

What the Fuzz

# Cornelius Aschermann

Researcher at Ruhr University Bochum

Verification & Automated Bug Finding

Security Consultant



@is\_eqv



[github.com/eqv](https://github.com/eqv)



[cornelius.aschermann@rub.de](mailto:cornelius.aschermann@rub.de)

# Sergej Schumilo

Researcher at Ruhr University Bochum

Automated Bug Finding & Everything Low Level  
Security Consultant

 @ms\_s3c

 [github.com/schumilo](https://github.com/schumilo)

 [sergej.schumilo@rub.de](mailto:sergej.schumilo@rub.de)



# Manual Analysis

(doesn't scale that well)



# Verification

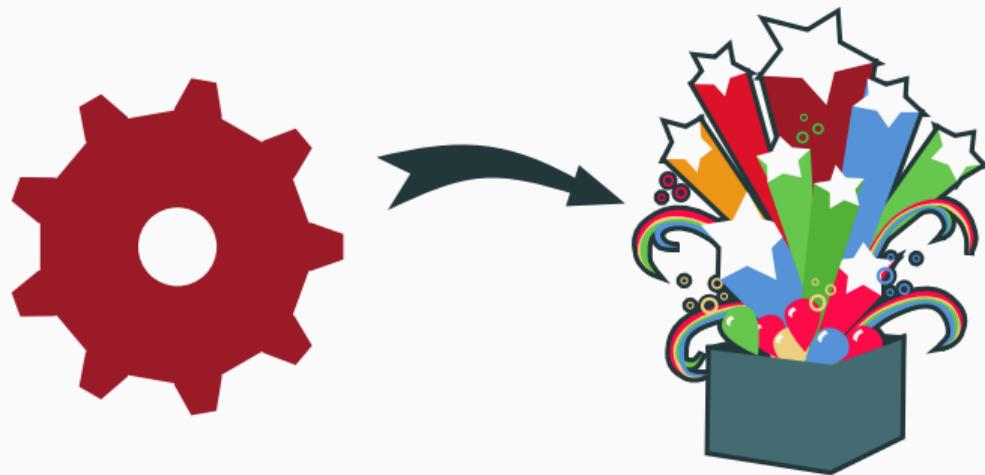
Veri~~s~~ication

# Fuzzers

# Fuzzing



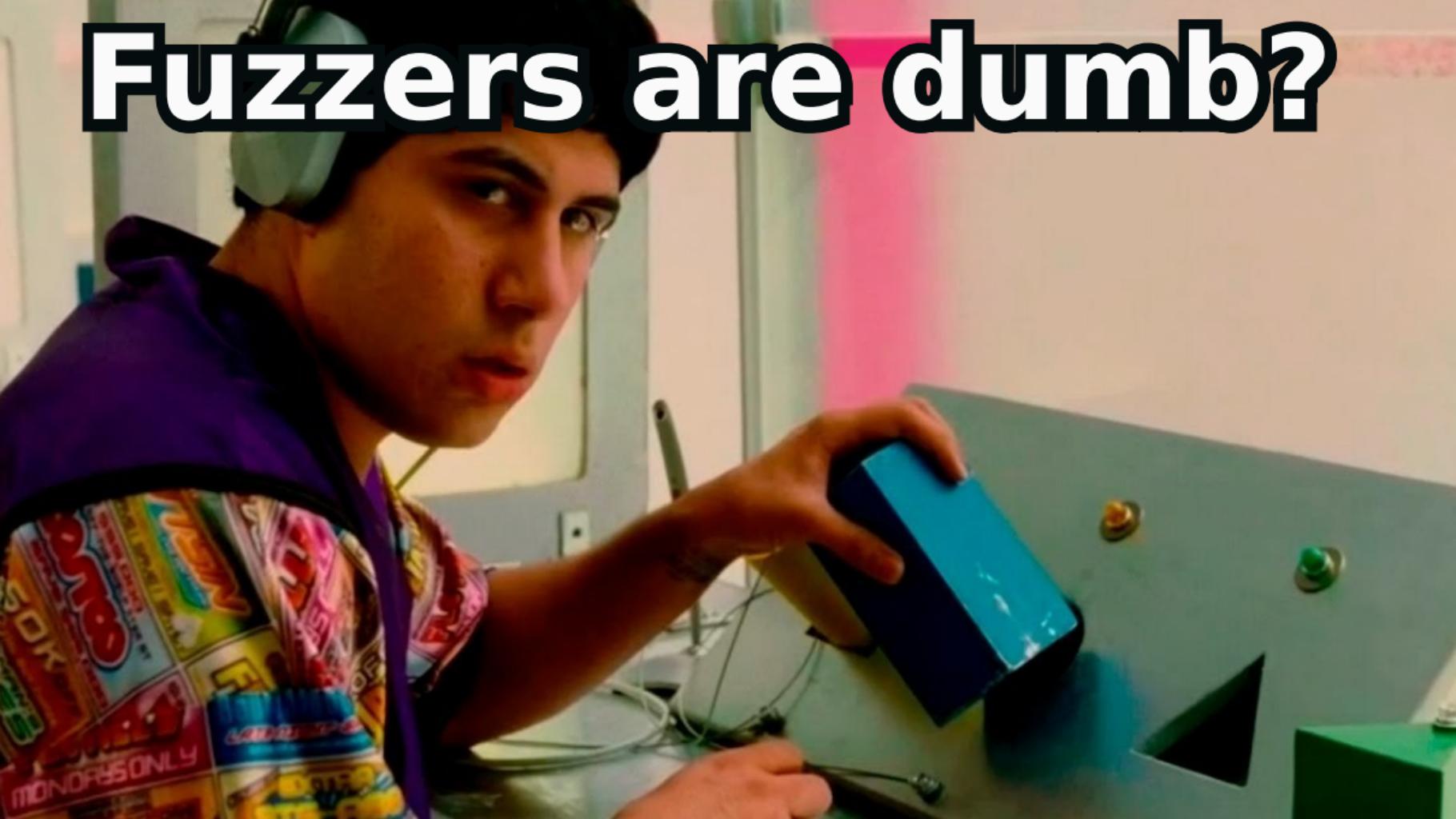
# Fuzzing



# Fuzzing



# Fuzzers are dumb?



# Demo







8 min

# How do Fuzzer Work?

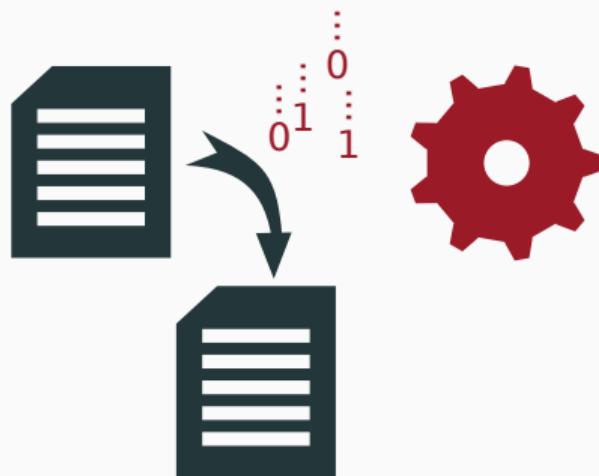
# How do Fuzzer Work?



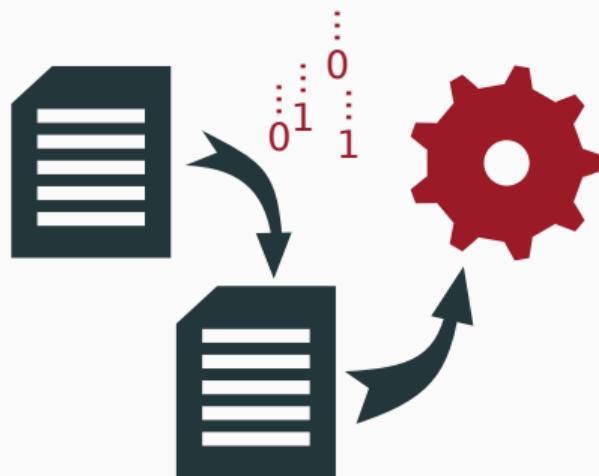
# How do Fuzzer Work?



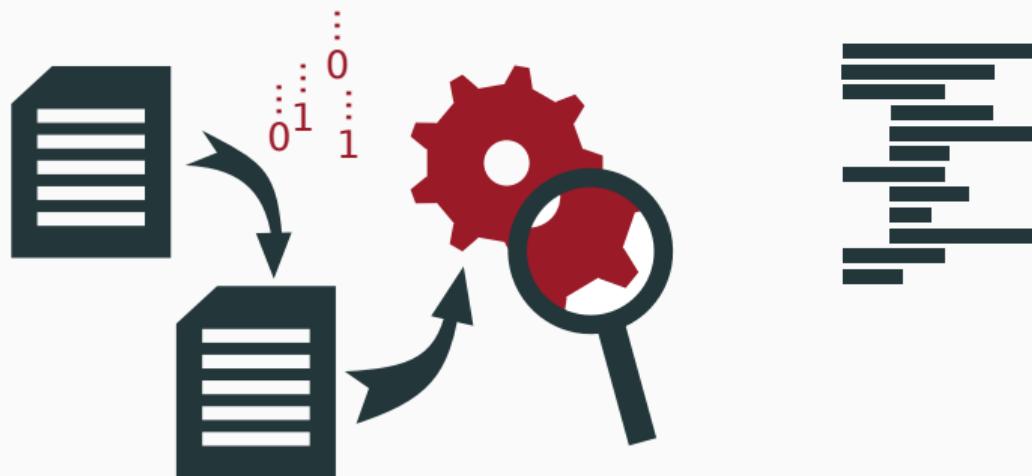
# How do Fuzzers Work?



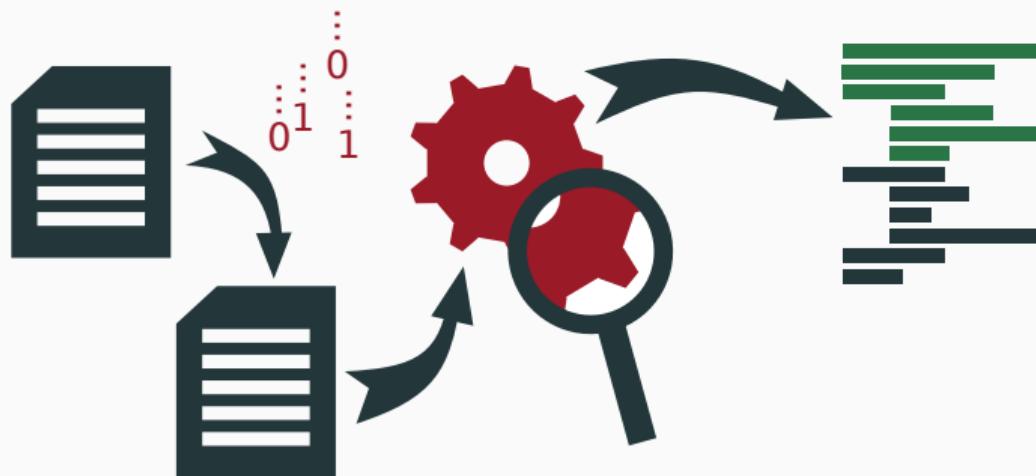
# How do Fuzzers Work?



# How do Fuzzers Work?



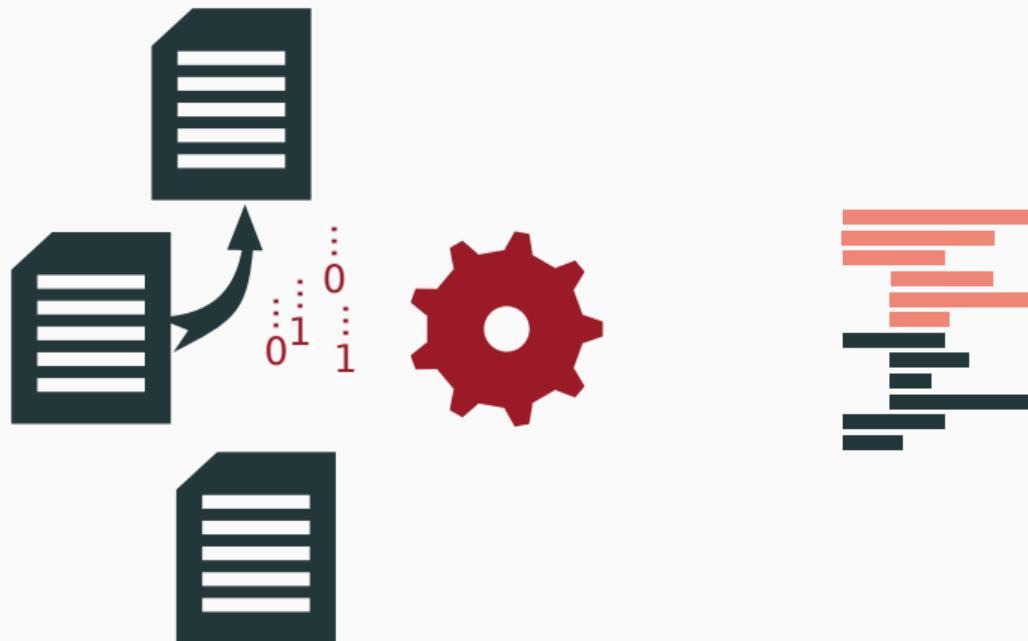
# How do Fuzzers Work?



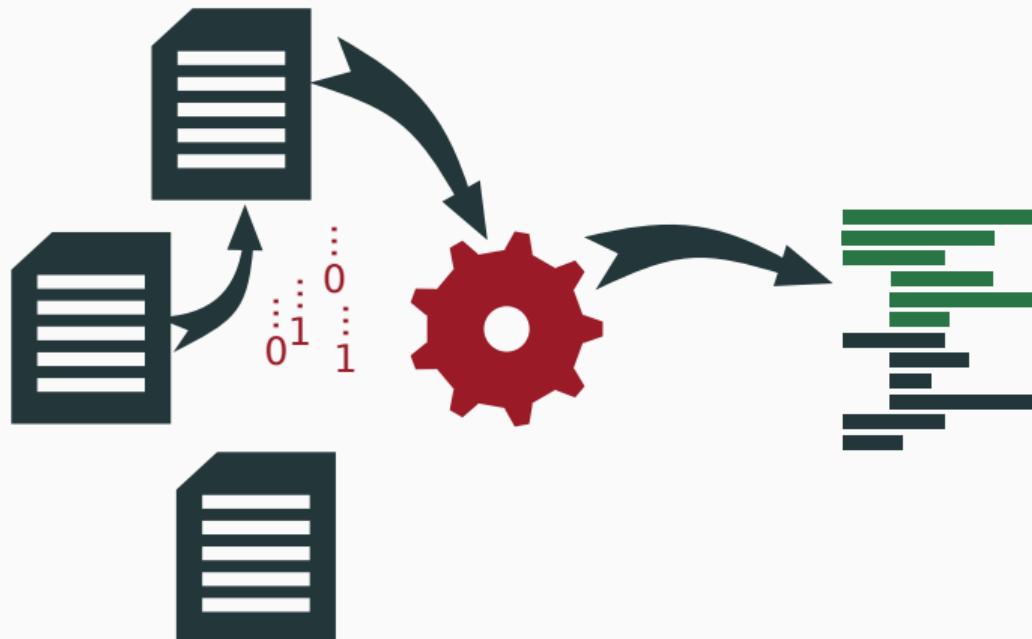
# How do Fuzzers Work?



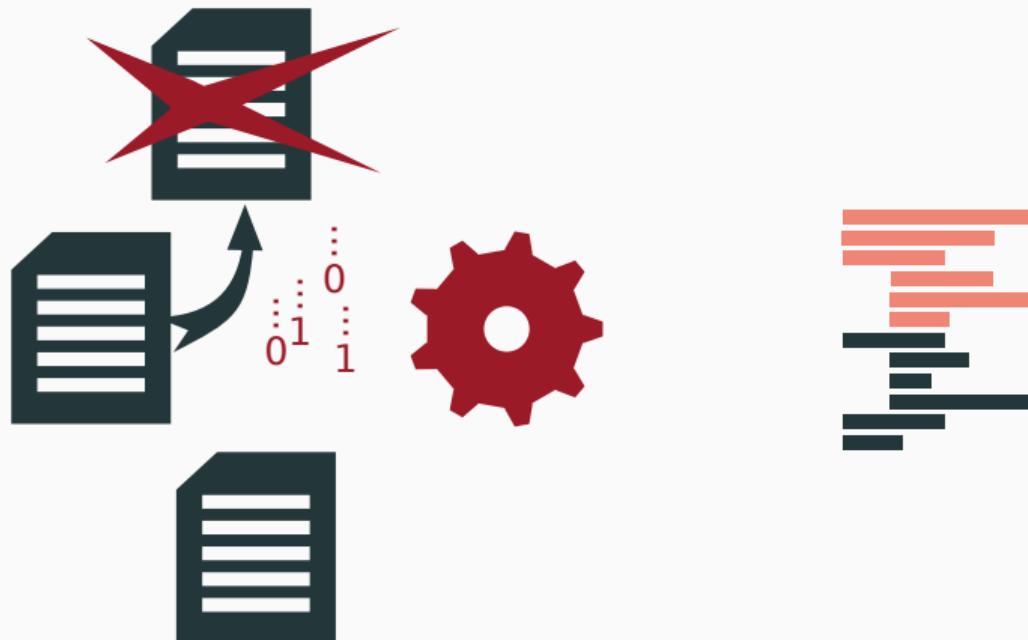
# How do Fuzzers Work?



# How do Fuzzers Work?



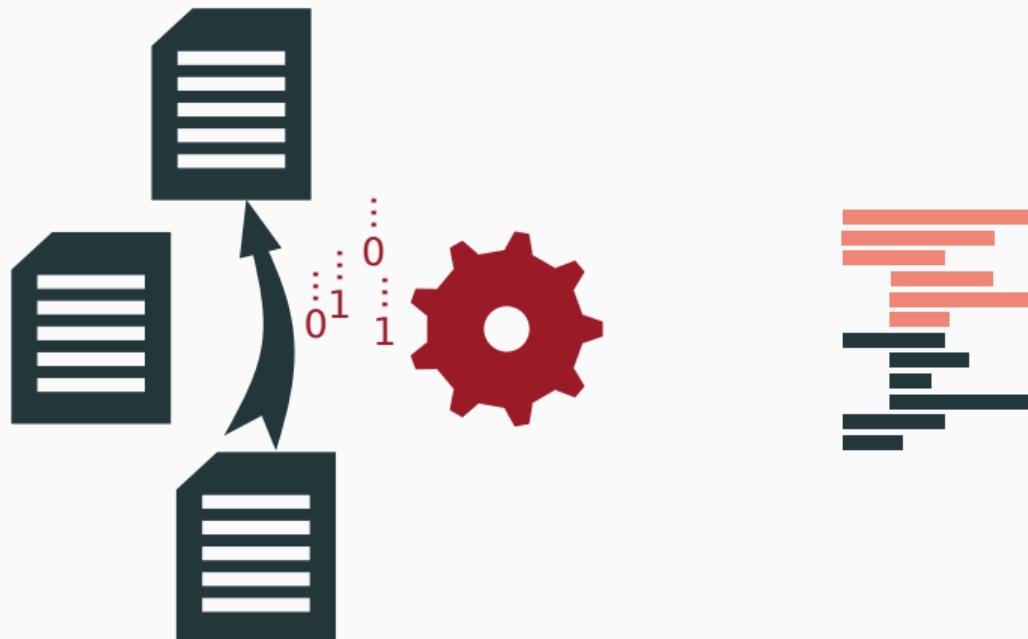
# How do Fuzzers Work?



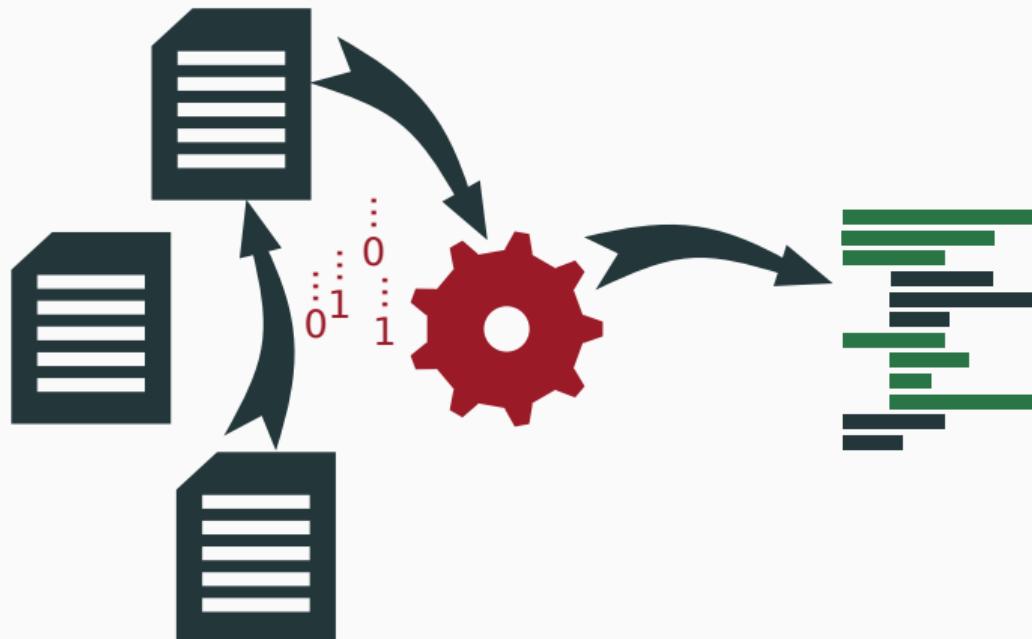
# How do Fuzzer Work?



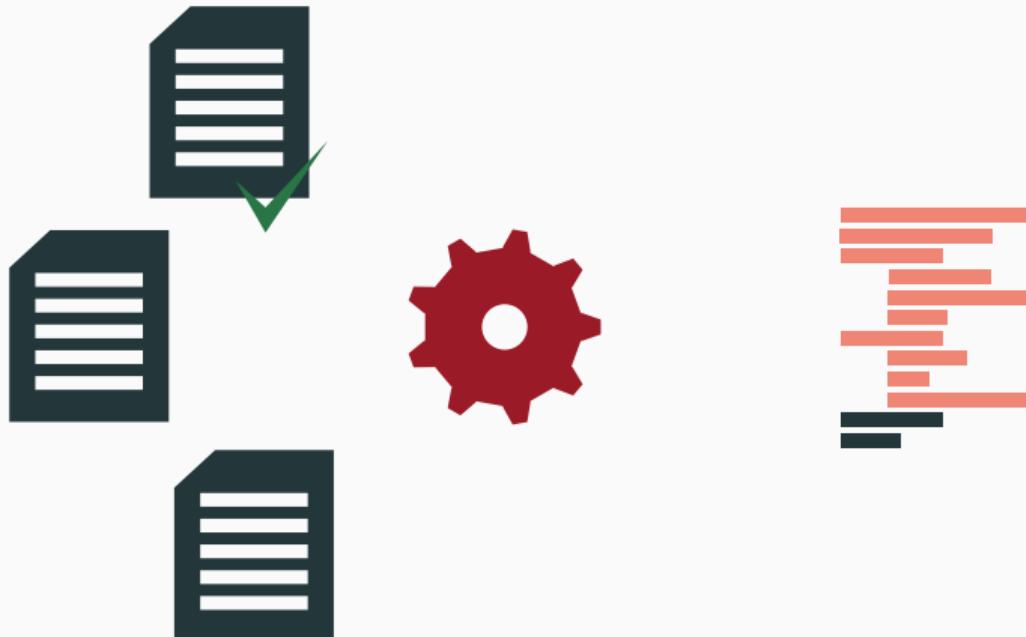
# How do Fuzzers Work?



