

PATE Verifier User Manual (Version 0.9)

Galois (pate-darpa-amp@galois.com)

July 10, 2024

The PATE verifier is a static relational verification tool designed to ensure that security micropatches applied to binaries are safe and free from unintended consequences. The verifier generates detailed reports that precisely identify the conditions under which two binary versions exhibit identical behavior. This equivalence information can reveal any unforeseen side effects of a binary patch, such as changes to program behaviors beyond those intended by the original fix.

The verifier is intended to enable users to:

- precisely reason about the effects of patches applied to binaries,
- explain potential differences in observable behaviors, accounting for all possible execution paths, and thus
- reduce the time required to develop safe binary patches.

Contents

1	Introduction	3
2	Installing the PATE Verifier	3
2.1	Recommended: Docker Container Image	3
2.2	Alternative: Building from Source	4
3	Invoking the PATE Verifier	4
4	The PATE Terminal UI	6
4.1	Example Usage	7
4.2	Status Indicators	10
4.3	Navigation Commands	11
4.4	Diagnostic Commands	11
5	The PATE Binary Ninja Plugin	11
5.1	Installation	11
5.2	Usage	12
5.3	Replays	14
5.4	MCAD Integration	15
6	Acknowledgements	16

1 Introduction

This User Manual describes the PATE verifier as of July 2024, and is maintained in the PATE source repository¹.

The PATE verifier is a static relational verifier for binaries that builds assurance that micropatches have not introduced any adverse effects. The verifier is a static relational verifier that attempts to prove that two binaries have the same observable behaviors. When it cannot, the verifier provides detailed explanations that precisely characterize the difference in behavior between the two binaries. After applying a micropatch to a binary, domain experts can apply the verifier to ensure that the effects are intended.

Note that while the verifier attempts to prove that the original and patched binaries have the same observable behaviors under all possible inputs, it is expected that they do not (or the patch would have had no effect). When the two binaries can exhibit different behaviors, the verifier provides the user with an explanation of how and where the behavior is different.

If DWARF debugging information is available in either the original or patched binary, the verifier will use that information to improve diagnostics. Currently, function names, function argument names, local variable names, and global variable names can be used to make diagnostics more readable, for example, by replacing synthetic names with their source-level counterparts. If working with binaries that do not come with DWARF debug information natively, see the `dwarf-writer`² tool for a possible approach to adding DWARF debug information.

PATE is designed to analyze binaries produced by applying a micropatch at the binary level where overall the pair of binaries are “mostly” similar. It is more difficult for PATE to compare binaries with substantially different control flow due to the challenges in finding corresponding slices to align for analysis. Major control flow divergences may require user input to guide PATE in its analysis process. We have observed that in some cases, compiling two programs with similar source (such as making a small source-level modification and rebuilding) can result in binaries that are more different than the small source code change might imply, as a result of various modern compiler heuristics and optimizations.

Currently, the verifier supports 32-bit ARM binaries, and 64-bit and 32-bit PowerPC binaries.

2 Installing the PATE Verifier

2.1 Recommended: Docker Container Image

We recommend using PATE via Docker.

If available, load the Docker image file from a file using:

```
docker load -i /path/to/pate.tar
```

Otherwise, build the Docker image from the PATE source repo. Building PATE is a memory-intensive process. We build the Docker image in an environment with 16GB of RAM available to

¹<https://github.com/GaloisInc/pate>

²<https://github.com/immunant/dwarf-writer>

Docker. Build the image using the following commands:

```
git clone git@github.com:GaloisInc/pate.git
cd pate
git submodule update --init
docker build . -t pate
```

PATE may subsequently be used via Docker, such as:

```
docker run --rm -it \
  --platform linux/amd64 \
  -v "$(pwd)"/tests/integration/packet/exe:/target \
  pate \
  --original /target/packet.exe \
  --patched /target/packet.patched.exe \
  -s parse_packet
```

Please see later sections for detailed usage information.

2.2 Alternative: Building from Source

Alternatively, PATE may be compiled from source and run on a host system. The PATE tool is written in Haskell and requires the GHC compiler³ and cabal⁴ to build.

