INL/EXP-24-79608-Revision-0

Forensic Analysis of SOHO Router Binaries

August 2024

Clara Beatrice Ness

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXP-24-79608-Revision-0

Forensic Analysis of SOHO Router Binaries

Clara Beatrice Ness

August 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

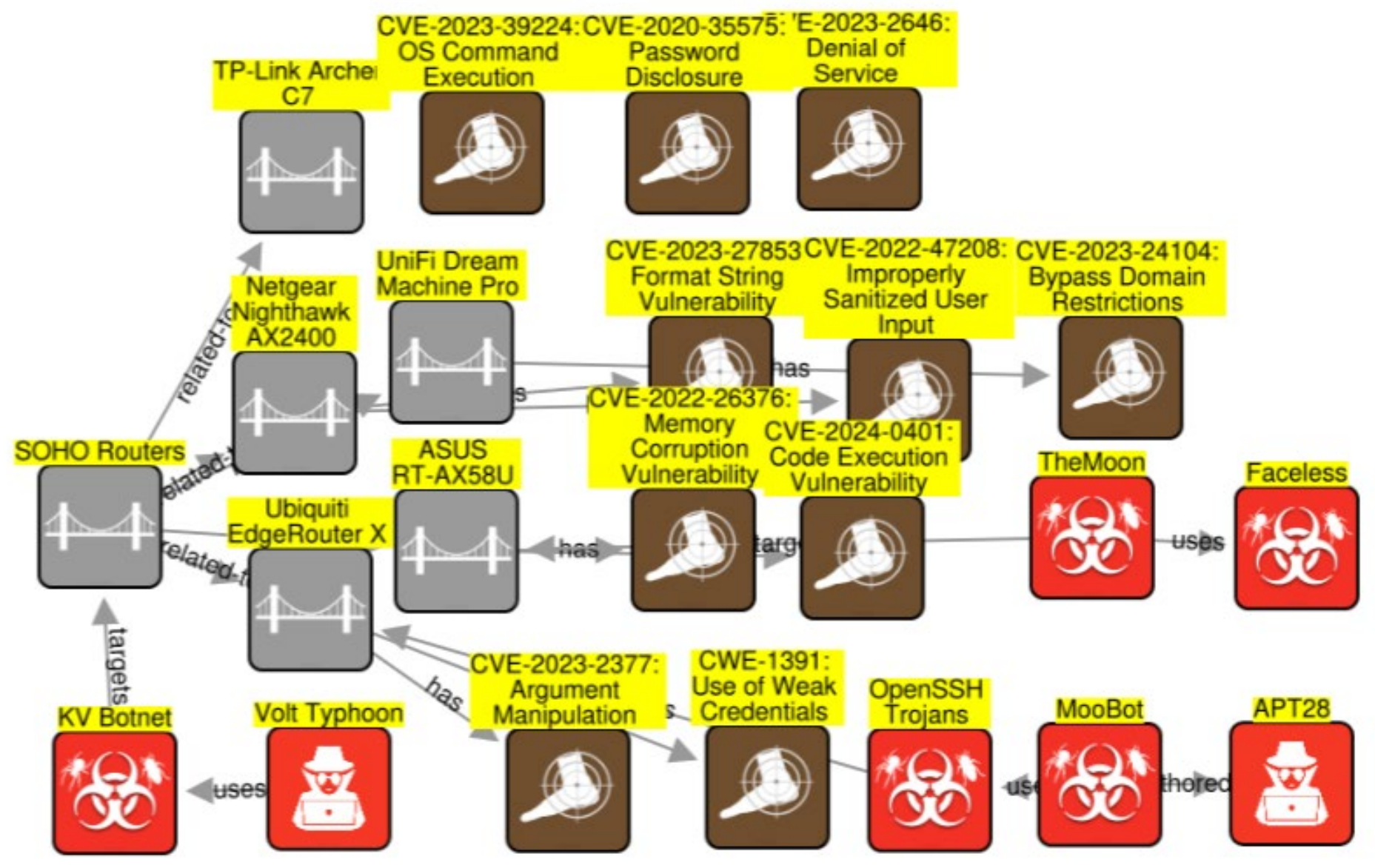
Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Forensic Analysis of SOHO Router Binaries

Clara Ness | The University of Tulsa | D320 | Mentor: Dr. Shaya Wolf

Problem

Small Office/Home Office (SOHO) routers are used by millions of consumers across the United States, and are commensurately vulnerable. **Forensic analysis of SOHO router firmware** helps to understand and mitigate those vulnerabilities.



