Cybersecurity & Information Systems
Information Analysis Center

CSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Current Landscape and Technologies of Binary Code Scanning Tools

Report Number:

CSIAC-BCO-2023-447

Completed June 2023

CSIAC is a U.S. Department of Defense
Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443-360-4600

REPORT PREPARED BY:
Olutobi Oyinlade
Office: CSIAC

Information contained in this report does not constitute endorsement by the U.S. Department of Defense of any nonfederal entity or technology sponsored by a nonfederal entity.

CSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. CSIAC is operated by the SURVICE Engineering Company.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 06-06-2023	**2. REPORT TYPE** Technical Research Report	**3. DATES COVERED** *(From – To)*

4. TITLE AND SUBTITLE Current Landscape and Technologies of Binary Code Scanning Tools	**5a. CONTRACT NUMBER** FA8075-21-D-0001 **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Olutobi Oyinlade	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Cybersecurity & Information Systems Information Analysis Center (CSIAC) SURVICE Engineering Company 4695 Millennium Drive Belcamp, MD 21017-1505	**8. PERFORMING ORGANIZATION REPORT NUMBER** CSIAC-BCO-2023-447
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center (DTIC) 8725 John J. Kingman Road Fort Belvoir, VA 22060-6218	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This technical inquiry report provides information on the current landscape and technologies used to scan firmware samples for detection of cybervulnerabilities. The aim of this research is to identify and describe what binary code scanning (also called binary code analysis [BCA]) tools exist to scan firmware samples for the detection of cybervulnerabilities. The Cybersecurity & Information Systems Information Analysis Center subject matter experts researched online sources, open-source documents, and published articles on the topic. A wide range of open source and commercially available tools for performing BCA was found. This report includes details on the usage of BCA tools and a brief description of 12 tools identified, as well as resources for comparing BCA tools.

15. SUBJECT TERMS
binary code scanning, cybervulnerabilities, code scanners, source code scanners

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Ted Welsh, CSIAC Director
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	12	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

About DTIC and CSIAC

DTIC and CSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense's (DoD's) annual multibillion-dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision-makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (DoDIAC), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a DoDIAC sponsored by DTIC to provide expertise in four technical focus areas: cybersecurity; knowledge management & information sharing; modeling & simulation; and software data & analysis. CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

TI Research

A chief service of the U.S. Department of Defense's Information Analysis Centers is free technical inquiry (TI) research limited to four research hours per inquiry. This TI response report summarizes the research findings of one such inquiry. Given the limited duration of the research effort, this report is not intended to be a deep, comprehensive analysis but rather a curated compilation of relevant information to give the reader/inquirer a "head start" or direction for continued research.

Abstract

This technical inquiry report provides information on the current landscape and technologies used to scan firmware samples for detection of cybervulnerabilities. The aim of this research is to identify and describe what binary code scanning (also called binary code analysis [BCA]) tools exist to scan firmware samples for the detection of cybervulnerabilities. The Cybersecurity & Information Systems Information Analysis Center subject matter experts researched online sources, open-source documents, and published articles on the topic. A wide range of open source and commercially available tools for performing BCA was found. This report includes details on the usage of BCA tools and a brief description of 12 tools identified, as well as resources for comparing BCA tools.

Contents

1.0 TI Request

1.1 Inquiry

What tools exist for detecting cybervulnerabilities in firmware samples? In addition, what binary code scanning (also called binary code analysis [BCA]) tools exist to scan firmware samples for the detection of cyber vulnerabilities? The National Institute of Science and Technology Software Quality Group maintains a list of a few such tools, but there are likely others. The inquirer is seeking to identify a pool of binary code scanner tools that can be used to scan a set of 10–15 firmware samples to identify potential cybervulnerabilities.

1.2 Description

The purpose of this TI request is to identify and describe binary code scanner tools that can be used to detect cybervulnerabilities within firmware samples. Both open-source and commercially available tools were researched, and 12 tools were identified. Binary analysis solutions are critical for identifying open-source components, security vulnerabilities, license obligations, and additional sensitive information that could lead to a breach.