The current version of PATE is developed using GHC version 9.6.2 and cabal version 3.10.2.0. Additionally, the verifier requires a SMT solver to be available in `PATH`. We recommend `yices`. The `z3` and `cvc4` solvers may also work but are not regularly tested with PATE.

Building from source can be accomplished as follows:

```
git clone git@github.com:GaloisInc/pate.git
cd pate
git submodule update --init
cp cabal.project.dist cabal.project
cabal configure pkg:pate
./pate.sh --help
```

Note that `./pate.sh` should be used to build PATE (not `cabal build` or similar).

Once built, invoke PATE locally using the `pate.sh` script.

3 Invoking the PATE Verifier

Once PATE has been built as described in Section 2, use the Docker container (or `pate.sh` script if building locally from source) to invoke PATE.

Invoking PATE presents the user with an interactive terminal user interface for analyzing a pair

³<https://www.haskell.org/ghc/>

⁴<https://www.haskell.org/cabal/>

of binaries. Users provide at least the paths to two (the “original” and “patched”) binaries at the command line when invoking PATE. Additionally, we recommend also specifying the desired entry point, using `-s <symbol>`. Providing the specific function of interest will enable PATE to begin reasoning closer to the relevant functionality of interest, greatly reducing the total analysis time required compared to starting from the program entry point. An example invocation using Docker looks like:

```
docker run --rm -it \
  --platform linux/amd64 \
  -v "$(pwd)"/z:/z \
  pate \
  --original /z/my.original.exe \
  --patched /z/my.patched.exe \
  -s start_function_name
```

Users may also wish to provide “hint” inputs that provide metadata that maps symbol names to addresses, easing analysis of stripped binaries. Please see the listing below for details.

The verifier accepts the following command line arguments:

<code>-h,--help</code>	Show this help text
<code>-o,--original EXE</code>	Original binary
<code>-p,--patched EXE</code>	Patched binary
<code>-b,--blockinfo FILENAME</code>	Block information relating binaries
<code>-s,--startsymbol ARG</code>	Start analysis from the function with this symbol
<code>-d,--nodiscovery</code>	Don't dynamically discover function pairs based on calls.
<code>--solver ARG</code>	The SMT solver to use to solve verification conditions. One of CVC4, Yices, or Z3 (default: Yices)
<code>--goal-timeout ARG</code>	The timeout for verifying individual goals in seconds (default: 300)
<code>--heuristic-timeout ARG</code>	The timeout for verifying heuristic goals in seconds (default: 10)
<code>--original-anvill-hints ARG</code>	Parse an Anvill specification for code discovery hints
<code>--patched-anvill-hints ARG</code>	Parse an Anvill specification for code discovery hints
<code>--original-probabilistic-hints ARG</code>	Parse a JSON file containing probabilistic function name/address hints
<code>--patched-probabilistic-hints ARG</code>	Parse a JSON file containing probabilistic function name/address hints
<code>--original-csv-function-hints ARG</code>	Parse a CSV file containing function name/address

```

                                hints
--patched-csv-function-hints ARG
                                Parse a CSV file containing function name/address
                                hints
--original-bsi-hints ARG Parse a JSON file containing function name/address
                                hints
--patched-bsi-hints ARG Parse a JSON file containing function name/address
                                hints
--no-dwarf-hints             Do not extract metadata from the DWARF information in
                                the binaries
-V,--verbosity ARG          The verbosity of logging output (default: Info)
--save-macaw-cfgs DIR       Save macaw CFGs to the provided directory
--solver-interaction-file FILE
                                Save interactions with the SMT solver during symbolic
                                execution to this file
--proof-summary-json FILE
                                A file to save interesting proof results to in JSON
                                format
--log-file FILE             A file to save debug logs to
-e,--errormode ARG          Verifier error handling mode
                                (default: ThrowOnAnyFailure)
-r,--rescopemode ARG        Variable rescoping failure handling mode
                                (default: ThrowOnEqRescopeFailure)
--skip-unnamed-functions    Skip analysis of functions without symbols
--skip-divergent-control-flow
                                <DEPRECATED>
--target-equiv-regs ARG     Compute an equivalence condition sufficient to
                                establish equality on the given registers after the
                                toplevel entrypoint returns. <DEPRECATED>
--ignore-segments ARG       Skip segments (0-indexed) when loading ELF
--json-toplevel             Run toplevel in JSON-output mode (interactive mode
                                only)
--read-only-segments ARG    Mark segments as read-only (0-indexed) when loading
                                ELF
--script FILENAME           Save macaw CFGs to the provided directory
--no-assume-stack-scope     Don't add additional assumptions about stack frame
                                scoping
--ignore-warnings ARG       Don't raise any of the given warning types

