What the Fuzz

Cornelius Aschermann

Researcher at Ruhr University Bochum

Verification & Automated Bug Finding

Security Consultant


@is_eqv


github.com/eqv


cornelius.aschermann@rub.de

Sergej Schumilo

Researcher at Ruhr University Bochum

Automated Bug Finding & Everything Low Level

Security Consultant


@ms_s3c

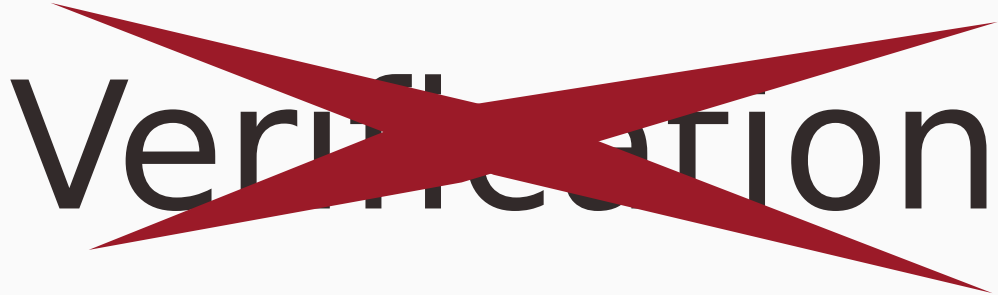

github.com/schumilo


sergej.schumilo@rub.de

Manual Analysis

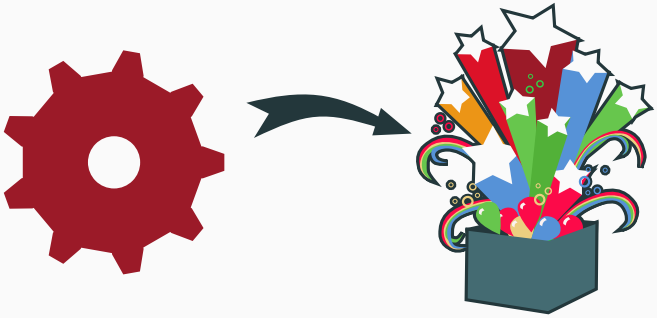
(doesn't scale that well)

Verification


Verification

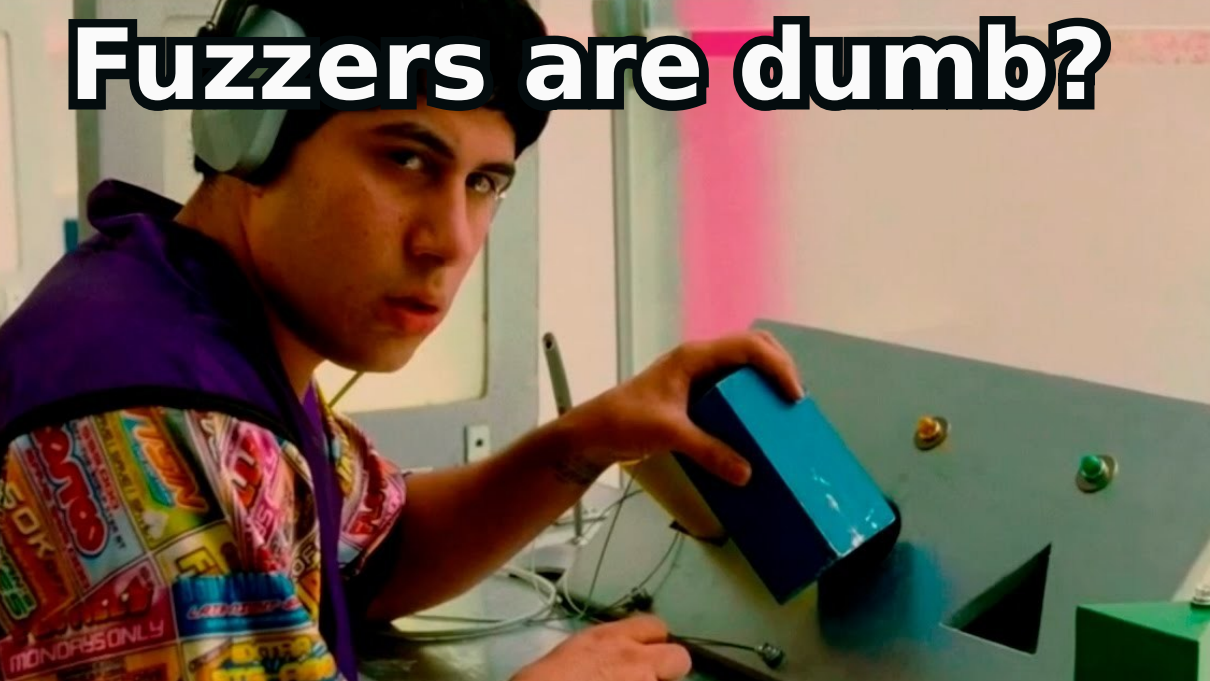
Fuzzers

Fuzzing

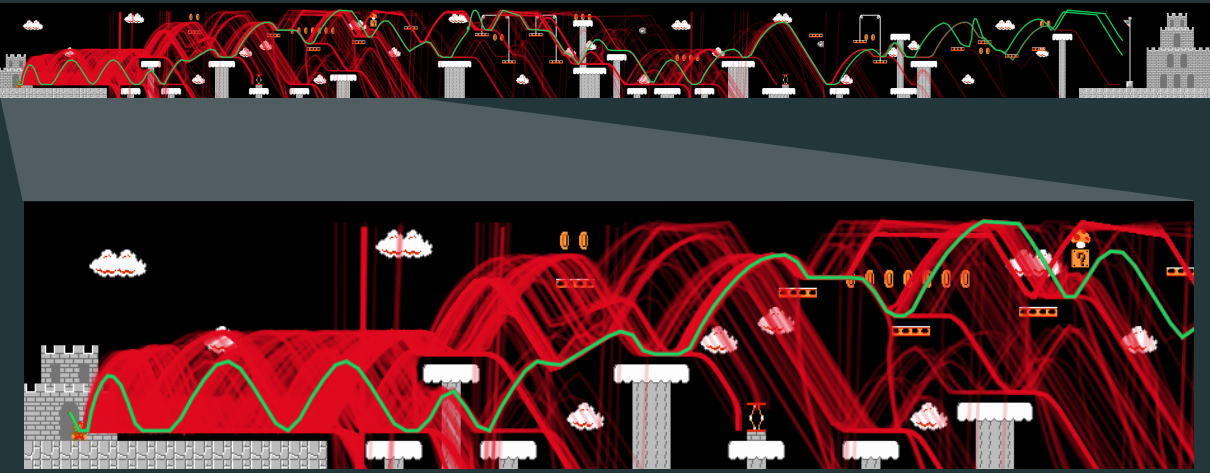


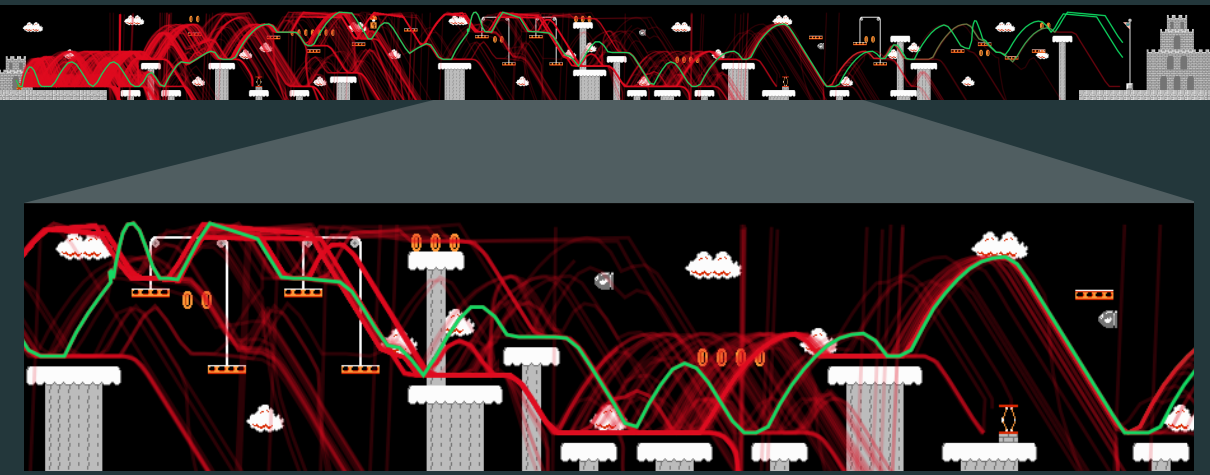
Fuzzing

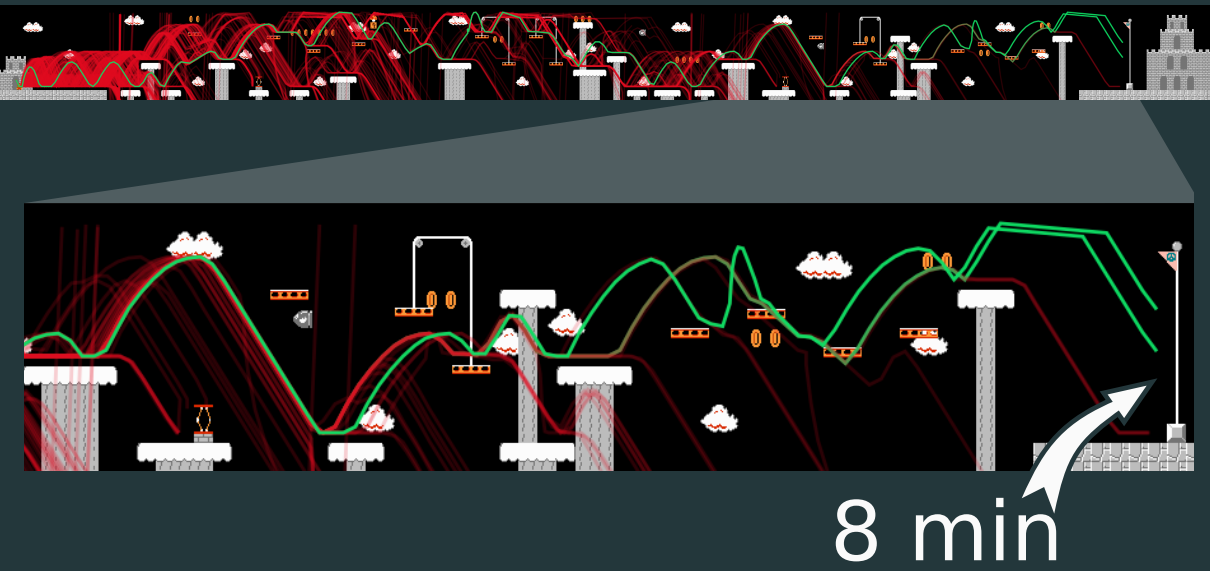
Fuzzers are dumb?



Demo





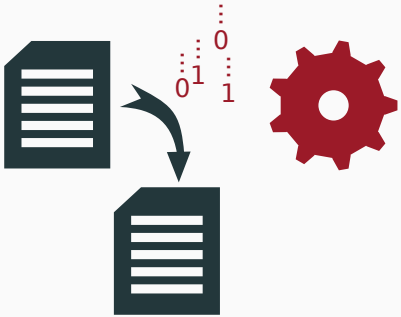

8 min

How do Fuzzer Work?

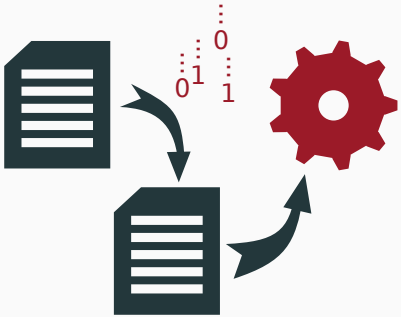
How do Fuzzer Work?

How do Fuzzer Work?

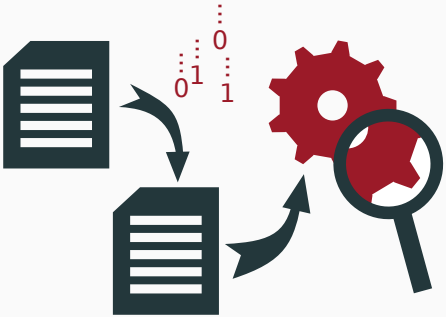
How do Fuzzer Work?