TP-Link Archer C7
CVE-2023-39224: OS Command Execution
CVE-2020-35575: Password Disclosure
E-2023-2646: Denial of Service
Netgear Nighthawk AX2400
UniFi Dream Machine Pro
CVE-2023-27853: Format String Vulnerability
CVE-2022-47208: Improperly Sanitized User Input
CVE-2023-24104: Bypass Domain Restrictions
SOHO Routers
ASUS RT-AX58U
CVE-2022-26376: Memory Corruption Vulnerability
CVE-2024-0401: Code Execution Vulnerability
TheMoon
Faceless
Ubiquiti EdgeRouter X
related-to
has
targets
uses
CVE-2023-2377: Argument Manipulation
CWE-1391: Use of Weak Credentials
OpenSSH Trojans
KV Botnet
Volt Typhoon
MooBot
APT28

Figure 1: A visual representation of recent SOHO router vulnerabilities using Structured Threat Intelligence Graph (STIG). [1]

Introduction

Analysis starts with extraction of publicly-available firmware for SOHO routers in a multitude of formats, such as .bin, .img, and .w.

- Tools like Binwalk are used to decompress firmware from ASUS, Netgear, Ubiquiti, and TP-Link routers **into a complete squashfs Linux filesystem** [2].
- Analysis focused especially on analyzing BusyBox executables, a software suite that provides several Unix utilities in a single file [3]

Impact

The BusyBox version inside each router filesystem **rarely changed,** even across **months or years of firmware updates.** This demonstrates the importance of **constant firmware scrutiny**, by both venders and consumers, to protect against security vulnerabilities.

Analysis

BinWalk

- Firmware analysis tool for analyzing, reverse engineering, and extracting firmware images
- Used to **extract firmware images** for Ubiquiti, TP-Link, Netgear routers
- A different tool, called UnBlob, was used to extract ASUS routers. [4]
- Binwalk was also used to **build entropy graphs, extract Linux kernel images, and identify CPU architectures.**