```

4 The PATE Terminal UI

Once PATE has been invoked at the command line (see Section 3), the user is presented with an interactive terminal user interface.

Internally, PATE maintains a tree representing the state of the analysis. The interactive interface allows users to inspect the tree by selecting from a list of options based on the users current “location” in the tree. The user makes a selection by entering a number representing the node of

interest and hitting enter, or by entering a command.

4.1 Example Usage

Launch PATE on the binaries in the `tests/integration/packet/exe/` directory with:

```
docker run --rm -it \  
  --platform linux/amd64 \  
  -v "$(pwd)"/tests/integration/packet/exe:/target \  
  pate \  
  --original /target/packet.exe \  
  --patched /target/packet.patched.exe \  
  -s parse_packet
```

Once launched, PATE presents the user is presented with a list of entry points and makes a selection:

```
Choose Entry Point  
0: Function Entry "_start" (segment1+0x435)  
1: Function Entry "parse_packet" (segment1+0x554)  
?> 1
```

We indicate user input with a yellow highlight. Here the user enters 1, selecting `parse_packet`. This starts PATE's analysis at this point, and the user sees output of:

```
.....  
0: Function Entry "parse_packet" (segment1+0x554) (User Request).....  
1: segment1+0x580 [ via: "parse_packet" (segment1+0x554) ]  
  (Widening Equivalence Domains).....  
2: segment1+0x5ac [ via: "parse_packet" (segment1+0x554) ]  
  (Widening Equivalence Domains)  
3: Return "parse_packet" (segment1+0x554)  
  (Widening Equivalence Domains).....  
4: segment1+0x5cc [ via: "parse_packet" (segment1+0x554) ]  
  (Widening Equivalence Domains).....  
5: segment1+0x5e0 [ via: "parse_packet" (segment1+0x554) ]  
  (Widening Equivalence Domains).....  
6: segment1+0x600 [ via: "parse_packet" (segment1+0x554) ]  
  (Widening Equivalence Domains)  
7: Return "parse_packet" (segment1+0x554)  
  (Widening Equivalence Domains).....  
8: segment1+0x624 [ via: "parse_packet" (segment1+0x554) ]  
  (Widening Equivalence Domains).....  
Handle observable difference:  
0: Emit warning and continue  
1: Assert difference is infeasible (defer proof)  
2: Assert difference is infeasible (prove immediately)  
3: Assume difference is infeasible
```

4: Avoid difference with equivalence condition

?> 4

PATE represents the analysis as a tree that can be navigated by the user. The top level of the interactive process (reachable via the `top` command) is a list of all analysis steps that were taken, starting from the selected entry point. Each pair of address and calling contexts defines a unique toplevel proof “node.” A given address and context may appear multiple times in the toplevel list, corresponding to each individual time that the address/context pair was analyzed. The latest (highest-numbered) entry corresponds to the most recent analysis of an address/context.

Each entry point is associated with an equivalence domain: a set of locations (registers, stack slots and memory addresses) that are potentially not equal at this point. Locations outside of this set have been proven to be equal (ignoring skipped functions). The analysis takes the equivalence domain of an entry point and computes an equivalence domain for each possible exit point (according to the semantics of the block).