# How do Fuzzer Work?



# How do Fuzzer Work?



# Fuzzers

Artificial Intelligence for Testcase Generation

# Key Takeaways:



# Key Takeaways:



I SHOULD FUZZ MY CODE

# The Rest of this Talk



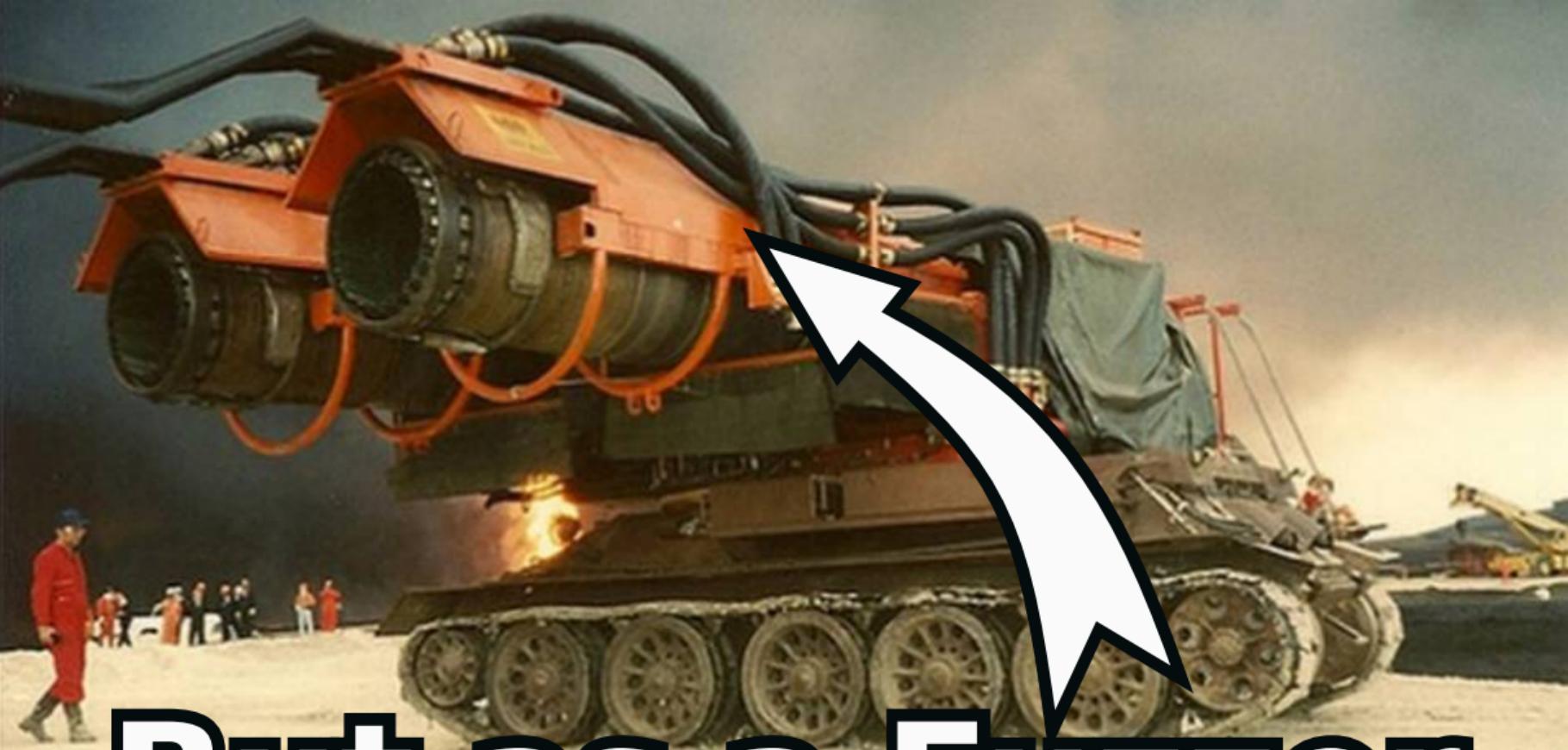
# The Rest of this Talk

Past Research



Goal





**But as a Fuzzer**

Objective C

C

Pascal

Haskell

C++

x86

Ada

Go

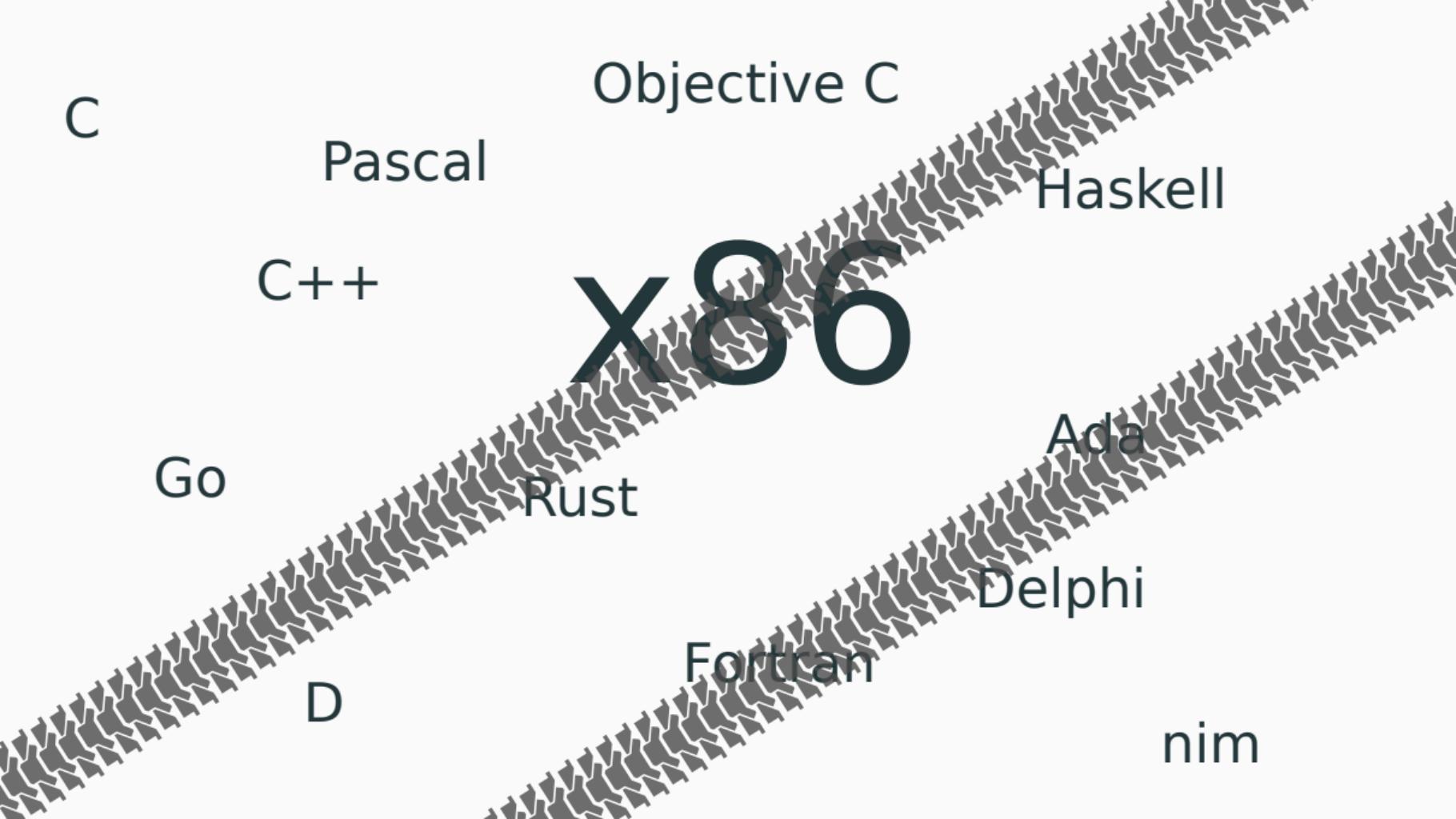
Rust

Delphi

Fortran

D

nim



C

Pascal

Objective C

Haskell

C++

x86

Go

Rust

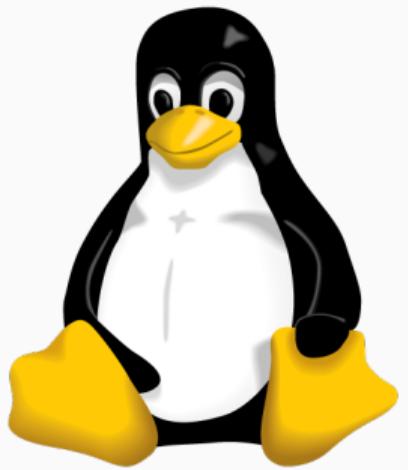
Ada

Delphi

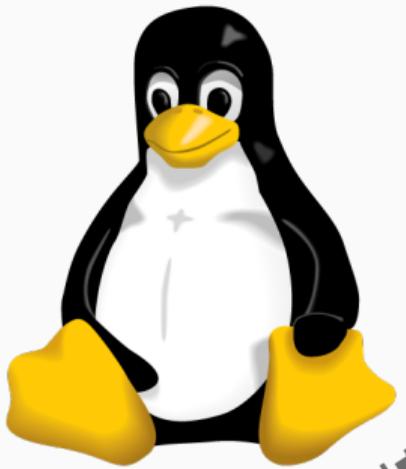
D

Fortran

nim



Mac



Mac

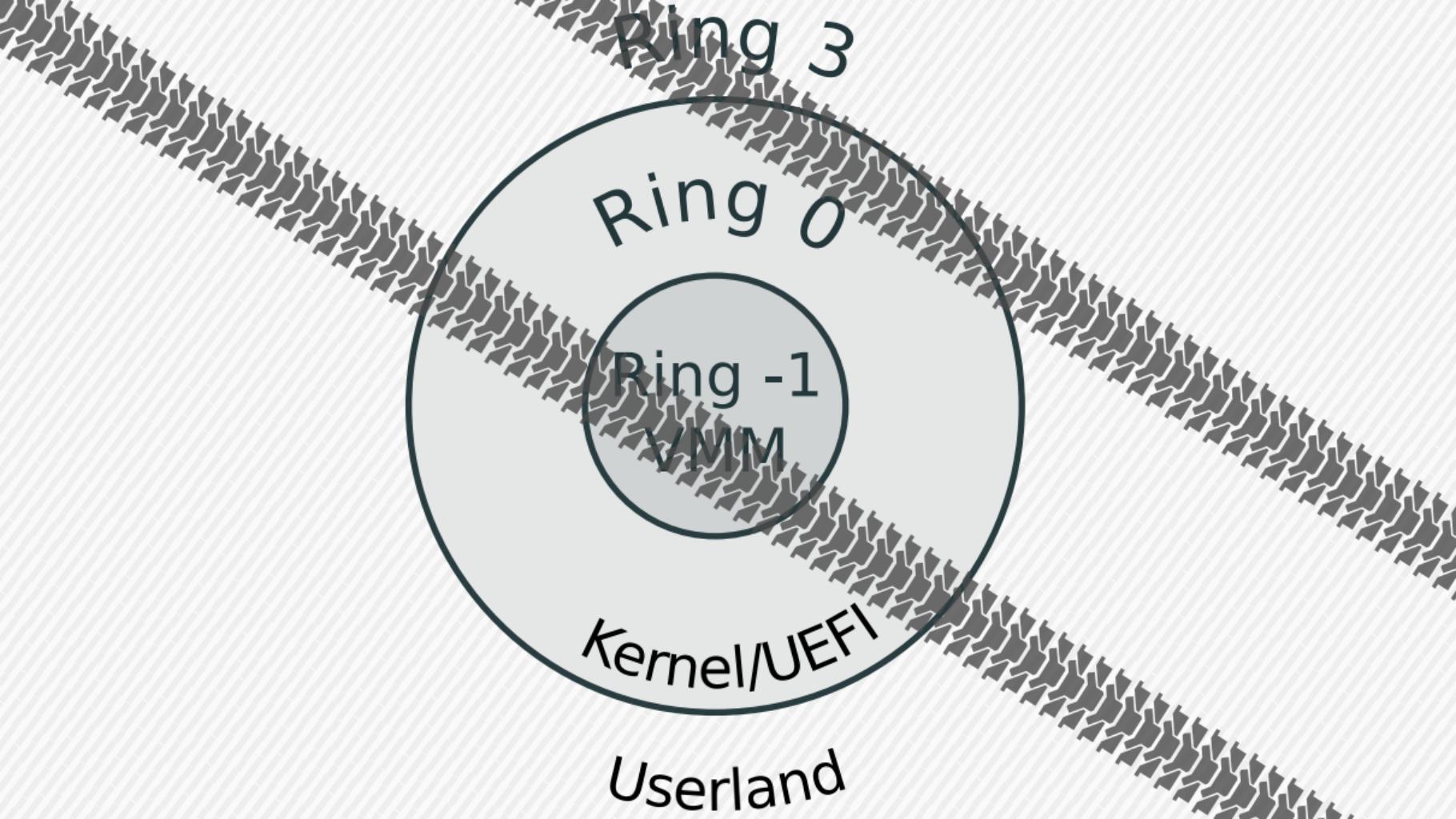
Ring 3

Ring 0

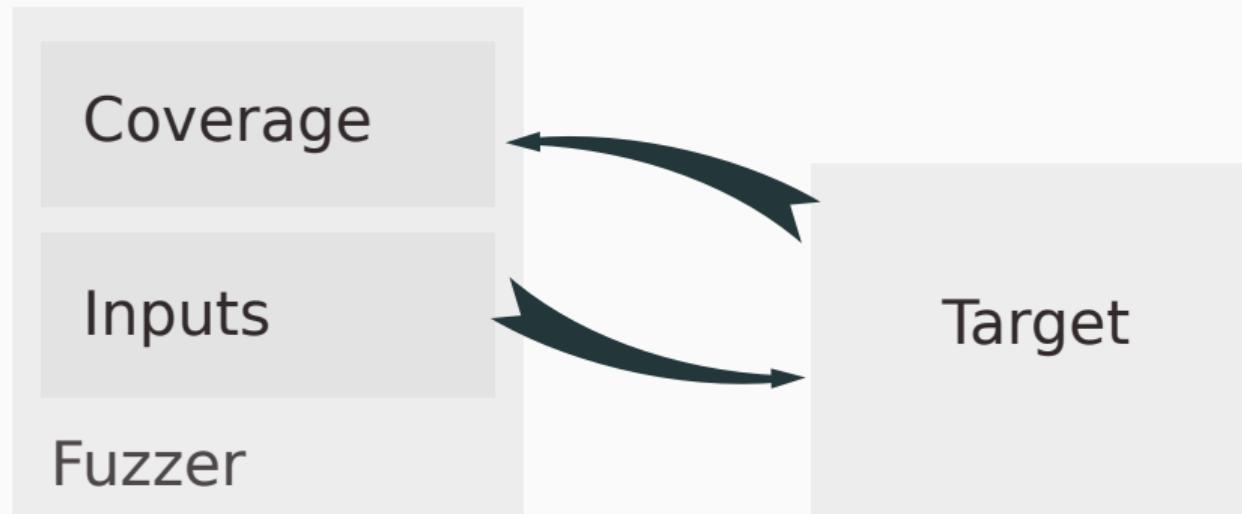
Ring -1  
VMM

Kernel/UEFI

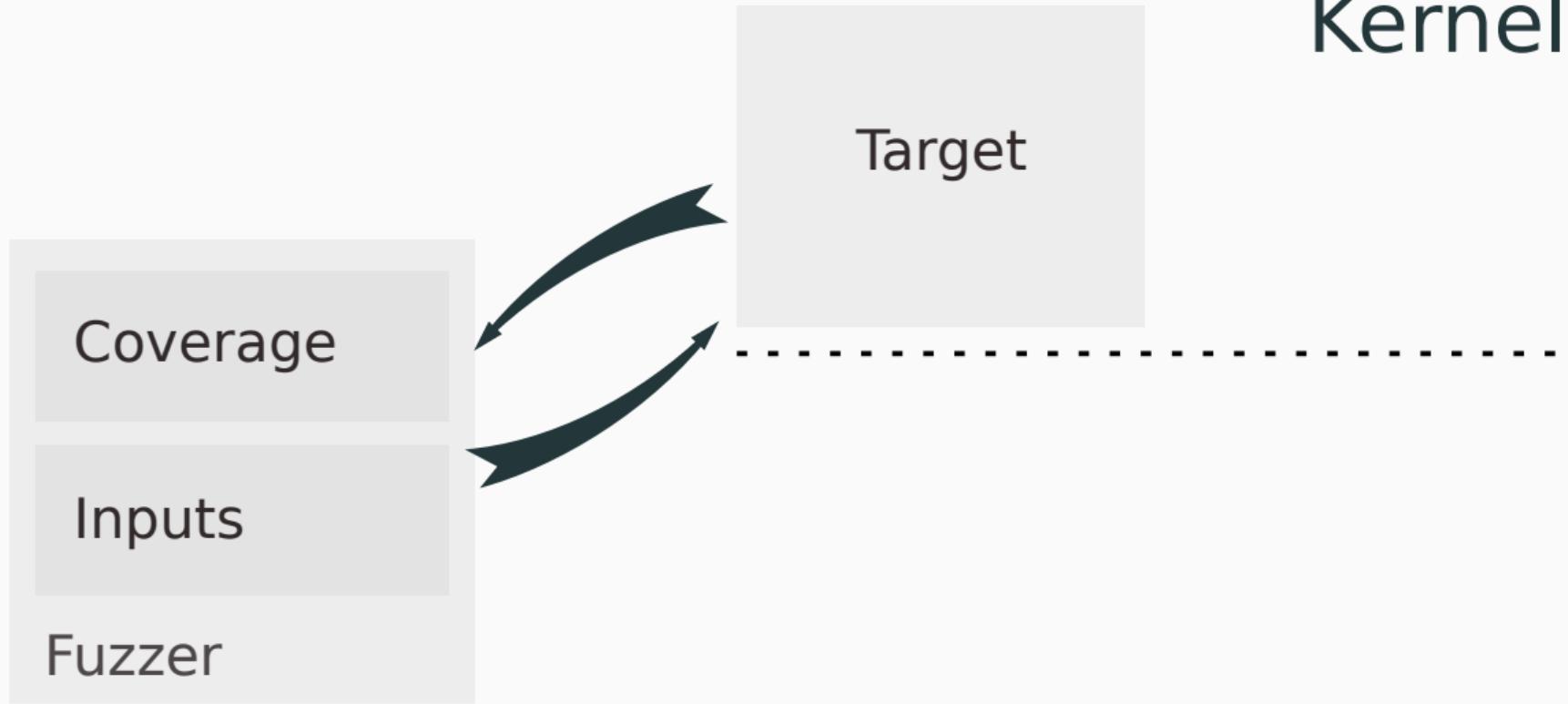
Userland



Nyx

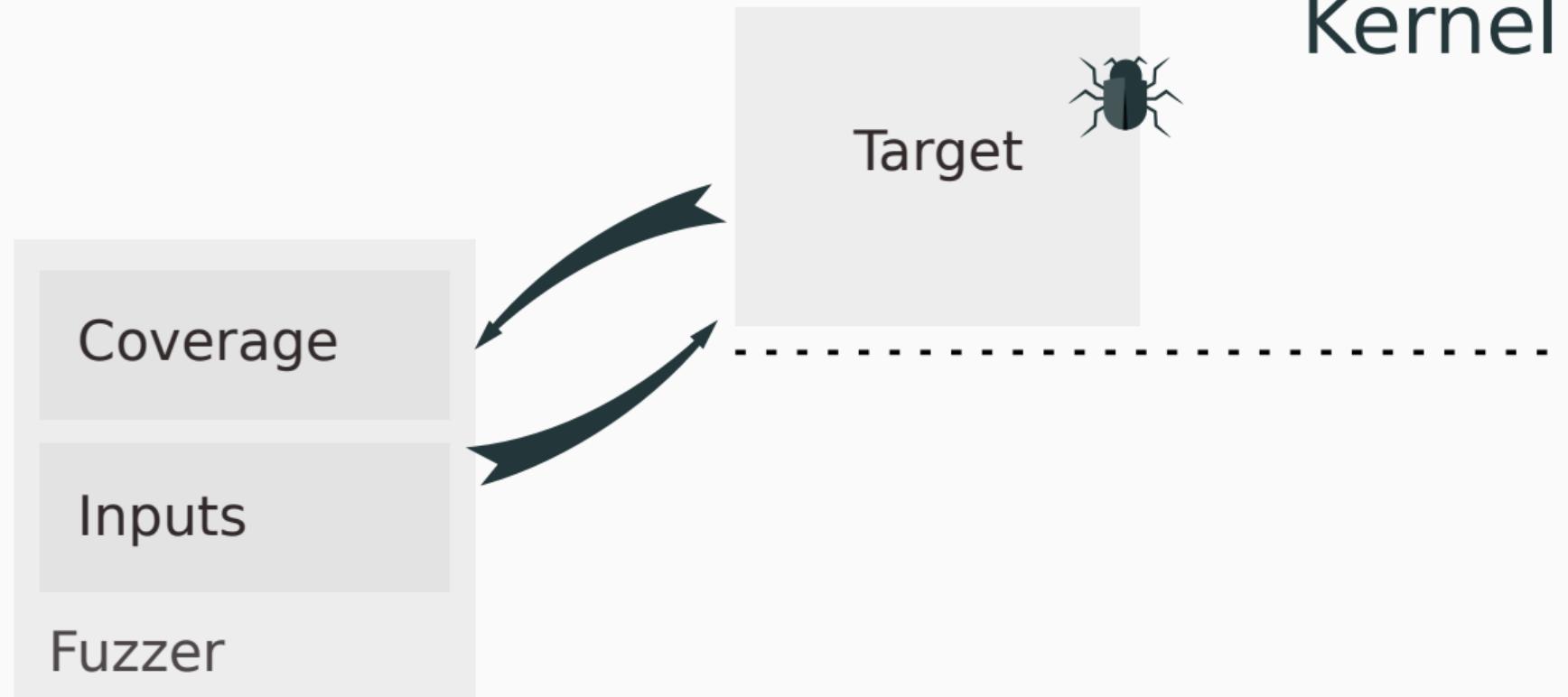


Kernel



Fuzzer

Userland



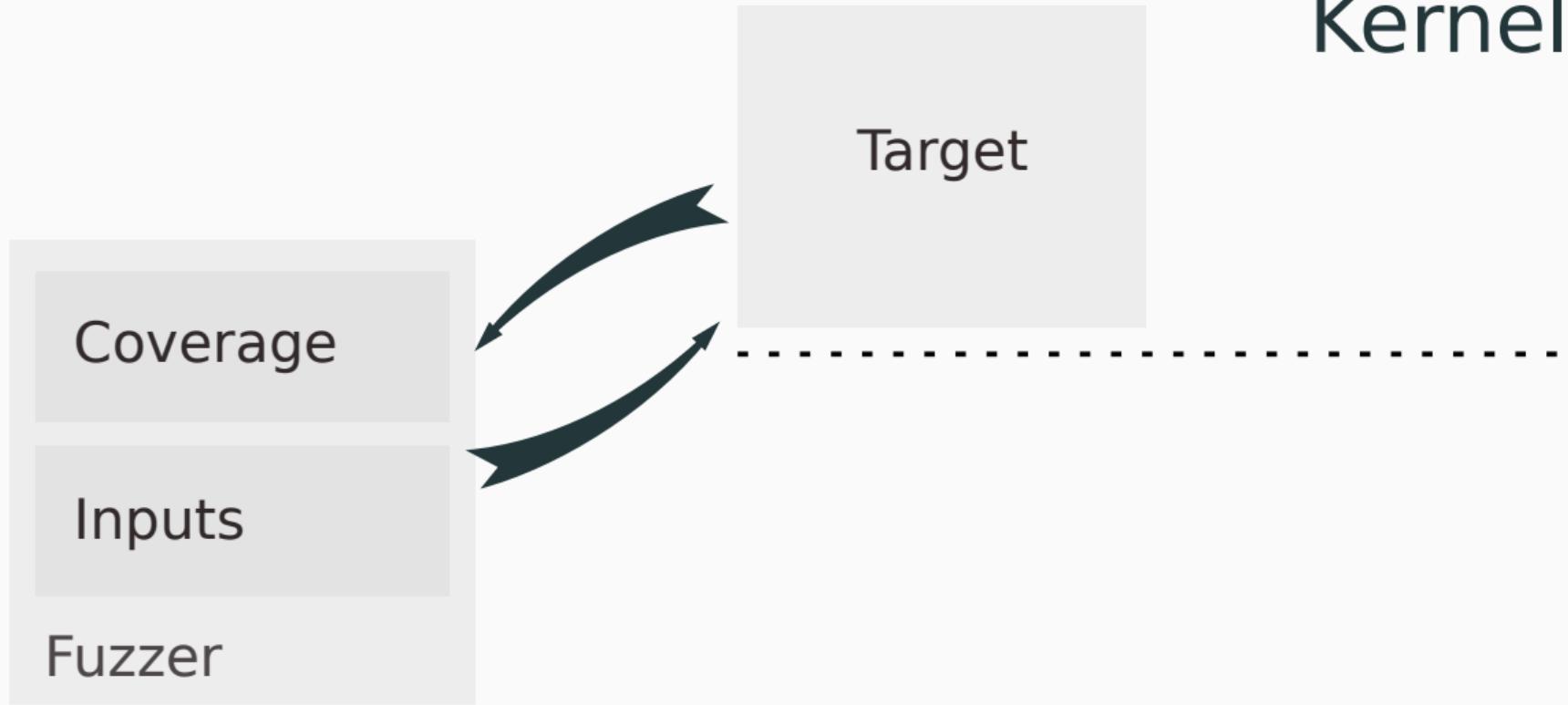
Userland



Input  
Fuzzer

Userland

Kernel

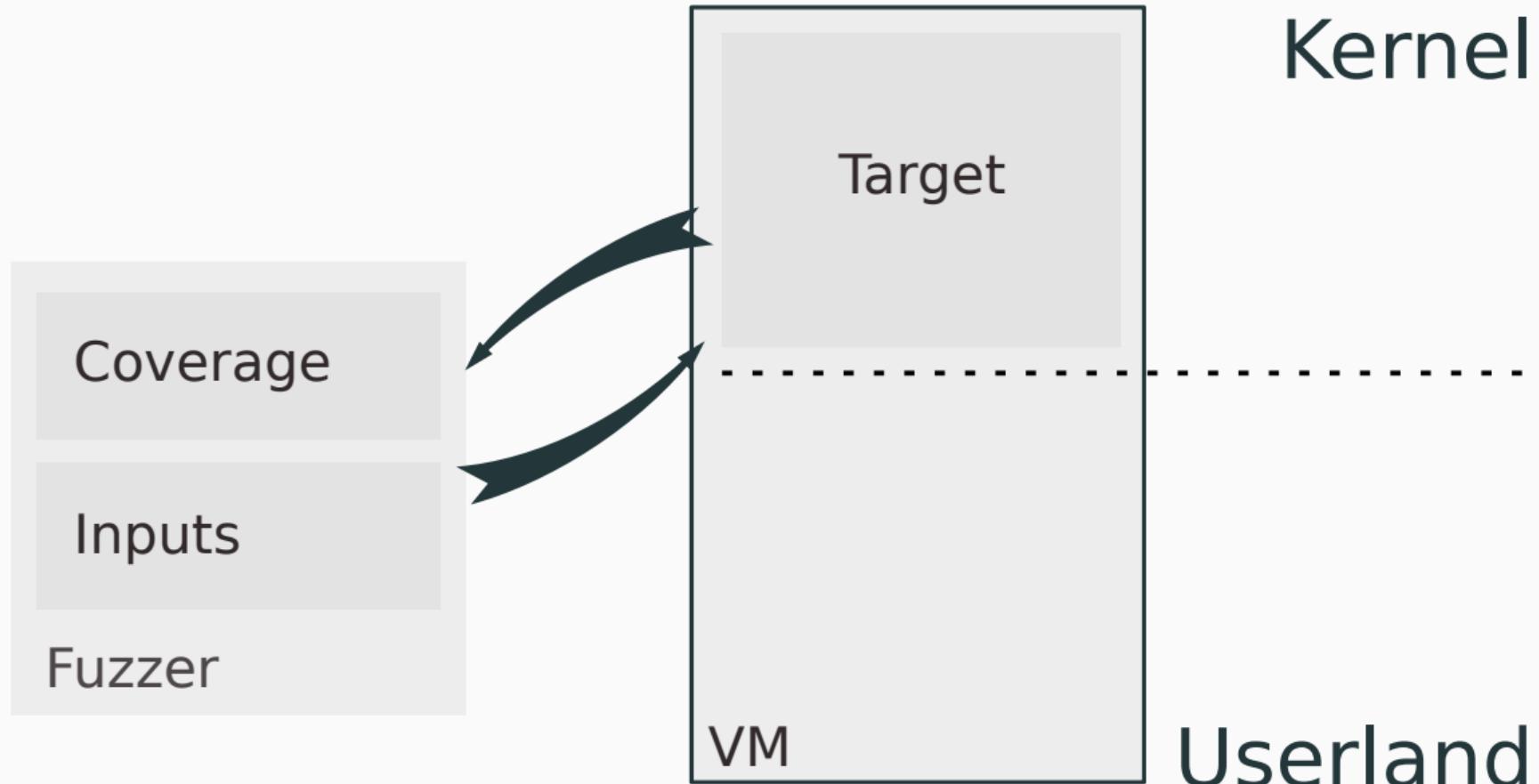


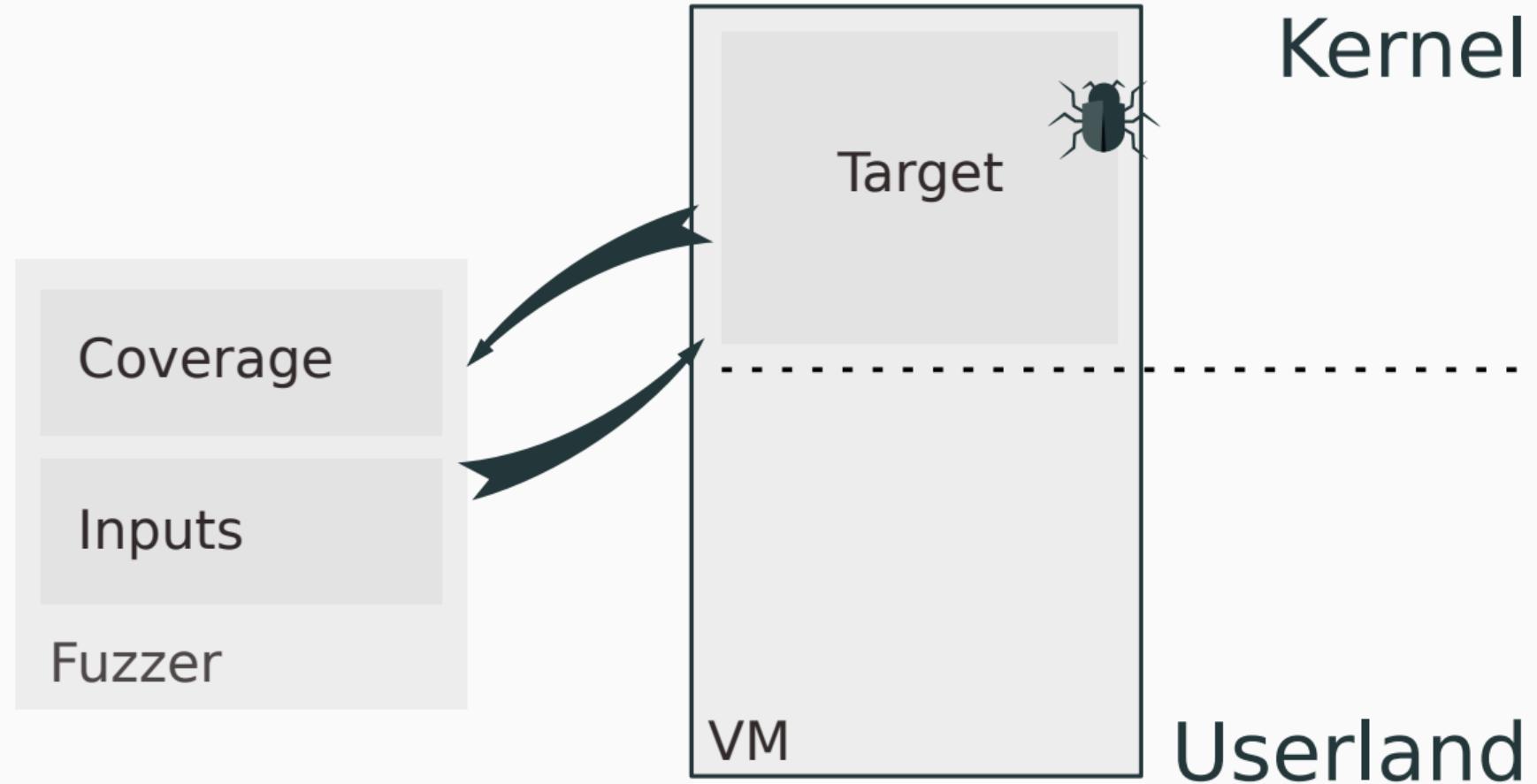
Fuzzer

Userland

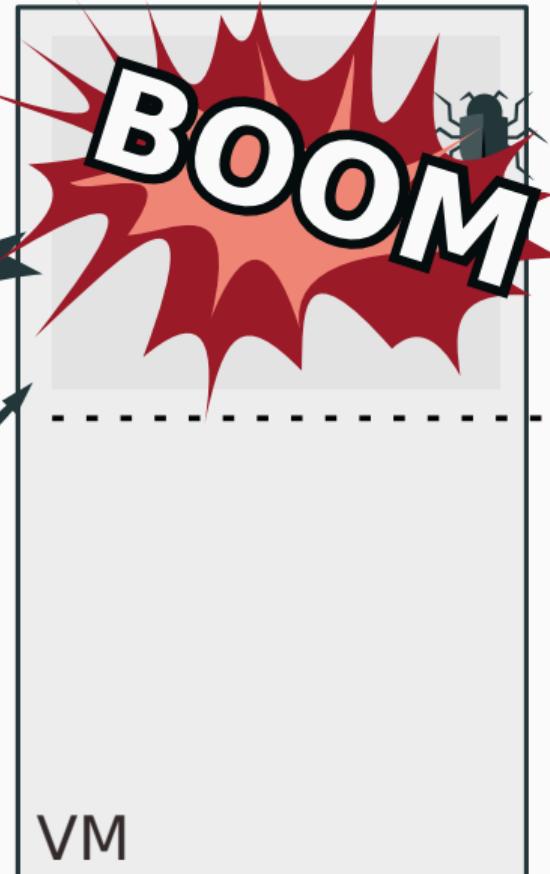
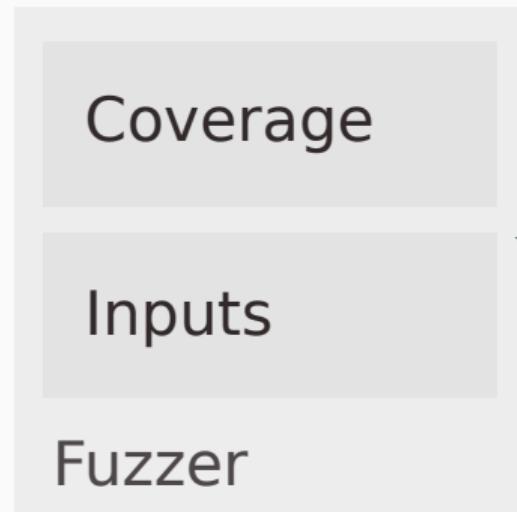
# Architecture

