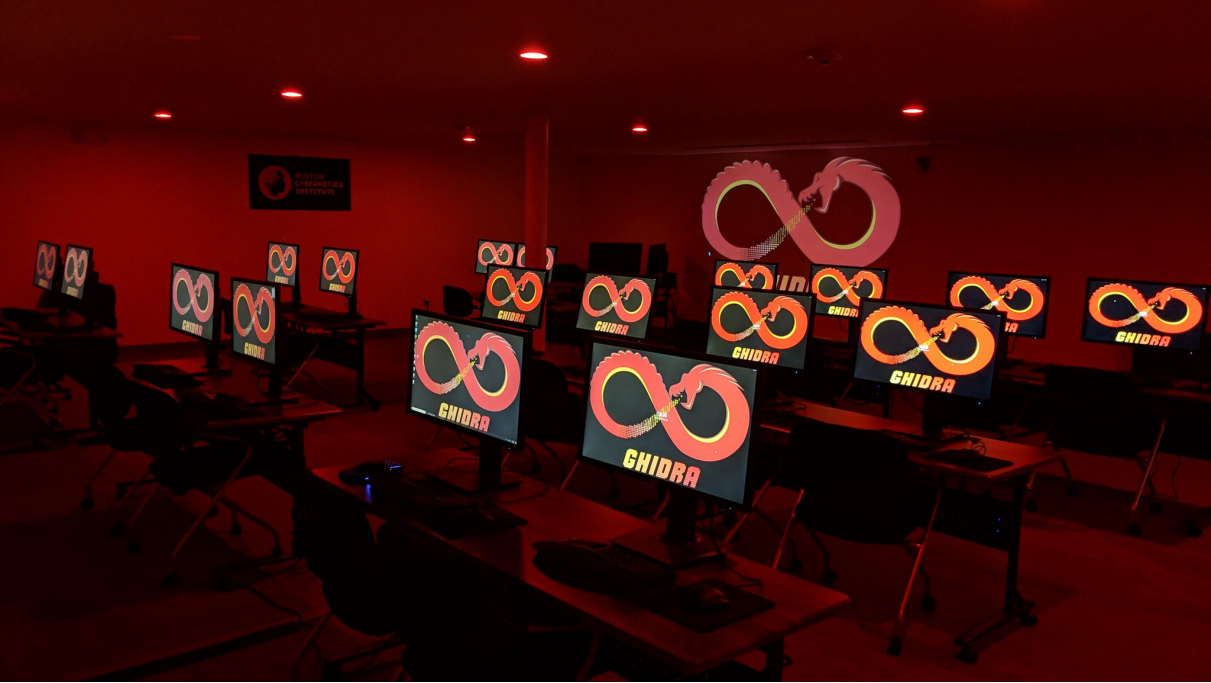
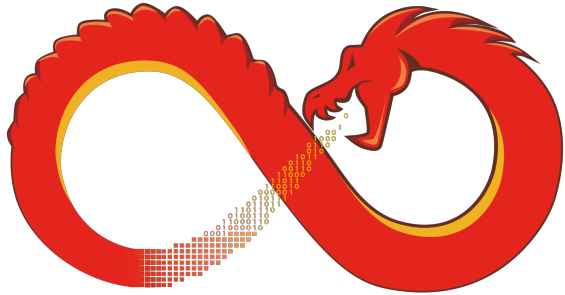

BOSTON CYBERNETICS INSTITUTE
GHIDRA



Reverse Engineering with NSA's Ghidra

Jeremy Blackthorne

Boston Security Meetup

April 18th, 2019

https://github.com/JeremyBlackthorne/Public-Presentations

For Cleared Audience Members

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

Introduction

USMC

- 1st Battalion / 7th Marines, 2002 – 2006
- MOS 0311: 2003, 2005
- MOS 8541: 2006

Education

- BS in CS, University of Michigan-Dearborn, 2007 – 2011
- MS in CS, Rensselaer Polytechnic Institute, 2011 – 2015
- PhD candidate in CS, Rensselaer Polytechnic Institute

MIT Lincoln Laboratory

- Cyber System Assessments Group, 2015 – 2017
- Researched cyber survivability
- Trained Navy, Air Force, and SOCOM

Boston Cybernetics Institute

- Public benefit corporation (PBC) founded 2017
- **Mission:** Provide cybersecurity training and research in support of national defense
- Located at 30 JFK St, Cambridge (Harvard Square)
- Public and Private Classes:
  - Malware Analysis
  - Reverse-Engineering
  - Vulnerability Assessment
  - Embedded Systems
- Contact
  - Boston-Cyber.Eventbrite.com
  - www.BostonCyber.org
  - @BosCybernetics

What is 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

Demo!

- Example binary pulled from http://reversing.kr
- EasyCrack.exe

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 History?

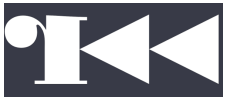
```
user@gunmetal ~/D/ghidra-Ghidra_9.0.2_build> grep -r 199[0-9] * --include "*.java"
Ghidra/Framework/SoftwareModeling/src/main/java/ghidra/program/model/address/AddressOutOfBoundsException.java: * @version 1999-0
Ghidra/Framework/SoftwareModeling/src/main/java/ghidra/program/model/scalar/ScalarOverflowException.java: * @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
```

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

Architectures

Architectures	Radare2	Binary Ninja Demo	Binary Ninja	Hopper Demo	Hopper	JEB	IDA Pro	IDA Pro Demo
arm	✅	✅	✅	✅	✅	✅	✅	✅
arm64	✅	🚫	✅	✅	✅	✅	✅	🚫
avr	✅	🚫	✅	🚫	🚫	🚫	✅	🚫
dalvik	✅	🚫	✅	🚫	🚫	✅	✅	🚫
java	✅	🚫	🚫	🚫	🚫	🚫	🚫	🚫
mips	✅	🚫	✅	✅	✅	✅	✅	🚫
mips64	✅	🚫	✅	✅	✅	✅	✅	🚫
ppc	✅	🚫	🚫	✅	✅	🚫	✅	🚫
x86	✅	✅	✅	✅	✅	✅	✅	✅
x86_64	✅	🚫	✅	✅	✅	✅	✅	🚫

“Unfair comparison between **r2**, **IDA Pro** and **Hopper**.”

-https://rada.re/r/cmp.html

Summary

Ghidra:

- Free and open source: https://ghidra-sre.org/
- Extendable
- Scriptable
- Good disassembler and decompiler
- “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/

Contact Info:

- jblackthorne@bostoncyber.org
- @0xJeremy