At this point in the example, PATE is asking how a detected observable difference should be handled. The user selects 4 to capture the difference in the equivalence condition, and PATE continues its analysis:

```
0: Function Entry "parse_packet" (segment1+0x554) (User Request)
1: segment1+0x580 [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains)
2: segment1+0x5ac [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains)
3: Return "parse_packet" (segment1+0x554)
  (Widening Equivalence Domains)
4: segment1+0x5cc [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains)
5: segment1+0x5e0 [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains)
6: segment1+0x600 [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains)
7: Return "parse_packet" (segment1+0x554)
  (Widening Equivalence Domains)
8: segment1+0x624 [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains)
9: segment1+0x644 [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains).....
10: segment1+0x644 [ via: "parse_packet" (segment1+0x554) ]
  (Re-checking Block Exits).....
11: segment1+0x654 (original) vs. segment1+0x668 (patched)
  [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains).....
12: segment1+0x668 (original) vs. segment1+0x67c (patched)
  [ via: "parse_packet" (segment1+0x554) ]
  (Widening Equivalence Domains)
13: Return "parse_packet" (segment1+0x554)
```



```

(Widening Equivalence Domains)
Continue verification?
0: Finish and view final result
1: Restart from entry point
2: Handle pending refinements
?> 0

```

The user selects 0 to finish and view the final result.

The PATE analysis tree can be navigated by the user with `top` to move to the top of the tree, numbers to navigate “into” nodes, `up` to move “up” a node, and `ls` to redisplay the nodes available at a current level.

For example, to inspect the analysis results in the running example, the user may provide input as follows to view the equivalence condition:

```

...
15: Final Result
> 15
Final Result
0: Assumed Equivalence Conditions
1: segment1+0x644 [ via: "parse_packet" (segment1+0x554) ]
2: Binaries are conditionally, observably equivalent
3: Toplevel Result
> 1
segment1+0x644 [ via: "parse_packet" (segment1+0x554) ]
0: -----
1: original
2: patched
3: let -- segment1+0x684.. in not v40494
> 3
let -- segment1+0x684
    v40487 = select (select cInitMemBytes@40467:a 0) 0x11045:[32]
    -- segment1+0x684
    v40490 = select (select cInitMemBytes@40344:a 0) 0x11044:[32]
    -- segment1+0x684
    v40494 = and (eq 0x80:[8] v40487) (not (eq v40490 (bvSum v40487 0x80:[8])))
in not v40494
0: With condition assumed
1: Event Trace: segment1+0x644 .. segment1+0x650 (original) vs.
    segment1+0x644 .. segment1+0x664 (patched)
2: With negation assumed
3: Event Trace: segment1+0x644 .. segment1+0x650 (original) vs.
    segment1+0x644 .. segment1+0x664 (patched)
>

```

Continuing on, the user may view, for example, an example trace showing where the equivalence condition above does not hold:

```

0: With condition assumed
1:  Event Trace: segment1+0x644 .. segment1+0x650 (original) vs.
    segment1+0x644 .. segment1+0x664 (patched)
2: With negation assumed
3:  Event Trace: segment1+0x644 .. segment1+0x650 (original) vs.
    segment1+0x644 .. segment1+0x664 (patched)
> 3
== Initial Original Registers ==
pc <- 0x644:[32]
r0 <- 0x0:[32]
r1 <- 0x1:[32]
r10 <- (3243, 0x0:[32])
r11 <- (3342, 0x0:[32])
r12 <- (2490, 0x0:[32])
...
== Original sequence ==
(segment1+0x644)
  Read 0x688:[32] -> 0x108:[32]
  r0 <- 0x108:[32]
(segment1+0x648) r0 <- 0x758:[32]
...
== Initial Patched Registers ==
pc <- 0x644:[32]
r0 <- 0x0:[32]
r1 <- 0x1:[32]
r10 <- (3243, 0x0:[32])
r11 <- (3342, 0x0:[32])
r12 <- (2490, 0x0:[32])
...
== Patched sequence ==
(segment1+0x644)
  Read 0x11044:[32] -> 0x80:[8]
  r1 <- 0x80:[32]
(segment1+0x648)
  Read 0x11045:[32] -> 0x80:[8]
  r2 <- 0x80:[32]

```

See the following subsections for details about how to interpret and interact with the terminal user interface.