Kernel





Kernel



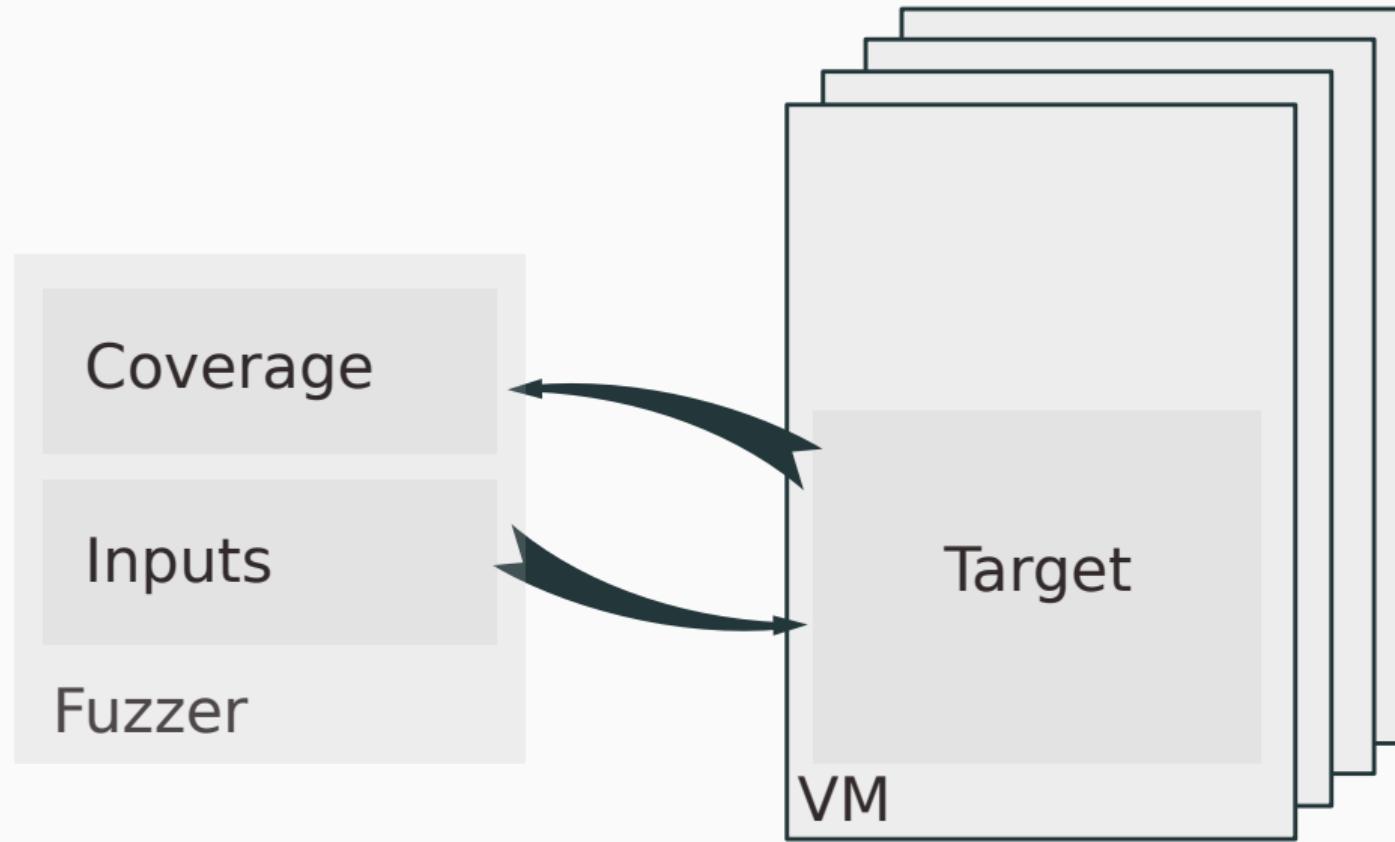
# Target in a VM:

+ Fault Tolerance

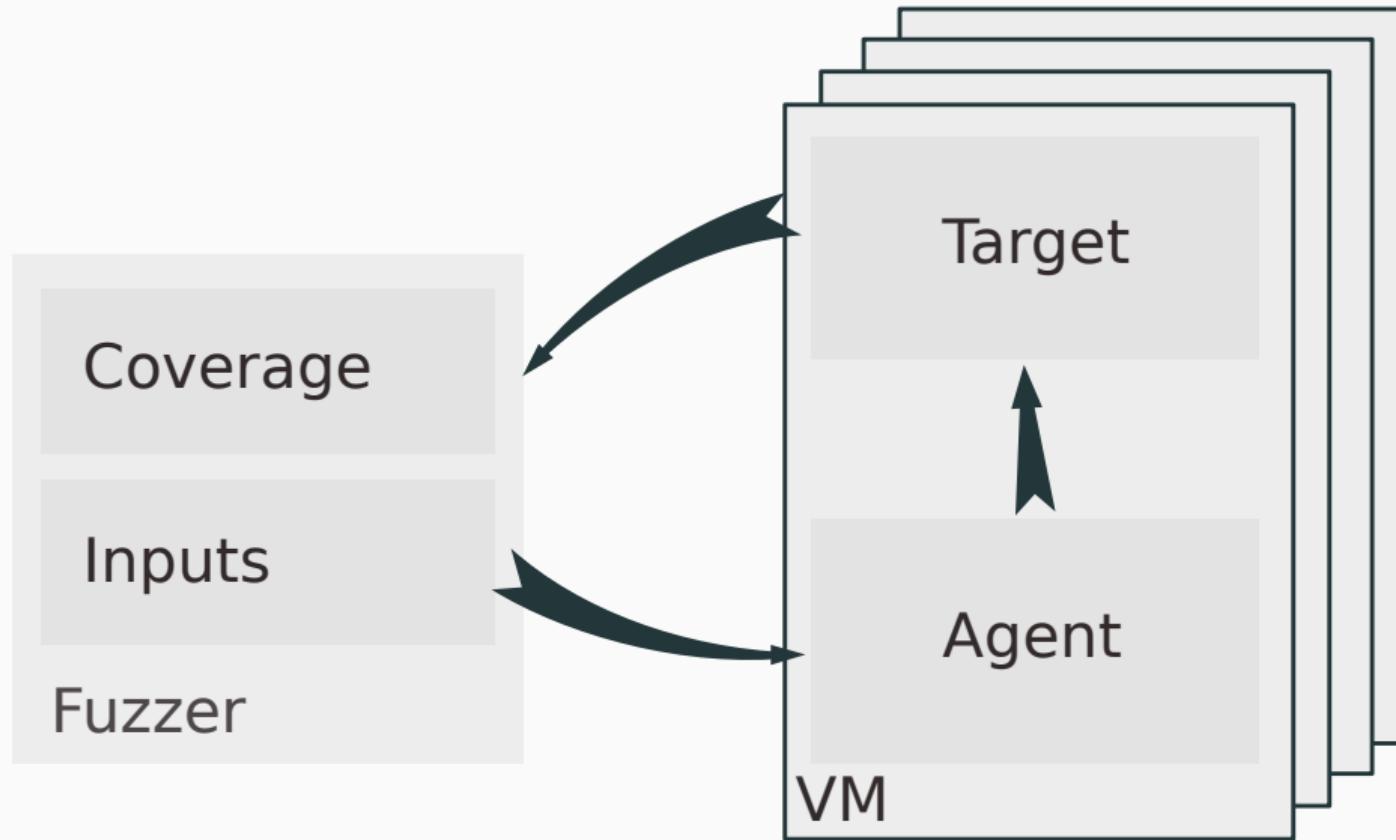
# Target in a VM:

- + Fault Tolerance
- + Parallelization

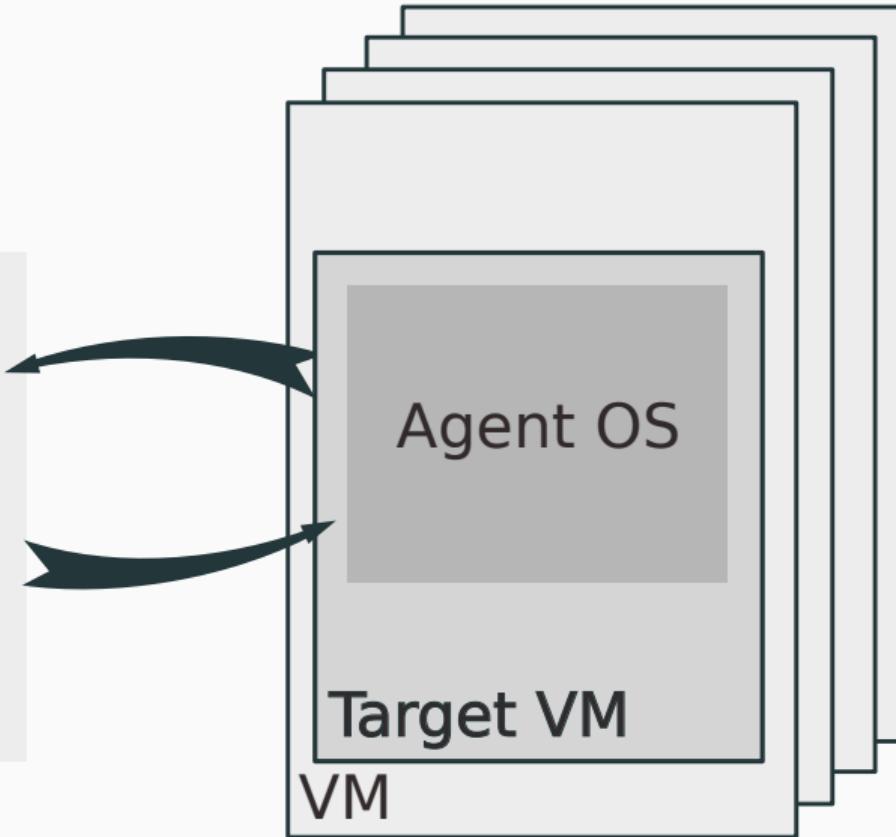
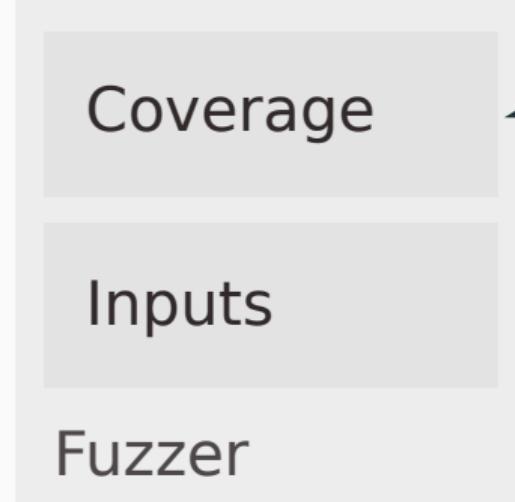
# Architecture



# Architecture



# Architecture



# Key Takeaways:

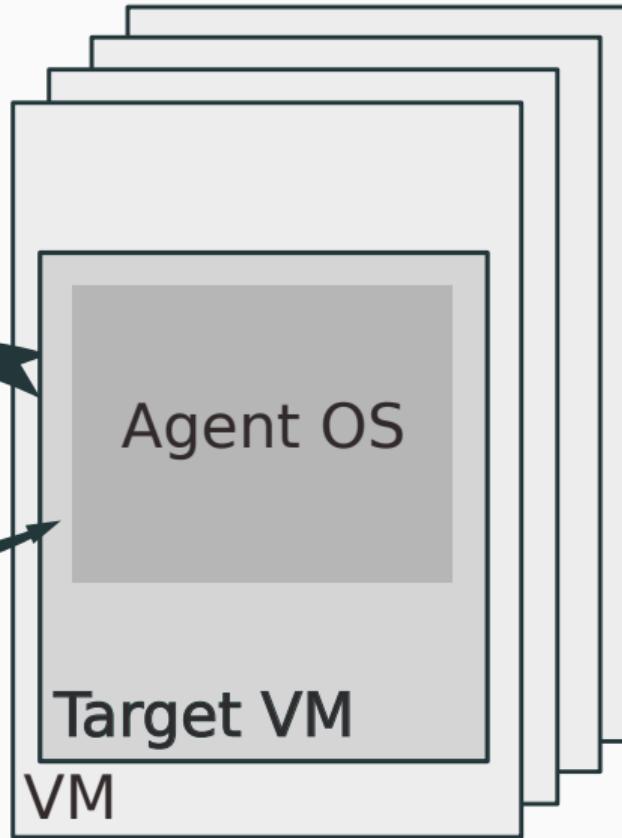
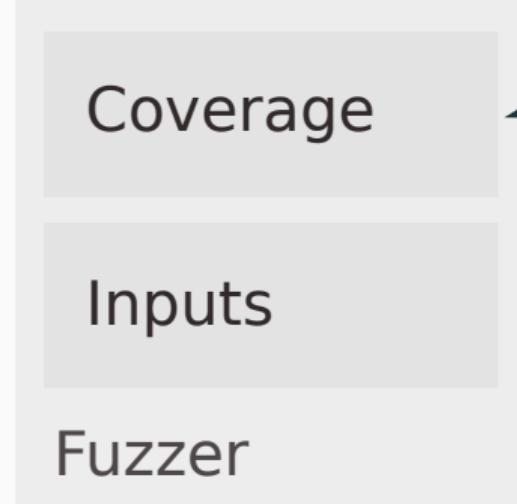


# Key Takeaways:

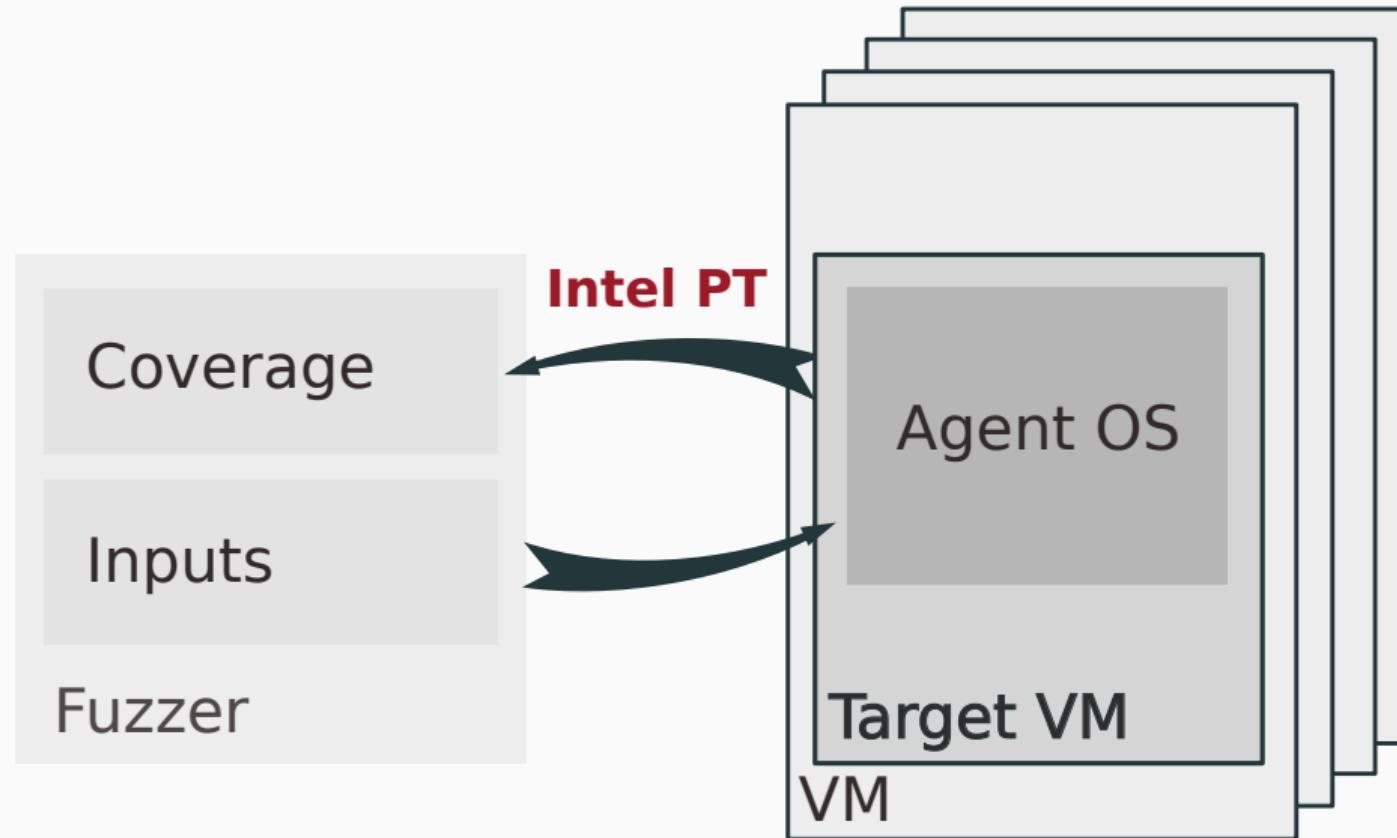
YO DAWG I HEARD YOU LIKE VIRTUAL  
MACHINES

SO I PUT A VIRTUAL MACHINE IN YOUR VIRTUAL  
MACHINE SO YOU CAN VIRTUAL MACHINE WHILE YOU  
VIRTUAL MACHINE

# Architecture



# Architecture



# Intel Processor Trace

## Intel PT Data

Taken

Not Taken

Target IP (0x1009)

Target IP (0x1055)

# Intel Processor Trace

Memory Dump

Intel PT Data

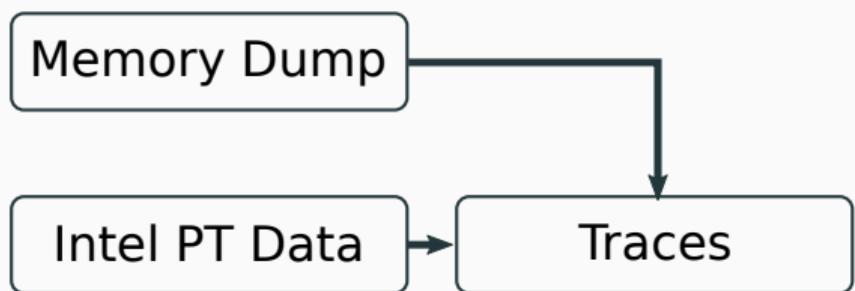
Taken

Not Taken

Target IP (0x1009)

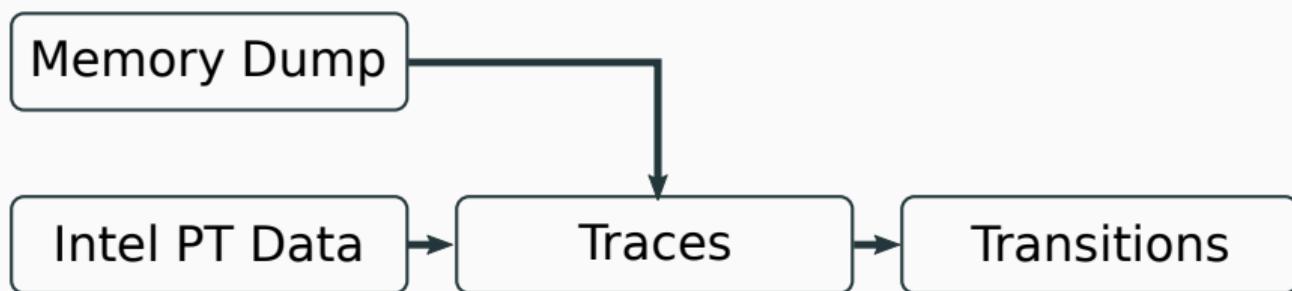
Target IP (0x1055)

# Intel Processor Trace



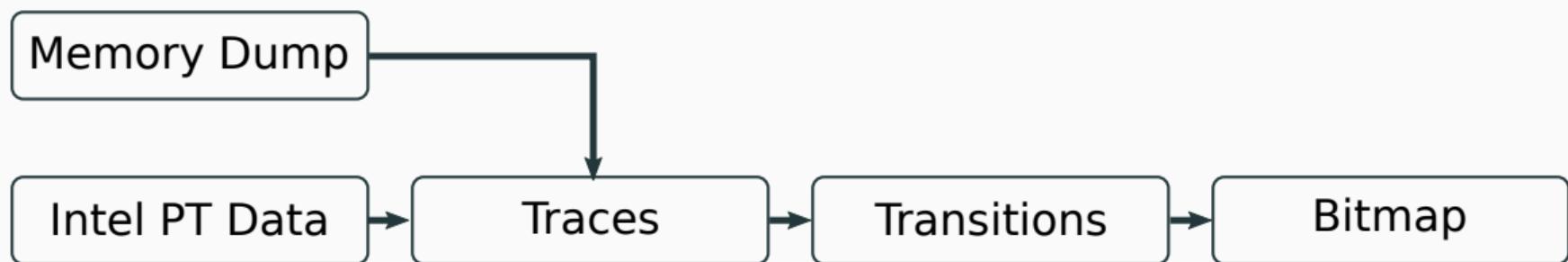
Taken	0x1000
Not Taken	0x1004
Target IP (0x1009)	0x1009
Target IP (0x1055)	0x1055

# Intel Processor Trace

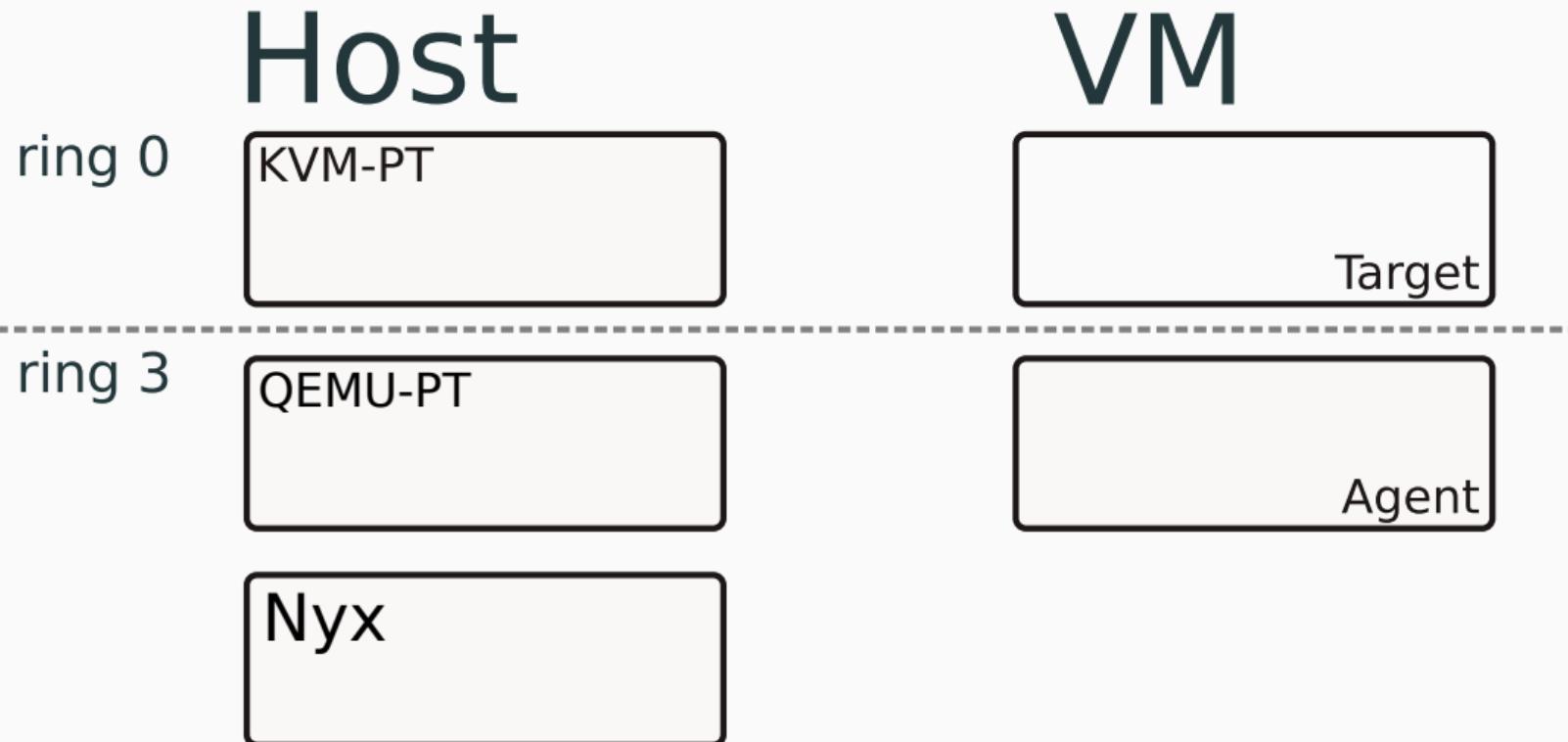


Taken	0x1000	0x0000 -> 0x1000
Not Taken	0x1004	0x1000 -> 0x1004
Target IP (0x1009)	0x1009	0x1004 -> 0x1009
Target IP (0x1055)	0x1055	

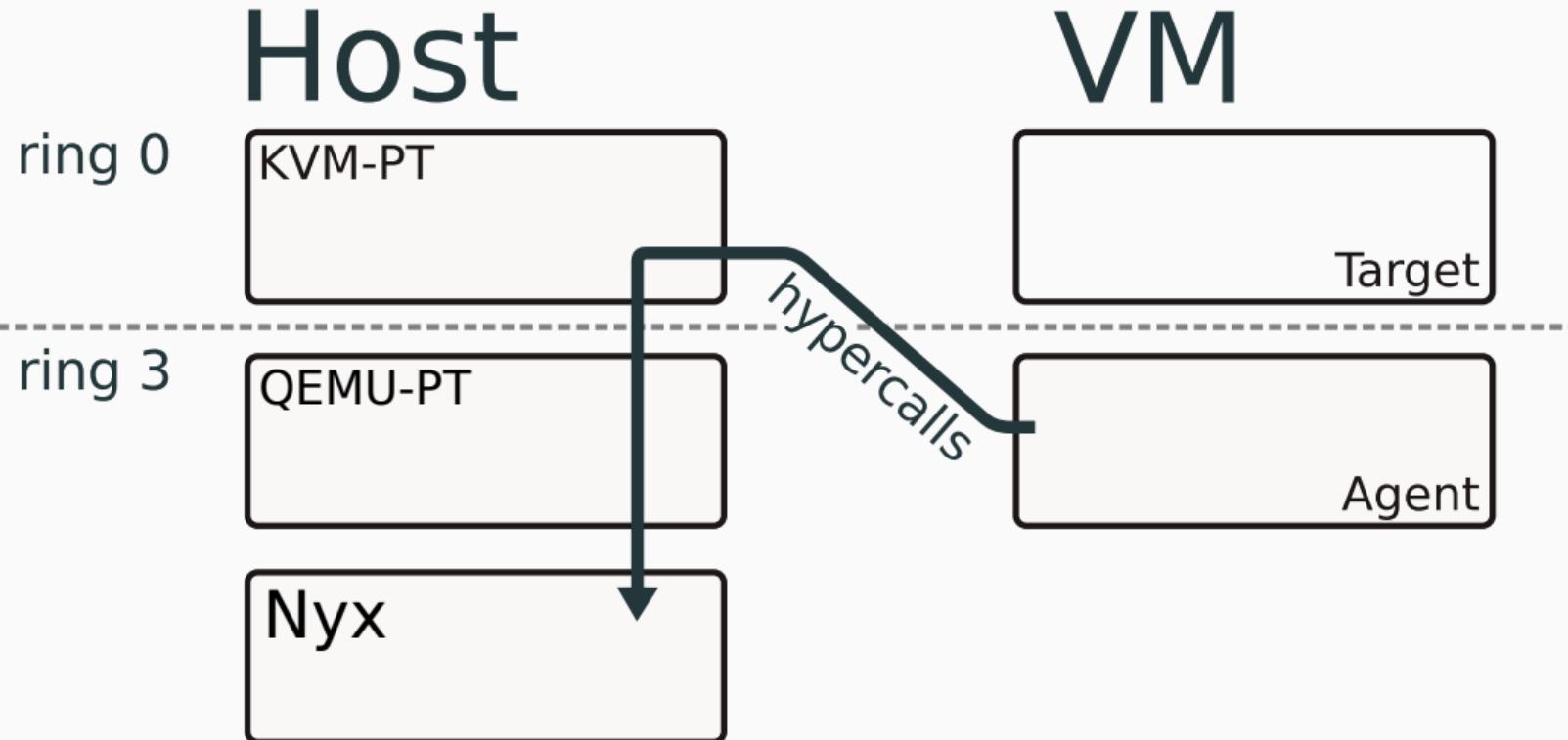
# Intel Processor Trace

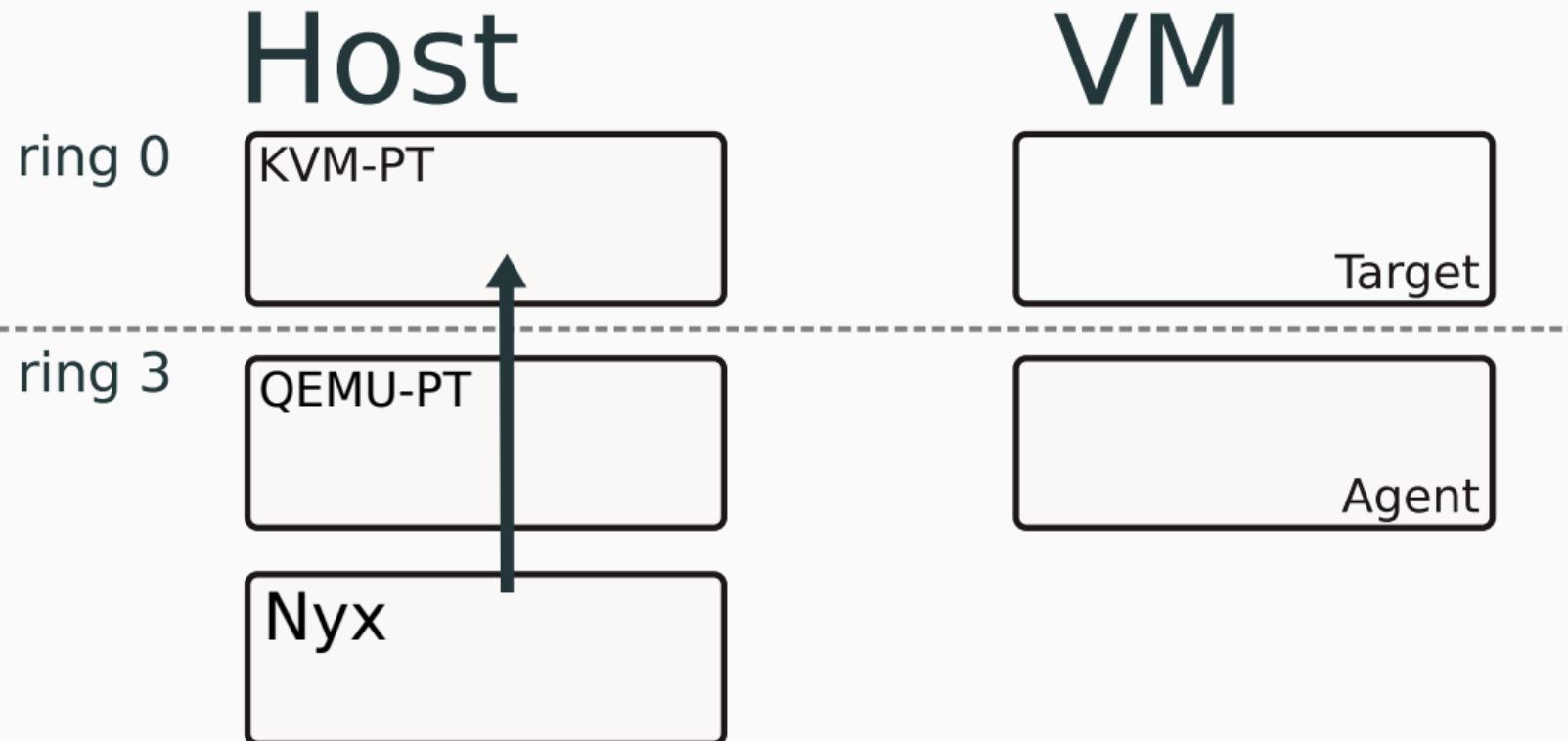


Taken	0x1000	0x0000 -> 0x1000	10010010100101
Not Taken	0x1004	0x1000 -> 0x1004	
Target IP (0x1009)	0x1009	0x1004 -> 0x1009	
Target IP (0x1055)	0x1055		