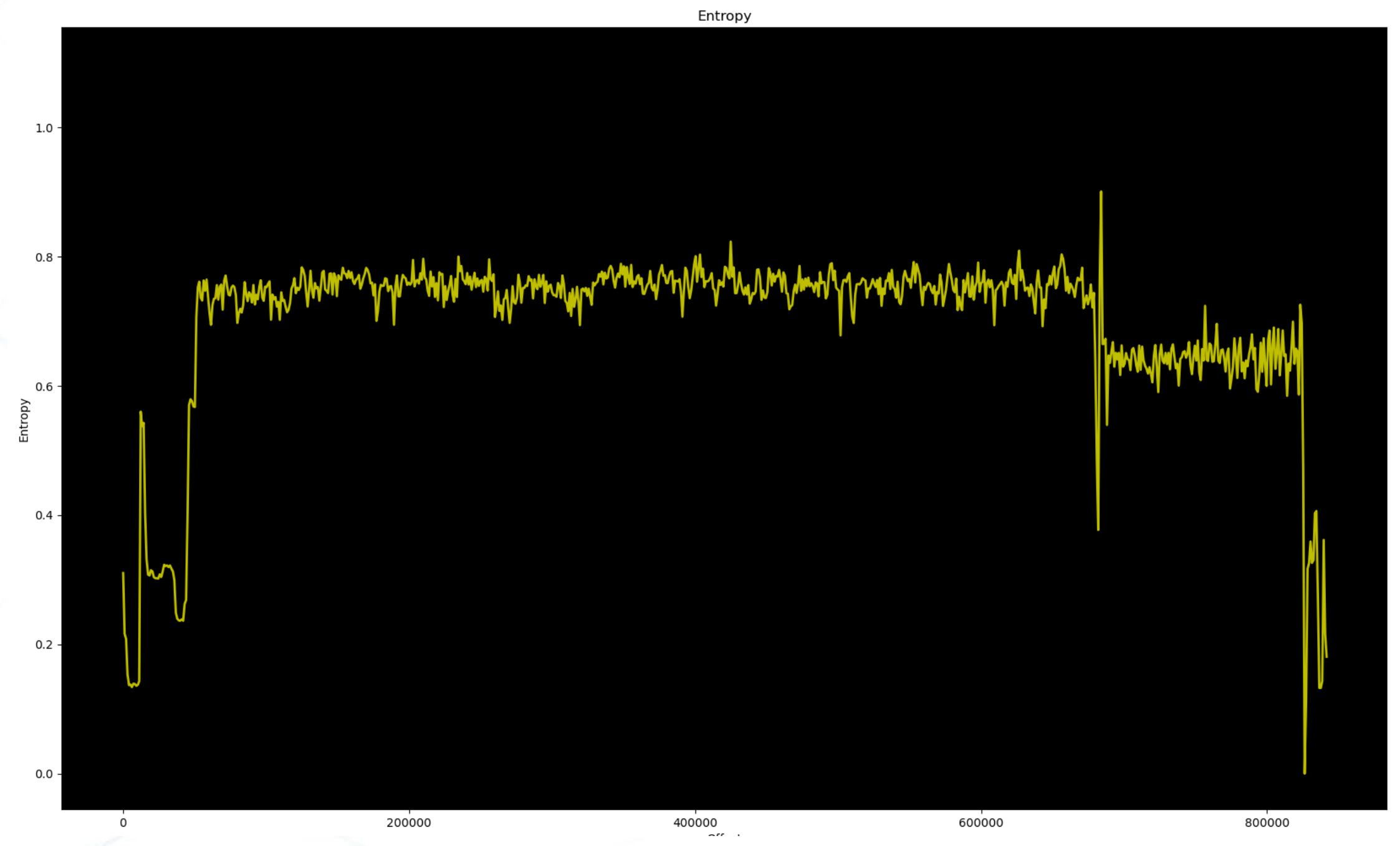
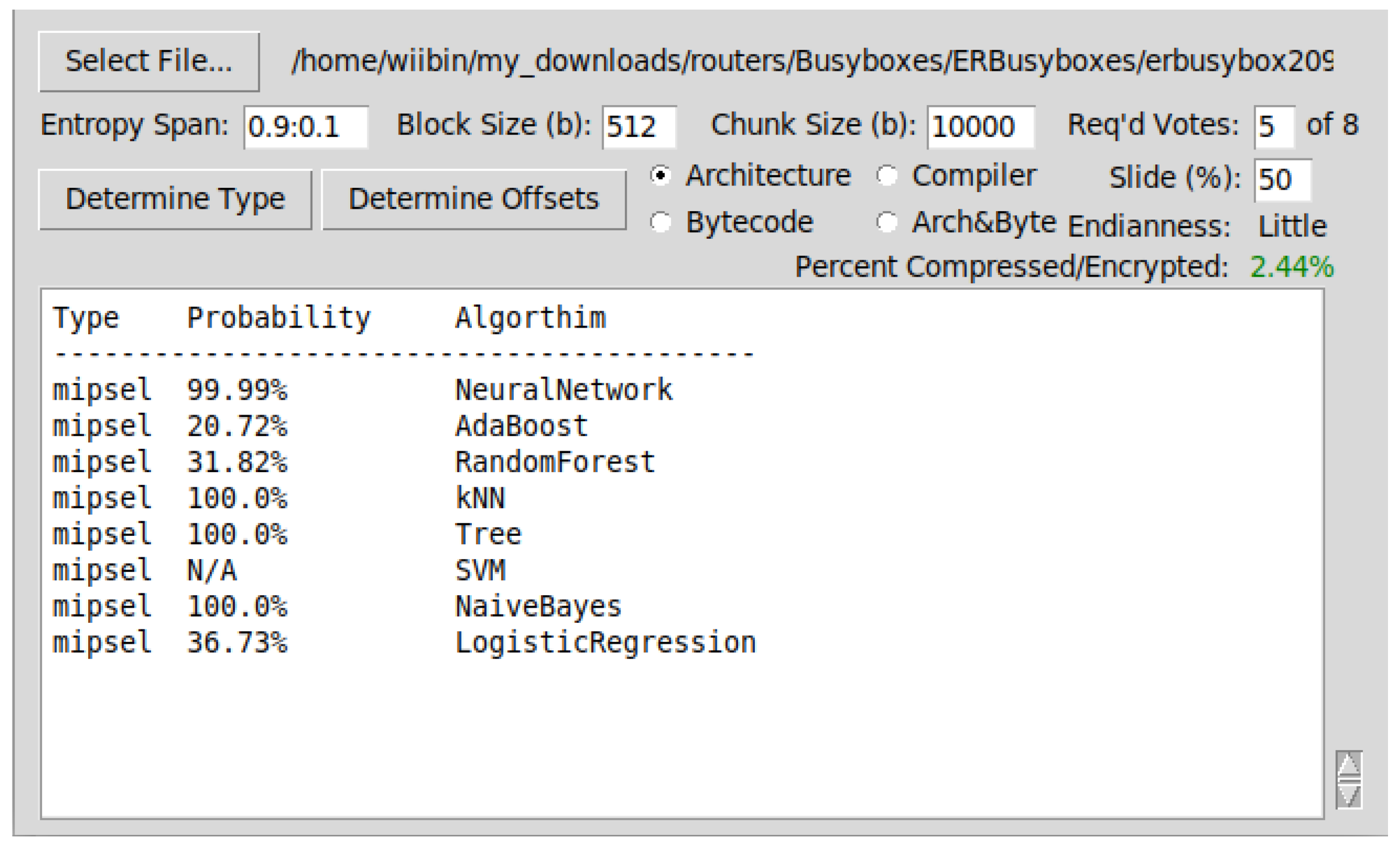