4.2 Status Indicators

The *prompt* indicates the status of the current node as follows:

- `*>` current node still has some active task running
- `?>` current node requires user input
- `!>` current node has raised a warning
- `x>` current node has raised an error

- `>` current node, and all sub-nodes, have finished processing

Similar to the prompt, nodes may be printed with a suffix that indicates some additional status as follows:

- `(*)` node still has some active task running
- `(?)` node requires user input
- `(!)` node has raised a warning
- `(x)` node has raised an error

A status suffix indicates that the node, or some sub-node, has the given status. e.g. at the toplevel the prompt `x>` indicates that an error was thrown during some block analysis, while the corresponding node for the block will have a `(x)` suffix.

4.3 Navigation Commands

- `#` - navigate to a node, printing its contents
- `up` - navigate up one tree level
- `top` - navigate to the toplevel
- `goto_err` - navigate to the first leaf node with an error status
- `next` - navigate to the highest-numbered node at the current level

4.4 Diagnostic Commands

- `status` - print the status of the current node
- `full_status` - print the status of the current node, without truncating the output
- `ls` - print the list of nodes at the current level
- `wait` - wait at the current level for more results. Exits when the node finishes, or the user provides any input

When the prompt is `?>`, the verifier is waiting for input at some sub-node. To select an option, simply navigate (i.e. by entering `#`) to the desired choice. For example, `goto_prompt` - navigate to the first leaf node waiting for user input.

5 The PATE Binary Ninja Plugin

The PATE Binary Ninja plugin enables user to invoke and interact with PATE directly within the Binary Ninja reverse engineering platform.

The PATE plugin requires a commercially-licensed Binary Ninja installation. We have tested PATE with Binary Ninja stable version 4.0.5336.

5.1 Installation

First, install the PATE Docker container as described in Section 2.

Second, copy (or create a symlink from) the `pate_binja/` directory from the PATE source repo to your local Binary Ninja `plugins/` directory. Typically these are found in:

macOS \$HOME/Library/Application Support/Binary Ninja/plugins/
Linux \$HOME/.binaryninja/plugins/

The Binary Ninja plugin requires a relatively recent version of Python (3.10 or newer) and requires the `grpcio` package. If these are not present on the system, we recommend creating a Python `venv` or similar on your host, with something like:

```
python -m venv /path/to/new/virtual/environment
source /path/to/new/virtual/environment/bin/activate
pip install grpcio
```

and then modifying Binary Ninja Python settings appropriately in the Binary Ninja Preferences list to point to this new environment. Specifically, check the settings for:

- Python Path Override
- Python Interpreter
- Python Virtual Environment Site-Packages

Once these steps have been completed, restart Binary Ninja. If the plugin is correctly installed and initialized, then the “Plugins” menu will now have a “Pate...” menu option.

5.2 Usage

In Section 4 we examined the `packet.exe` example using the PATE terminal UI. In this section, we describe analyzing the same example using the PATE Binary Ninja plugin.

Once installed, invoke the PATE plugin from the Binary Ninja “Plugins → Pate...” menu option.

The PATE plugin opens a window to select a *run configuration* file in JSON format. This file must end in the suffix `.run-config.json`. The run configuration must contain a key-value map with the following keys:

original (absolute or relative) file path to the original binary
patched (absolute or relative) file path to the patched binary
args a list additional arguments to pass to PATE

For example, the file `tests/integration/packet/packet.run-config.json` contains:

```
{
  "original": "exe/packet.original.exe",
  "patched": "exe/packet.patched.exe",
  "args": [
    "-s parse_packet"
  ]
}
```

After selecting the run configuration file, the PATE plugin will open three Binary Ninja tabs: one for each of the original and patched binaries, and a third PATE *analysis* tab.