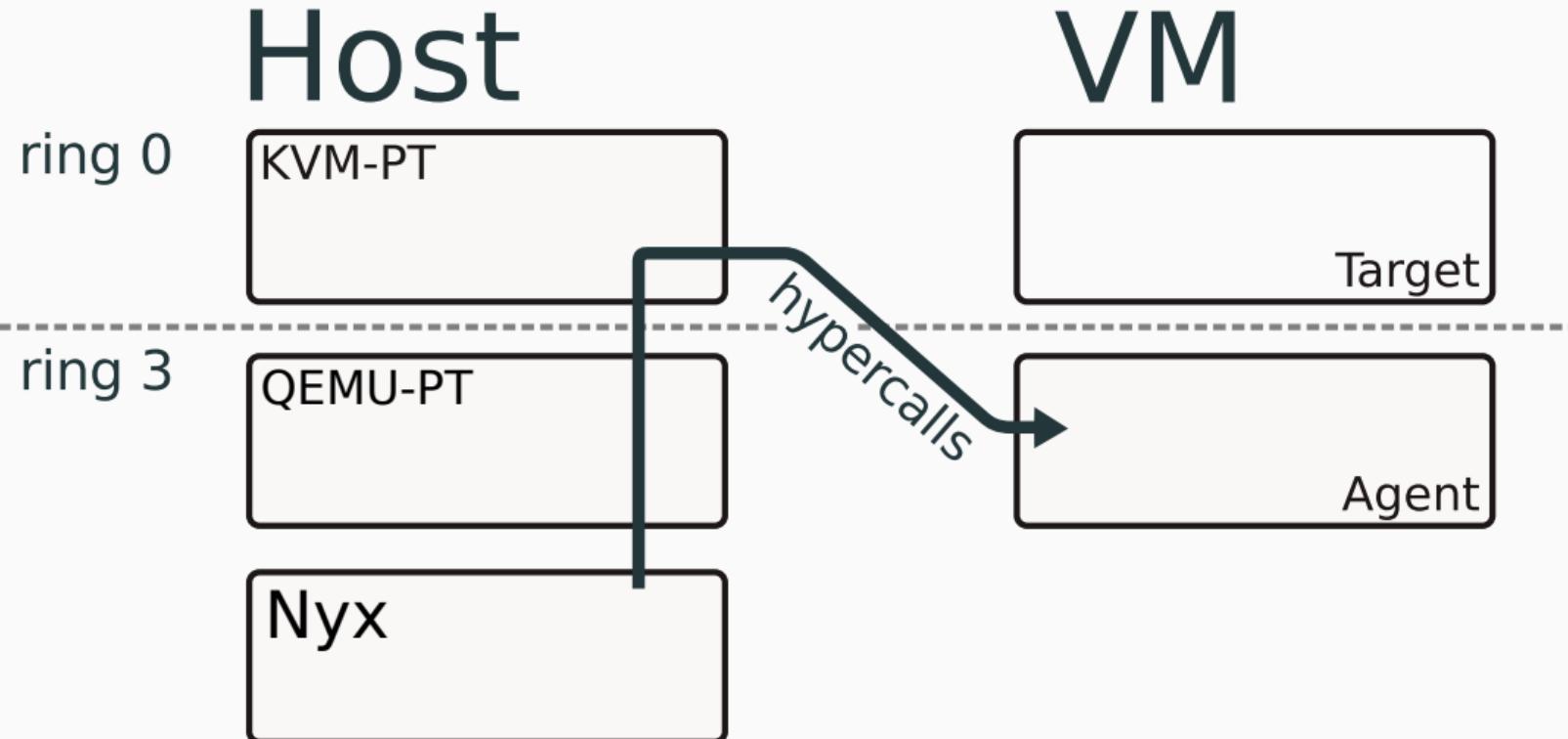


# Nyx - One Input

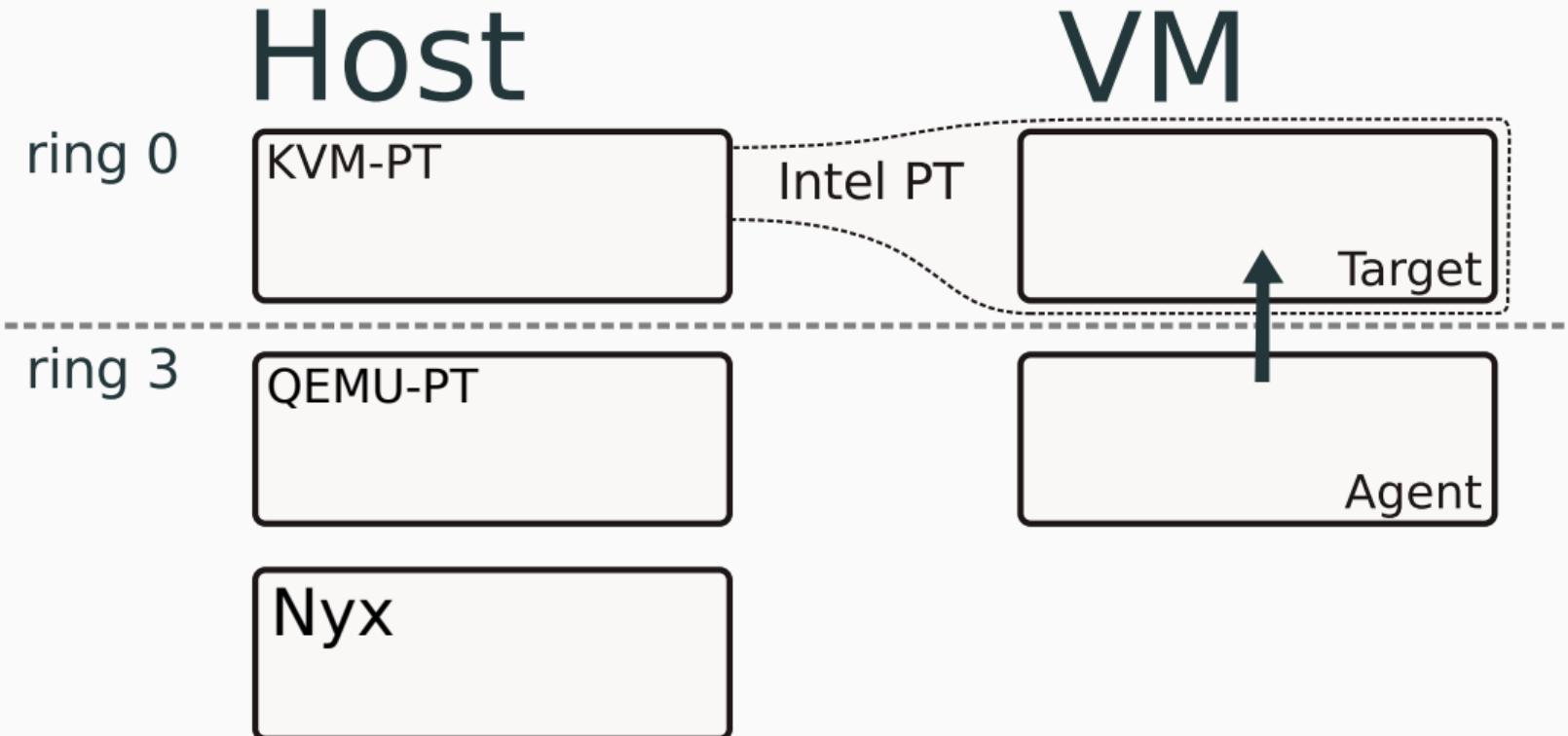




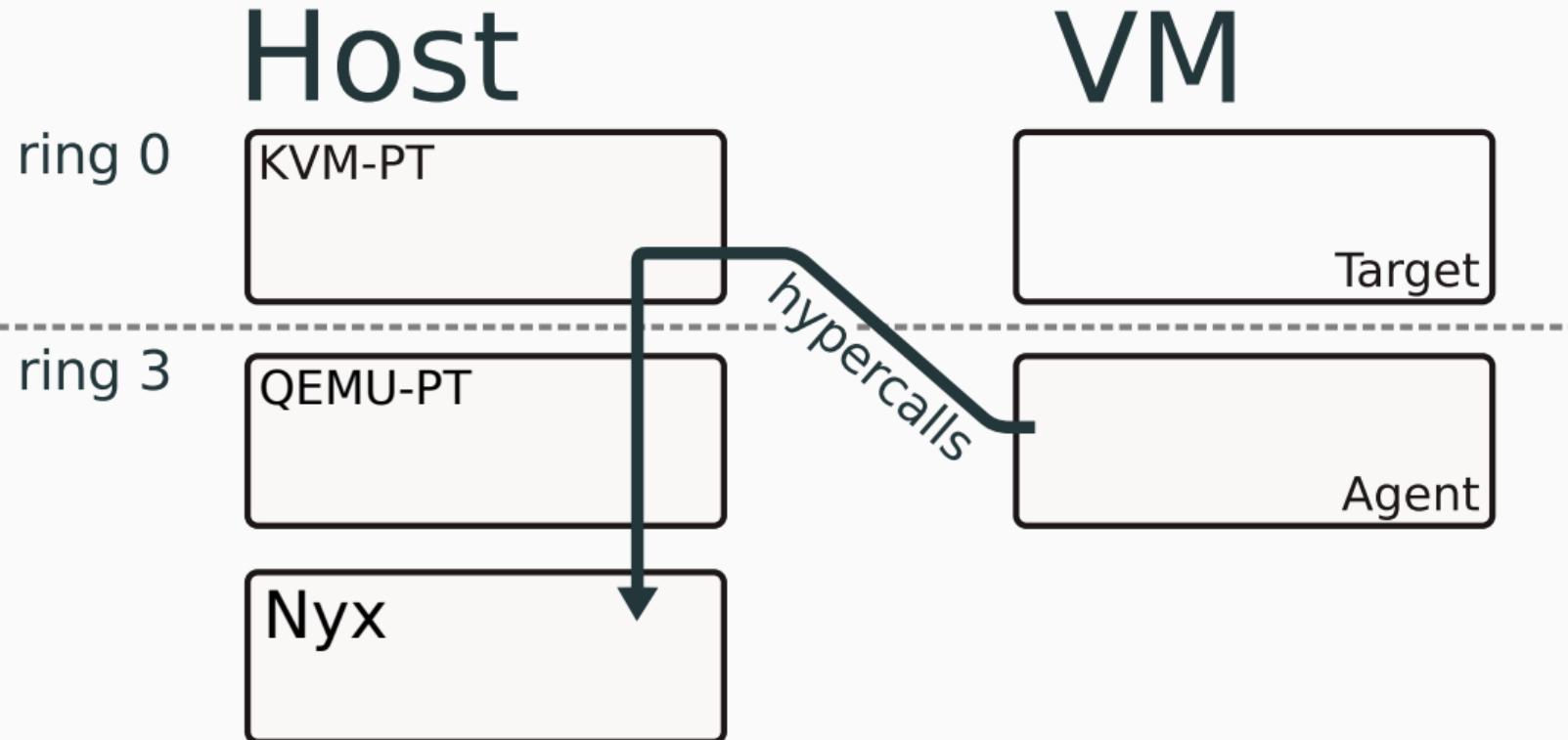
# Nyx - One Input



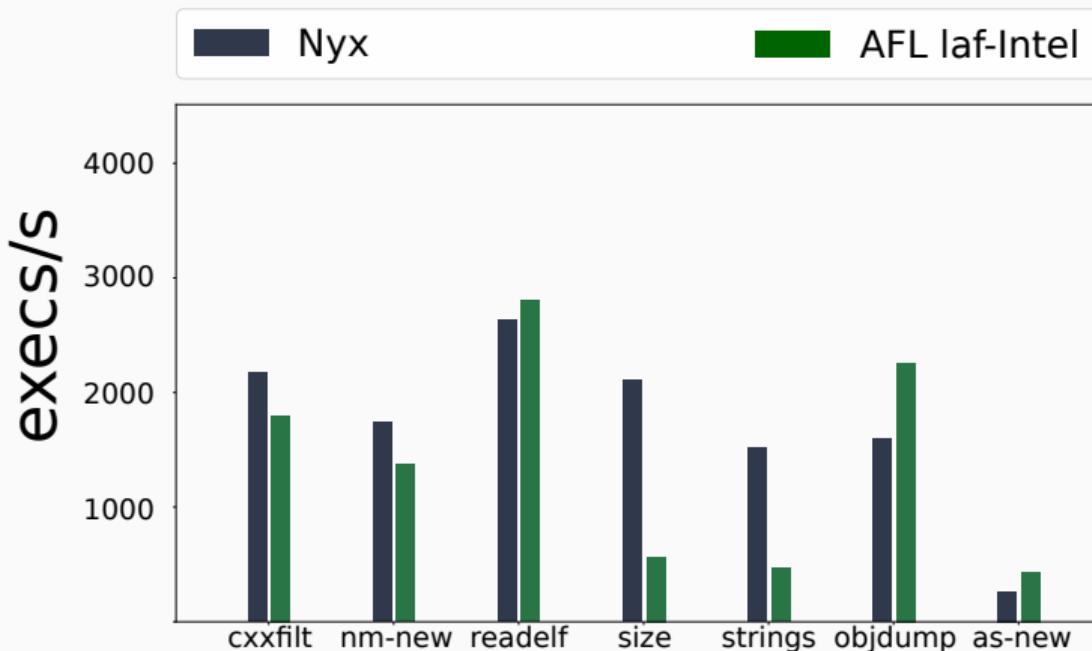
# Nyx - One Input



# Nyx - One Input



# Nyx - Performance



# Key Takeaways:



# What if I told you



...

# What if I told you



# We can be even faster!

Super Fast VM Reloads

~6000

times per second

## Flatten Qemu VMState Tree

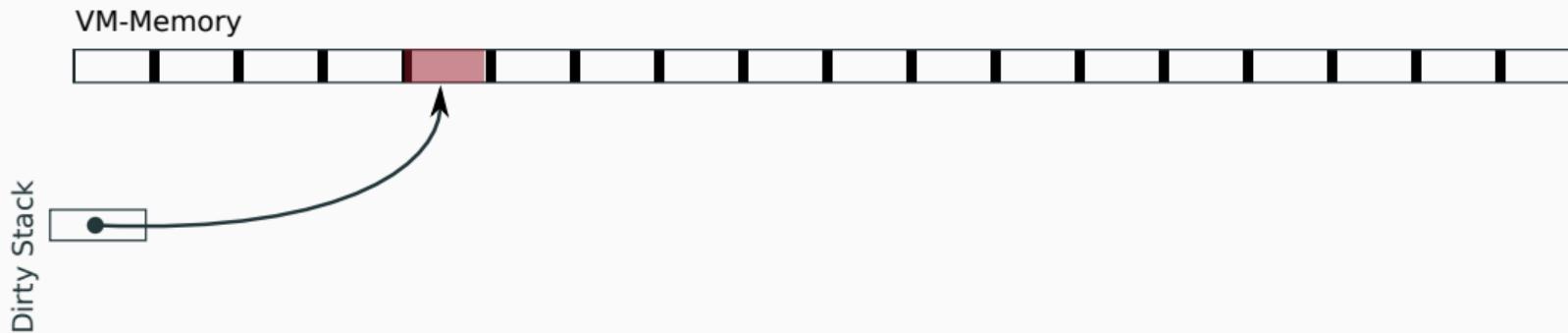


## Dirty Page Logging

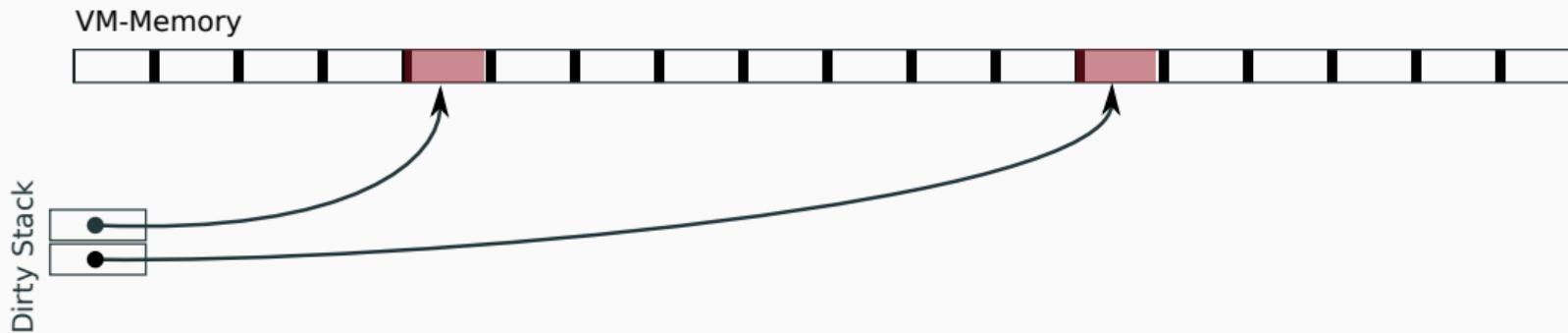
VM-Memory



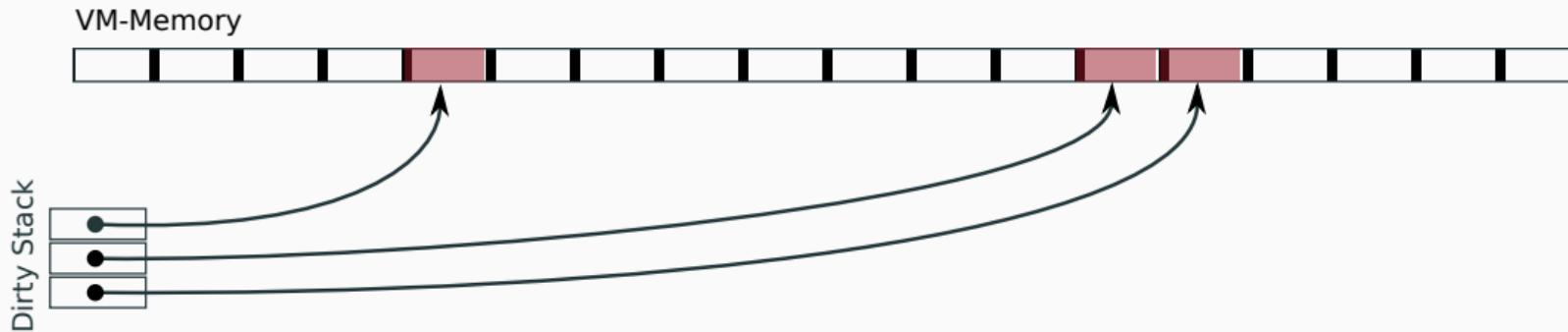
## Dirty Page Logging



## Dirty Page Logging



## Dirty Page Logging



Custom In-Memory  
Copy-On-Write  
Block Device Layer

O(1) Reset

Test: gdiplus\_test.exe

## Test: gdiplus\_test.exe

Just Spawning Processes  
*~80 execs/sec*

## Test: gdiplus\_test.exe

Just Spawning Processes  
*~80 execs/sec*

Spawn & File Write  
*~40 execs/sec*

## Test: gdiplus\_test.exe

Just Spawning Processes  
*~80 execs/sec*

Spawn & File Write  
*~40 execs/sec*

Nyx w. Intel PT & File Writes & Full System Reloads  
*~145 execs/sec!!!*



# Faster than Light

# Snapshots:

Avoid Startup Time

# Snapshots:

Avoid Startup Time

+ Noise free

# Snapshots:

Avoid Startup Time

+ Noise free

+ Statefulness

# Bugs



macOS High Sierra



TigerVNC



WINE



Parallels Desktop



binutils



Perl



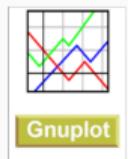
Qtjs



curl://



vmware Fusion



mruby



Fraunhofer FDK  
for Android™





macOS High Sierra



TigerVNC



WINE



Parallels Desktop



php



binutils



Perl



curl://



nasm  
the  
netwide  
assembler



Libxml2

Chakra  
Core

Windows

intel ACRN

EMU



ORACLE

VirtualBox



mtr



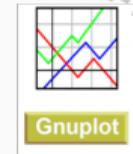
Lua

bhyve



libtiff

TCPDUMP



Gnuplot



BASH  
THE SOURCE-MATE SHELL

COUNTER STRIKE  
SOURCE

Fraunhofer FDK  
for Android™





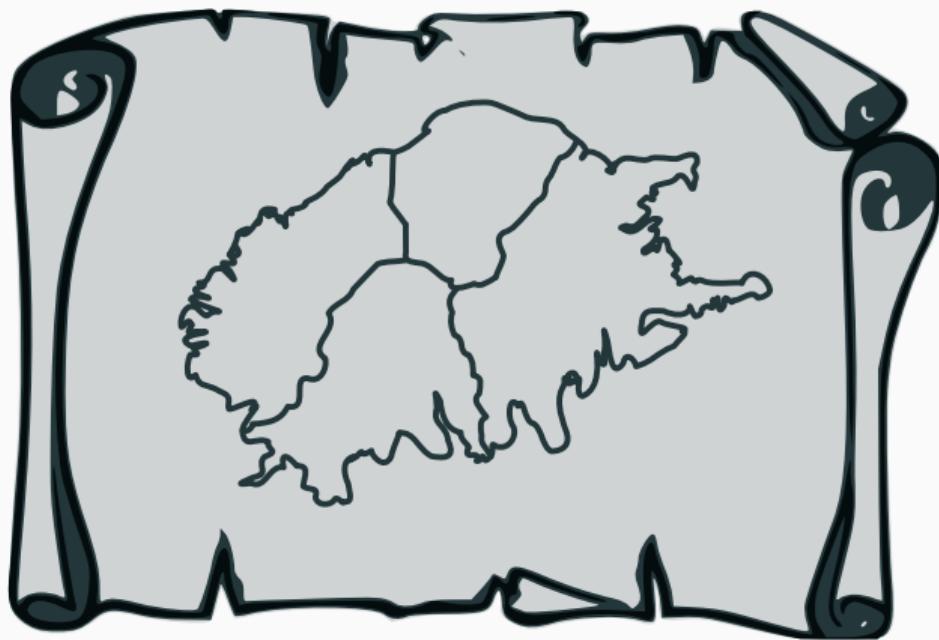
# Key Takeaways:



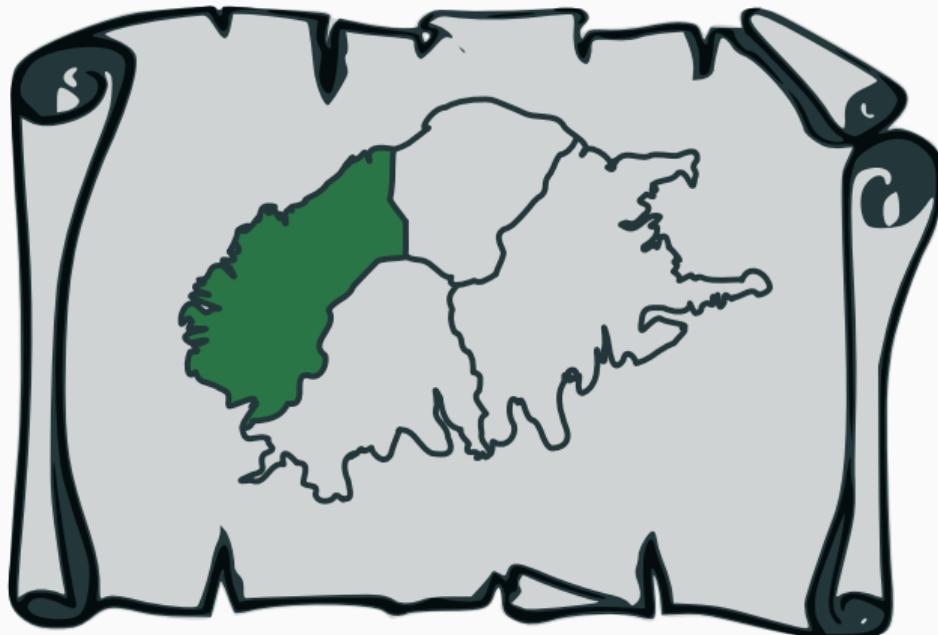
# The Rest of this Talk



The Future of  
Fuzzing



# Harnesses



# Harnesses



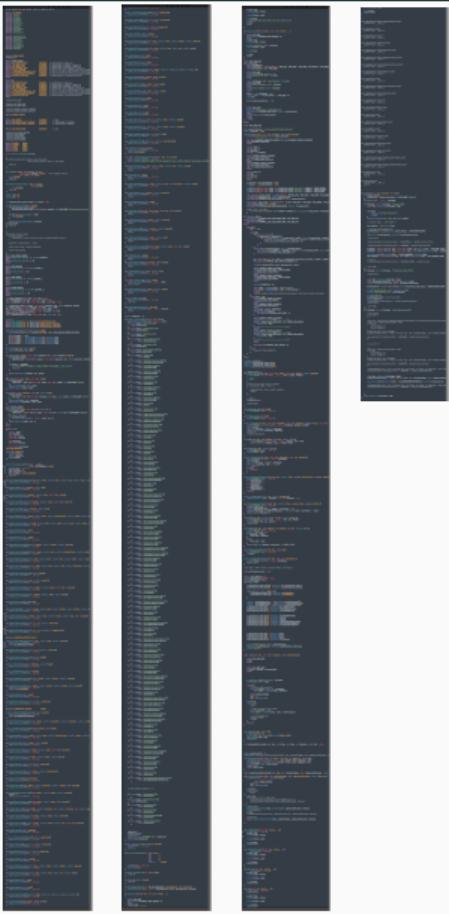
# Harnesses



# Harnesses



# Harnesses



# Harnesses

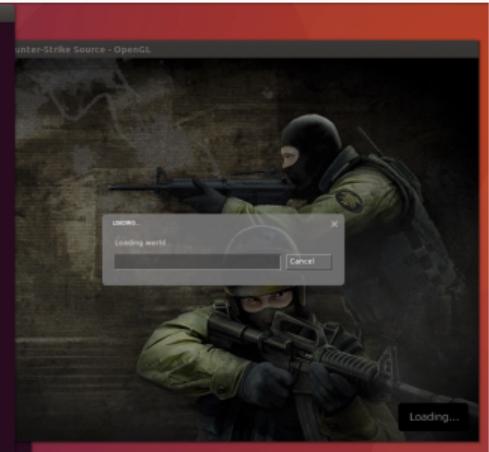


```
sergej@ubuntu:~/steam/steam/steamapps/common/Counter-Strike Source
Continuing.
[New Thread 0x1c1410b40 ((LWP 112252))]
[New Thread 0x1c1cfb40 ((LWP 112253))]
[New Thread 0x1ebdb40 ((LWP 112254))]
[Thread 0x1b0e40 ((LWP 112254) exited)]
[New Thread 0x1a9db40 ((LWP 112255))]
[New Thread 0x1e9bb40 ((LWP 112256))]
[New Thread 0x1e9bb40 ((LWP 112257))]
[Thread 0x190c40 ((LWP 112256) exited)]
[Thread 0x180b40 ((LWP 112257) exited)]
[New Thread 0x178a40 ((LWP 112258))]
[New Thread 0x178a40 ((LWP 112259))]
[Thread 0x178a40 ((LWP 112259) exited)]
[New Thread 0x1e15b040 ((LWP 112260))]
[New Thread 0x1e9cb40 ((LWP 112261))]
[New Thread 0x1ebdb40 ((LWP 112262))]

Thread 1 "hz_linux" received signal SIGSEGV, Segmentation fault.
[regs]
ECX: 0x00000000 EDX: 0x1f000000 ECX: 0x1f000000 EDX: 0x1f000000 ESI: 0x1e15b040 ECX: 0x1e15b040 EDX: 0x1e15b040 EIP: 0x00000000
CS: 0x0000 DS: 0x0000 FS: 0x0000 GS: 0x0000 SS: 0x0000

...[code]
=> 0x7e5ffff <_memcpy_sse2_unaligned+639: movntdq XMMWORD PTR [eb0],xmm0
0x7e56000 <_memcpy_sse2_unaligned+640: movntdq XMMWORD PTR [eb0+0x10],xmm1
0x7e56008 <_memcpy_sse2_unaligned+648: movntdq XMMWORD PTR [eb0+0x18],xmm2
0x7e560d0 <_memcpy_sse2_unaligned+653: movntdq XMMWORD PTR [eb0+0x20],xmm3
0x7e560d2 <_memcpy_sse2_unaligned+658: movntdq XMMWORD PTR [eb0+0x40],xmm4
0x7e560d7 <_memcpy_sse2_unaligned+663: movntdq XMMWORD PTR [eb0+0x50],xmm5
0x7e560d9 <_memcpy_sse2_unaligned+668: movntdq XMMWORD PTR [eb0+0x60],xmm6
0x7e560d1 <_memcpy_sse2_unaligned+673: movntdq XMMWORD PTR [eb0+0x70],xmm7

_memcpy_sse2_unaligned () at ..//sysdeps/i386/i686/multarch/_memcpy_sse2-unaligned.S:628
02B ..//sysdeps/i386/i686/multarch/_memcpy_sse2-unaligned.S: No such file or directory.
gdb: 1
```