2.0 TI Response

2.1 Introduction

BCA, also referred to as binary analysis or code review, is a form of static analysis that does threat assessment and vulnerability testing at the binary code level. This analysis looks at the raw binaries that compose a complete application, which is especially helpful when there is no access to the source code. Static binary code scanners are used like source code security analyzers [1]. However, they detect vulnerabilities through disassembly and pattern recognition [2]. One advantage that binary code scanners have over source code scanners is the ability to look at the compiled result and factor in any vulnerabilities created by the compiler itself. Furthermore, library function code or other code delivered only as a binary can be examined [3].

2.2 Binary Code Scanners

Finding commercially available binary code scanners that strictly fit into the definition of this class of tool was challenging. The following list includes tools that assist in performing binary analysis and service providers that perform binary analysis. Binary analysis tools are typically used for binary analysis, malware analysis, and reverse engineering. Users for these tools include malware analysts and security professionals.

- Interactive Disassembler (IDA) Pro [4]:

  IDA Pro as a disassembler is capable of creating maps of their execution to show the binary instructions that are actually executed by the processor in a symbolic representation (assembly language). Advanced techniques have been implemented into IDA Pro so that it can generate assembly language source code from machine-executable code and make this complex code more human-readable.

- Binary Analysis Platform (BAP) [5]:

  The main purpose of BAP is to provide a toolkit for program analysis. This platform comes as a complete package with a set of tools, libraries, and related plugins. There are bindings available for C, Python, and Rust.

- Binary Ninja [6]:

  Binary Ninja is an interactive decompiler, disassembler, debugger, and binary analysis platform built by reverse engineers, for reverse engineers. Developed with a focus on delivering a high-quality [application programming interface] API for automation and a clean and usable [graphical user interface] GUI, Binary Ninja is in active use by malware analysts, vulnerability researchers, and software developers worldwide. Decompile software built for many common architectures on Windows, macOS, and Linux for a single price, or try out our limited (but free!) Cloud version.

- Ghidra [7]:

  A software reverse engineering (SRE) suite of tools developed by [the National Security Agency's] NSA's Research Directorate in support of the cybersecurity mission.

- Manticore (Dynamic Binary Analysis Tool) [8]

  Manticore is a so-called symbolic execution tool to perform a binary analysis. It supports Linux [executable and linkable format] ELF binaries and Ethereum smart contracts. The tool helps with researching binaries and their behavior. This might be useful to learn how malware works and troubleshooting.

- CodeSonar [9]:

  CodeSonar is a static code analysis solution that helps you find and understand quality and security defects in your source code or binaries. CodeSonar makes it easy to integrate Static application security testing (SAST) into your development process with support for over 100 compilers and compiler versions, numerous integrations to popular development tools and [integrated development environments] IDEs, and whole-program analysis that finds issues other tools miss.

- OllyDbg [10, 11]:

  OllyDbg is a 32-bit debugging tool used to analyze binary code. Its popularity is tied to the fact that people can do so despite not having access to the source code. OllyDbg can be used to evaluate and debug malware. OllyDbg is a popular debugger due to its ease of use and being freeware [10].

- x64dbg [12]:

  x64dbg is a debugging software that can debug x64 and x32 applications.

- Radare [13]:

  Radare is the highly featured reverse engineering framework.

- Black Duck Binary Analysis [14]:

  Black Duck® Binary Analysis gives you visibility into open source and third-party dependencies that have been compiled into executables, libraries, containers, and firmware. You can analyze individual files using an intuitive user interface or Black Duck multifactor open source detection, which automates the scanning of binary artifacts.

- Fortify [15]:

  OpenText™ Fortify™ Static Code Analyzer pinpoints the root cause of security vulnerabilities in the source code, prioritizes the most serious issues, and provides detailed guidance on how to fix them. Plus, centralized software security management helps developers resolve issues in less time.