As shown in Figure 1, the PATE analysis tab is composed of two primary regions. The bottom

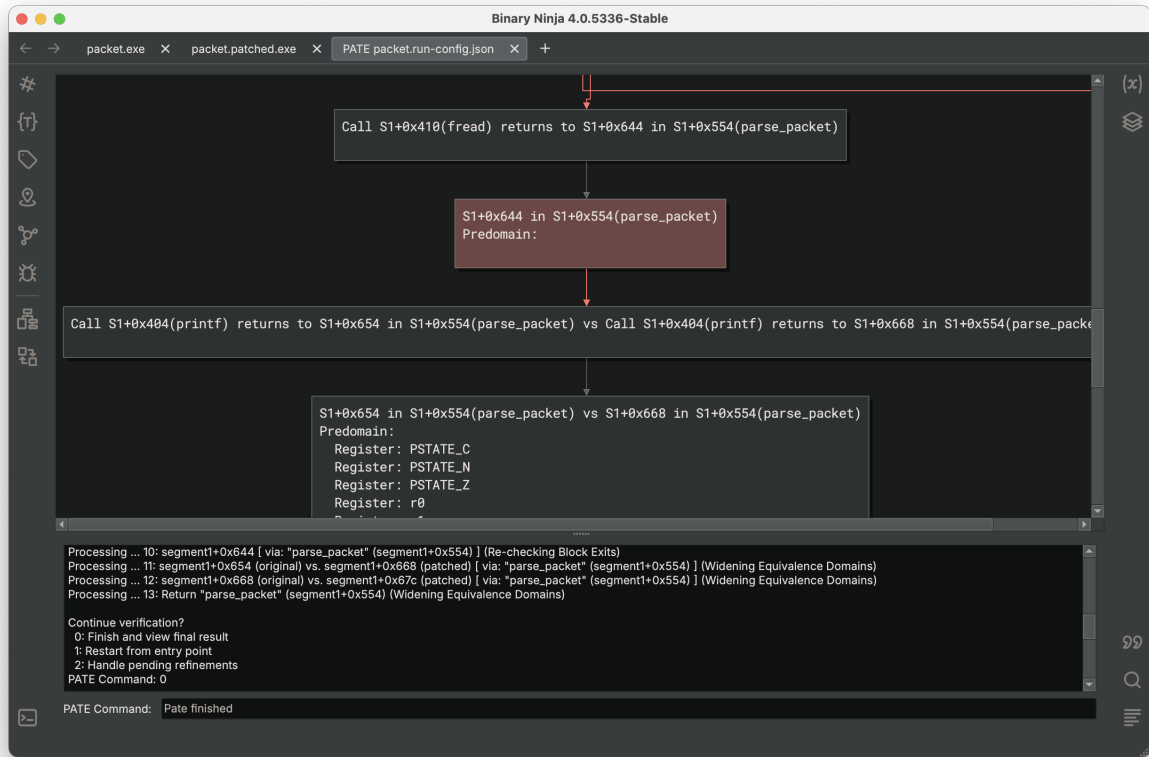


Figure 1: The PATE Binary Ninja Plugin. The top region is the PATE analysis overview graph. The bottom panel is used by the operator to interact with the PATE verifier.

portion is an interactive text view that corresponds to the terminal user interface. The user interacts with this region through the text input field at the bottom of the window. In the `packet.exe` example, the user enters the same commands described in Section 4 through the **Finish and view final result** step, at which point results will be rendered in the interactive Binary Ninja view.

The top portion of the PATE analysis tab is a graph view showing the current state of the PATE analysis. When PATE analysis is complete (via interaction in the bottom portion), the PATE graph shows rectangles for each slice of the program analyzed by PATE. Default-colored rectangles represent a pair of programs slices that were able to matched up between the original and patched binary. Green rectangles represent slices present only in the original program, if any. Blue rectangles represent slices present only in the patched program, if any. Right click on a rectangle for options to jump directly to the relevant program location in the appropriate tab for the corresponding binary.