# Harnesses

\$ █

# Harnesses

```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
WARNING: Readline services not available or not loaded.
WARNING: The auto-indent feature requires the readline library
Reading symbols from target...done.
gdb> █
```

# Harnesses

```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
WARNING: Readline services not available or not loaded.
WARNING: The auto-indent feature requires the readline library
Reading symbols from target...done.
gdb> b recv
Breakpoint 1 at 0x406d70
gdb> █
```

# Harnesses

```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
WARNING: Readline services not available or not loaded.
WARNING: The auto-indent feature requires the readline library
Reading symbols from target...done.
gdb> b recv
Breakpoint 1 at 0x406d70
gdb> run
Starting program: /tmp/target

Breakpoint 1, 0x406d70 in main ()
gdb> █
```

# Harnesses

```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
WARNING: Readline services not available or not loaded.
WARNING: The auto-indent feature requires the readline library
Reading symbols from target...done.
gdb> b recv
Breakpoint 1 at 0x406d70
gdb> run
Starting program: /tmp/target

Breakpoint 1, 0x406d70 in main ()
gdb> list
>...
123 recv_size = recv(fd, buf, max_size, flags);
>...
gdb> █
```

# Harnesses

```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
WARNING: Readline services not available or not loaded.
WARNING: The auto-indent feature requires the readline library
Reading symbols from target...done.
gdb> b recv
Breakpoint 1 at 0x406d70
gdb> run
Starting program: /tmp/target

Breakpoint 1, 0x406d70 in main ()
gdb> list
>...
123 recv_size = recv(fd, buf, max_size, flags);
>...
gdb> fuzz_set_size &recv_size
gdb> █
```

# Harnesses

```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
WARNING: Readline services not available or not loaded.
WARNING: The auto-indent feature requires the readline library
Reading symbols from target...done.
gdb> b recv
Breakpoint 1 at 0x406d70
gdb> run
Starting program: /tmp/target

Breakpoint 1, 0x406d70 in main ()
gdb> list
>...
123 recv_size = recv(fd, buf, max_size, flags);
>...
gdb> fuzz_set_size &recv_size
gdb> fuzz_set_max_size max_size
gdb> █
```

# Harnesses

```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
WARNING: Readline services not available or not loaded.
WARNING: The auto-indent feature requires the readline library
Reading symbols from target...done.
gdb> b recv
Breakpoint 1 at 0x406d70
gdb> run
Starting program: /tmp/target

Breakpoint 1, 0x406d70 in main ()
gdb> list
//...
123 recv_size = recv(fd, buf, max_size, flags);
//...
gdb> fuzz_set_size &recv_size
gdb> fuzz_set_max_size max_size
gdb> fuzz_set_buff buf
gdb> █
```

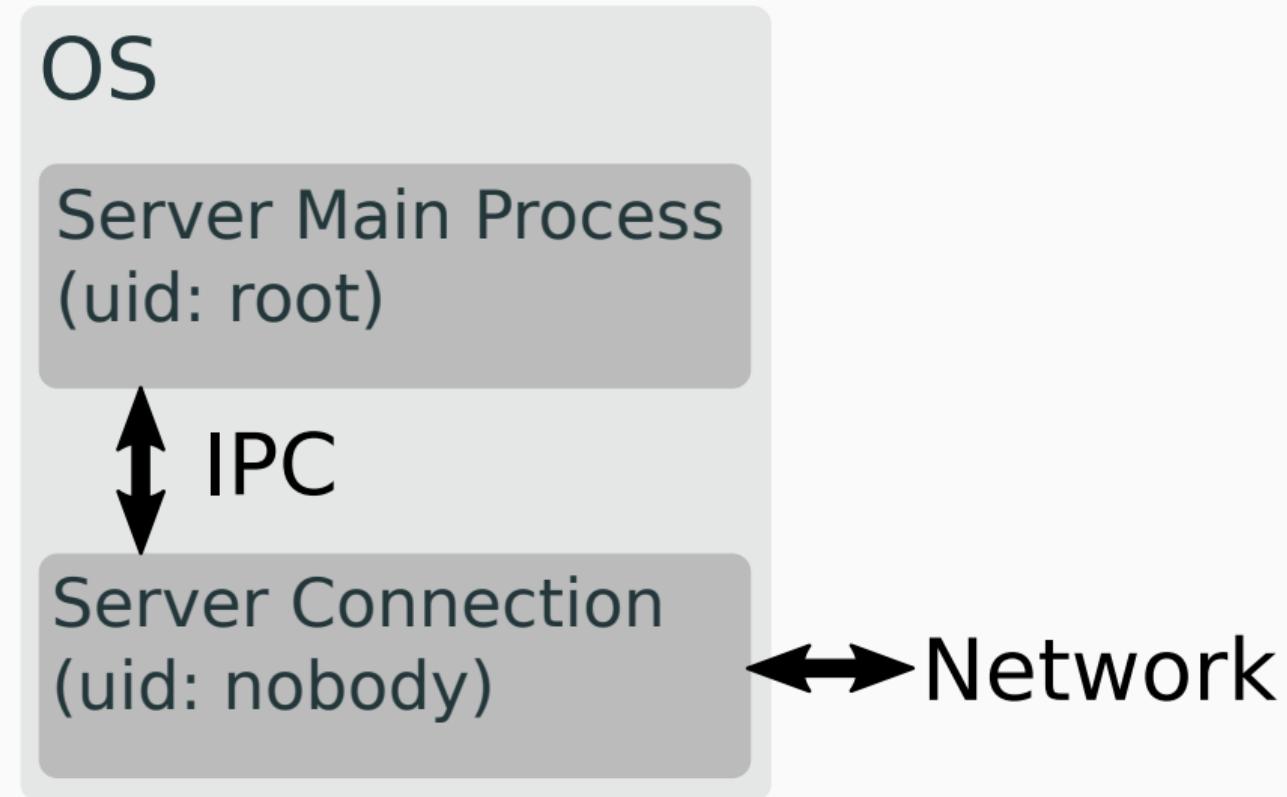
# Harnesses

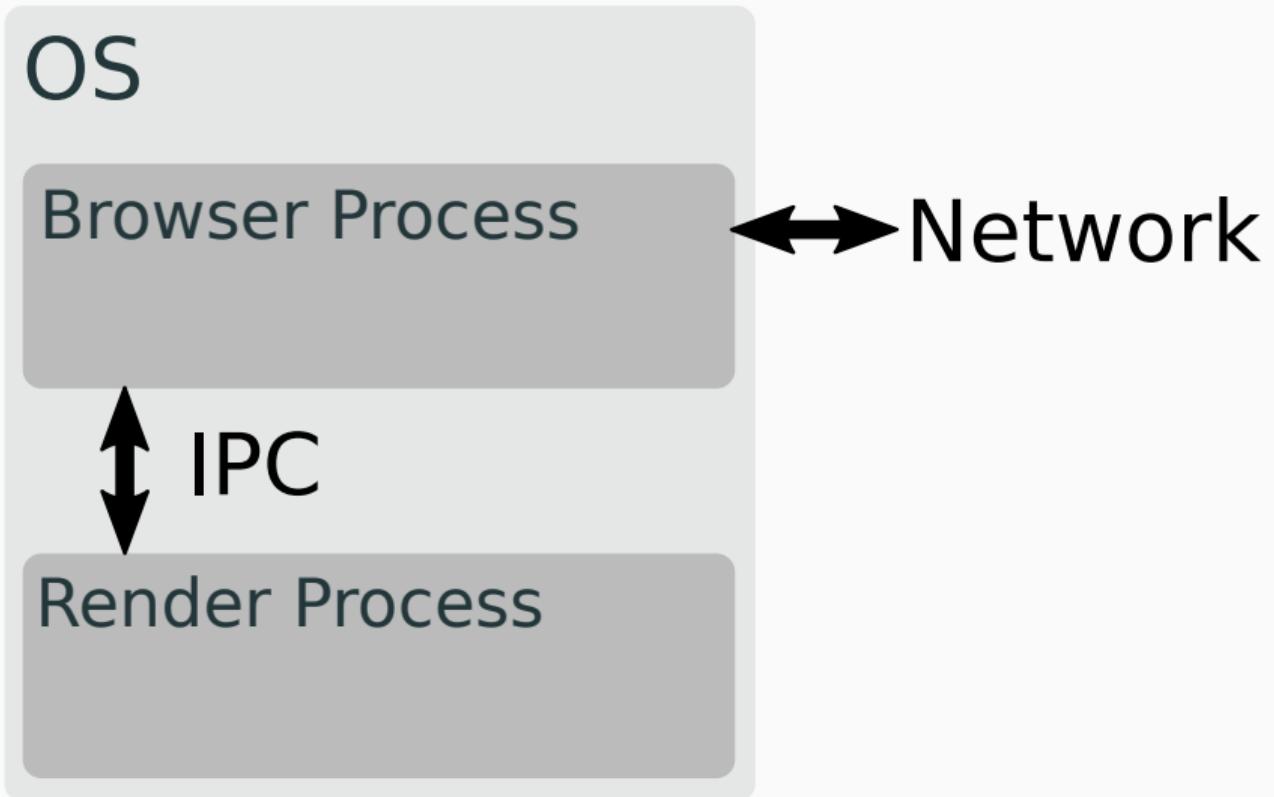
```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
WARNING: Readline services not available or not loaded.
WARNING: The auto-indent feature requires the readline library
Reading symbols from target...done.
gdb> b recv
Breakpoint 1 at 0x406d70
gdb> run
Starting program: /tmp/target

Breakpoint 1, 0x406d70 in main ()
gdb> list
//...
123 recv_size = recv(fd, buf, max_size, flags);
//...
gdb> fuzz_set_size &recv_size
gdb> fuzz_set_max_size max_size
gdb> fuzz_set_buff buf
gdb> run_fuzzer
```

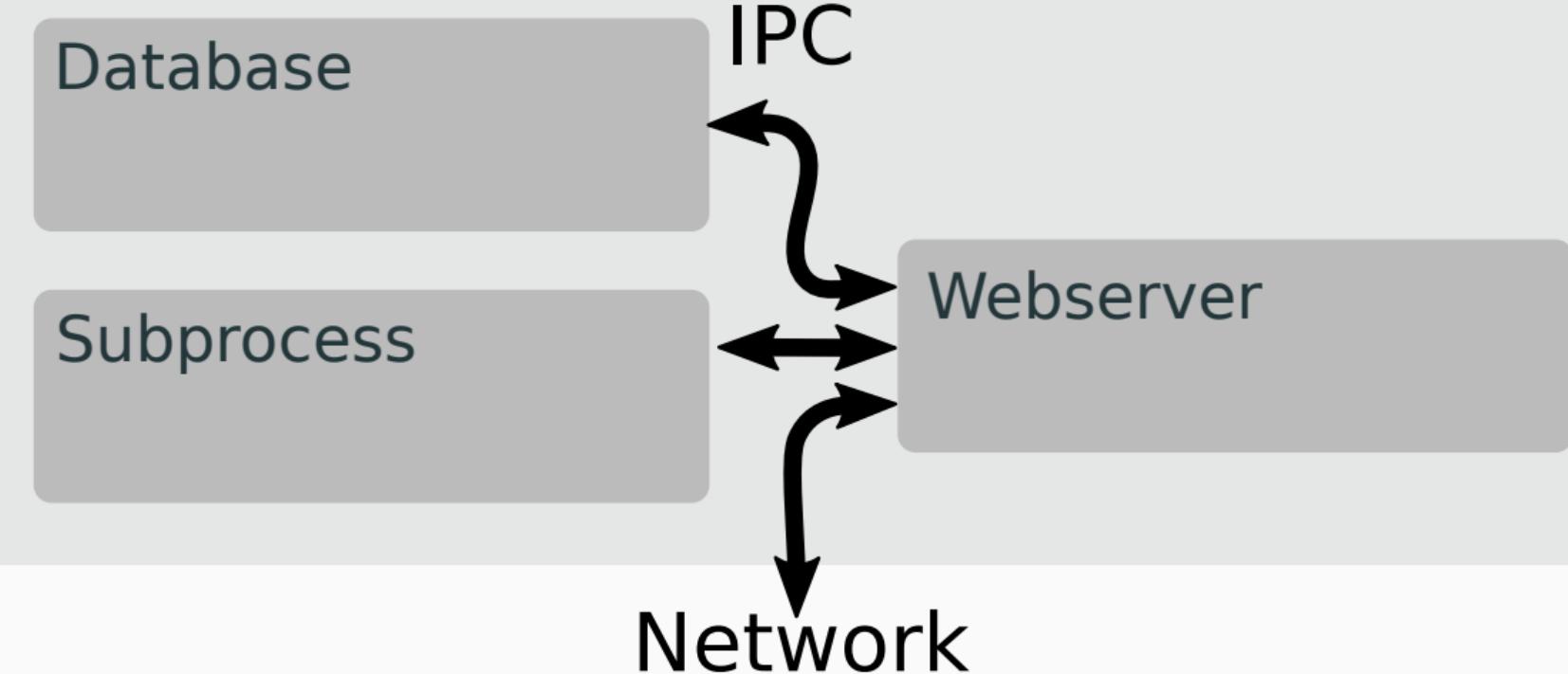
# Harnesses

american fuzzy lop 2.52b (target)		
process timing	run time : 0 days, 0 hrs, 0 min, 23 sec last new path : 0 days, 0 hrs, 0 min, 0 sec last uniq crash : none seen yet last uniq hang : none seen yet	overall results cycles done : 0 total paths : 142 uniq crashes : 0 uniq hangs : 0
cycle progress	now processing : 81 (57.04%) paths timed out : 0 (0.00%)	map coverage map density : 0.44% / 2.22% count coverage : 1.73 bits/tuple
stage progress	now trying : splice 13 stage execs : 23/24 (95.83%) total execs : 73.9k exec speed : 3140/sec	findings in depth favored paths : 72 (50.70%) new edges on : 100 (70.42%) total crashes : 0 (0 unique) total timeouts : 0 (0 unique)
fuzzing strategy yields	bit flips : n/a, n/a, n/a byte flips : n/a, n/a, n/a arithmetics : n/a, n/a, n/a known ints : n/a, n/a, n/a dictionary : n/a, n/a, n/a havoc : 99/47.7k, 25/24.0k trim : 60.68%/992, n/a	path geometry levels : 4 pending : 94 pend fav : 35 own finds : 124 imported : 16 stability : 100.00%
[cpu000: 14%]		

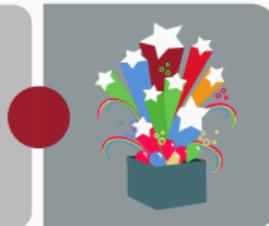




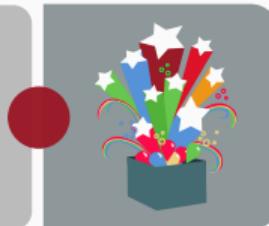
OS



Database



Subprocess



Webserver



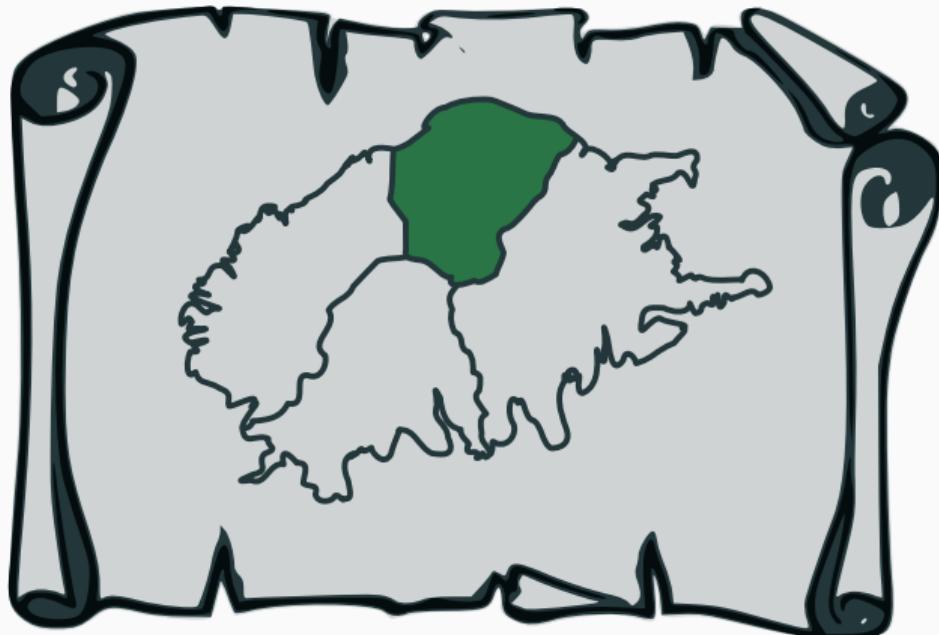
# Key Takeaways:



Improve

Usability

# Interactive Targets



# Interactive Targets



# Specify Test Scenarios

```
img = Data(0x00, 0x23, 0x54, ... )
mnt = mount(img);
dat = "";
path = "/a"
mnt.create_file(path, data);
mnt.cwd(path);
mnt.umount();
```

# Specify Test Scenarios

```
img = Data(0x00, 0x23, 0x54, ... )  
mnt = mount(img);  
dat = "";  
path = "/a"  
mnt.create_file(path, data);  
mnt.cwd(path);  
mnt.umount();
```



Grammar  
Fuzzing?

# Specify Test Scenarios

```
img = Data(0x00, 0x23, 0x54, ... )  
mnt = mount(img);  
dat = "";  
path = "/a"  
mnt.create_file(path, data);  
mnt.cwd(path);  
mnt.umount();
```



Mutated  
AFL-Style

# Specify Test Scenarios

```
img = NtfsImg(headers, clusters, ...)  
mnt = mount(img);  
dat = "";  
path = "/a"  
mnt.create_file(path, data);  
mnt.cwd(path);  
mnt.umount();
```



Structural  
Mutations

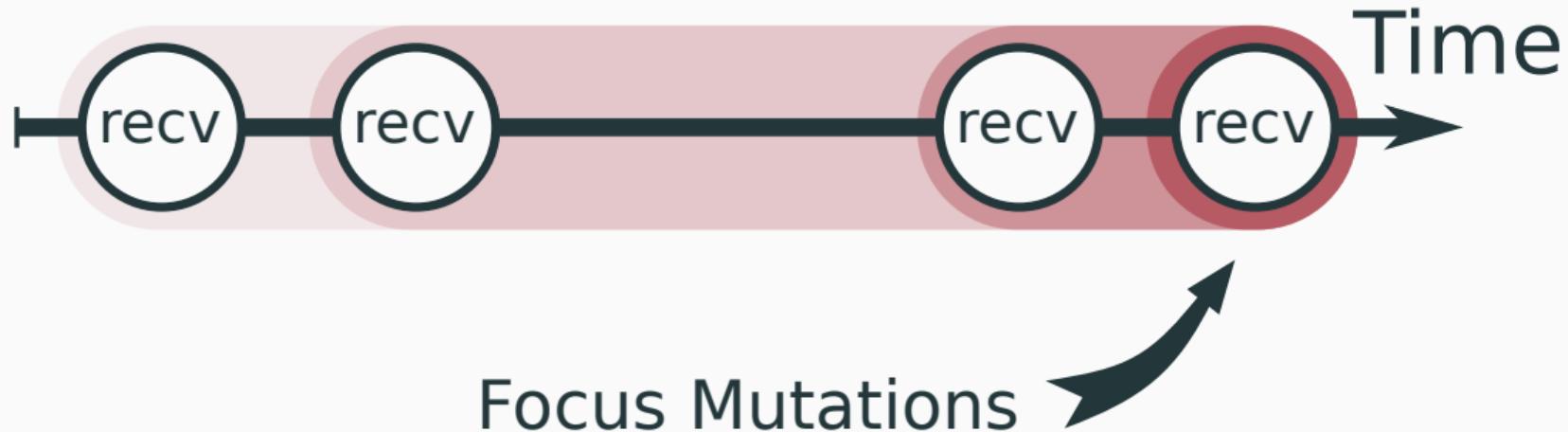
# Specify Test Scenarios

```
img = Data(0x00, 0x23, 0x54, ... )  
mnt = mount(img);  
dat = "";  
path = "/a"  
mnt.create_file(path, data);  
mnt.cwd(path);  
mnt.umount();
```



Not reused

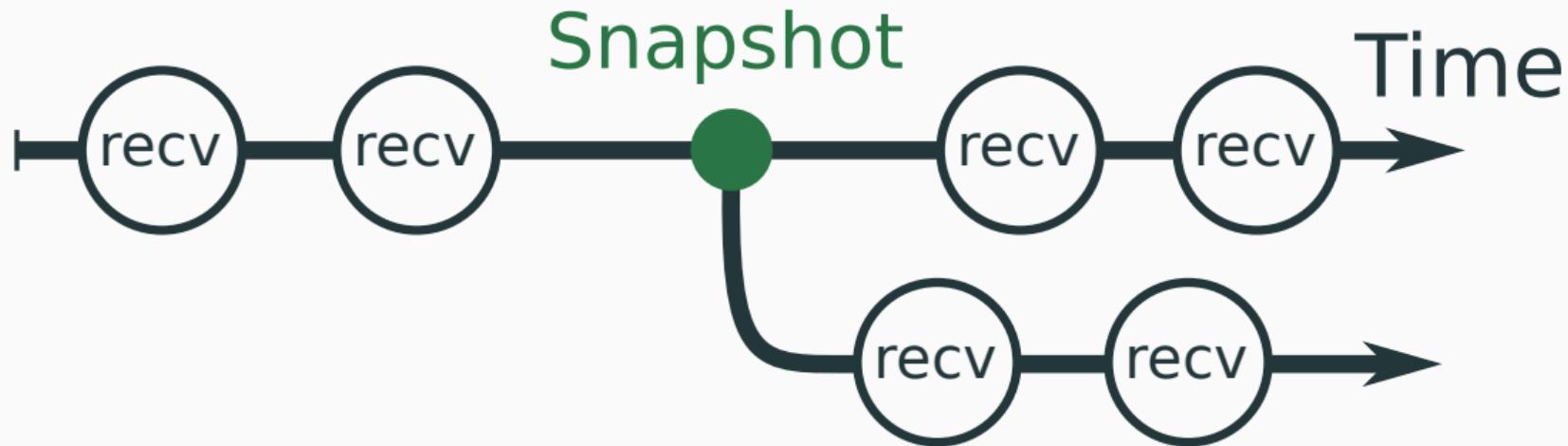
# Interactive Targets



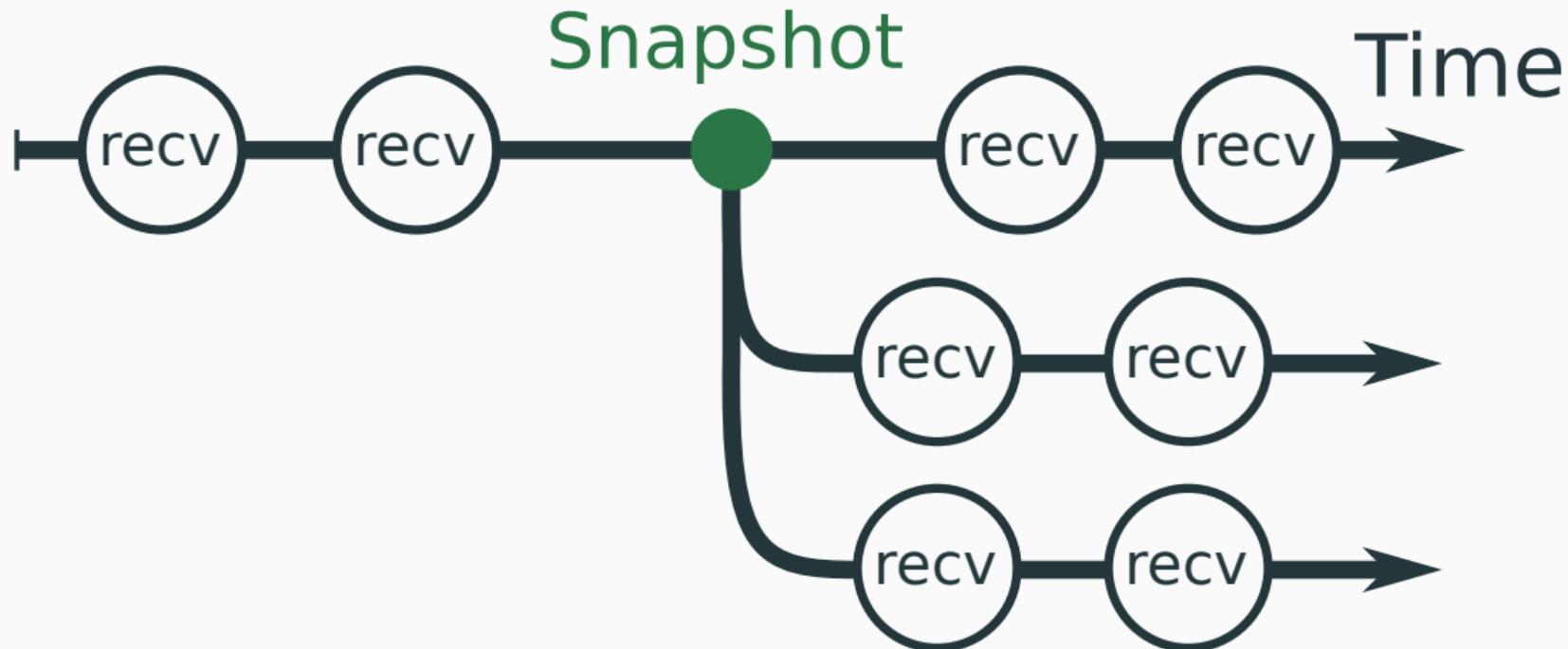
# Interactive Targets

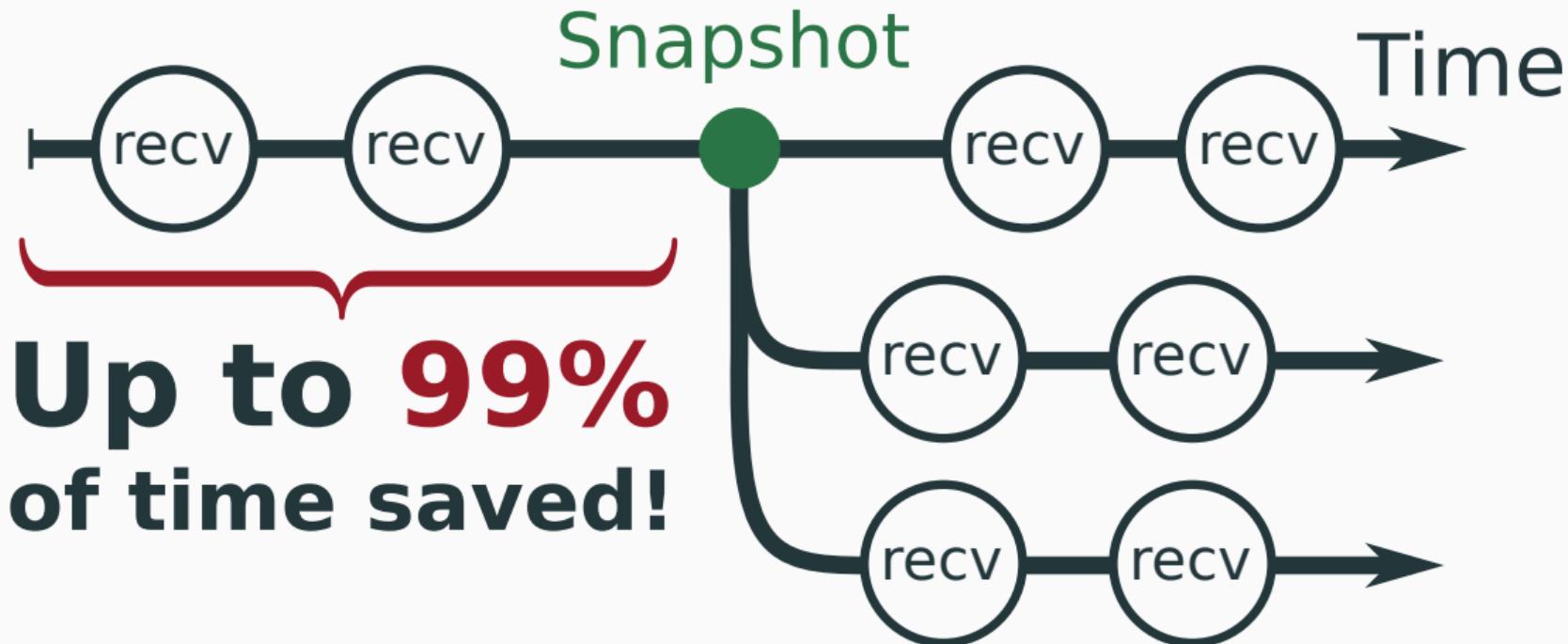


# Interactive Targets



# Interactive Targets





**Up to 99%**  
**of time saved!**

# Kernel Testing meets Feedback Fuzzing

[1] <https://github.com/google/syzkaller>

# Network Protocol meets Feedback Fuzzing

# Webcrawler meets Feedback Fuzzing

# Key Takeaways:

We need

Bigger Guns

A man with long hair and tattoos, wearing a vest, sits on a motorcycle with a large machine gun mounted on the front. He is in a desert-like environment with barrels and a burning fire in the background.