Figure 2: The entropy graph of the Unifi UDM Pro v1.9.2 BusyBox executable.

WiiBin

- After firmware images have been decompressed into a filesystem, WiiBin processes the binaries inside to find their **endianness, architecture, the percent compressed/encrypted, and compiler data**. [5]
- WiiBin can be scripted to analyze multiple files at once
- Found **near-exact data** for Busyboxes from **different versions of the same firmware**



/home/wiibin/my_downloads/routers/Busyboxes/ERBusyboxes/erbusybox209

Entropy Span: 0.9:0.1 Block Size (b): 512 Chunk Size (b): 10000 Req'd Votes: 5 of 8

● Architecture ○ Compiler Slide (%): 50

○ Bytecode ○ Arch&Byte Endianness: Little

Percent Compressed/Encrypted: 2.44%

```
Type    Probability     Algorthim
-----------------------------------------
mipsel  99.99%          NeuralNetwork
mipsel  20.72%          AdaBoost
mipsel  31.82%          RandomForest
mipsel  100.0%          kNN
mipsel  100.0%          Tree
mipsel  N/A             SVM
mipsel  100.0%          NaiveBayes
mipsel  36.73%          LogisticRegression
```

Figure 3: Determining the architecture of a Ubiquiti EdgeRouter X In WiiBin using eight different machine learning algorithms.

@DisCo

- @DisCo is a machine learning tool used **to determine function similarity in disassembled binaries.** [6]
- Analyzed similarities and determined versions of extracted BusyBox files from each router; 4-6 versions of each router were used
- Surprisingly, there was **very little overlap** between files that did not derive from the same router.
- Venders from all five routers utilized the **same version** of the BusyBox software across **different firmware updates**
- These files all contained the **same open-source software**, so such distinct differences between venders was unexpected.