- Contrast Security Contrast Scan [16]:

  Contrast Scan provides static code scanning with 30+ languages and frameworks supported. In some cases, runtime security with [interactive application security testing] IAST needs to be supplemented with static scanning to meet the needs of your internal controls or potentially cover some legacy application code. Contrast Scan meets those needs to make code security testing as routine as a code commit while focusing on the most imperative vulnerabilities to deliver fast, accurate, and actionable results.

References

[1] National Institute of Standards and Technology. "Source Code Security Analyzers." *NIST,* https://www.nist.gov/itl/ssd/software-quality-group/source-code-security-analyzers, accessed June 2023.

[2] National Institute of Standards and Technology. "Binary Code Scanners." *NIST,* https://www.nist.gov/itl/ssd/software-quality-group/binary-code-scanners, accessed June 2023.

[3] Contrast Security. "What Is Binary Code Analysis?" *Binary Code Analysis,* https://www.contrastsecurity.com/glossary/binary-code-analysis, accessed June 2023.

[4] Hex-Rays. "A Powerful Disassembler and a Versatile Debugger." *IDA Pro*, https://hex-rays.com/ida-pro/, accessed June 2023.

[5] Linux Security. "BAP (Binary Analysis Platform)." *Training Security Tools*, https://linuxsecurity.expert/tools/bap/, accessed June 2023.

[6] Vector 35. "Binary Ninja: A Major Version for Major Features. 4.0 Is out With a Massive Set of New Features and Fixes." *Binary Ninja,* https://binary.ninja/, accessed June 2023.

[7] National Security Agency. "GHIDRA: A Software Reverse Engineering (SRE) Sweet of Tools Developed by NSA's Research Directorate in Support of the Cybersecurity Mission." *Ghidra,* https://ghidra-sre.org/, accessed June 2023.

[8] Linux Security. "Manticore." *Training Security Tools,* https://linuxsecurity.expert/tools/manticore/, accessed June 2023.

[9] CodeSecure. "CodeSonar." *CS: CodeSecure,* https://codesecure.com/our-products/codesonar/, accessed June 2023.

[10] Appleby, T. "OllyDbg." *Infosec*, https://resources.infosecinstitute.com/topic/ollydbg/#:~:text=OllyDbg%20is%20a%2032%2Dbit,of%20use%20and%20being%20freeware, 28 August 2019.

[11] Yuschuk, O. "OllyDbg Is a 32-Bit Assembler Level Analysing Debugger for Microsoft® Windows®." *OllyDbg,* https://www.ollydbg.de/, 21 April 2022.

[12] x64dbg. "x64dbg: An Open-Source x64/x32 Debugger for Windows." *x64dbg,* https://x64dbg.com/, accessed June 2023.

[13] Alvarez, S. "Free Reversing Toolkit." *Radare,* https://rada.re/n/, accessed June 2023.

[14] Synopsis, Inc. "Black Duck Binary Analysis." *Synopsis,* https://www.synopsys.com/software-integrity/software-composition-analysis-tools/binary-analysis.html*,* accessed June 2023.

[15] Open Text Corporation. "OpenText Fortify Static Code Analyzer." *OpenText,* https://www.opentext.com/products/fortify-static-code-analyzer, accessed June 2023.

[16] Contrast Security. "Contrast Scan." *Contrast Security.* https://www.contrastsecurity.com/contrast-scan, accessed June 2023.

Biography

Olutobi Oyinlade, Ph.D., is a development, security, and operations (DevSecOps) engineer of the SURVICE Engineering Company. She possesses a Doctor of Philosophy in biochemistry and cellular and molecular biology from Johns Hopkins School of Medicine. She transitioned to Cloud Engineering with over 8 years of experience working with GovCloud. She has acquired several professional certificates in Cloud Engineering and is considered an expert in DevSecOps.