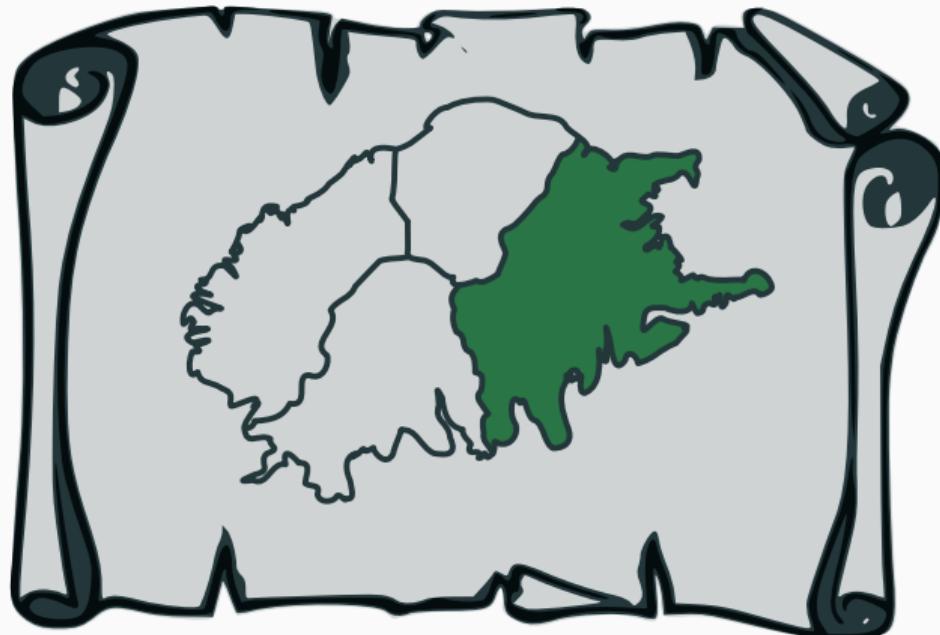
# Key Takeaways:

We need

Better Specs



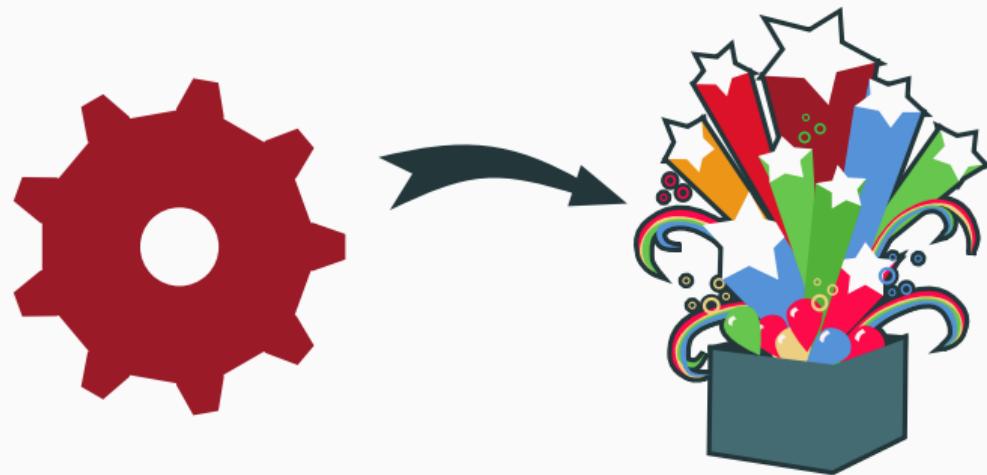
# Using Fuzzers



# Fuzzing



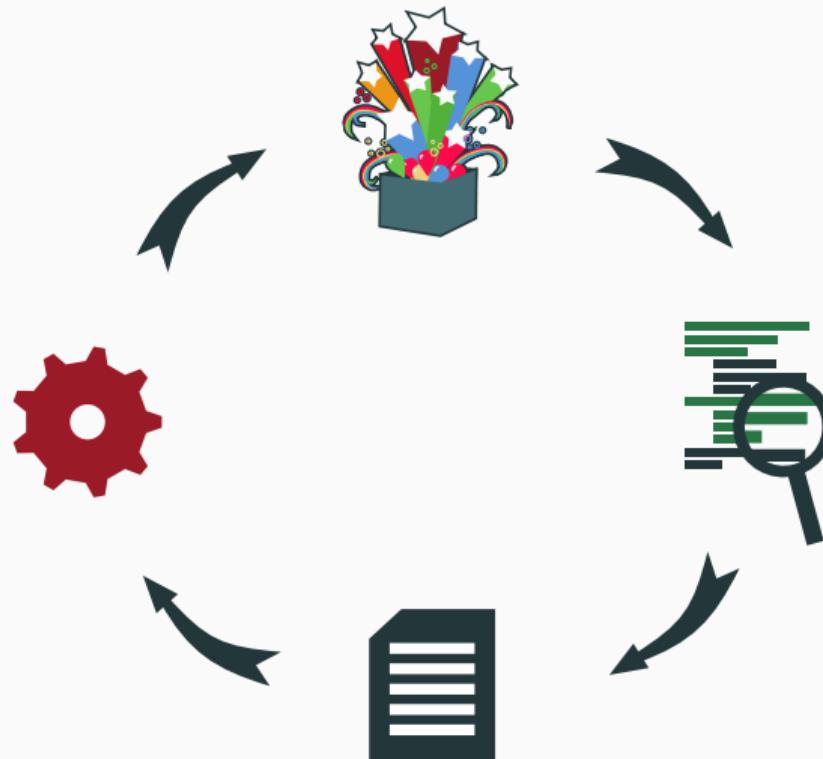
# Fuzzing



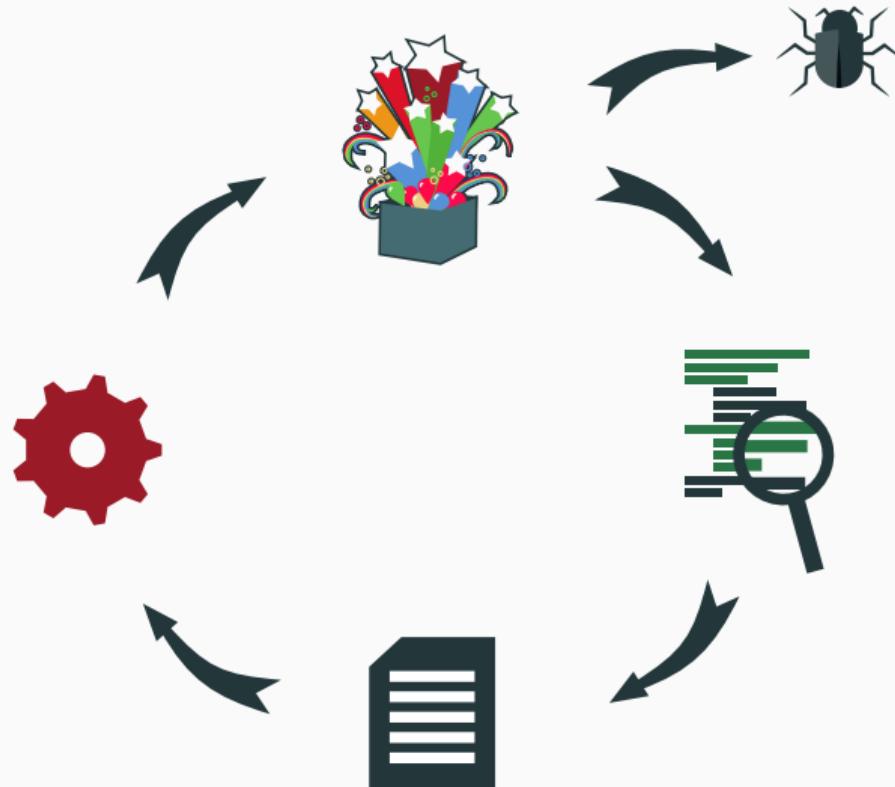
# Fuzzing



# Fuzzing



# Fuzzing



# Fuzzing

RUHR  
UNIVERSITÄT  
BOCHUM

RUB

IJON 🐸 Dashboard Coverage Queue

Files

Transitions Inputs (1) Search Filter

Ret:

↳ line 29

↳ line 28

test\_data/test.c 22/24

```
3 void foo(int a){  
4     printf("got %d\n", a);  
5 }  
  
6 void test(int a,int b){  
7     while(a>0){  
8         if(b==0){printf("b<a\n");return;}  
9         a--;  
10        b--;  
11    }  
12 }  
13 if(b==0){printf("b==a\n");return;}  
14 printf("b>a\n");  
15 return;  
16 }  
17  
18 int main()  
19 {  
20     int a,b;  
21     printf("Enter something:\n");  
22     scanf("%d", &a);  
23     printf("Enter something else:\n");  
24     scanf("%d", &b);  
25     if(a > 0 && b < 50){  
26         if(b > 0 && b < 50){  
27             foo(a);  
28             foo(b);  
29             test(a,b);  
30         }  
31     }  
32 }  
33 return 0;  
34 }  
35  
36  
37  
38  
39  
40  
41 //some  
42 //more  
43 //lines  
44 //just  
45 //to  
46 //test  
47 //long  
48 //files  
49 //  
50 //  
51 //  
52 //  
53 //  
54 //  
55 //  
56 //  
57 //
```

```
^0x400646 push rbp  
0x400647 mov rbp, rsp  
0x400648 sub rsp, 0x10  
0x400649 mov dword ptr [rbp - 4], edi  
0x400651 mov eax, dword ptr [rbp - 4]  
0x400651 mov esi, eax  
0x400652 xor edx, 0x40077f4  
0x400653 mov eax, 0  
0x400654 call 0x4800510  
0x400655 nop  
0x400656 leave  
0x400657 ret  
0x400658 push rbp  
0x400659 mov rbp, rsp  
0x400660 sub rsp, 0x10  
0x400670 mov dword ptr [rbp - 4], edi  
0x400673 mov dword ptr [rbp - 8], esi  
0x400674 jne 0x480692  
0x400675 cmp dword ptr [rbp - 8], 0  
0x400676 jne 0x480680  
0x400677 mov edi, 0x48077fc  
0x400683 call 0x48084f8  
0x400688 jmp 0x4806b5  
0x400689 sub dword ptr [rbp - 4], 1  
0x40068e sub dword ptr [rbp - 8], 1  
0x400692 cmp dword ptr [rbp - 4], 0  
0x400696 jg 0x480670  
0x400698 cmp dword ptr [rbp - 8], 0  
0x40069c jne 0x48069a  
0x40069e mov edi, 0x4808000  
0x4006a3 call 0x48084f8  
0x4006a8 jmp 0x4806b5  
0x4006a9 mov edi, 0x4808005  
0x4006af call 0x48084f8  
0x4006b1 nop  
0x4006b2 leave  
0x4006b3 ret  
0x4006b7 push rbp  
0x4006b8 mov rbp, rsp  
0x4006b9 sub rsp, 0x10  
0x4006bf mov rax, qword ptr fs:[0x20]  
0x4006c5 mov qword ptr [rbp - 8], rax  
0x4006cc xor eax, eax  
0x4006ca mov edi, 0x4808000  
0x4006d3 call 0x48084f8  
0x4006d5 lea rax, qword ptr [rbp - 0x10]  
0x4006dc mov rsi, rax  
0x4006d7 mov edi, 0x480881a  
0x4006e4 mov eax, 0  
0x4006e9 call 0x4808538  
0x4006ee mov edi, 0x480881d  
0x4006f3 call 0x48084f8  
0x4006f8 lea rax, qword ptr [rbp - 0xc]  
0x4006fc mov rsi, rax  
0x4006ff mov edi, 0x480881a  
^0x4006f4 mov eax, 0
```

# Demo

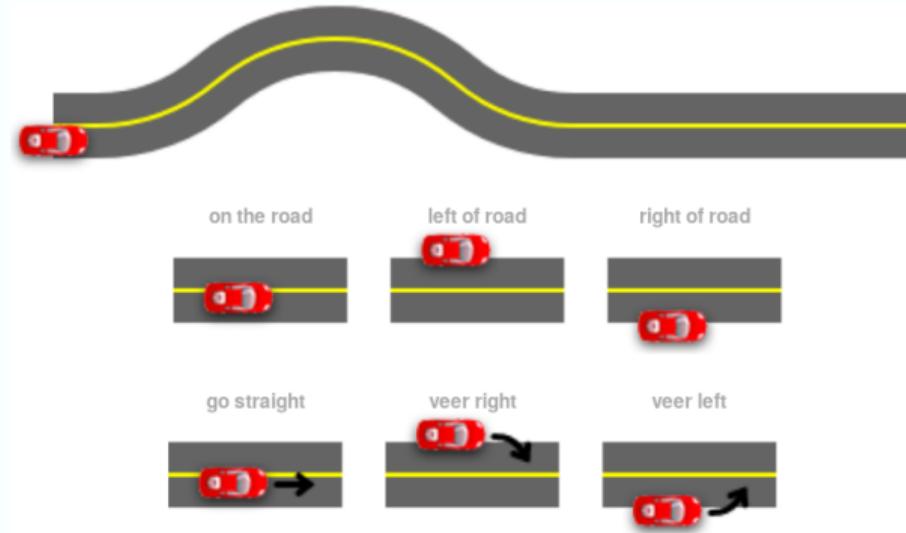
# Fuzzing

Create Analysis Tools that  
**Abstract away Inputs**

# Fuzzing



# Fuzzing



# Fuzzing



Debugger (gdb, olly, ... )

# Fuzzing



Debugger (gdb, olly, ... )

# Fuzzing



Debugger (gdb, olly, ... )

# Fuzzing



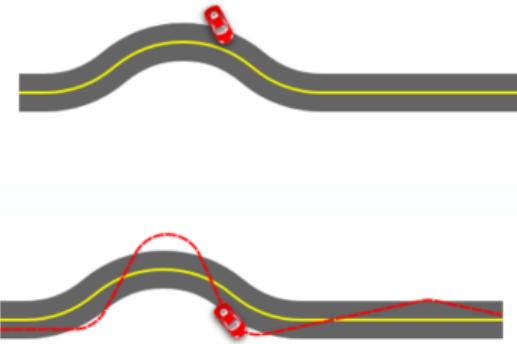
Debugger (gdb, olly, ... )

# Fuzzing



Debugger (gdb, olly, ... )

# Fuzzing

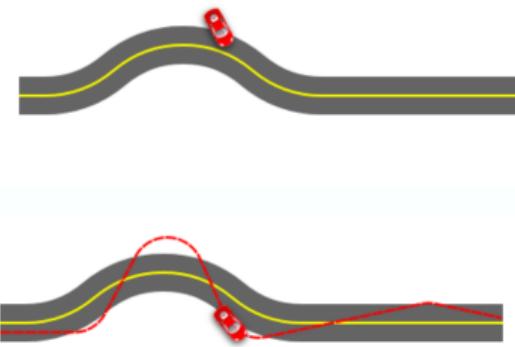


Debugger (gdb, olly, ... )



**Abstract away Time**  
Time traveling Debugger  
(rr, REVEN, ... )

# Fuzzing



Debugger (gdb, olly, ... )

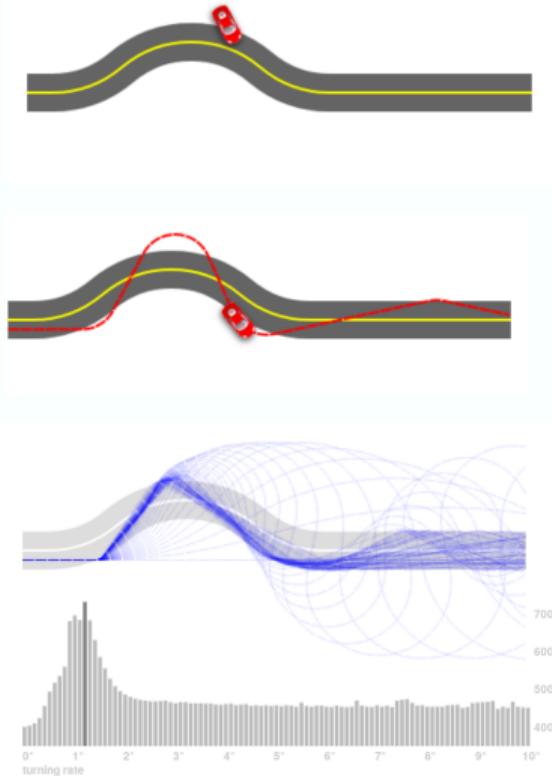


**Abstract away Time**  
Time traveling Debugger  
(rr, REVEN, ... )



**Abstract away Inputs**  
Fuzzing Debugger  
????

# Fuzzing



Debugger (gdb, olly, ... )

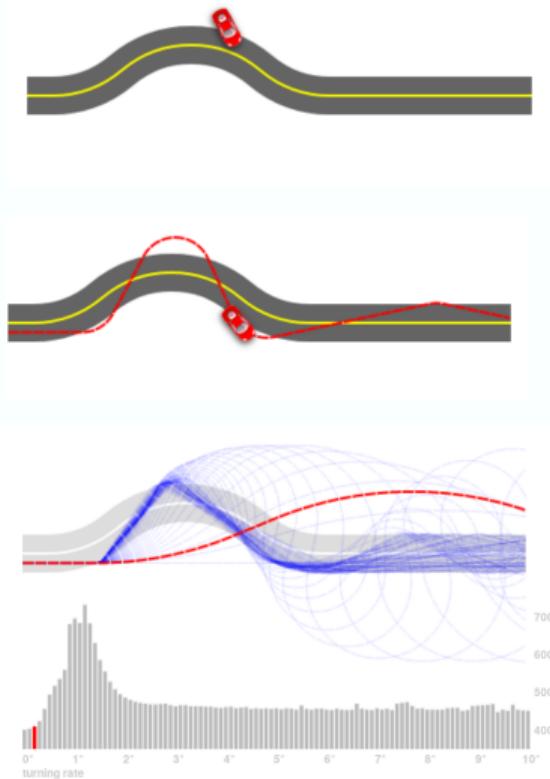


**Abstract away Time**  
Time traveling Debugger  
(rr, REVEN, ... )



**Abstract away Inputs**  
Fuzzing Debugger  
????

# Fuzzing



Debugger (gdb, olly, ... )

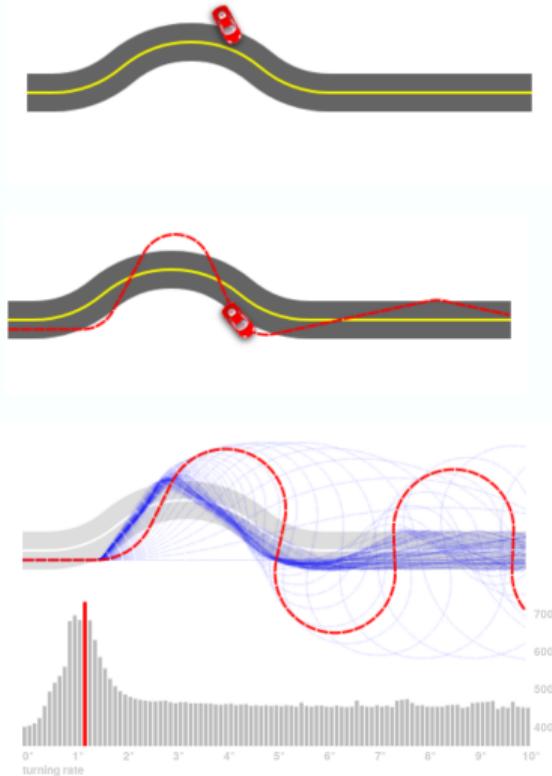


**Abstract away Time**  
Time traveling Debugger  
(rr, REVEN, ... )



**Abstract away Inputs**  
Fuzzing Debugger  
????

# Fuzzing



Debugger (gdb, olly, ... )

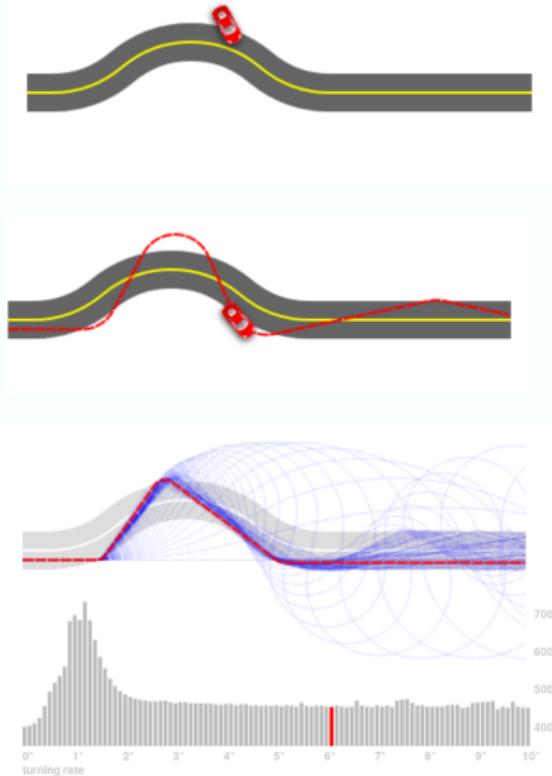


**Abstract away Time**  
Time traveling Debugger  
(rr, REVEN, ... )



**Abstract away Inputs**  
Fuzzing Debugger  
????

# Fuzzing



Debugger (gdb, olly, ... )



**Abstract away Time**  
Time traveling Debugger  
(rr, REVEN, ... )



**Abstract away Inputs**  
Fuzzing Debugger  
????

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken:  
↳ line 520

Not Taken:  
↳ line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
516 }
```

id:00000000,src:0000001,op:havoc,rep:8,+cov

00000000: 0000 1337 0000 0000 3730 0000 0000 0000	00000010: 3df8 0600 0000 0000 0204 000f a85d 492b	00000020: 0404 004d c0bb e574 0708 00dc a741 0c05	00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2	00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991	00000050: 0e08 005f 30b5 89fd 294f 454f	....7....70..... =.....]I+ ...M....t....A.. ..6.....8:P.. ...{....S%...Y.. ..._0...)OE0
---	---	---	---	---	---	--

Watch Points

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken:  
↳ line 520

Not Taken:  
↳ line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op.code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
516 }
```

id:00000000,src:0000001,op:havoc,rep:8,+cov

00000000: 0000 1337 0000 0000 3730 0000 0000 0000	00000010: 3df8 0600 0000 0000 0204 000f a85d 492b	00000020: 0404 004d c0bb e574 0708 00dc a741 0c05	00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2	00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991	00000050: 0e08 005f 30b5 89fd 294f 454f
---	---	---	---	---	---

Watch Points

.....7.....70.....	=.....]I+
...M....t.....A..	
..6.....8:P..	
...{.....S%....Y.	
...._0...)OE0	

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```

477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }

```

Taken: ⚡ line 520  
Not Taken: ⚡ line 490

88044cfe9 xor ecx, ecx  
88044cfcb cmp eax, ebx  
88044cfed jb 0x884d4021  
88044cfef mov ecx, dword ptr [0x8850628]  
88044cff5 mov edx, dword ptr gs:[edi]  
88044cff8 mov esi, 0x14df  
88044cffd xor edx, esi  
88044cff inc byte ptr [ecx + edx]  
88044d902 mov dword ptr gs:[edi], 0xaaf  
88044d909 mov ecx, dword ptr [0x8850628]  
88044d90f lea ecx, dword ptr [ecx + ecx\*2]  
88044d912 lea ecx, dword ptr [ebx + ecx\*8]  
88044d915 cmp eax, ecx  
88044d917 mov ecx, 0  
88044d91c cmovae eax, ecx  
88044d91f mov ecx, eax  
88044d921 mov eax, dword ptr [0x8850628]  
88044d926 mov edx, dword ptr gs:[edi]  
88044d929 mov esi, 0x3b8  
88044d92e xor edx, esi  
88044d930 inc byte ptr [eax + edx]  
88044d933 mov dword ptr gs:[edi], 0x29d8  
88044d934 movzx edx, byte ptr [0x8850628]  
88044d941 shr edx, 0x10  
88044d944 movzx eax, word ptr [0x8850628]  
88044d948 or eax, edx  
88044d94d movzx edx, ah  
88044d950 cmp edx, 4  
88044d953 jne 0x884d174 Add Watch Point  
88044d959 mov edx, dword ptr gs:[edi]  
88044d95f mov esi, dword ptr gs:[edi]  
88044d962 mov ebp, 0x2dcf  
88044d967 xor esi, ebp  
88044d969 inc byte ptr [edx + esi]  
88044d96c mov dword ptr gs:[edi], 0x10e7  
88044d973 test al, al  
88044d977 je 0x884d37f  
88044d97c mov edx, dword ptr [0x8850628]

id:000000,src:000001,op:havoc,rep:8,+cov

00000000: 0000 1337 0000 0000 3730 0000 0000 0000	....7....70.....
00000010: 3df8 0600 0000 0000 0204 000f a85d 492b	=.....]I+
00000020: 0404 004d c0bb e574 0708 00dc a741 0c05	...M....t....A..
00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2	..6.....8:P..
00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991	...{....S%....Y.
00000050: 0e08 005f 30b5 89fd 294f 454f	...._0...)OE0

Watch Points

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken:  
↳ line 520

Not Taken:  
↳ line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
516 }
```

Add Watch Point

id:00000000,src:0000001,op:havoc,rep:8,+cov	Watch Points
00000000: 0000 1337 0000 0000 3730 0000 0000 0000 00000010: 3df8 0600 0000 0000 0204 000f a85d 492b 00000020: 0404 004d c0bb e574 0708 00dc a741 0c05 00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2 00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991 00000050: 0e08 005f 30b5 89fd 294f 454f	....7....70..... =.....]I+ ...M....t....A.. ..6.....8:P.. ...{....S%....Y.. ..._0...)OE0

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken:  
↳ line 520

Not Taken:  
↳ line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op.code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
516 }
```

Expr  OK

id:00000000,src:0000001,op:havoc,rep:8,+cov

00000000:	0000 1337 0000 0000 3730 0000 0000 0000	....7....70.....
00000010:	3df8 0600 0000 0000 0204 000f a85d 492b	=.....]I+
00000020:	0404 004d c0bb e574 0708 00dc a741 0c05	...M....t....A..
00000030:	aa10 361b 040c 00da bf00 9138 3a50 1ba2	.6.....8:P..
00000040:	c381 a37b 0908 00ff 9853 25c5 15cd 5991	...{....S%...Y..
00000050:	0e08 005f 30b5 89fd 294f 454f	...._0...)OE0

Watch Points

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```

477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }

```

Taken: ⚡ line 520  
Not Taken: ⚡ line 490

Expr: edx [OK]

id:000000,src:000001,op:havoc,rep:8,+cov	00000000: 0000 1337 0000 0000 3730 0000 0000 0000 00000010: 3df8 0600 0000 0000 0204 000f a85d 492b 00000020: 0404 004d c0bb e574 0708 00dc a741 0c05 00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2 00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991 00000050: 0e08 005f 30b5 89fd 294f 454f	....7....70..... =.....]I+ ...M....t....A.. ..6.....8:P.. ...{....S%....Y.. ..._0...)OE0
Watch Points		

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken: ⚡ line 520  
Not Taken: ⚡ line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op.code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507         }
508
509         last_id = &transaction->id;
510     }
511     else if (pkthdr.pkt_type == FIN && last_transaction)
512     {
513         last_id = NULL;
514         transaction = last_transaction;
515     }

```

Expr  OK

Watch Points

id	src	op	havoc	rep	8	+cov		
00000000	0000	1337	0000	0000	3730	0000	0000	0000
00000010	3df8	0600	0000	0000	0204	000f	a85d	492b
00000020	0404	004d	c0bb	e574	0708	00dc	a741	0c05
00000030	aa10	361b	040c	00da	bf00	9138	3a50	1ba2
00000040	c381	a37b	0908	00ff	9853	25c5	15cd	5991
00000050	0e08	005f	30b5	89fd	294f	454f		

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```

477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }

```

Taken: ⚡ line 520  
Not Taken: ⚡ line 490

88044c8e9 xor ecx, ecx  
88044cfb9 cmp eax, ebx  
88044cfed9 jb 0x884d4021  
88044cef9 mov ecx, dword ptr [8x8850628]  
88044cff59 mov edx, dword ptr gs:[edi]  
88044cff9 mov esi, 0x14df  
88044cffd9 xor edx, esi  
88044cff inc byte ptr [ecx + edx]  
88044d9029 mov dword ptr gs:[edi], 0xaaf  
88044d9099 mov ecx, dword ptr [8x8850628]  
88044d90f9 lea ecx, dword ptr [ecx + ecx\*2]  
88044d9129 lea ecx, dword ptr [ebx + ecx\*8]  
88044d9159 cmp eax, ecx  
88044d9179 mov ecx, 0  
88044d91c9 cmovae eax, ecx  
88044d91f9 mov ecx, eax  
88044d9219 mov eax, dword ptr [8x8850628]  
88044d9269 mov edx, dword ptr gs:[edi]  
88044d9299 mov esi, 0x3b38  
88044d92e9 xor edx, esi  
88044d9309 inc byte ptr [eax + edx]  
88044d9339 mov dword ptr gs:[edi], 0x29d8  
88044d9349 movzx edx, byte ptr [8x8850628]  
88044d9419 shl edx, 0x10  
88044d9449 movzx eax, word ptr [8x8850628]  
88044d9489 or eax, edx  
88044d94d9 movzx edx, ah  
88044d9599 cmp edx, 4  
88044d9539 jne 0x884d174  
88044d9599 mov edx, dword ptr [8x8850628]  
88044d95f9 mov esi, dword ptr gs:[edi]  
88044d9629 mov ebp, 0x2dcf  
88044d9679 xor esi, ebp  
88044d9699 inc byte ptr [edx + esi]  
88044d96c9 mov dword ptr gs:[edi], 0x10e7  
88044d9739 test al, al  
88044d9739 je 0x884d37f7  
88044d9759 mov edx, dword ptr [8x8850628]

id:000000,src:000001,op:havoc,rep:8,+cov	....7.....70..... =.....]I+ ...M....t....A.. ..6.....8:P.. ...{....S%...Y.. ..._0...)OE0	Watch Points
		0804d050: edx