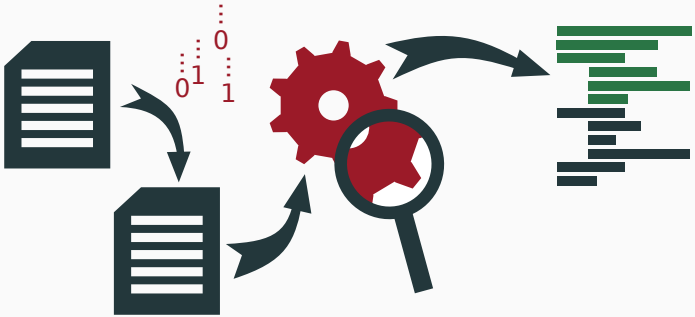
How do Fuzzer Work?



How do Fuzzer Work?

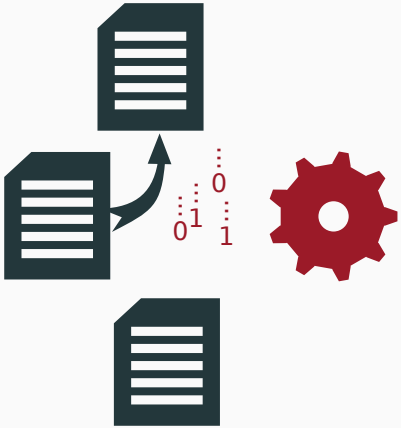


How do Fuzzer Work?

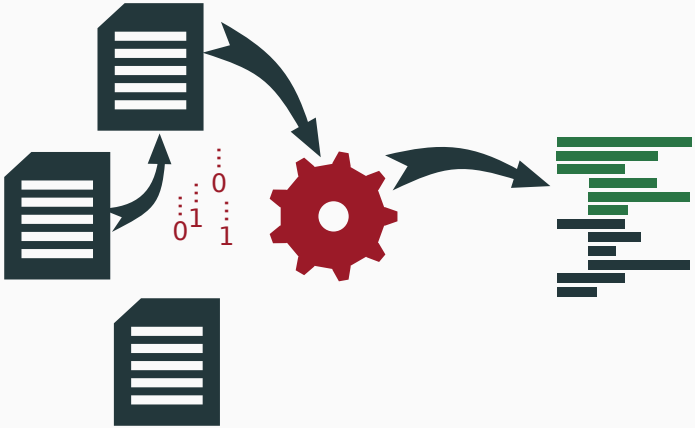


How do Fuzzer Work?

How do Fuzzer Work?



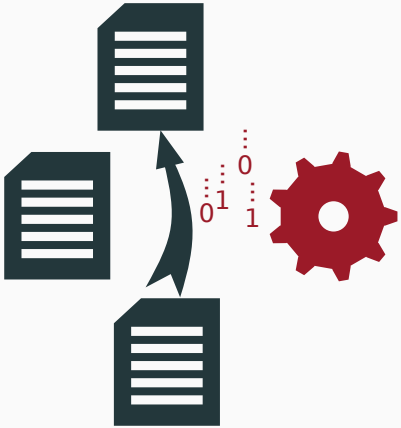
How do Fuzzer Work?



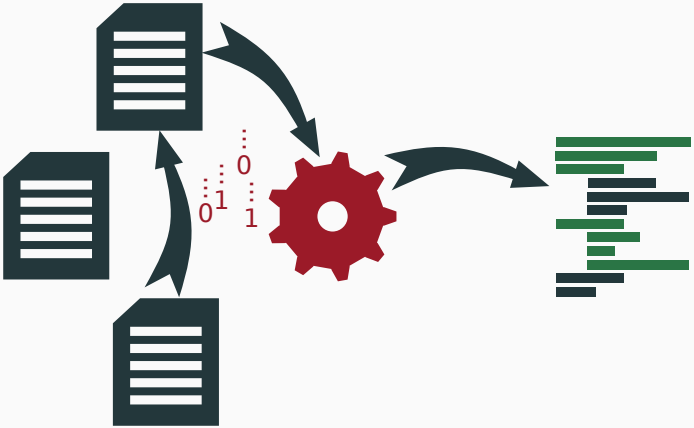
How do Fuzzer Work?

How do Fuzzer Work?

How do Fuzzer Work?



How do Fuzzer Work?



How do Fuzzer Work?

Fuzzers

Artificial Intelligence for Testcase Generation

Key Takeaways:

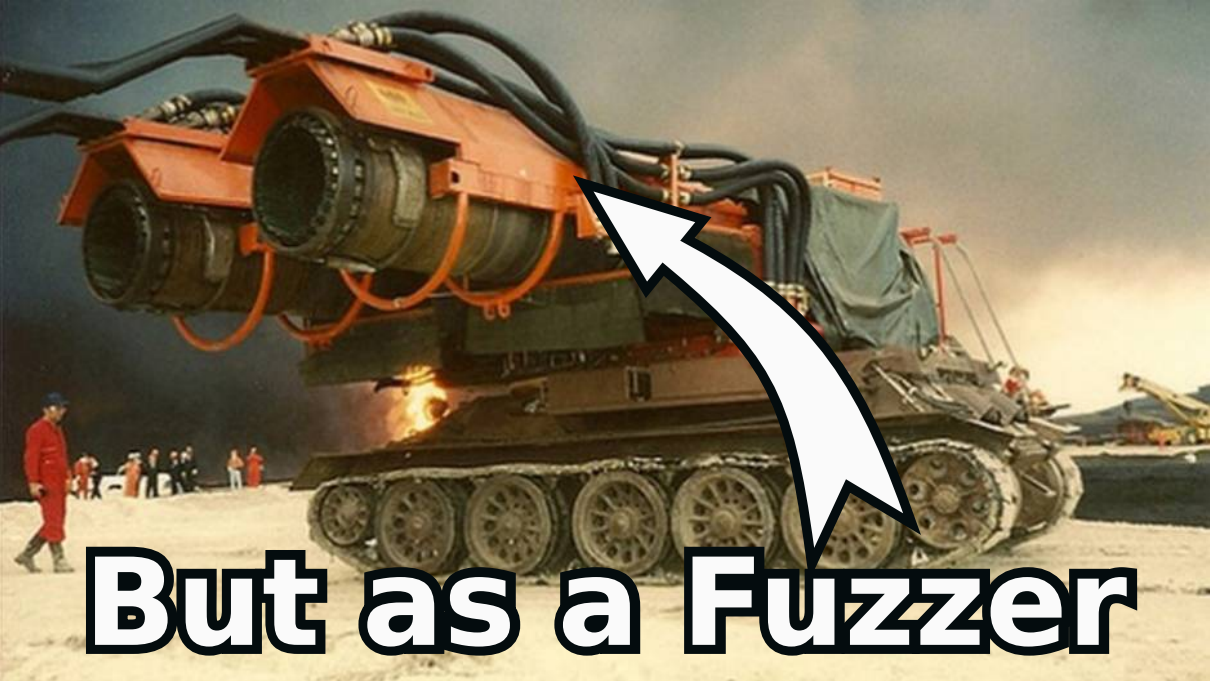
Key Takeaways:

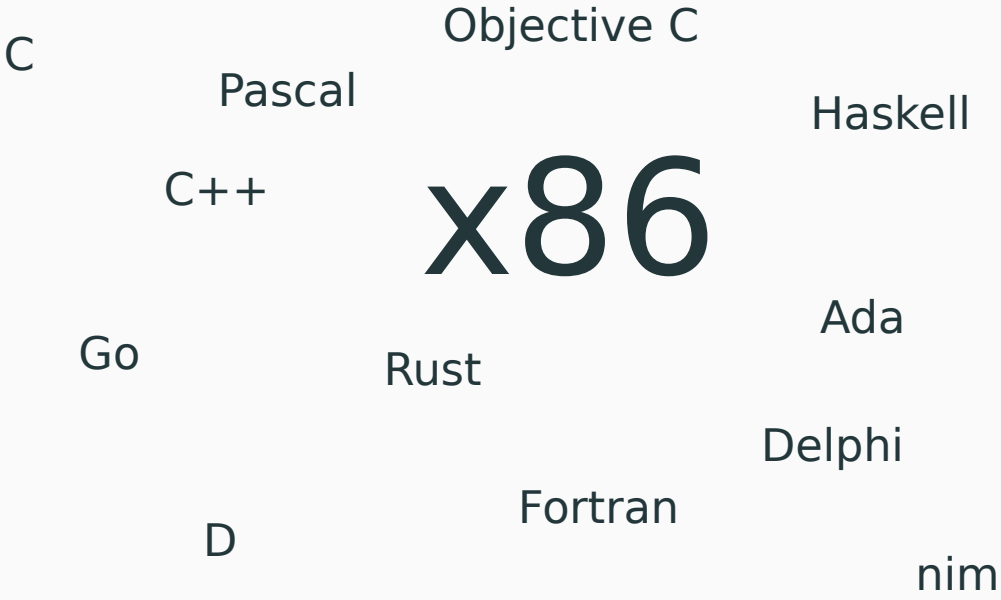
The Rest of this Talk

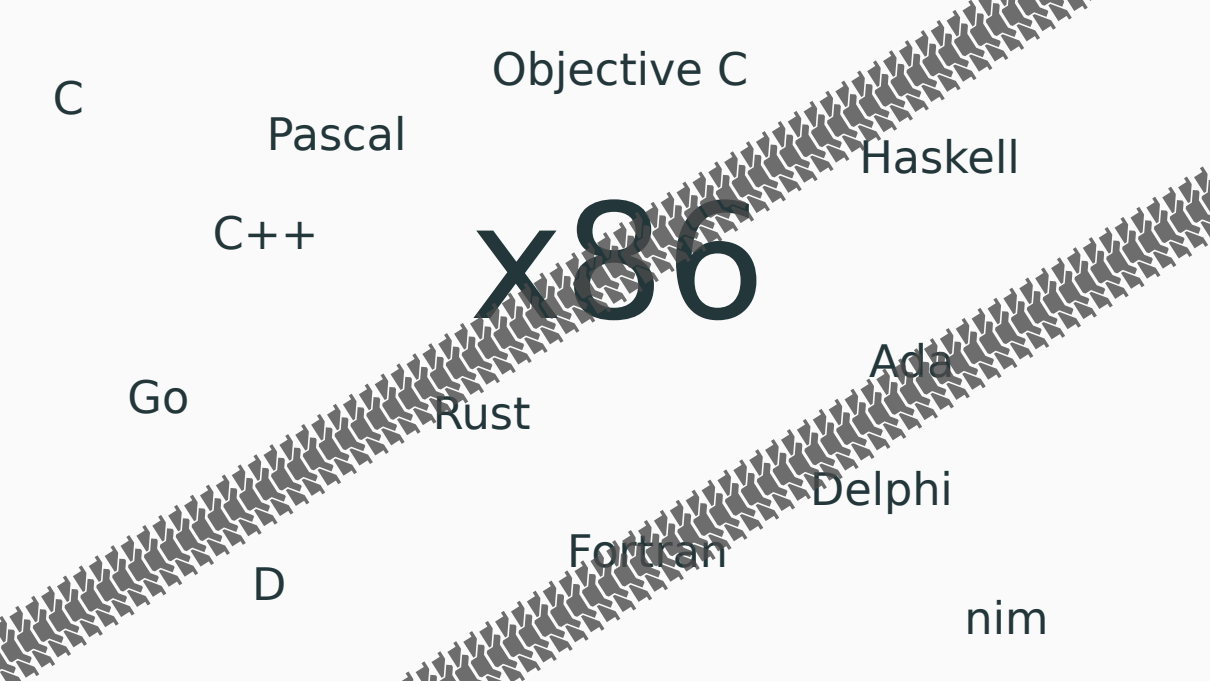
The Rest of this Talk

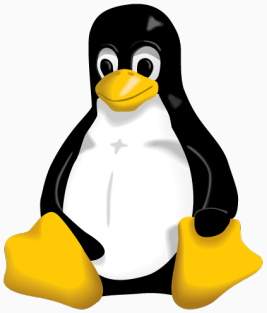
Past Research

Goal

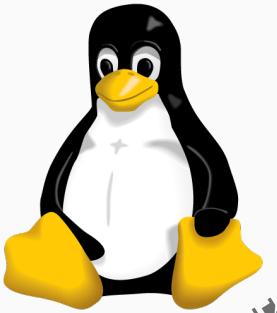

But as a Fuzzer


C
Objective C
Pascal
Haskell
C++
x86
Ada
Go
Rust
Delphi
Fortran
D
nim

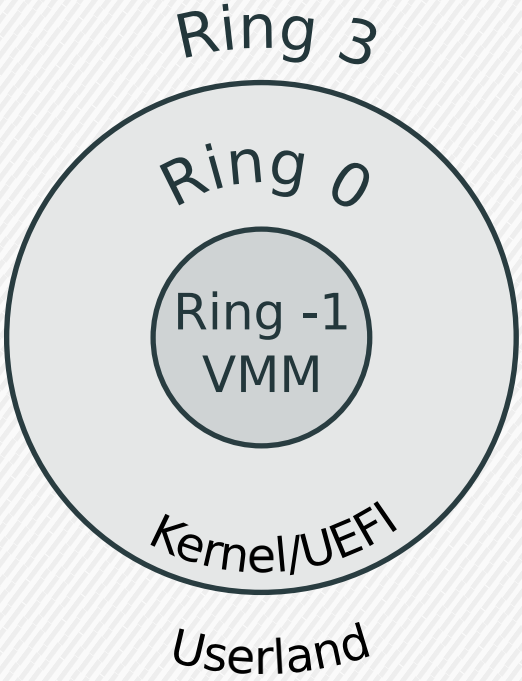

C
Objective C
Pascal
Haskell
C++
x86
Ada
Go
Rust
Delphi
Fortran
D
nim

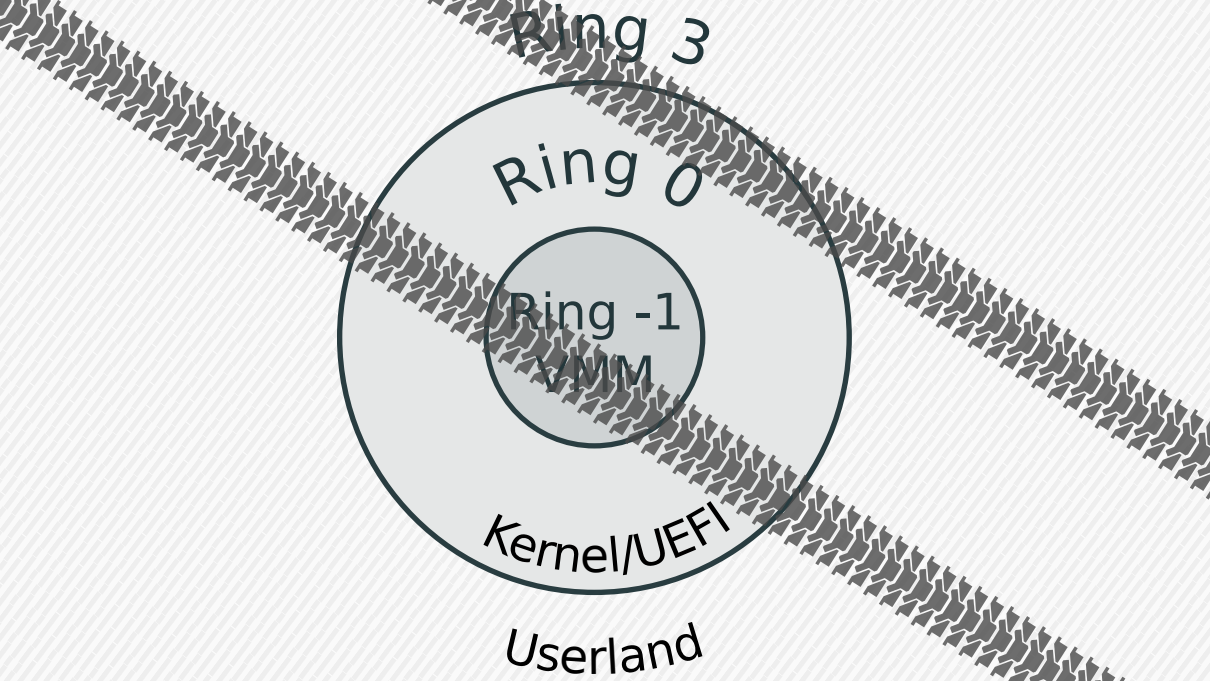



Mac



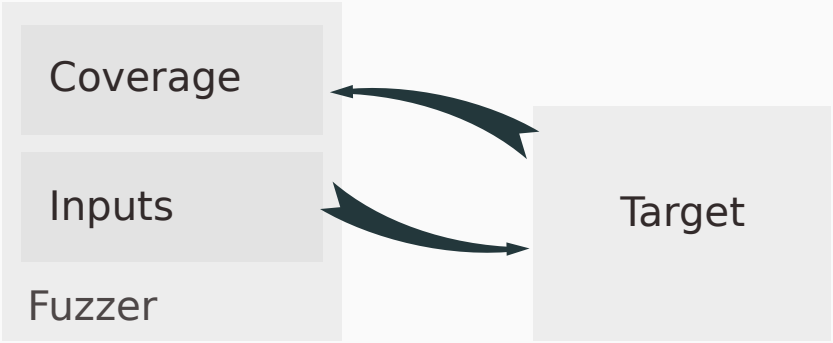
Mac


Ring 3
Ring 0
Ring -1
VMM
Kernel/UEFI
Userland

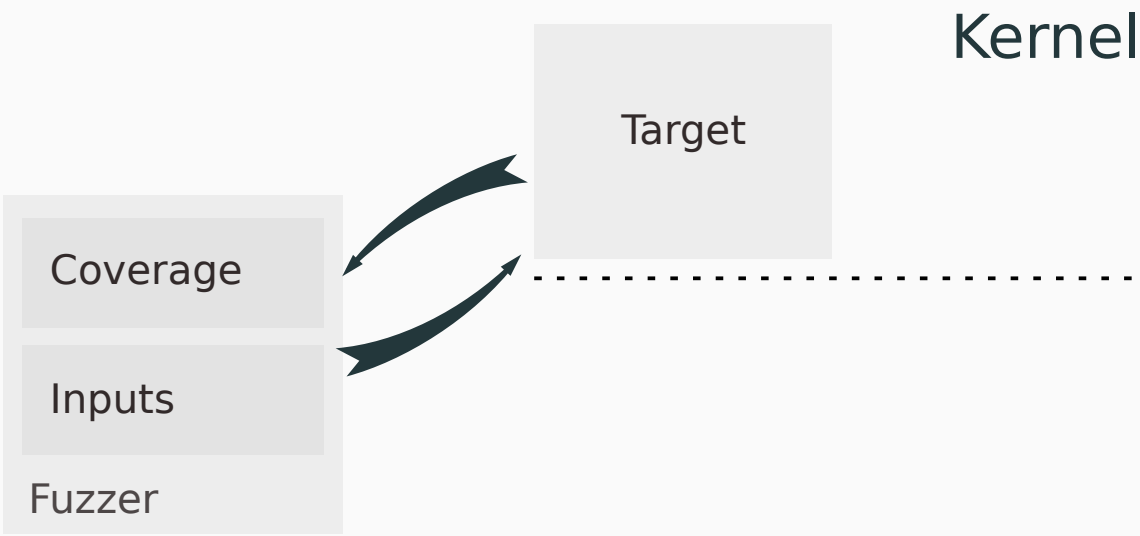

Ring 3
Ring 0
Ring -1
VMM
Kernel/UEFI
Userland

Nyx