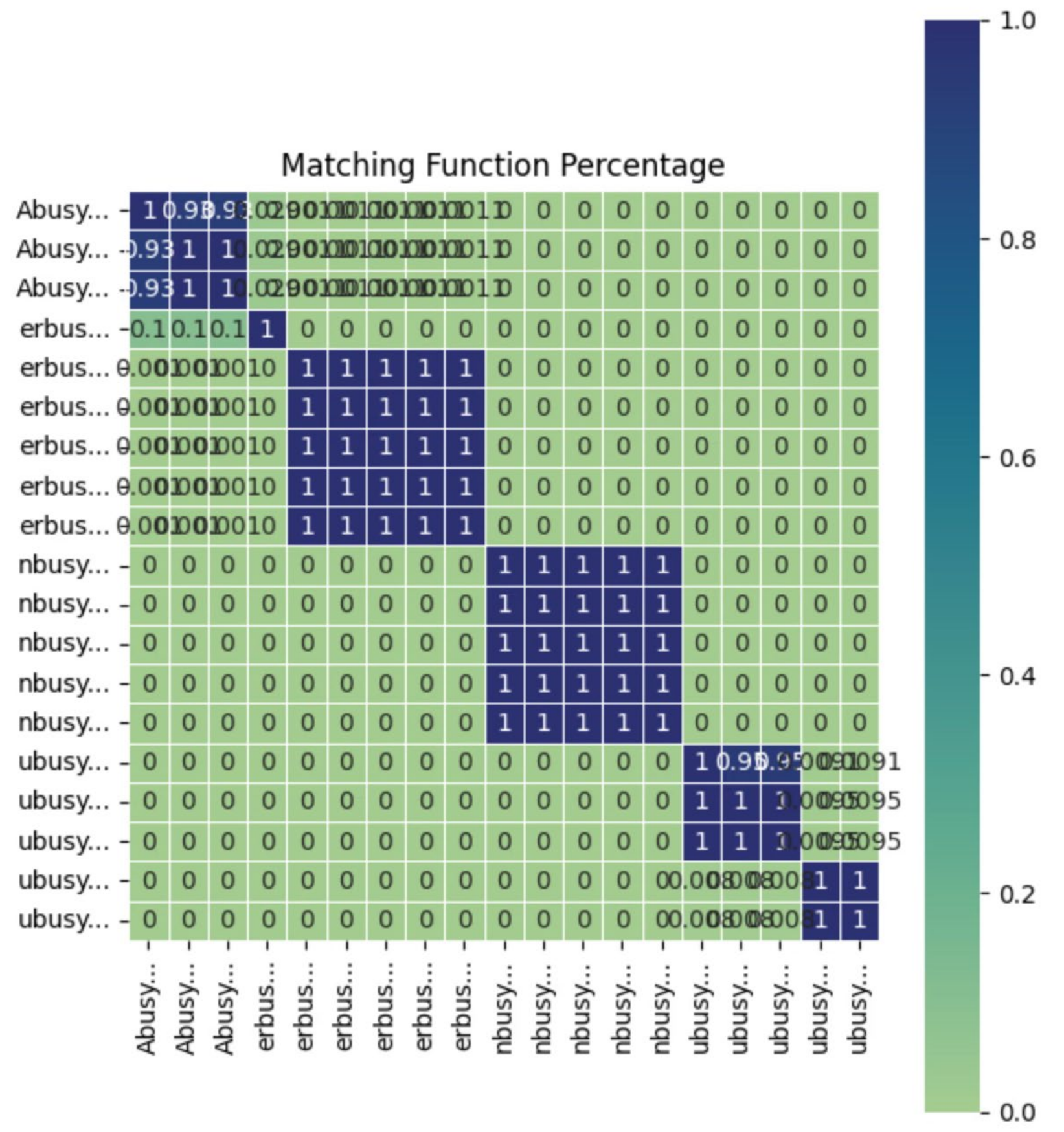


Figure 4: A @DisCo similarity heat map comparing all 19 router Busybox files against each other. Most Busyboxes from related versions are exact matches, with no similarities to other routers.

References:

[1] idaholab, “STIG,” *GitHub*, Aug. 27, 2019. https://github.com/idaholab/STIG (accessed Jul. 22, 2024).

[2]ReFirmLabs, “binwalk,” *GitHub*, Jan. 04, 2021. https://github.com/ReFirmLabs/binwalk (accessed Jul. 22, 2024).

[3] E. Andersen, “BusyBox: The Swiss Army Knife of Embedded Linux,” *busybox.net*. https://busybox.net/about.html (accessed Jul. 22, 2024).

[4] ONEKEY, “unblob,” *GitHub*, Jul. 22, 2024. https://github.com/onekey-sec/unblob (accessed Jul. 22, 2024).

[5] idaholab, “WiiBin,” *GitHub*, Jun. 21, 2024. https://github.com/idaholab/WiiBin (accessed Jul. 22, 2024).

[6] idaholab, “atDisco,” *GitHub*, Nov. 28, 2023. https://github.com/idaholab/atDisco (accessed Jul. 22, 2024).

www.inl.gov
INL/EXP-24-79608

THE UNIVERSITY *of* TULSA

Idaho National Laboratory