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken:  
↳ line 520

Not Taken:  
↳ line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
516 }
```

id:00000000,src:0000001,op:havoc,rep:8,+cov

00000000: 0000 1337 0000 0000 3730 0000 0000 0000	00000010: 3df8 0600 0000 0000 0204 000f a85d 492b	00000020: 0404 004d c0bb e574 0708 00dc a741 0c05	00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2	00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991	00000050: 0e08 005f 30b5 89fd 294f 454f
---	---	---	---	---	---

Watch Points

0804d050: edx
---------------

.....7.....70.....  
=.....]I+  
...M....t....A..  
.6.....8:P..  
...{....S%...Y..  
...\_0...)OE0

# A Better Tool...

File Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ijon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```

477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }

```

Taken: ↗ line 520

Not Taken: ↗ line 490

8804cfe4 xor ecx, ecx
8804cfcb cmp eax, ebx
8804cfed jb 0x804d021
8804cffc mov ecx, dword ptr [8x8050628]
8804cff5 mov edx, dword ptr gs:[edi]
8804cff8 mov esi, 0x14df
8804cffd xor edx, esi
8804cff inc byte ptr [ecx + edx]
8804d002 mov dword ptr gs:[edi], 0xa6ff
8804d009 mov ecx, dword ptr [8x8050608]
8804d00f lea ecx, dword ptr [ecx + ecx\*2]
8804d012 lea ecx, dword ptr [ebx + ecx\*8]
8804d015 cmp eax, ecx
8804d017 mov ecx, 0
8804d01c cmovae eax, ecx
8804d01f mov ecx, eax
8804d021 mov eax, dword ptr [8x8050628]
8804d026 mov edx, dword ptr gs:[edi]
8804d029 mov esi, 0x3b06
8804d02e xor edx, esi
8804d030 inc byte ptr [eax + edx]
8804d033 mov dword ptr gs:[edi], 0x29d0
8804d034 movzx edx, byte ptr [0x8050606]
8804d041 shl edx, 0x10
8804d044 movzx eax, word ptr [0x8050606c]
8804d048 or eax, edx
8804d04d movzx edx, ah
8804d050 cmp edx, 4
8804d053 jne 0x804d174
8804d059 mov edx, dword ptr [8x8050628]
8804d05f mov esi, dword ptr gs:[edi]
8804d062 mov ebp, 0x2dcf
8804d067 xor esi, ebp
8804d069 inc byte ptr [edx + esi]
8804d06c mov dword ptr gs:[edi], 0x10e7
8804d073 test al, al
8804d073 je 0x804d37f
8804d077 mov edx, dword ptr [8x8050628]

id:000000,src:000001,op:havoc,rep:8,+cov

00000000:	0000 1337 0000 0000 3730 0000 0000 0000	....7....70.....
00000010:	3df8 0600 0000 0000 0204 000f a85d 492b	=.....]I+
00000020:	0404 004d c0bb e574 0708 00dc a741 0c05	...M....t....A..
00000030:	aa10 361b 040c 00da bf00 9138 3a50 1ba2	.6.....8:P..
00000040:	c381 a37b 0908 00ff 9853 25c5 15cd 5991	...{....S%....Y.
00000050:	0e08 005f 30b5 89fd 294f 454f	...._0...)OE0

Watch Points

0804d050: edx Analyze Input

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken:  
↳ line 520

Not Taken:  
↳ line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
516 }
```

id:00000000,src:0000001,op:havoc,rep:8,+cov

00000000:	0000 1337 0000 0000 3730 0000 0000 0000	....7....70.....
00000010:	3df8 0600 0000 0000 0204 000f a85d 492b	=.....]I+
00000020:	0404 004d c0bb e574 0708 00dc a741 0c05	...M....t....A..
00000030:	aa10 361b 040c 00da bf00 9138 3a50 1ba2	.6.....8:P..
00000040:	c381 a37b 0908 00ff 9853 25c5 15cd 5991	...{....S%....Y.
00000050:	0e08 005f 30b5 89fd 294f 454f	...._0...)OE0

Watch Points

0804d050: edx Analyze input

# A Better Tool...

File Coverage Queue

Dashboard Inputs (8) Search Filter

/home/me/ijon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```

477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op.code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }

```

80044cfe0 xor ecx, ecx  
80044cfb0 cmp eax, ebx  
80044cfed0 jb 0x804d021  
80044cfef0 mov ecx, dword ptr [8x8050628]  
80044cff50 mov edx, dword ptr gs:[edi]  
80044cff80 mov esi, 0x14df  
80044cffd0 xor edx, esi  
80044cff inc byte ptr [ecx + edx]  
80044d0020 mov dword ptr gs:[edi], 0xaaf  
80044d0090 mov ecx, dword ptr [8x8050608]  
80044d00f0 lea ecx, dword ptr [ecx + ecx\*2]  
80044d0120 lea ecx, dword ptr [ebx + ecx\*8]  
80044d0150 cmp eax, ecx  
80044d0170 mov ecx, 0  
80044d01c0 cmovae eax, ecx  
80044d01f0 mov ecx, eax  
80044d0210 mov eax, dword ptr [8x8050628]  
80044d0260 mov edx, dword ptr gs:[edi]  
80044d0290 mov esi, 0x3b8  
80044d02e0 xor edx, esi  
80044d0300 inc byte ptr [eax + edx]  
80044d0330 mov dword ptr gs:[edi], 0x29d0  
80044d0340 movzx edx, byte ptr [8x8050606]  
80044d0410 shl edx, 0x10  
80044d0440 movzx eax, word ptr [8x8050606c]  
80044d0480 or eax, edx  
80044d04840 movzx edx, ah  
80044d0580 cmp edx, 4  
80044d0530 jne 0x804d174  
80044d0590 mov edx, dword ptr [8x8050628]  
80044d05f0 mov esi, dword ptr gs:[edi]  
80044d0620 mov ebp, 0x2dcf  
80044d0670 xor esi, ebp  
80044d0690 inc byte ptr [edx + esi]  
80044d06c0 mov dword ptr gs:[edi], 0x10e7  
80044d0730 test al, al  
80044d0737 je 0x804d37f  
80044d0770 mov edx, dword ptr [8x8050628]

id:000000,src:000001,op:havoc,rep:8,+cov	0000 1337 0000 0000 3730 0000 0000 0000 00000010: 3df8 0600 0000 0000 0204 000f a85d 492b 00000020: 0404 004d c0bb e574 0708 00dc a741 0c05 00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2 00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991 00000050: 0e08 005f 30b5 89fd 294f 454f	....7....70..... =.....]I+ ..M....t....A.. ..6.....8:P.. ...{....S%....Y.. ..._0...)OE0
--	--	--

Watch Points

0804d050: edx

# A Better Tool...

File Coverage Queue

Dashboard

Inputs (8) Search Filter

/home/me/ijon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken: ① line 520

Not Taken: ② line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRENO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488 ①     if (pkthdr.op.code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRENO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRENO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
516 }
```

if changed, we don't reach the breakpoint

0x10e7

8884d979 mov edx, dword ptr [0x8050628]

id:000008,src:000001,op:havoc,rep:8,+  
00000000: 0000 1337 0000 0000 3730 0000 0000 0000  
00000010: 3df8 0600 0000 0000 0204 000f a85d 492b  
00000020: 0404 004d c0bb e574 0708 00dc a741 0c05  
00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2  
00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991  
00000050: 0e08 005f 30b5 89fd 294f 454f

Watch Points

0804d050: edx

....7....70.....  
=.....]I+  
...M....t....A..  
..6.....8:P..  
...{....S%....Y..  
....\_0...)OE0

# A Better Tool...

Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

Taken: ↗ line 520

Not Taken: ↗ line 490

/home/me/ijon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRENO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op_code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRENO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRENO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
516 }
```

directly affects the value

id:000008,src:000001,op:havoc,rep:8,+cov	Watch Points
00000000: 0000 1337 0000 0000 3f 0000 0000 0000	0804d050: edx
00000010: b3df 0600 0000 0000 0204 000f a85d 492b	.....7....70.....
00000020: 0404 004d c0bb e574 0708 00dc a741 0c05	=.....]I+
00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2	...M....t....A..
00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991	.6.....8:P..
00000050: 0e08 005f 30b5 89fd 294f 454f	...{....S%....Y..
	...._0...)OE0

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken: ⚡ line 520

Not Taken: ⚡ line 490

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op.code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
```

id:000008,src:000001,op:havoc,reg:00000000,mem:0000000000000000

00000000:	0000 1337	0000 3730 0000 0000 0000
00000010:	3df8 0600 0000 0000 0204 000f a85d 492b	
00000020:	0404 004d c0bb e574 0708 00dc a741 0c05	
00000030:	aa10 361b 040c 00da bf00 9138 3a50 1ba2	
00000040:	c381 a37b 0908 00ff 9853 25c5 15cd 5991	
00000050:	0e08 005f 30b5 89fd 294f 454f	

Watch Points

0804d050: edx

8804cfe4 xor ecx, ecx  
8804cfcb cmp eax, ebx  
8804cfed jb 0x804d021  
8804cffc mov ecx, dword ptr [8x8050628]  
8804cff5 mov edx, dword ptr gs:[edi]  
8804cff8 mov esi, 0x14df  
8804cffd xor edx, esi  
8804cff inc byte ptr [ecx + edx]  
8804d002 mov dword ptr gs:[edi], 0xaaf  
8804d009 mov ecx, dword ptr [8x8050608]  
8804d00f lea ecx, dword ptr [ecx + ecx\*2]  
8804d012 lea ecx, dword ptr [ebx + ecx\*8]  
8804d015 cmp eax, ecx  
8804d017 mov ecx, 0  
8804d01c cmovae eax, ecx  
8804d01f mov ecx, eax  
8804d021 mov eax, dword ptr [8x8050628]  
8804d026 mov edx, dword ptr gs:[edi]  
8804d029 mov esi, 0x3b38  
8804d02e xor edx, esi  
8804d030 inc byte ptr [eax + edx]  
8804d033 mov dword ptr gs:[edi], 0x29d0  
8804d034 movzx edx, byte ptr [0x805060e]  
8804d041 shr edx, 0x10  
8804d044 movzx eax, word ptr [0x805060c]  
8804d048 or eax, edx  
8804d04d movzx edx, ah  
8804d050 cmp edx, 4  
8804d053 jne 0x804d174  
8804d059 mov edx, dword ptr [8x8050628]  
8804d05f mov esi, dword ptr gs:[edi]  
8804d062 mov ebp, 0x2dcf  
8804d067 xor esi, ebp  
8804d069 inc byte ptr [edx + esi]  
            ptr gs:[edi], 0x10e7  
            al  
            37f  
            dword ptr [8x8050628]

doesn't matter

# A Better Tool...

lJON 🧑 Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

Taken: ⚡ line 520

Not Taken: ⚡ line 490

/home/me/ljon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op.code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }
```

id:000008,src:000001,op:havoc,rep:8,+cov

00000000:	0000	1337	0000	0000	?	
00000010:	3df8	0600	0000	0000	00f	a130 1920
00000020:	0404	004d	c0bb	0708	00dc	a741 0c05
00000030:	aa10	361b	040c	0da	bf00	9138 3a50 1ba2
00000040:	c381	a37b	0908	00ff	9853	25c5 15cd 5991
00000050:	0e08	005f	30b5	89fd	294f	454f

```
0004cf09 xor ecx, ecx
0004cf0b cmp eax, ebx
0004cf0d jb 0x804d021
0004cf0f mov ecx, dword ptr [0x8050628]
0004cf11 mov edx, dword ptr gs:[edi]
0004cf13 mov esi, 0x14df
0004cf15 xor edx, esi
0004cf17 inc byte ptr [ecx + edx]
0004cf19 mov dword ptr gs:[edi], 0xaaf
0004cf1b mov ecx, dword ptr [0x8050608]
0004cf1d lea ecx, dword ptr [ecx + ecx*2]
0004cf1f lea ecx, dword ptr [ebx + ecx*8]
0004cf21 cmp eax, ecx
0004cf23 mov ecx, 0
0004cf25 cmovae eax, ecx
0004cf27 mov eax, eax
0004cf29 mov eax, dword ptr [0x8050628]
0004cf2b mov edx, dword ptr gs:[edi]
0004cf2d mov esi, 0x3b38
0004cf2f xor edx, esi
0004cf30 inc byte ptr [eax + edx]
0004cf32 mov dword ptr gs:[edi], 0x29d0
0004cf34 movzx edx, byte ptr [0x8050606]
0004cf36 shl edx, 0x10
0004cf38 movzx eax, word ptr [0x8050606c]
0004cf3a or eax, edx
0004cf3c movzx edx, ah
0004cf3e cmp edx, 4
0004cf3f jne 0x804d174
0004cf40 mov edx, dword ptr [0x8050628]
0004cf42 mov esi, dword ptr gs:[edi]
0004cf44 mov ebp, 0x2dcf
0004cf46 xor esi, ebp
0004cf48 inc byte ptr [edx + esi]
0004cf4a mov dword ptr gs:[edi], 0x10e7
0004cf4c test al, al
0004cf4e je 0x804d37f
0004cf50 mov edx, dword ptr [0x8050628]
```

affects the number how often the BP was hit

# A Better Tool...

File Coverage Queue

Dashboard

Files Transitions Inputs (8) Search Filter

/home/me/ijon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```

477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ERRNO_MP_NOT_FOUND, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     transaction_t *last_transaction = lookup_transaction(pkthdr.transaction_id);
487
488     if (pkthdr.op.code == ISSUE)
489     {
490         if (pkthdr.pkt_type == INIT)
491         {
492             transaction = cgc_new_transaction();
493             if (!transaction)
494             {
495                 cgc_send_error(ERRNO_MP_ALLOC, ALLOC_MSG);
496                 goto fail;
497             }
498
499             if (cgc_read_data(transaction) != 0)
500             {
501                 cgc_send_error(ERRNO_MP_UNK, UNK_ERROR_MSG);
502                 goto fail;
503             }
504
505             if (handle_issue() != 0)
506                 goto fail;
507
508             last_id = &transaction->id;
509         }
510         else if (pkthdr.pkt_type == FIN && last_transaction)
511         {
512             last_id = NULL;
513             transaction = last_transaction;
514         }
515     }

```

Taken: ↗ line 520

Not Taken: ↗ line 490

88044ce0 xor ecx, ecx  
88044cfb cmp eax, ebx  
88044cfed jb 0x804d021  
88044cef6 mov ecx, dword ptr [8x8050628]  
88044cff5 mov edx, dword ptr gs:[edi]  
88044cff8 mov esi, 0x14df  
88044cffd xor edx, esi  
88044cff inc byte ptr [ecx + edx]  
88044d902 mov dword ptr gs:[edi], 0xaaf  
88044d909 mov ecx, dword ptr [8x8050608]  
88044d90f lea ecx, dword ptr [ecx + ecx\*2]  
88044d912 lea ecx, dword ptr [ebx + ecx\*8]  
88044d915 cmp eax, ecx  
88044d917 mov ecx, 0  
88044d91c cmovae eax, ecx  
88044d91f mov ecx, eax  
88044d921 mov eax, dword ptr [8x8050628]  
88044d926 mov edx, dword ptr gs:[edi]  
88044d929 mov esi, 0x3b8  
88044d92e xor edx, esi  
88044d930 inc byte ptr [eax + edx]  
88044d933 mov dword ptr gs:[edi], 0x29d0  
88044d934 movzx edx, byte ptr [0x8050606]  
88044d941 shr edx, 0x10  
88044d944 movzx eax, word ptr [0x8050606c]  
88044d948 or eax, edx  
88044d94d movzx edx, ah  
88044d958 cmp edx, 4  
88044d953 jne 0x804d174  
88044d959 mov edx, dword ptr [8x8050628]  
88044d95f mov esi, dword ptr gs:[edi]  
88044d962 mov ebp, 0x2dcf  
88044d967 xor esi, ebp  
88044d969 inc byte ptr [edx + esi]  
88044d96c mov dword ptr gs:[edi], 0x10e7  
88044d973 test al, al  
88044d973 je 0x804d37f  
88044d975 mov edx, dword ptr [8x8050628]

id:000000,src:000001,op:havoc,rep:8,+cov	0000 1337 0000 0000 3730 0000 0000 0000 00000010: 3df8 0600 0000 0000 0204 000f a85d 492b 00000020: 0404 004d c0bb e574 0708 00dc a741 0c05 00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2 00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991 00000050: 0e08 005f 30b5 89fd 294f 454f	....7....70..... =.....]I+ ..M....t....A.. ..6.....8:P.. ...{....S%....Y.. ..._0...)OE0
--	--	--

Watch Points

0804d050: edx

# A Better Tool...

ijon Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

Taken: ➔ line 520

Not Taken: ➔ line 490

/home/me/ijon\_eval/cb-multios/challenges/Multipass/src/main.c 76/170

```
477     break;
478
479     transaction = NULL;
480     if (last_id != NULL && *last_id != pkthdr.transaction_id)
481     {
482         cgc_send_error(ENOENT, NOT_FOUND_MSG);
483         goto fail;
484     }
485
486     if (transaction == INIT)
487     {
488         transaction = cgc_new_transaction();
489         if (!transaction)
490         {
491             cgc_send_error(ENOMEM, ALLOC_MSG);
492             goto fail;
493         }
494         if (cgc_set_transaction(transaction))
495         {
496             cgc_send_error(ENOENT, ERROR_MSG);
497             if (transaction->type != 0)
498             {
499                 last_id = transaction;
500             }
501             else if (transaction->type == FIN && last_
502             {
503                 last_id = transaction;
504             }
505         }
506     }
507
508     last_id = transaction;
509
510     if (last_id->type == FIN && last_
511     {
512         last_id = transaction;
513     }
514 }
```

ptr [0x8050628]  
gs:[edi]

var ecx, ecx  
ebx  
eax  
edx  
esi, edi  
ebp  
inc byte ptr  
mov dword ptr  
movzx edx, byte  
shl edx, 0x10  
movzx eax, word  
add al, 4  
mov edx, dword  
mov est, dword  
mov ebp, dword  
mov [0x805059], edx, dwor

0804d059 mov edx, dwor  
0804d05f mov est, dwor  
0804d062 mov ebp, dwor  
0804d067 mov [0x805059], edx, dwor

Watch Points

0804d050: edx

7....70.....  
=.....]I+  
..M....A..  
.6.....8:P..  
...{....S%...Y..  
...\_0...)OE0



# A Better Tool...

```
[lcamtuf@raccoon afl]$ ./afl-analyze -e -i testcases/images/png/not_kitty.png ~/readpng
afl-analyze 2.00b by <lcamtuf@google.com>

[+] Read 218 bytes from 'testcases/images/png/not_kitty.png'.
[*] Performing dry run (mem limit = 25 MB, timeout = 1000 ms, edges only)...
[*] Analyzing input file (this may take a while)...
```

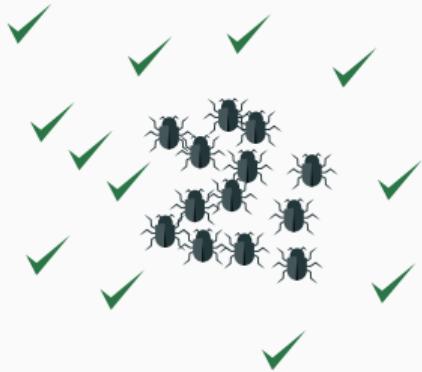
<p>01 - no-op block 01 - superficial content 01 - critical stream 01 - "magic value" section</p>	<p>01 - suspected length field 01 - suspected cksum or magic int 01 - suspected checksummed block</p>
--	---

```
[000000] #89 P N G #0d #0a #1a #0a #00 #00 #00 #0d I H D R >
[000016] #00 #00 #00 #20 #00 #00 #00 #20 #08 #03 #00 #00 #00 D #a4 #8a >
[000032] #c6 #00 #00 #00 #19 t E X t S o f t w a r >
[000048] e #00 A d o b e #20 I m a g e R e a >
[000064] d y q #c9 e < #00 #00 #00 #0f P L T E f #cc >
[000080] #cc #ff #ff #ff #00 #00 #00 3 #99 f #99 #ff #cc > L #af >
```

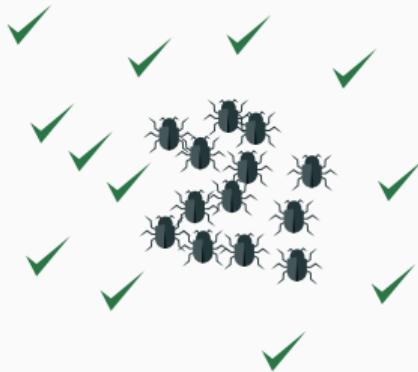
# Root Cause Analysis



# Root Cause Analysis

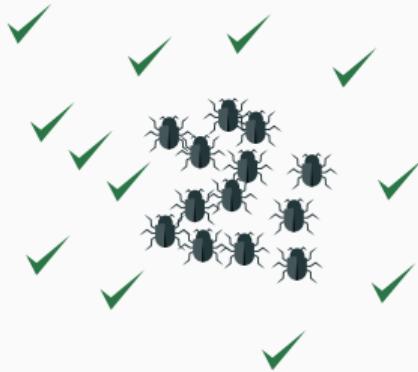


# Root Cause Analysis