A red rectangle represents the “active” region, where PATE has found an equivalence condition. Right click and select “Show Equivalence Condition” to open the Equivalence Condition window. Please see Figure 2 for an example screenshot of the equivalence condition window in the PATE Binary Ninja plugin. An equivalence condition window includes:

- the expression describing the conditions under which programs behave equivalently

- a generated (concretized) trace through the program(s) showing an example where the equivalence condition is met
- a generated (concretized) trace through the program(s) showing an example where the equivalence condition is *not* met

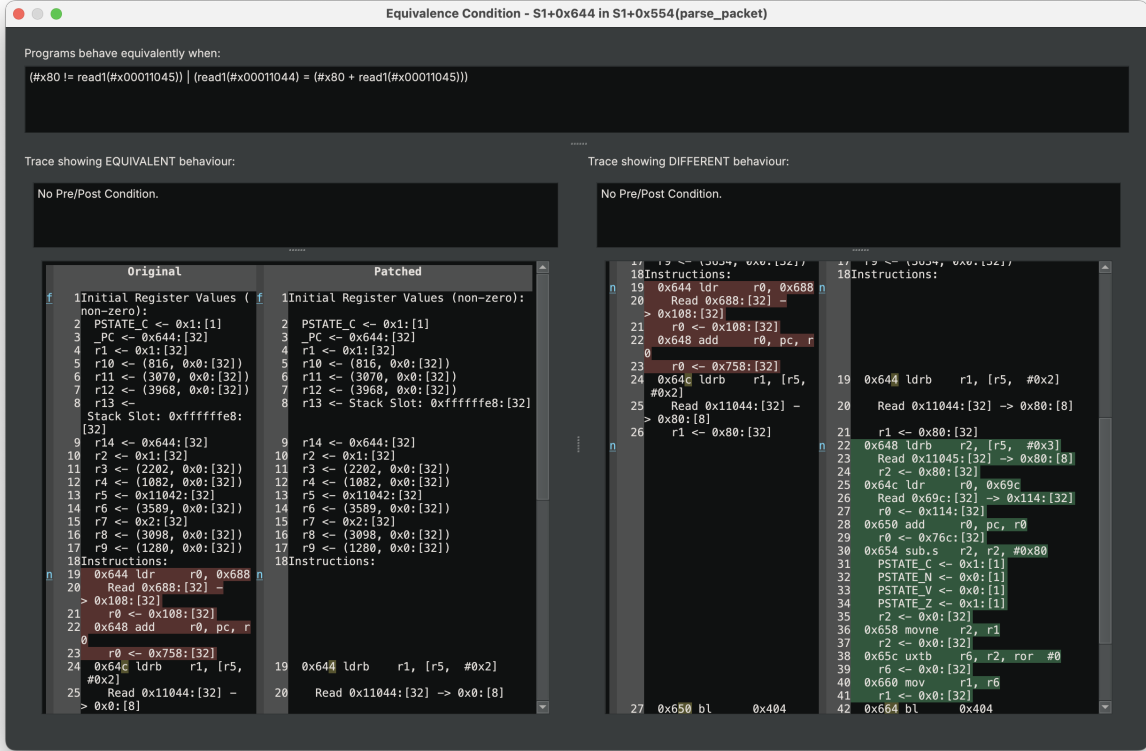


Figure 2: The PATE Binary Ninja plugin equivalence condition window.

Right clicking on a rectangle in the PATE analysis graph and selecting “Show Instruction Trees” will open a new window showing basic blocks from the original program on the left and corresponding basic blocks from the patched program on the right. At the bottom will be a linearized representation of the instruction trees in the original and patched program, with colored diff view. Instructions conditionally reachable through conditional control flow edges (if any) are prefixed by + or - to differentiate instructions in distinct branches. See Figure 3 for an example of the instruction tree view, with MCAD integration (described below).

5.3 Replays

Executing a run configuration file with the PATE plugin will produce a *replay* in a file named `lastrun.replay`, which can be preserved by renaming to another filename on disk. These files cache the user input and verifier output, enabling the user to load a previous interaction with PATE without having to re-execute the verifier analysis. If the user loads a replay rather than a run configuration, the process is mostly the same, except the command input field is already populated with the recorded user input, and the user just hits “enter” to proceed to the next step. Editing the input commands will have no effect, as the responses are recorded in the replay file.

That is, the user cannot deviate from the pre-recorded responses from the PATE verifier to perform any analysis other than the one recorded.