```
val.type != MRB_TT_EXCEPTION
```

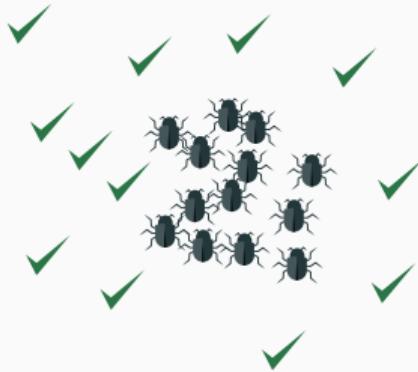
# Root Cause Analysis



val.type != MRB\_TT\_EXCEPTION

val.type < 123

# Root Cause Analysis

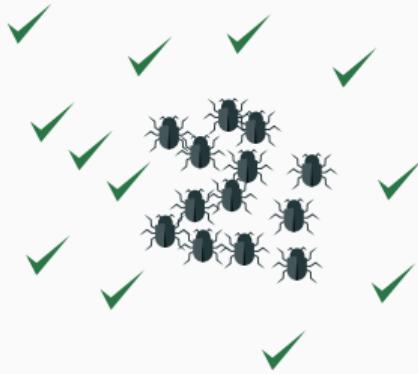


val.type != MRB\_TT\_EXCEPTION

val.type < 123

⋮

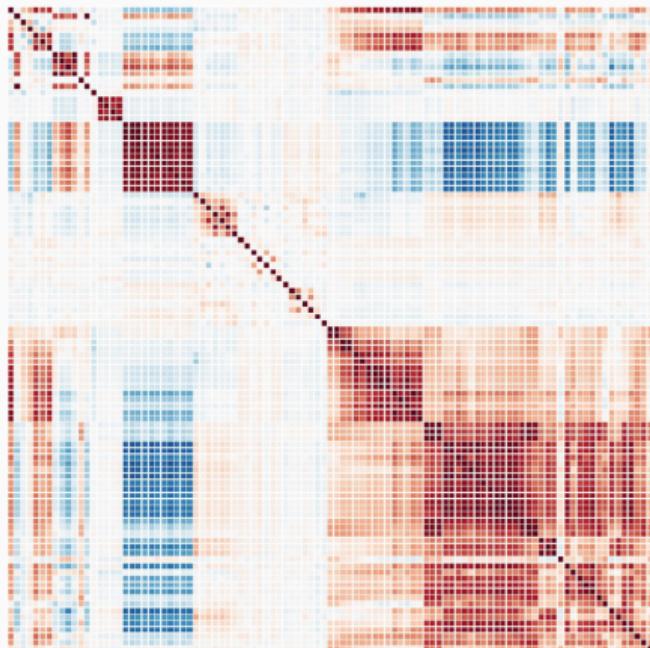
# Root Cause Analysis



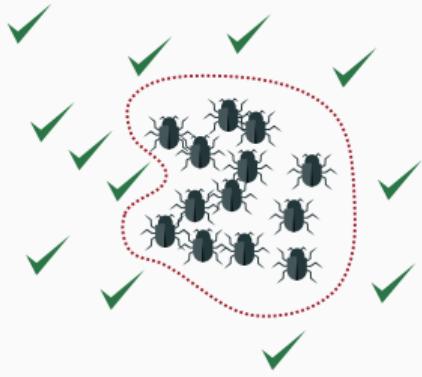
val.type != MRB\_TT\_EXCEPTION

val.type < 123

⋮



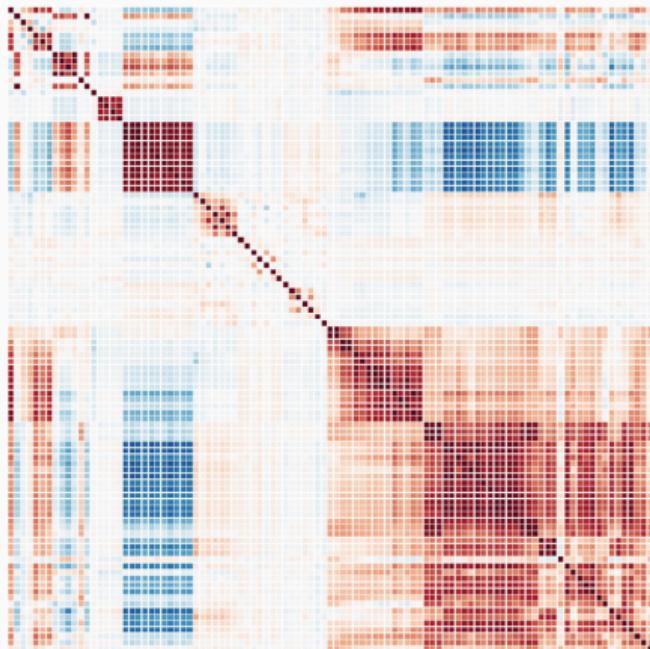
# Root Cause Analysis



val.type != MRB\_TT\_EXCEPTION

val.type < 123

⋮



# Heap Feng Shui



<https://sean.heelan.io/heaplayout/>

# Heap Feng Shui

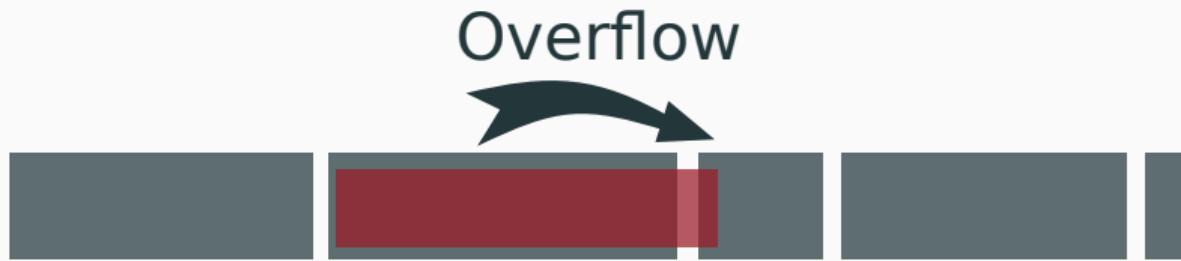


<https://sean.heelan.io/heaplayout/>

# Heap Feng Shui



<https://sean.heelan.io/heaplayout/>



<https://sean.heelan.io/heaplayout/>

# Key Takeaways:

**printf**

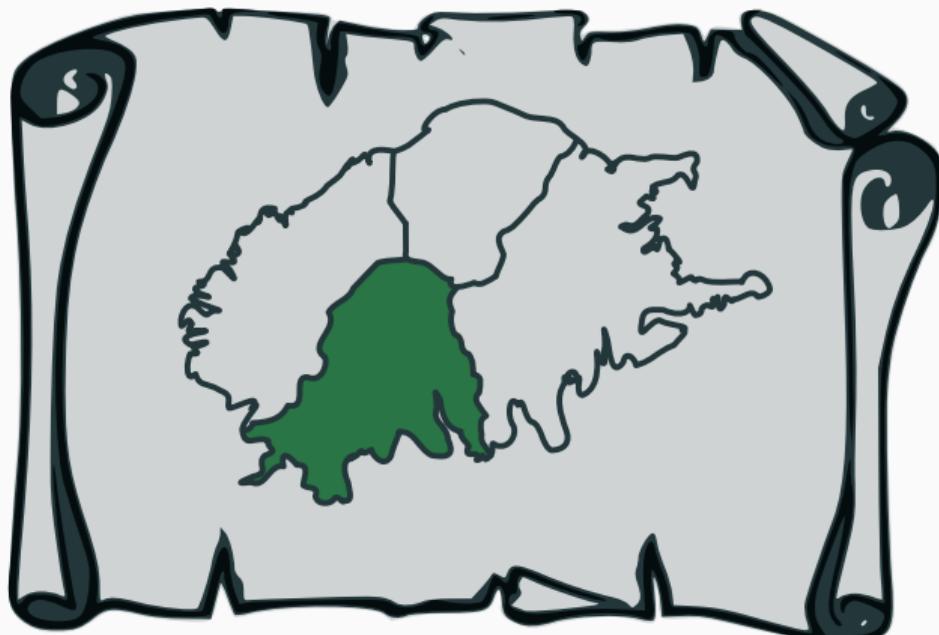
**Debugger**

**Time Traveling  
Debugger**

**Fuzzer + Debugger**



# Unfuzzable Code



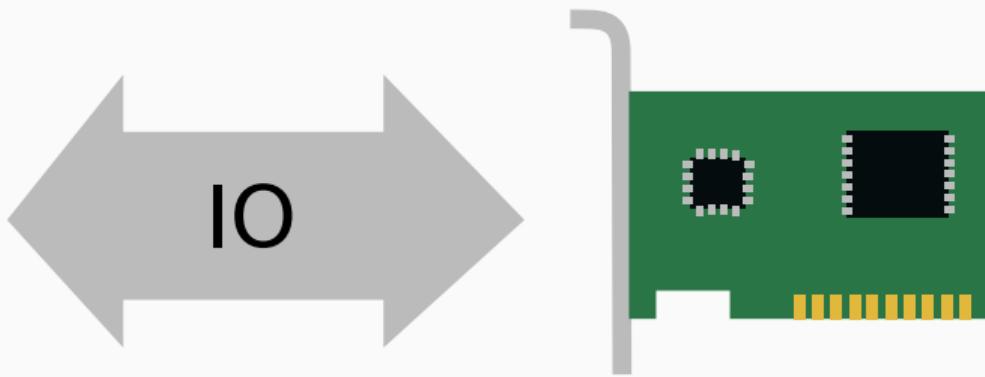
# Code that doesn't run?

# Code that doesn't run?

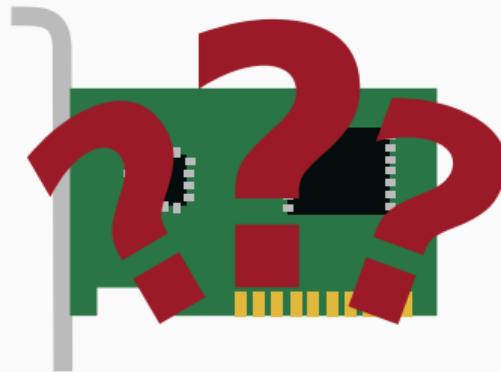
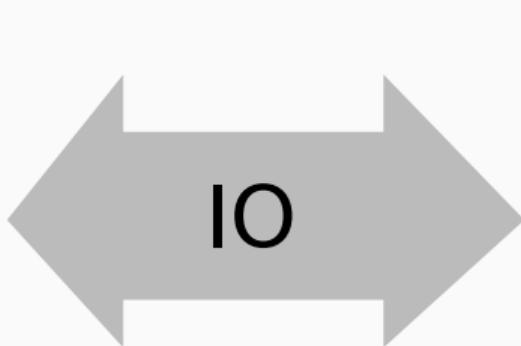
Firmware



# Code that doesn't run?

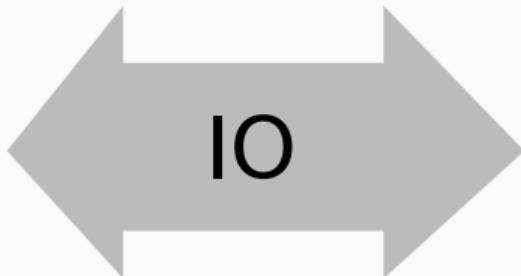


# Code that doesn't run?

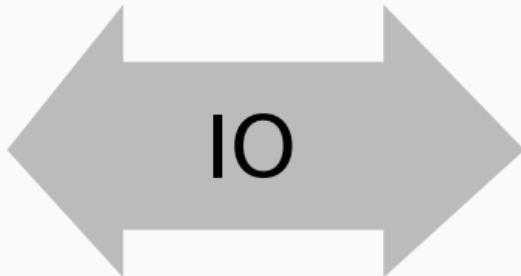


# Code that doesn't run?

Firmware



# Code that doesn't run?

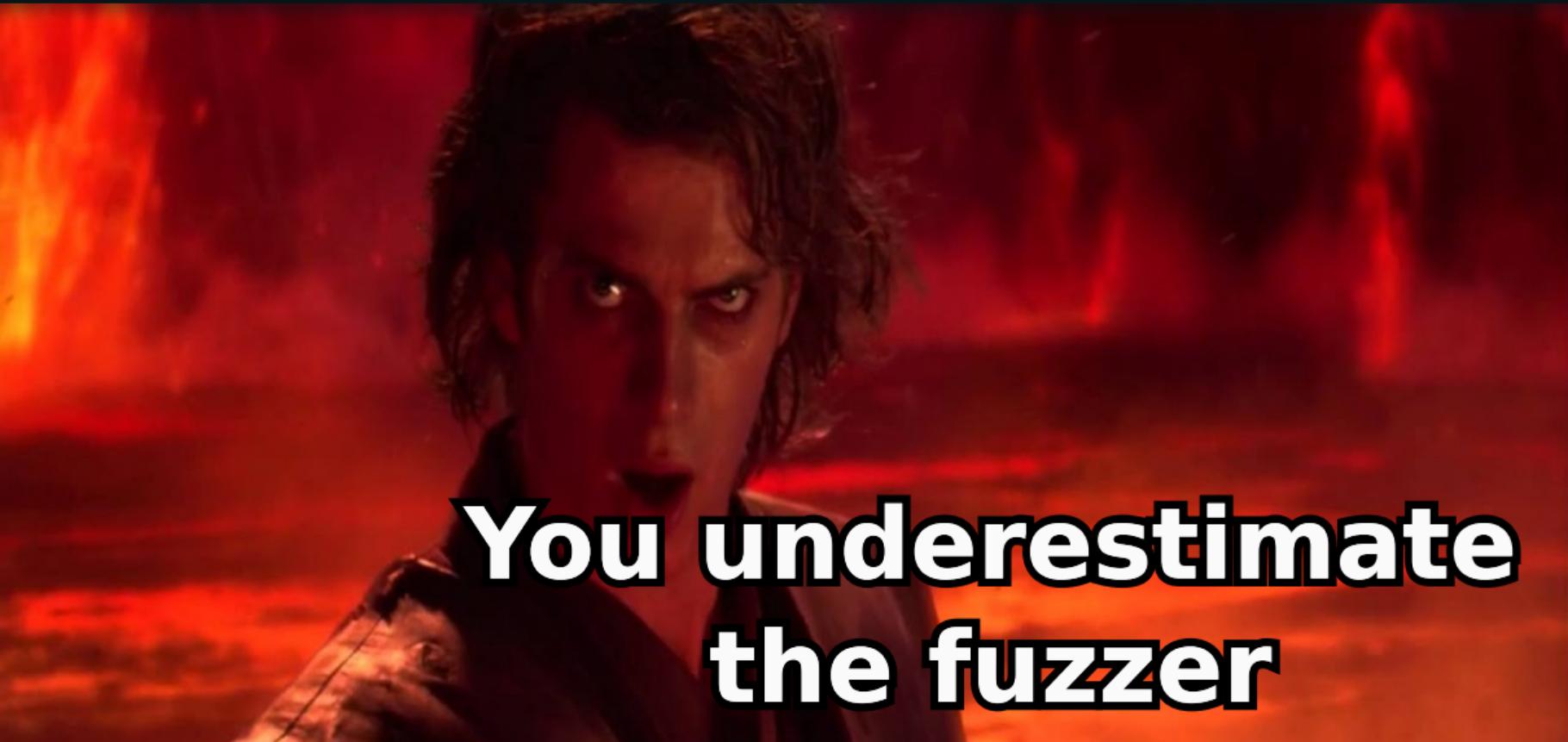


P<sup>2</sup>IM [1]  
HALucinator [2]

[1] <https://arxiv.org/pdf/1909.06472.pdf>

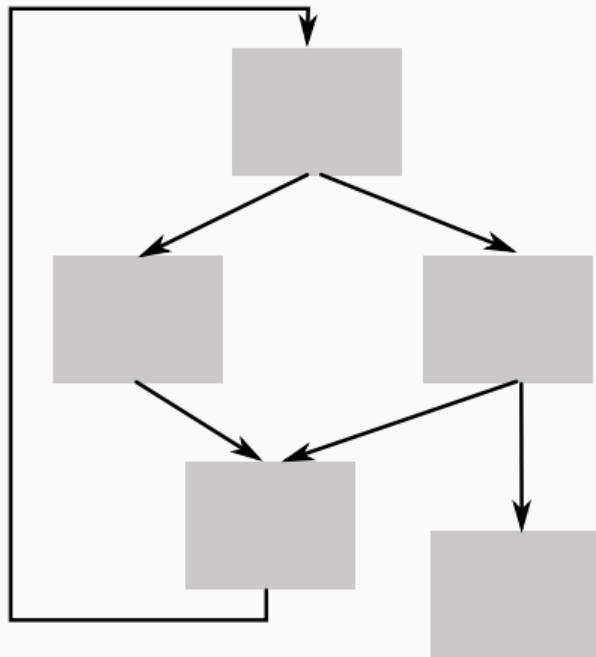
[2] <https://nebelwelt.net/publications/files/20SEC2.pdf>

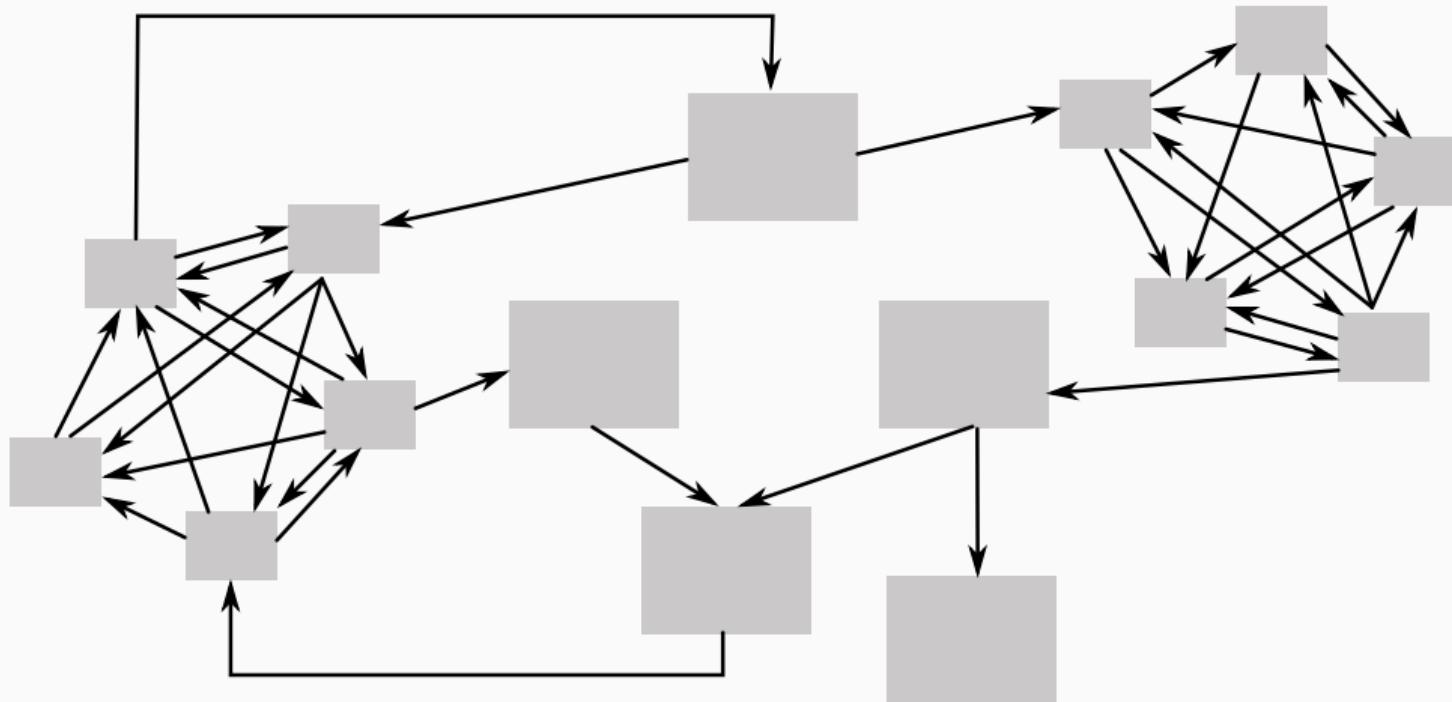
# Key Takeaways:

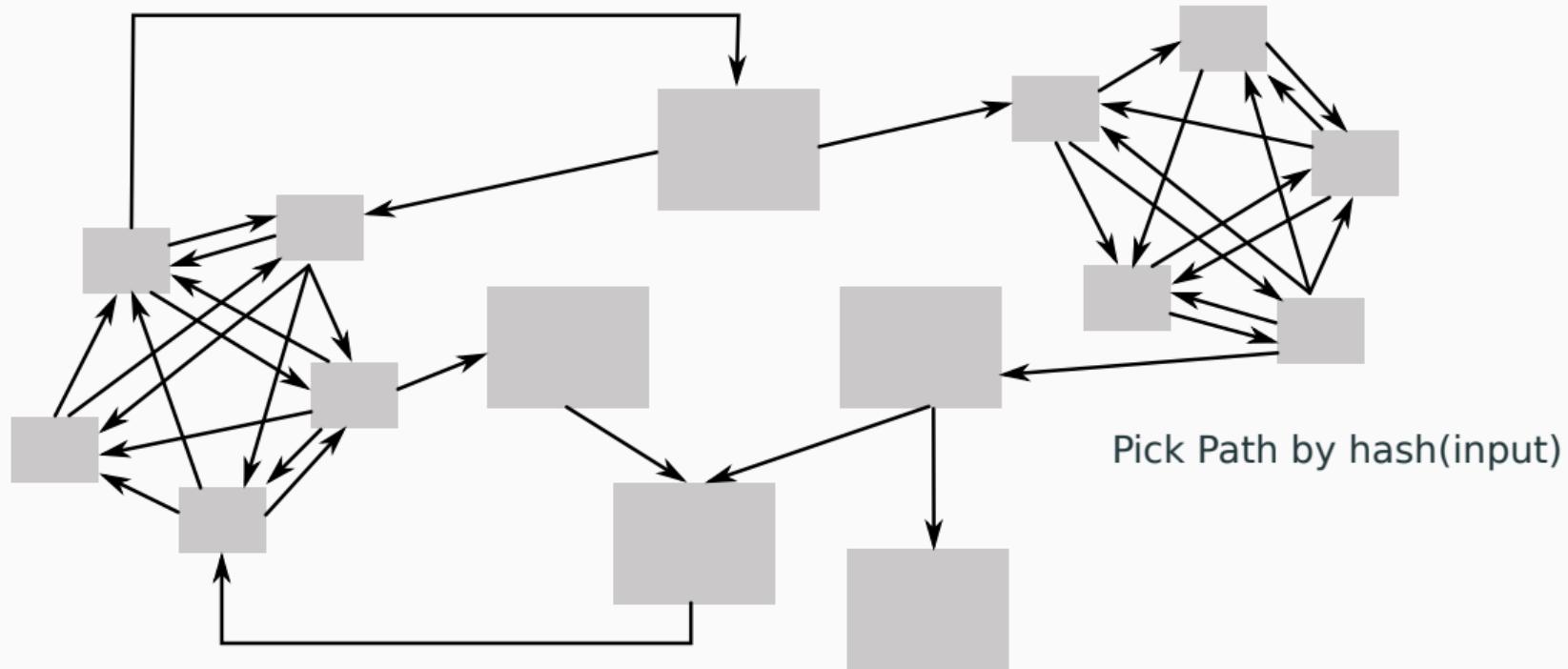


**You underestimate  
the fuzzer**

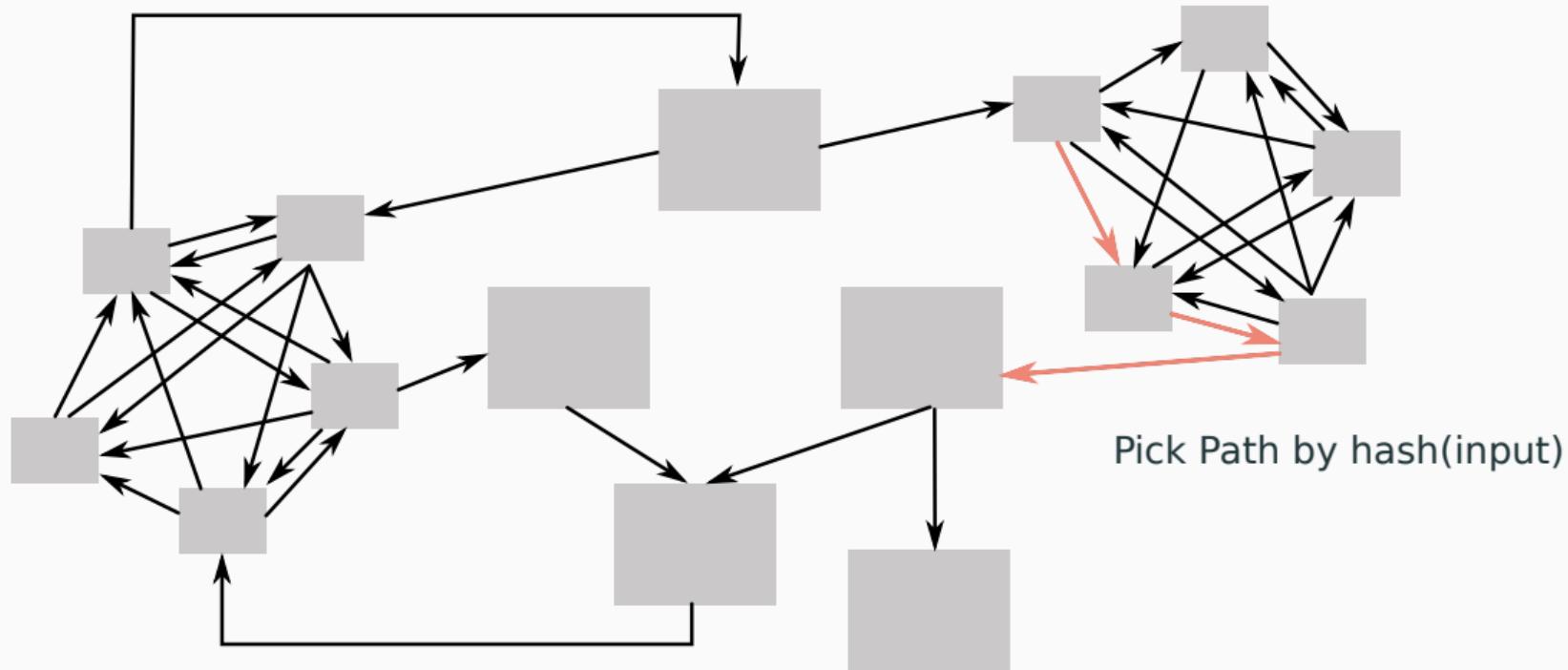
AntiFuzz



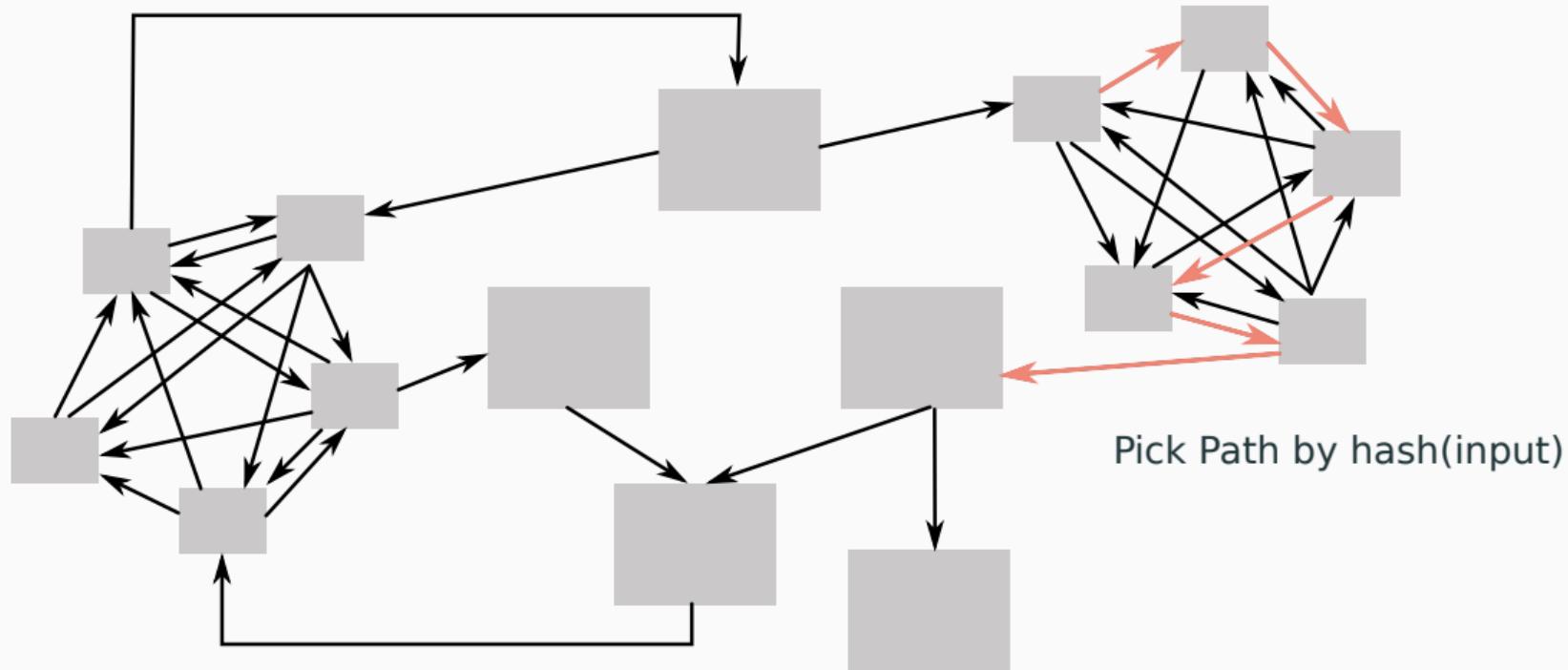




Pick Path by  $\text{hash}(\text{input})$



Pick Path by  $\text{hash}(\text{input})$





**SLOW  
DOWN!**

```
if(parse_error){  
    printf("couldn't parse\n");  
    exit(1);  
}
```

**SLOW  
DOWN!**

```
if(parse_error){  
    printf("couldn't parse\n");  
    delay(1); //expensive calc  
    exit(1);  
}
```

**SLOW  
DOWN!**

```
if(parse_error){  
    printf("couldn't parse\n");  
    delay(1); //expensive calc  
    exit(1);  
}
```



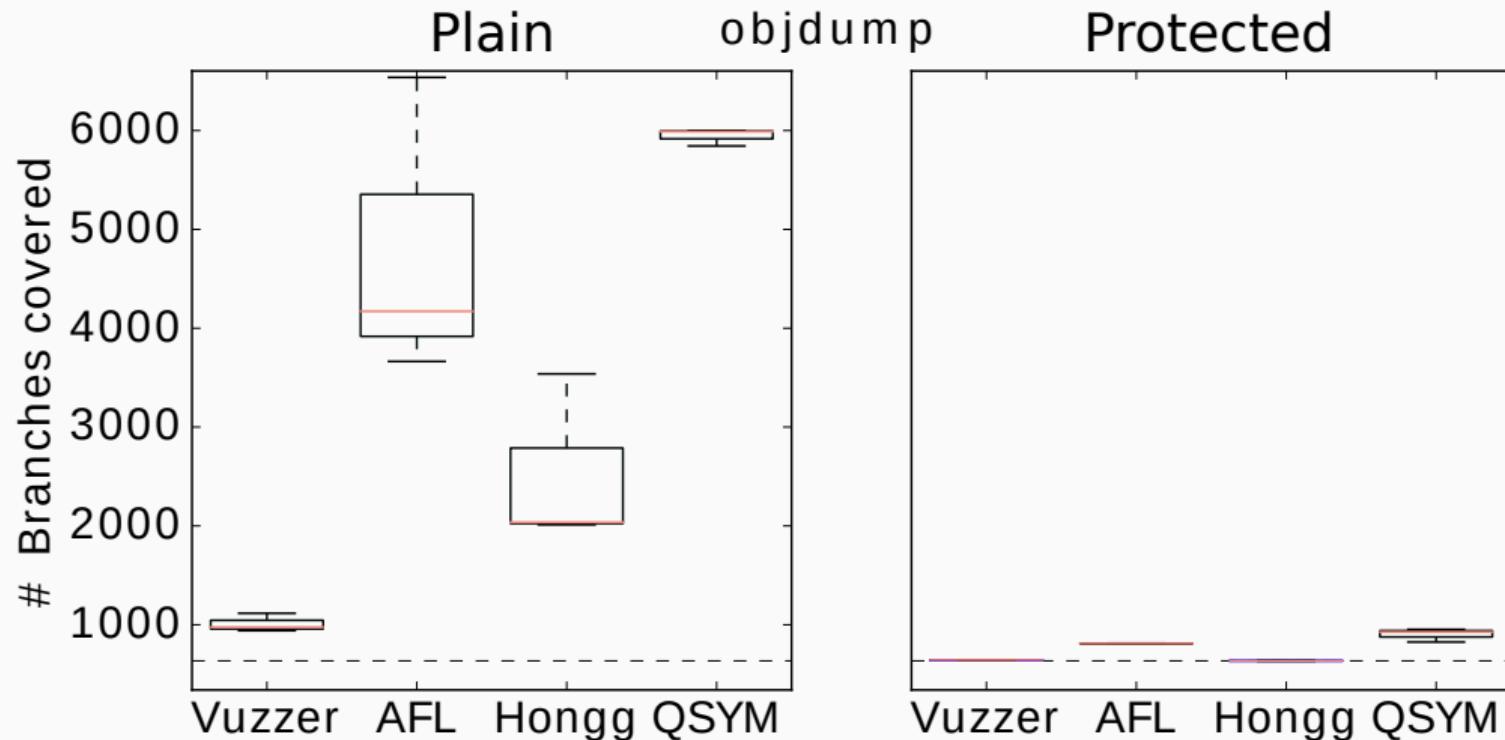
Signal Handler!

## Symbolic Execution? Taint Tracking?

## Symbolic Execution? Taint Tracking?

```
input = enc(dec(input));
```

# objdump



# Key Takeaways:



**Katelyn Gadd** @antumbral · 29.05

В отговор на [@johnregehr](#)

this sure seems like hostile research to me

"how can I ensure that software is full of vulnerabilities only known to me"

1

1

4

↑



**Katelyn Gadd** @antumbral · 29.05

we need a term for hostile researchers like this, sort of the "you are undermining the future of the human race" equivalent of "class traitor"

2

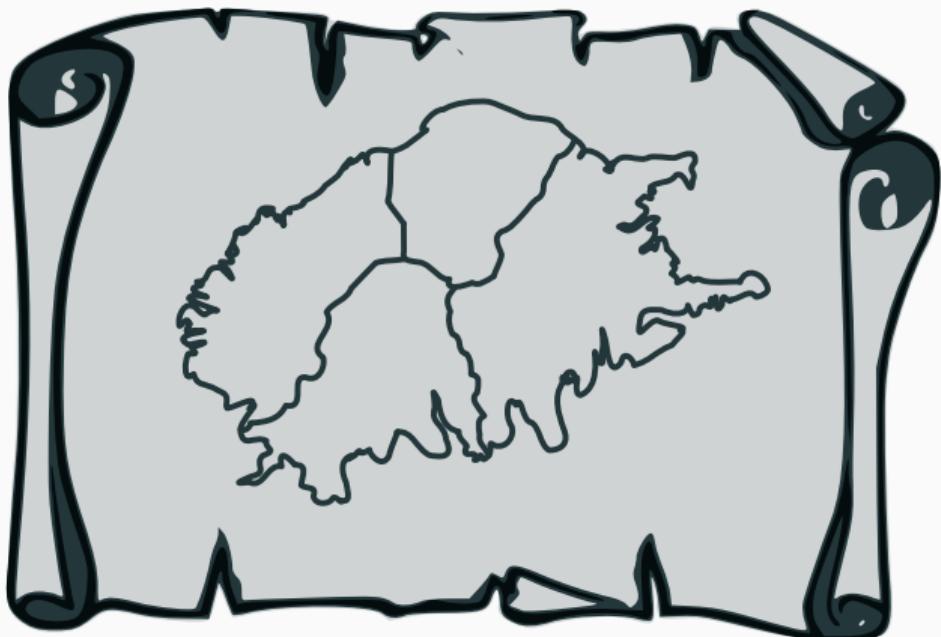
1

8

↑

# Key Takeaways:





# Fuzzers

As Building Blocks for a  
New Generation of Tools

A large-scale industrial photograph featuring a massive mining excavator in the foreground, its bucket suspended in mid-air. A small white SUV is parked on the ground in front of the excavator's body, providing a clear sense of scale. In the background, a multi-story building under construction is visible, with workers on the upper levels. The sky is overcast.

# Let's Build Better Tools

[github.com/RUB-SysSec/kAFL](https://github.com/RUB-SysSec/kAFL)

[github.com/RUB-SysSec/nautilus](https://github.com/RUB-SysSec/nautilus)

[github.com/RUB-SysSec/grimoire](https://github.com/RUB-SysSec/grimoire)

[github.com/RUB-SysSec/antifuzz](https://github.com/RUB-SysSec/antifuzz)

[github.com/eqv/fuzz\\_ui](https://github.com/eqv/fuzz_ui)



 @is\_eqv

 [github.com/eqv](https://github.com/eqv)

 [cornelius.aschermann@rub.de](mailto:cornelius.aschermann@rub.de)

 @ms\_s3c

 [github.com/schumilo](https://github.com/schumilo)

 [sergej.schumilo@rub.de](mailto:sergej.schumilo@rub.de)

### **Special Thanks to:**

Ali Abbasi, Tim Blazynko, Robert Gawlik,  
Emre Güler, Thorsten Holz, Moritz Schlägel,  
Daniel Teuchert, Simone Wörner, and all the  
others that made this research possible.