5.4 MCAD Integration

MCAD⁵ is a performance analysis tool that performs static prediction of instruction timings for sequences of instructions such as those identified by PATE. The details of the MCAD system is outside of the scope of this user guide, but if the MCAD Docker container is available, the PATE Binary Ninja plugin will show MCAD-predicted cycle counts next to each instruction in the Instruction Trees view, as shown in Figure 3. Use the PATE plugin preference option “MCAD Docker image name” to specify the name of the MCAD Docker container on the host in order to enable MCAD integration in the PATE plugin.

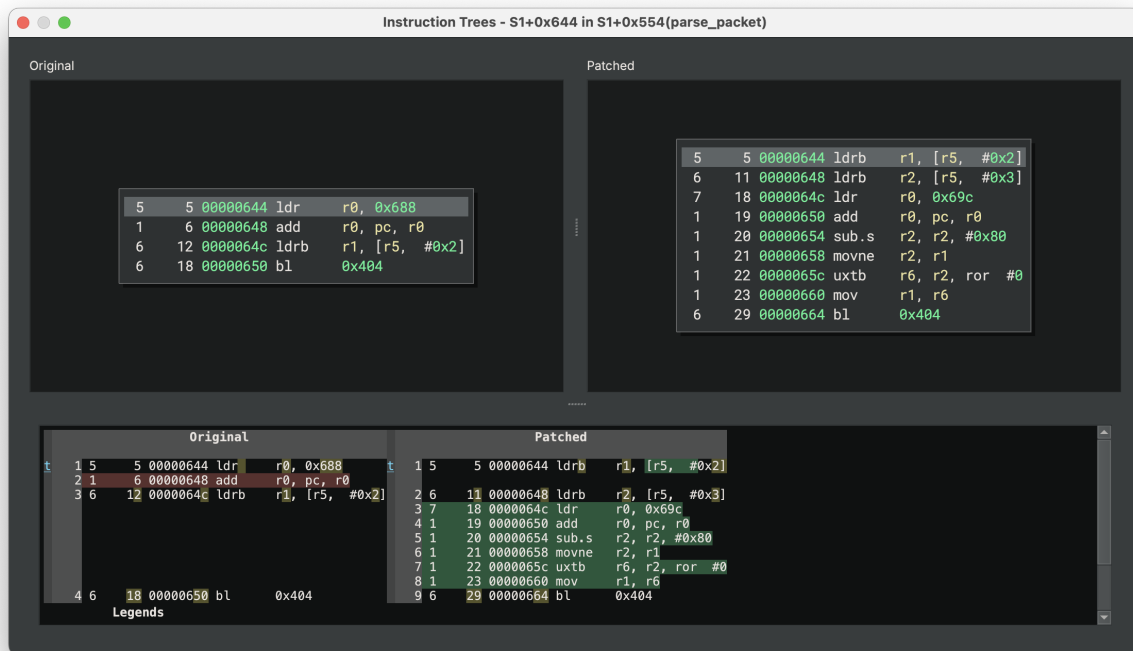


Figure 3: PATE Binary Ninja MCAD integration showing predicted cycle counts (per instruction, cumulative) for instructions in original (left) and patched (right) basic blocks.

⁵<https://github.com/securesystemslab/LLVM-MCA-Daemon>

6 Acknowledgements

This material is based upon work supported by the Defense Advanced Research Projects Agency (DARPA) and Naval Information Warfare Center Pacific (NIWC Pacific) under Contract Number N66001-20-C-4027. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the DARPA & NIWC Pacific.

SBIR DATA RIGHTS

Contract No 140D0423C0063

Contractor Name Galois, Inc.

Contractor Address 421 SW Sixth Ave., Suite 300, Portland, OR 97204

Expiration of SBIR Data Protection Period 06/07/2042

The Government's rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software marked with this legend are restricted during the period shown as provided in paragraph (b)(5) of the Rights in Noncommercial Technical Data and Computer Software-Small Business Innovation Research (SBIR) Program clause contained in the above identified contract. After the expiration date shown above, the Government has perpetual government purpose rights as provided in paragraph (b)(5) of that clause. Any reproduction of technical data, computer software, or portions thereof marked with this legend must also reproduce the markings.