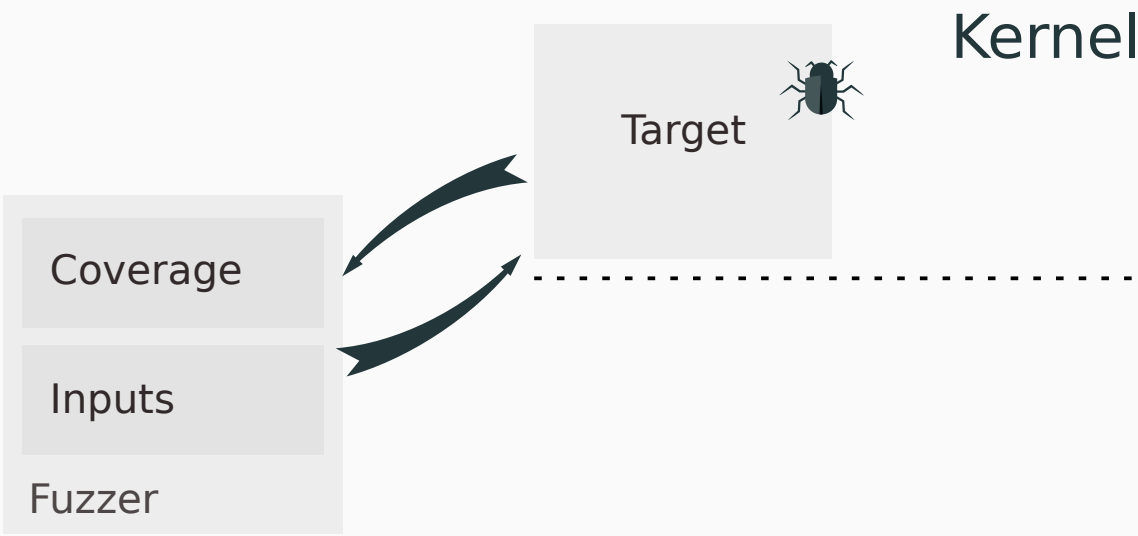
Architecture



Architecture

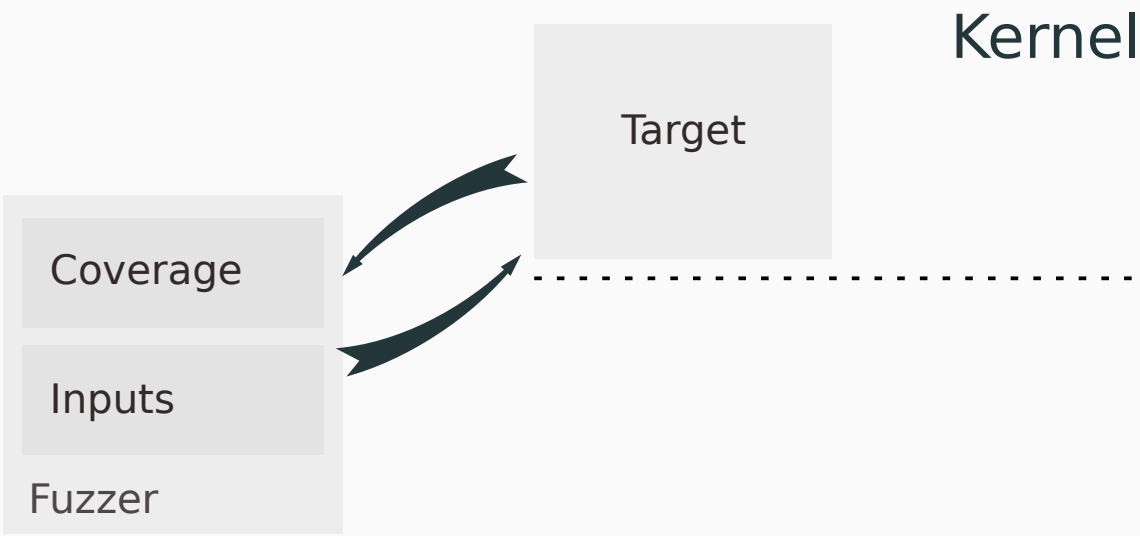


Architecture

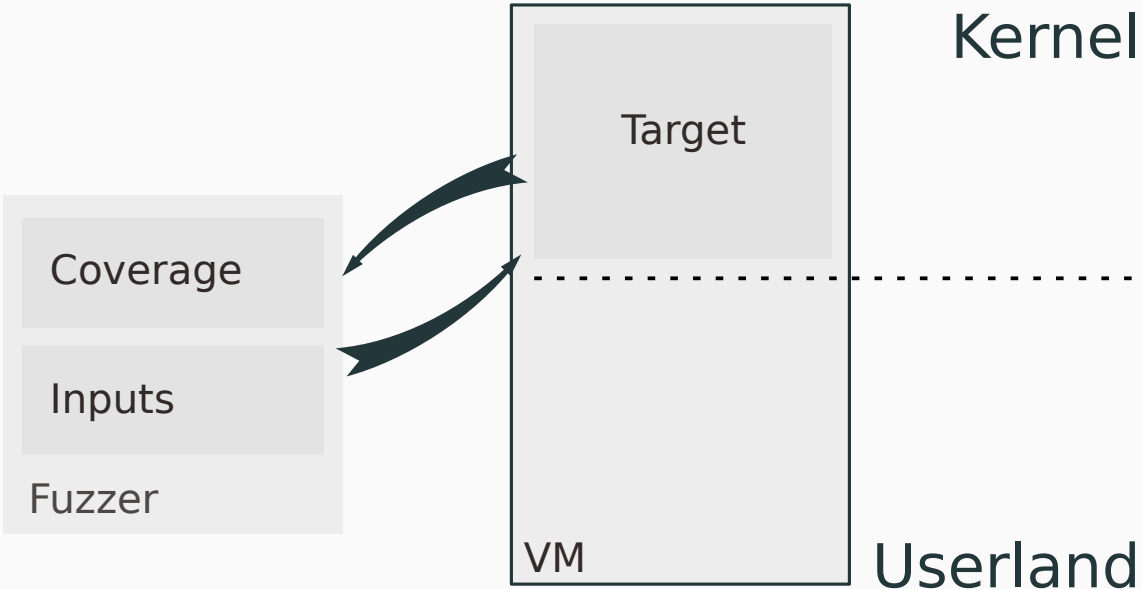



BOOM
Kernel
Input
Fuzzer
Userland

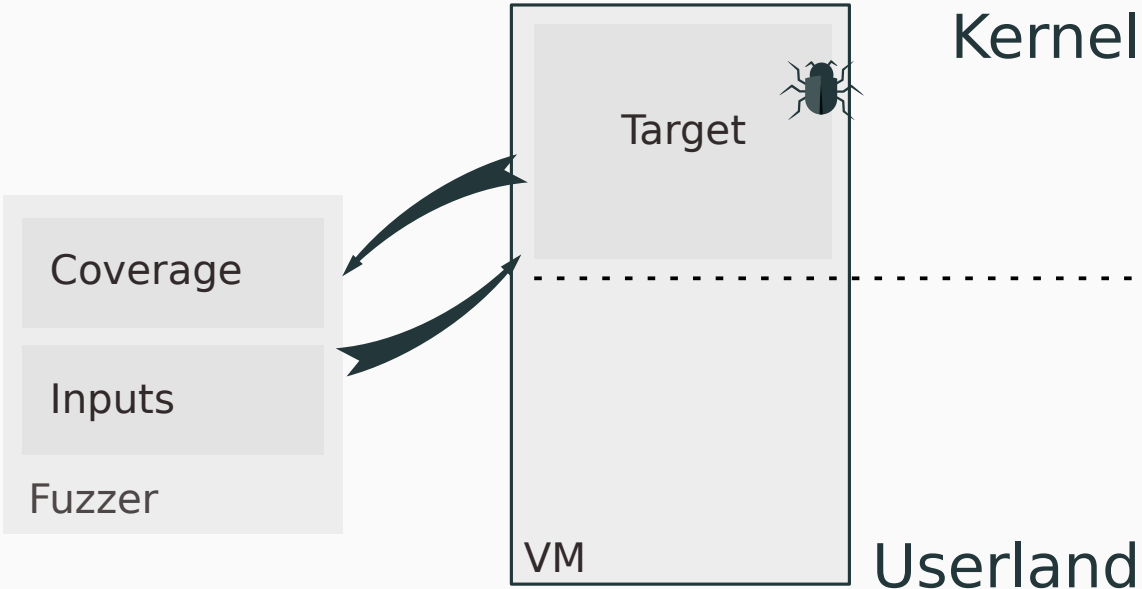
Architecture



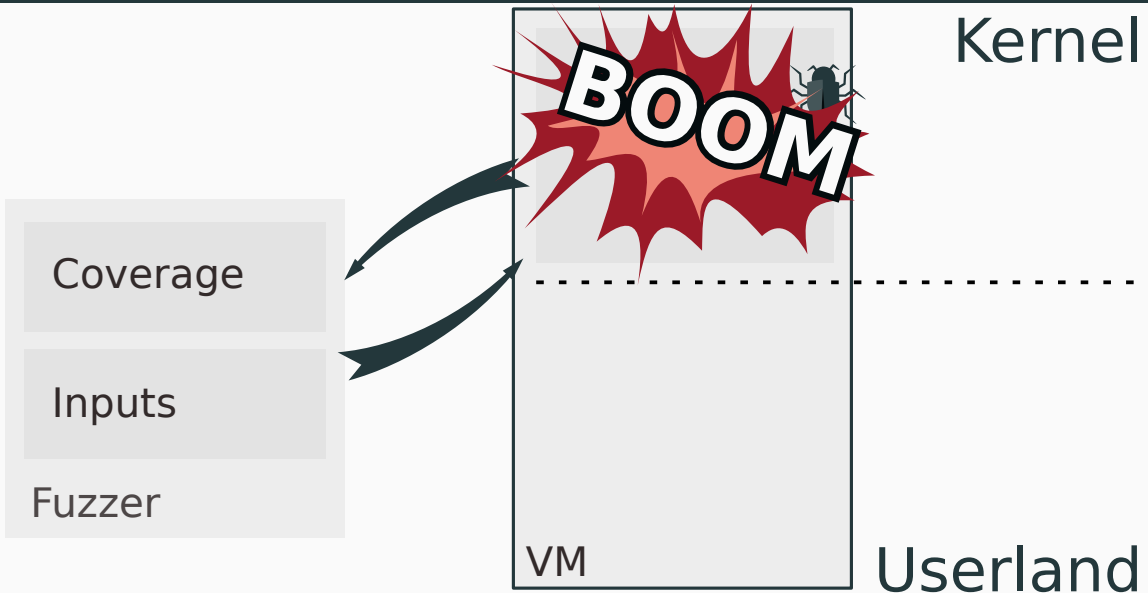
Architecture



Architecture



Architecture



Target in a VM:

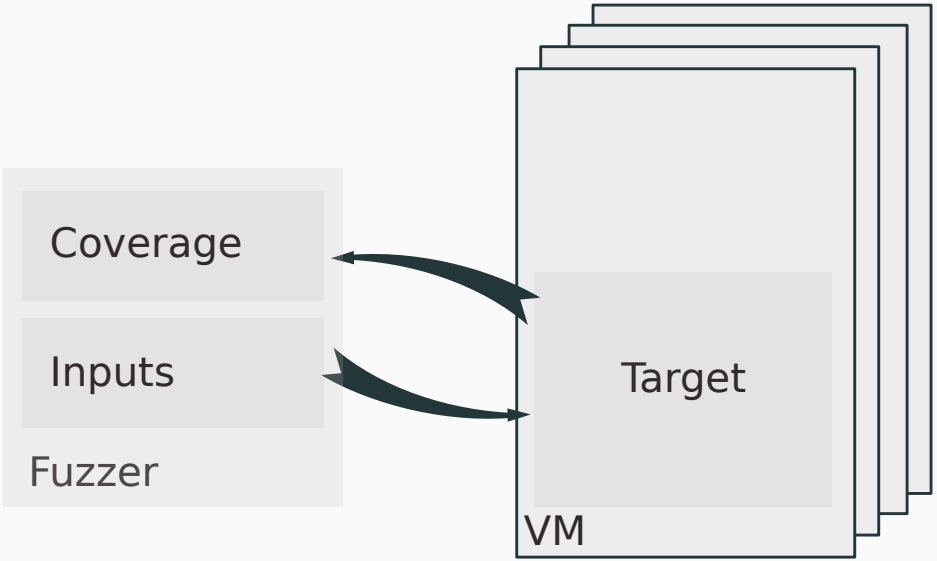
+ Fault Tolerance

Target in a VM:

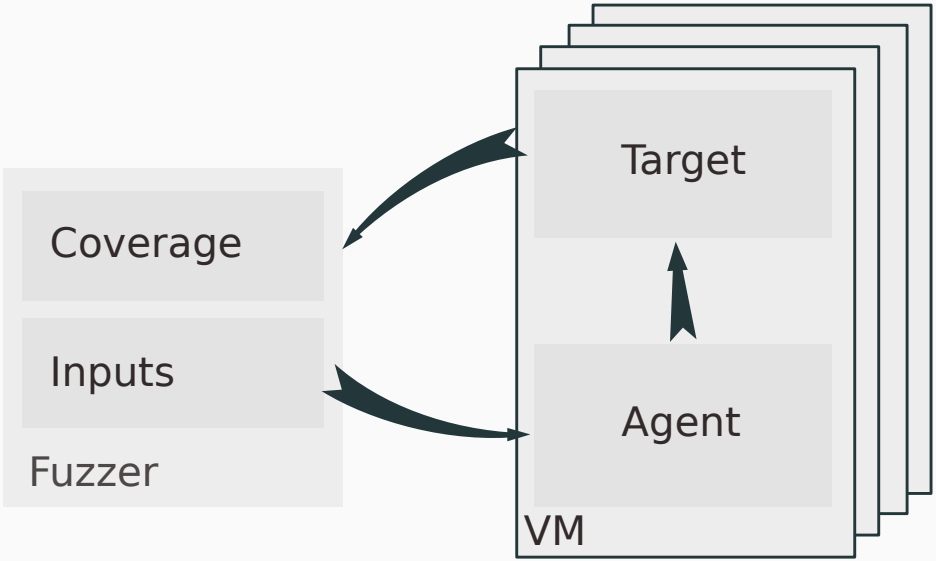
+ Fault Tolerance

+ Parallelization

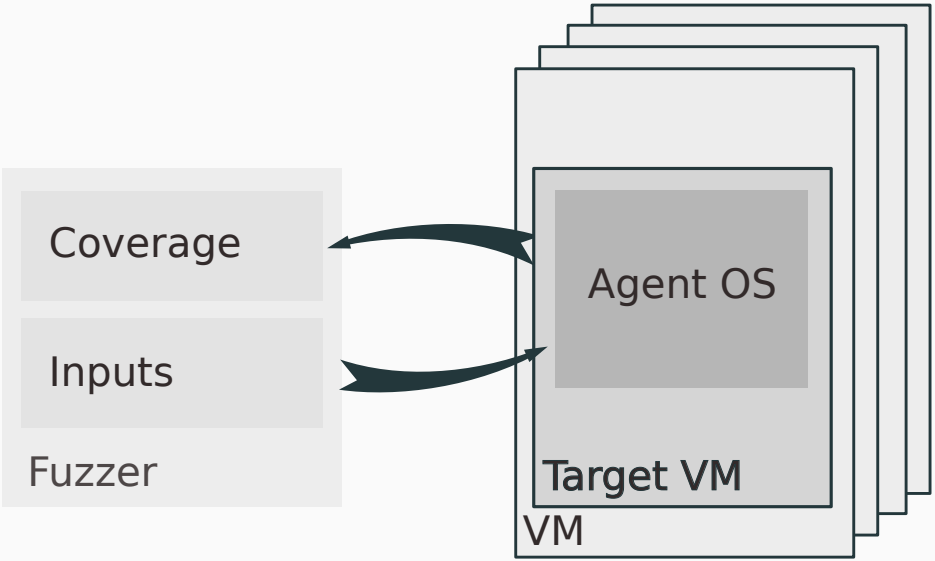
Architecture



Architecture

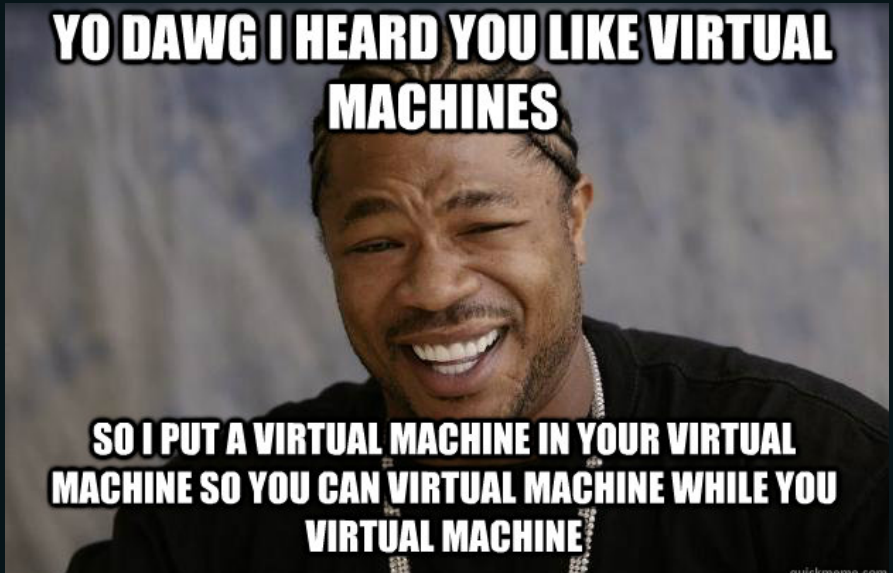


Architecture

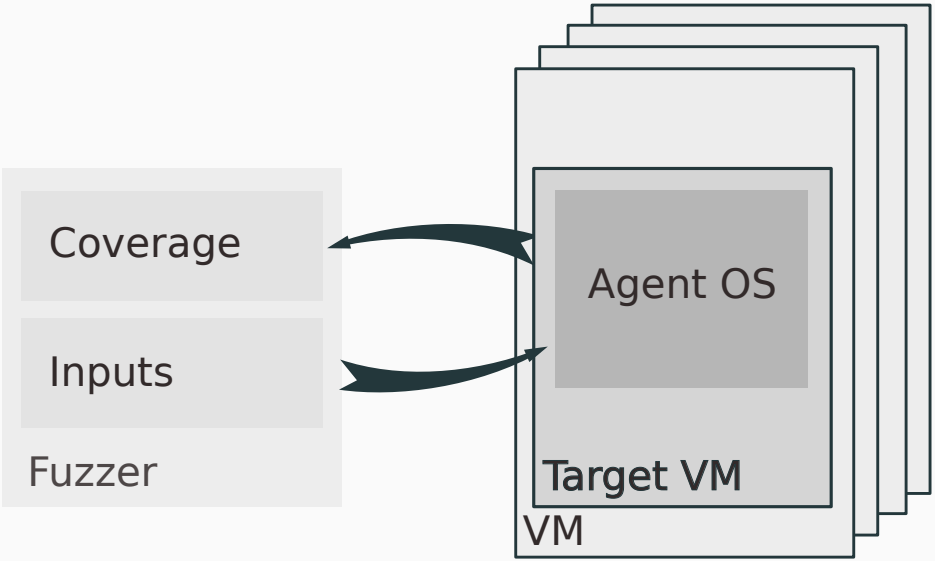


Key Takeaways:

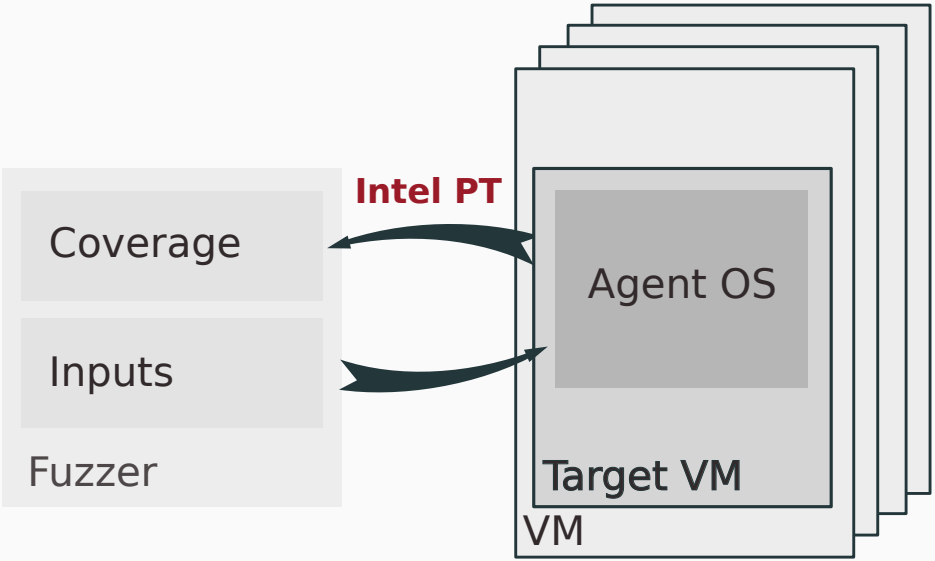
Key Takeaways:



Architecture



Architecture



Intel Processor Trace

Intel PT Data

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

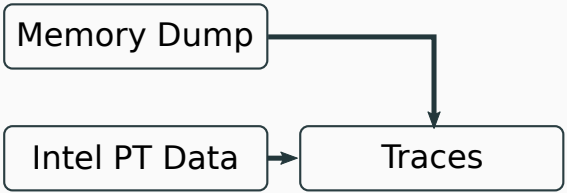
Intel Processor Trace

Memory Dump

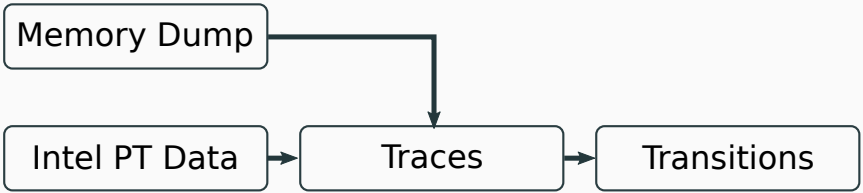
Intel PT Data

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

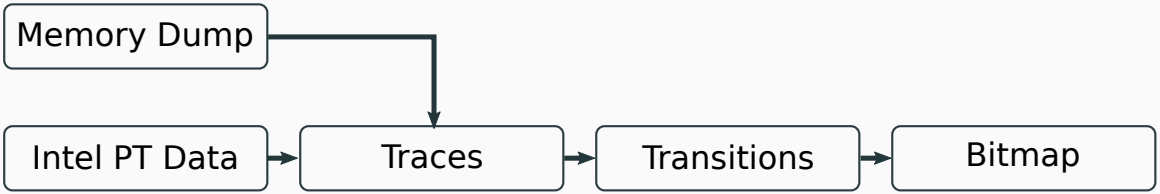
Intel Processor Trace



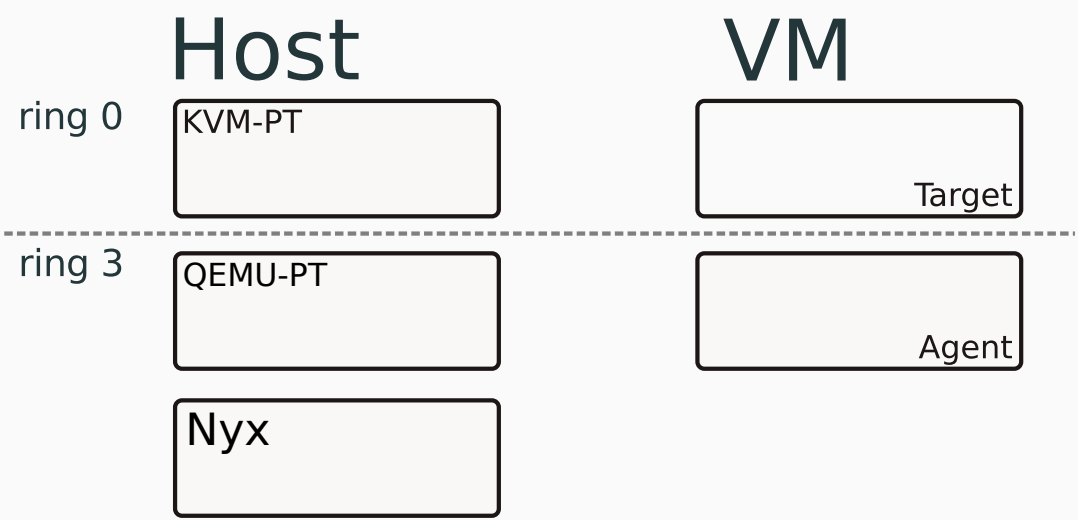
Intel Processor Trace



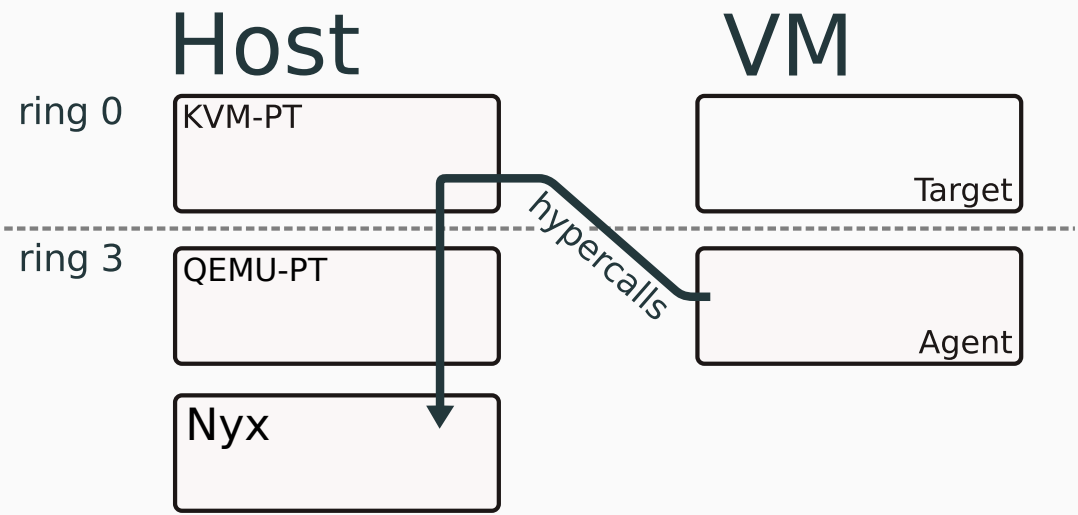
Intel Processor Trace



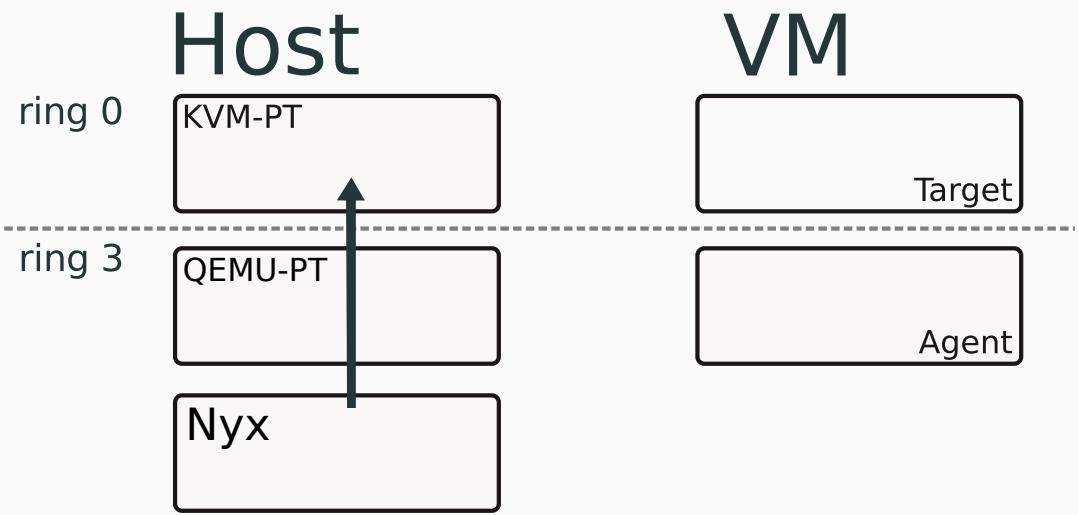
Nyx - One Input



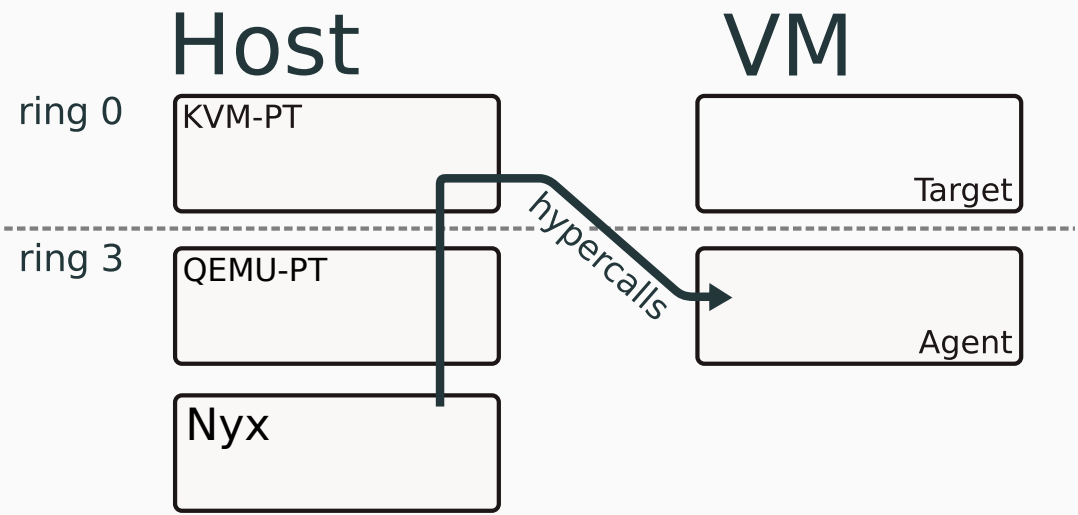
Nyx - One Input



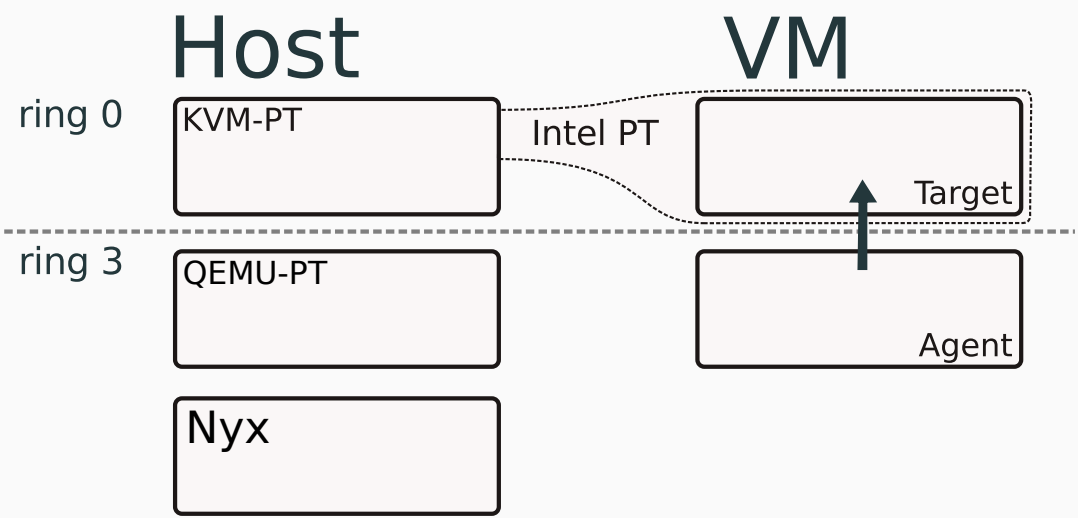
Nyx - One Input



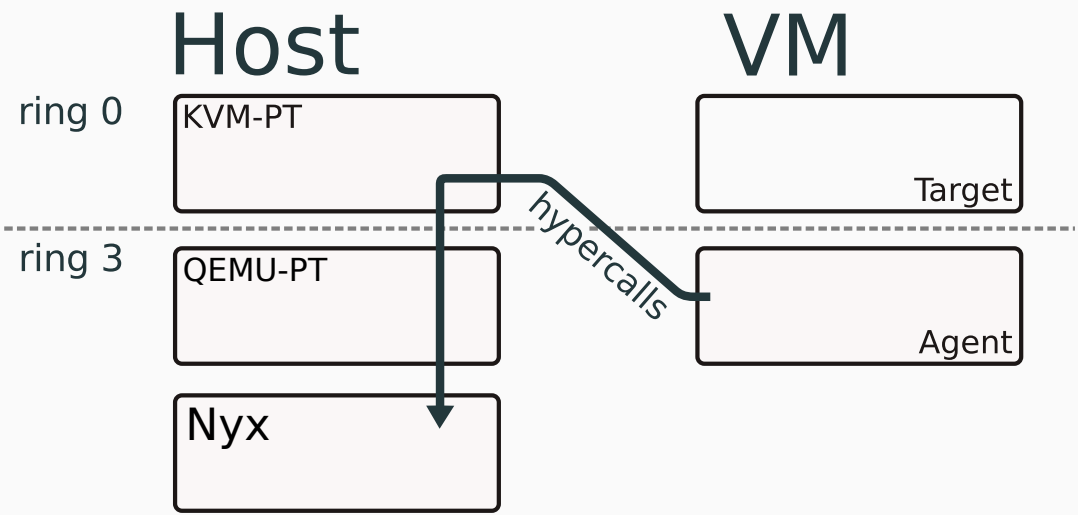
Nyx - One Input



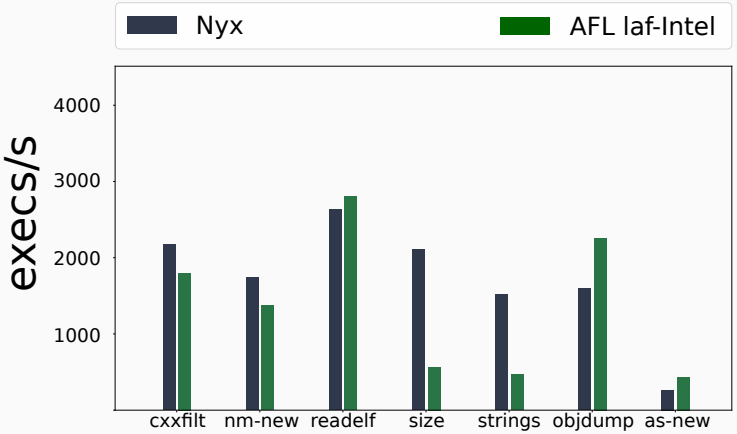
Nyx - One Input



Nyx - One Input



Nyx - Performance



Key Takeaways:


What if I told you
...

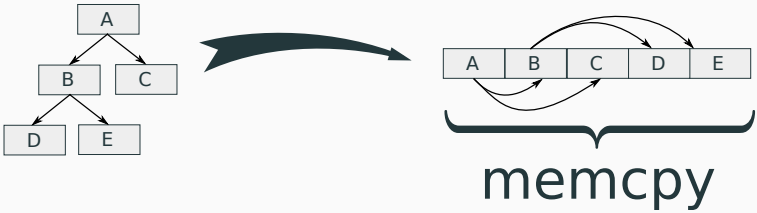

What if I told you
We can be even faster!

Super Fast VM Reloads

~6000

times per second

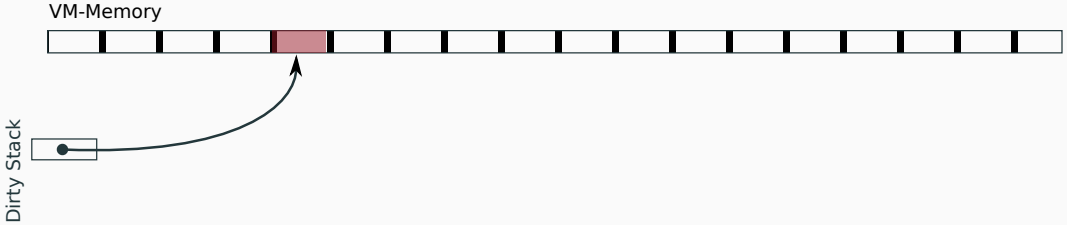
Flatten Qemu VMState Tree



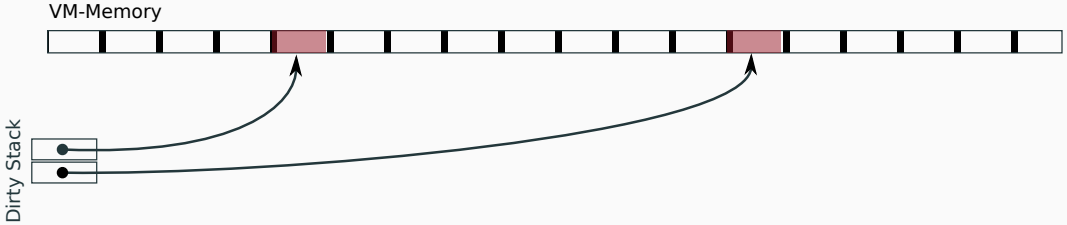
Dirty Page Logging

VM-Memory

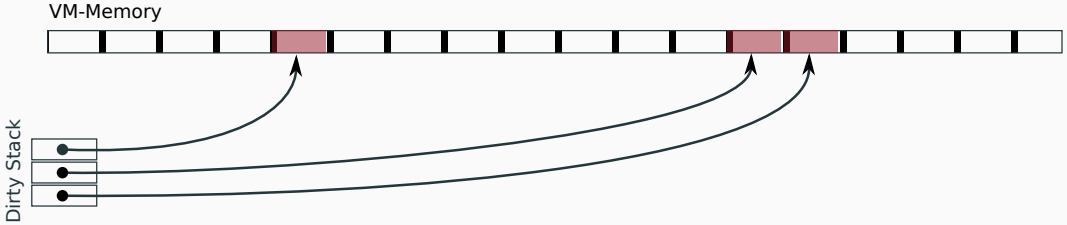
Dirty Page Logging



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 Spawing Processes
~80 execs/sec

Test: gdiplus_test.exe

Just Spawing Processes
~80 execs/sec

Spawn & File Write
~40 execs/sec

Test: gdiplus_test.exe

Just Spawing 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

php

binutils

Perl

Qt
Qtjs

vmware Fusion

intel ACRN

OpenLDAP

curl://

QEMU

mruby

nasm
the netwide assembler

Libxml2

tcc

VirtualBox

Lua

FreeBSD
bhyve

TIFF
libtiff

TCPDUMP

Chakra Core

Gnuplot

BASH
THE BOURNE-AGAIN SHELL

Fraunhofer FDK for Android

Windows

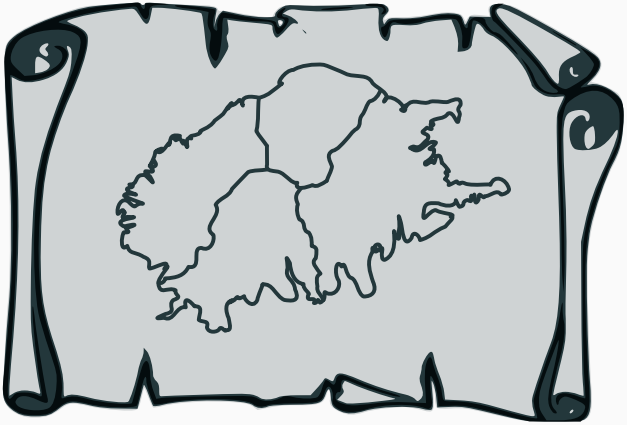
COUNTER-STRIKE SOURCE


macOS High Sierra
TigerVNC
WINE
Parallels Desktop
php
binutils
Perl
Qt
Qtjs
vmware Fusion
intel
ACRN
OpenLDAP
curl://
EMU
VirtualBox
nasm
the netwide assembler
Libxml2
Lua
FreeBSD
bhyve
TCPDUMP
TIFF
libtiff
Chakra Core
Gnuplot
BASH
Fraunhofer FDK for Android
Windows
COUNTER-STRIKE SOURCE

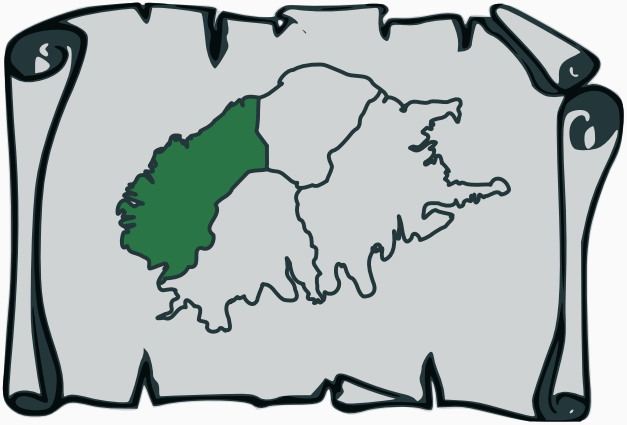
Key Takeaways:

The Rest of this Talk

The Future of Fuzzing



Harnesses

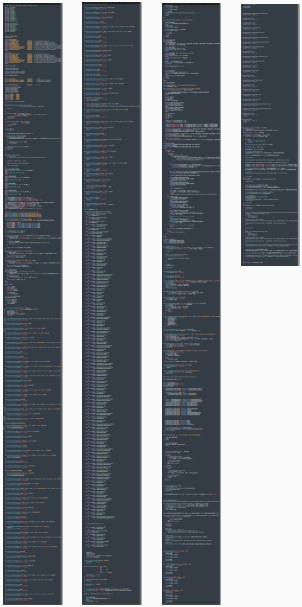


Harnesses

Harnesses

Harnesses

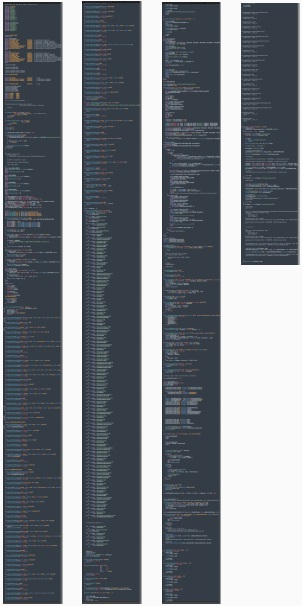
Harnesses

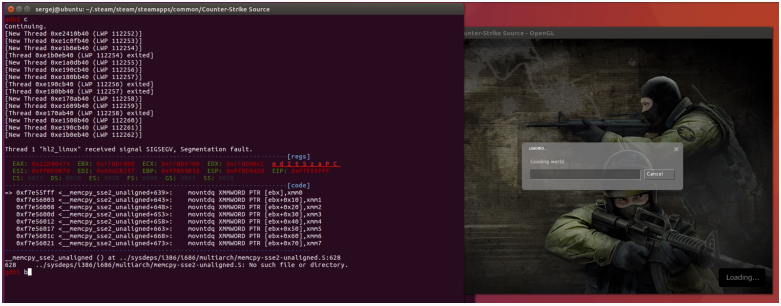


Harnesses

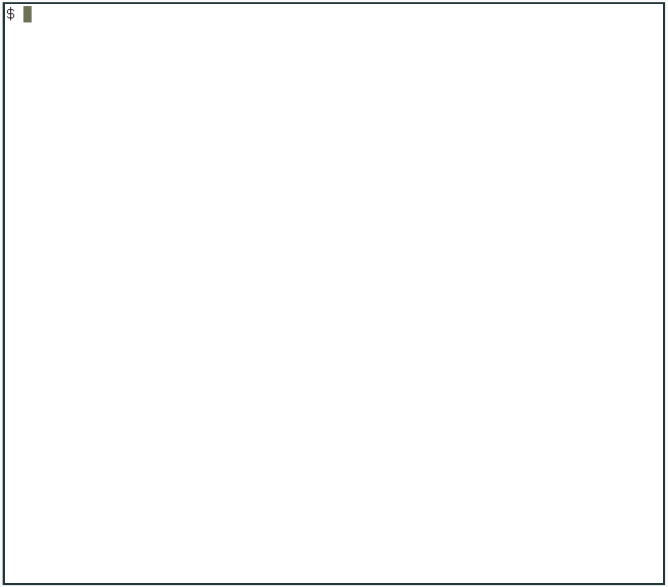
RUHR UNIVERSITÄT BOCHUM

RUB

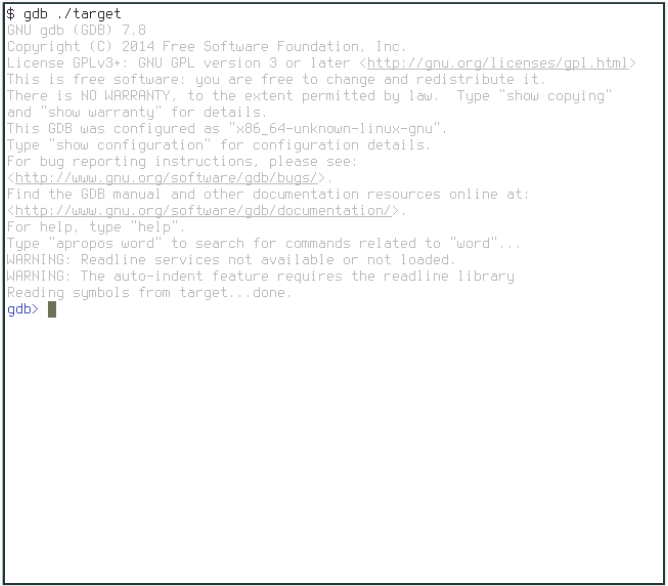




Harnesses



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

RUHR UNIVERSITÄT BOCHUM RUB

```
$ 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

RUHR UNIVERSITÄT BOCHUM RUB

```
$ 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

RUHR UNIVERSITÄT BOCHUM RUB

```
$ 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

RUHR UNIVERSITÄT BOCHUM RUB

```
$ 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>
```

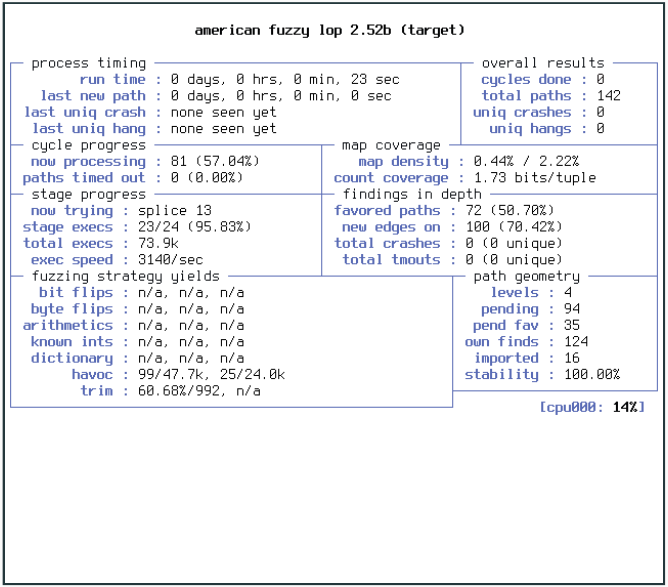
Harnesses

RUHR UNIVERSITÄT BOCHUM RUB

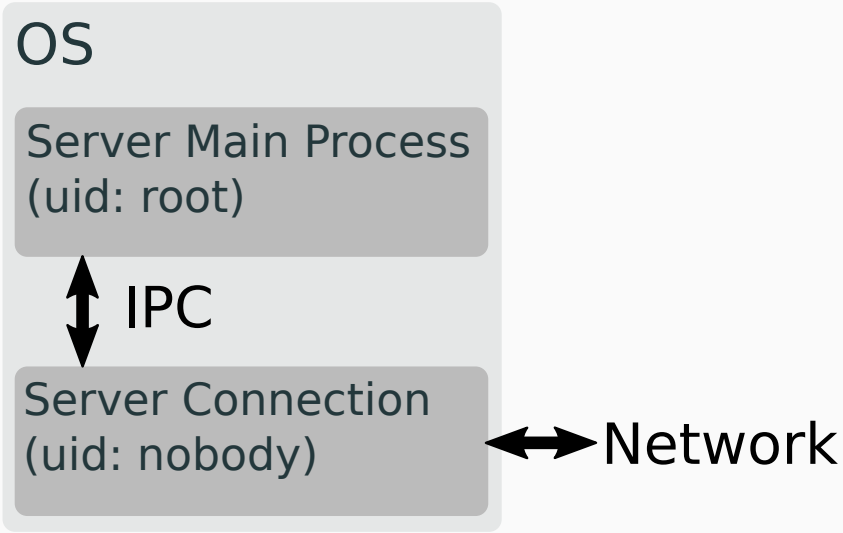
```
$ gdb ./target
GNU gdb (GDB) 7.8
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
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

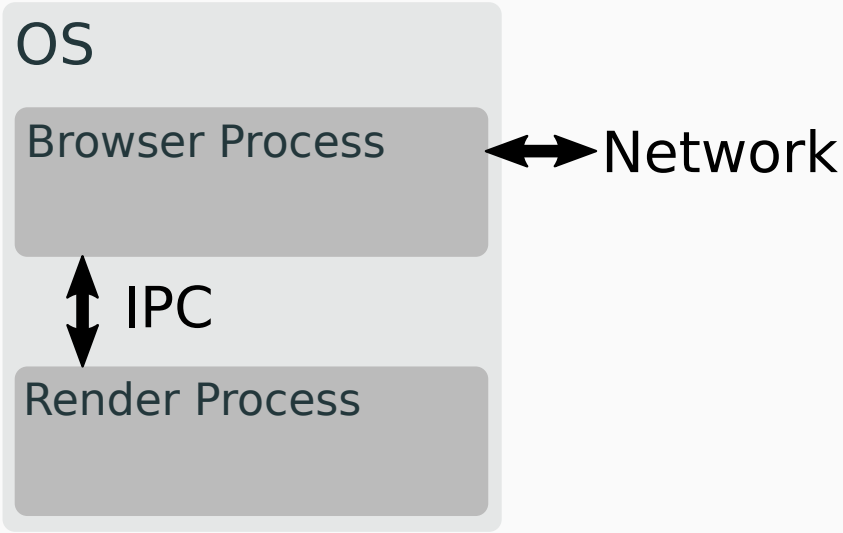
RUHR UNIVERSITÄT BOCHUM RUB



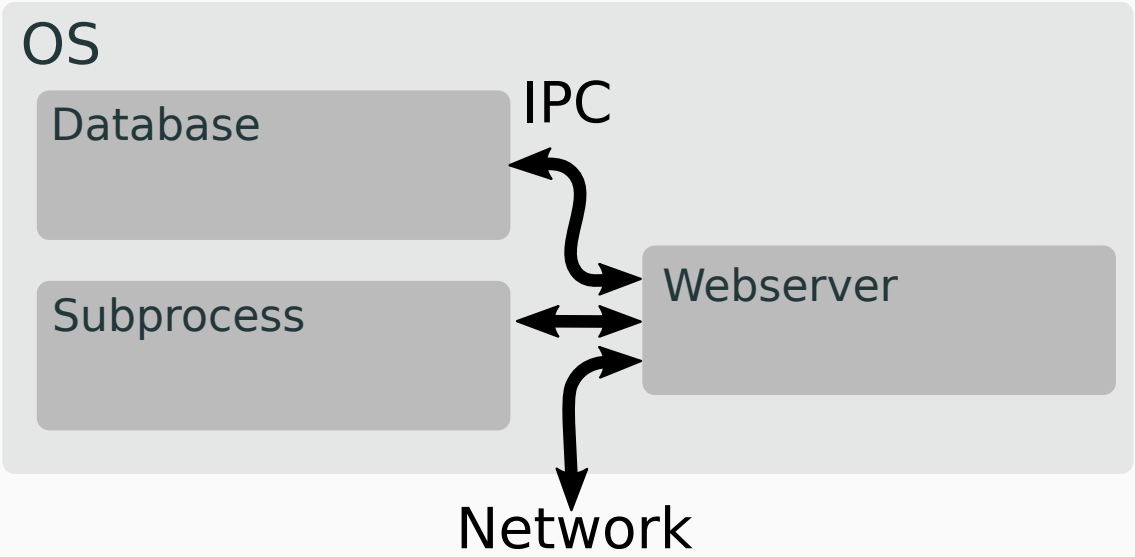
Harnesses


OS
Server Main Process
(uid: root)
IPC
Server Connection
(uid: nobody)
Network

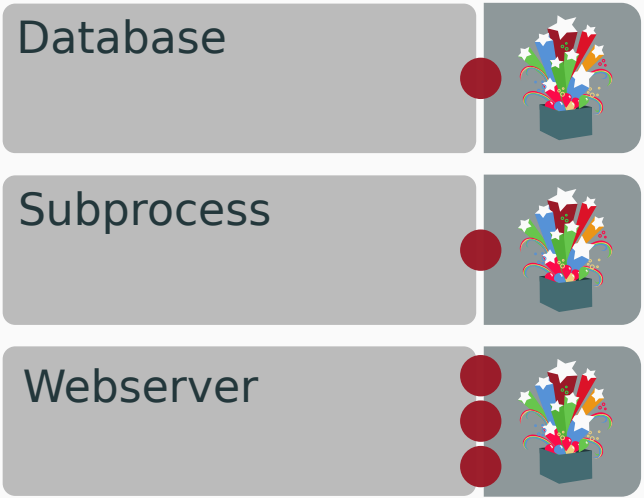
Harnesses



Harnesses

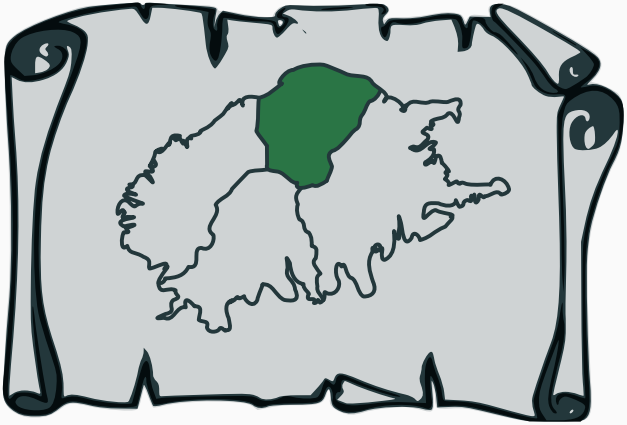


Harnesses



Key Takeaways:

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();
```

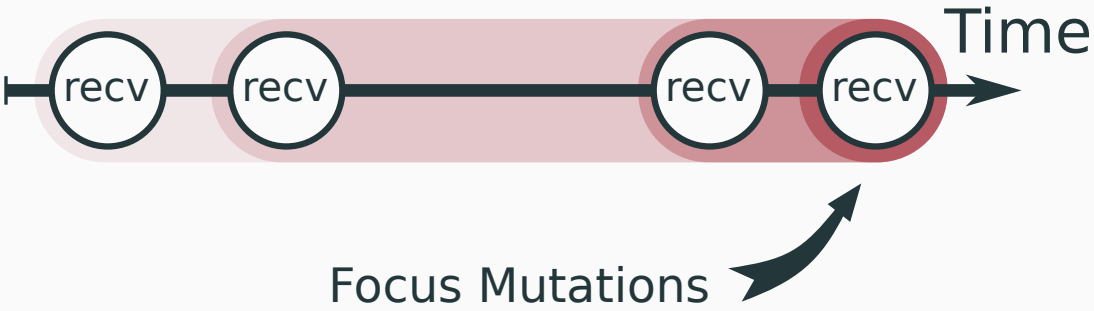
Structural Mutations

Specify Test Scenarios


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

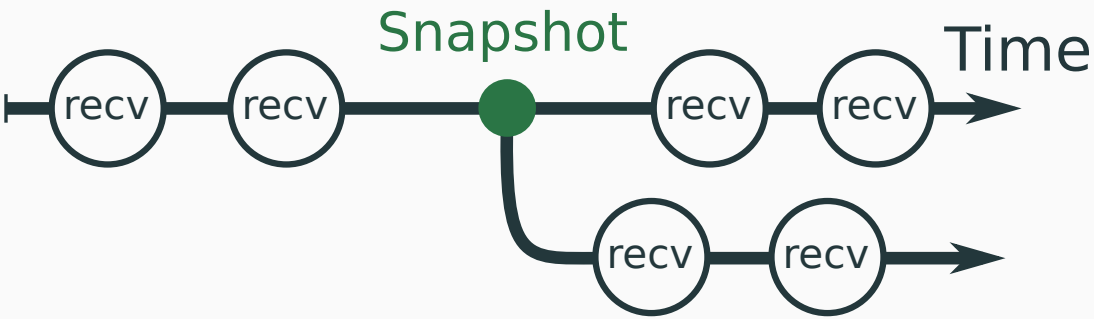
Not reused

Interactive Targets

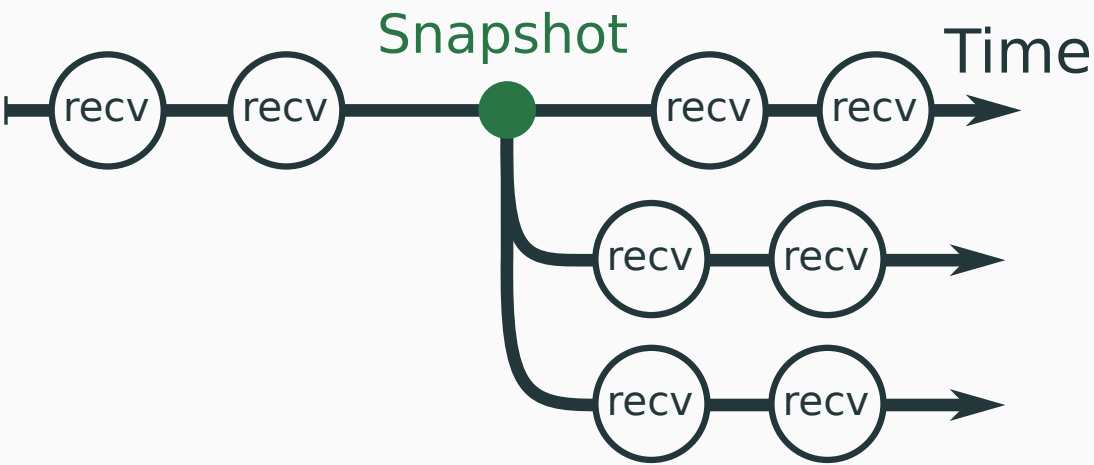


Interactive Targets

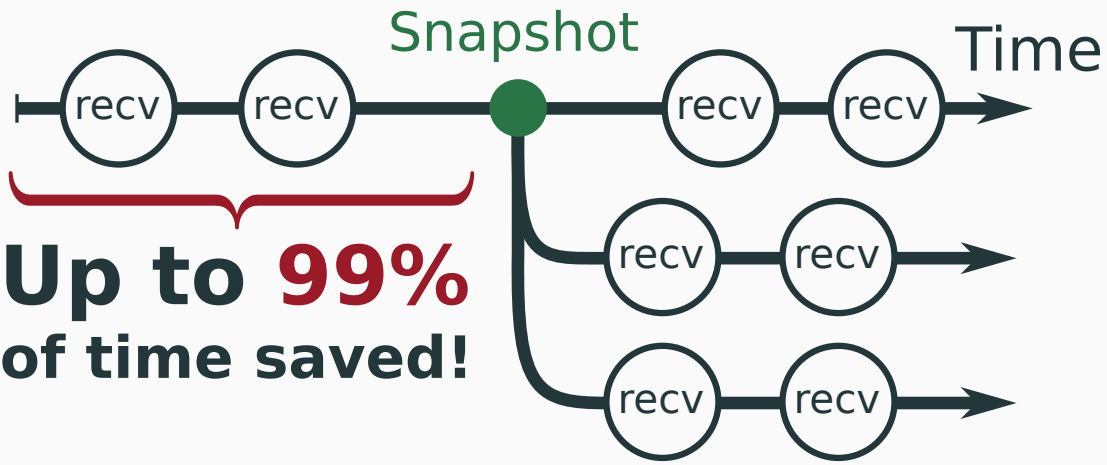
Interactive Targets



Interactive Targets



Interactive Targets



Kernel Testing
meets
Feedback Fuzzing

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

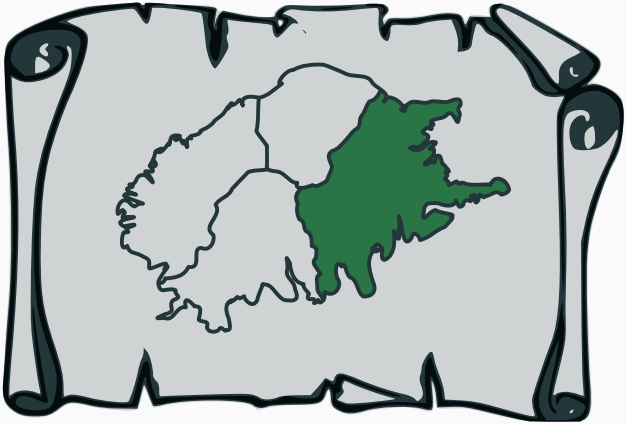
Network Protocol
meets
Feedback Fuzzing

Webcrawler
meets
Feedback Fuzzing

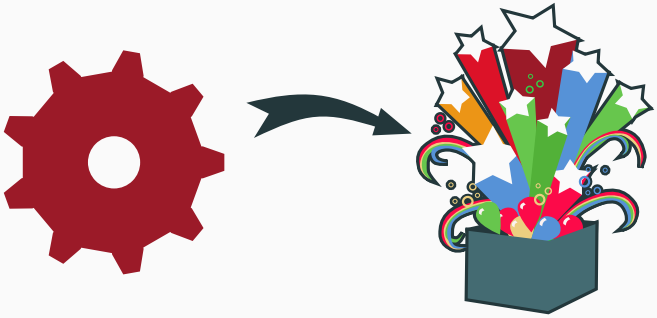
Key Takeaways:

Key Takeaways:

Using Fuzzers

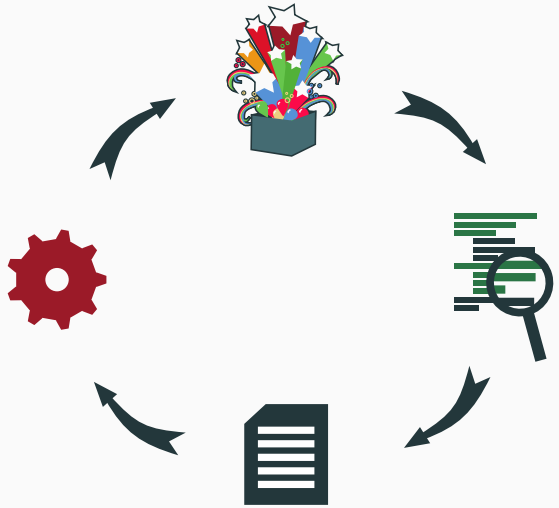


Fuzzing

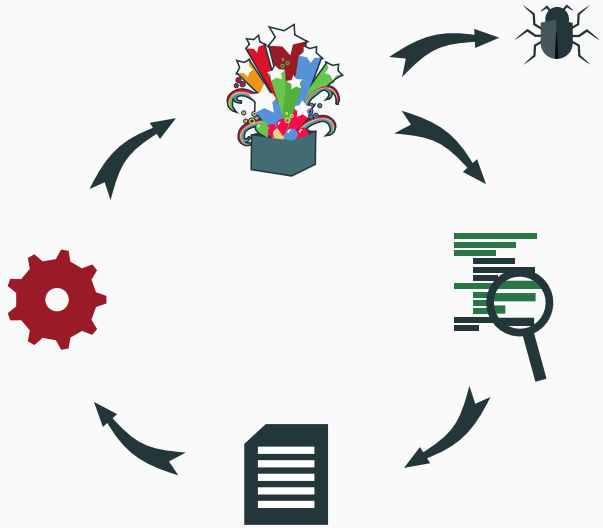


Fuzzing

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
7   void test(int a,int b){
8    while(a>0){
9           if(b==0){printf("b<a\n");return;}
10          a--;
11          b--;
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:\
22      scanf("%d", &a)
23     printf("Enter something el
24      scanf("%d", &b);
25   if(a > 0 && a < 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
42  //nop
43  //mov
44  //jmp
45  //jne
46  //je
47  //ret
48  //cmp
49  //files
50  //
51  //
52  //
53  //
54  //
55  //
56  //
```

```
00400646  push rbp
00400647  mov rbp, rsp
0040064a  sub rsp, 0x10
0040064e  mov dword ptr [rbp - 4], edi
00400651  mov eax, dword ptr [rbp - 4]
00400654  mov esi, eax
00400656  mov edi, 0x4007f4
0040065b  mov eax, 0
00400660  call 0x400510
00400665  nop
00400666  leave
00400667  ret
00400668  push rbp
00400669  mov rbp, rsp
0040066c  sub rsp, 0x10
00400670  mov dword ptr [rbp - 4], edi
00400673  mov dword ptr [rbp - 8], esi
00400676  jmp 0x400692
00400678  cmp dword ptr [rbp - 8], 0
0040067c  jne 0x40068a
0040067e  mov edi, 0x4007fc
00400683  call 0x4004f0
00400688  jmp 0x4006b5
0040068a  sub dword ptr [rbp - 4], 1
0040068e  sub dword ptr [rbp - 8], 1
00400692  cmp dword ptr [rbp - 4], 0
00400696  jg 0x400678
00400698  cmp dword ptr [rbp - 8], 0
0040069c  jne 0x4006aa
0040069e  mov edi, 0x400800
004006a3  call 0x4004f0
004006a8  jmp 0x4006b5
004006aa  mov edi, 0x400805
004006af  call 0x4004f0
004006b4  nop
004006b5  leave
004006b6  ret
004006b7  push rbp
004006b8  mov rbp, rsp
004006bb  sub rsp, 0x10
004006bf  mov rax, qword ptr fs:[0x28]
004006c8  mov qword ptr [rbp - 8], rax
004006cc  xor eax, eax
004006ce  mov edi, 0x400809
004006d3  call 0x4004f0
004006d8  lea rax, qword ptr [rbp - 0x10]
004006dc  mov rsi, rax
004006df  mov edi, 0x40081a
004006e4  mov eax, 0
004006e9  call 0x400530
004006ee  mov edi, 0x40081d
004006f3  call 0x4004f0
004006f8  lea rax, qword ptr [rbp - 0xc]
004006fc  mov rsi, rax
004006ff  mov edi, 0x40081a
00400704  mov eax, 0
```

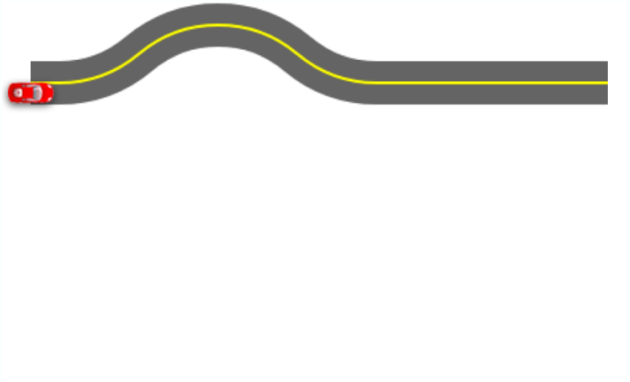
Demo

Create Analysis Tools that

Abstract away Inputs

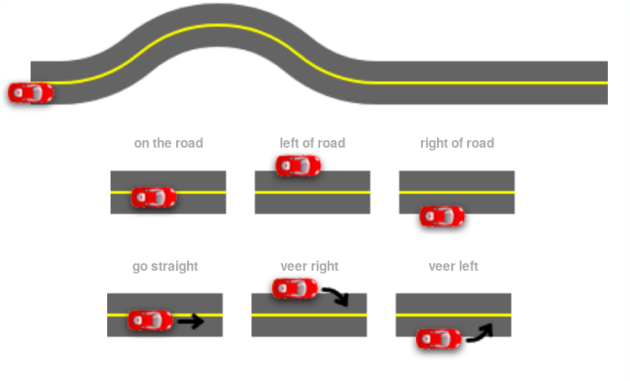
From http://worrydream.com/LadderOfAbstraction/

Fuzzing



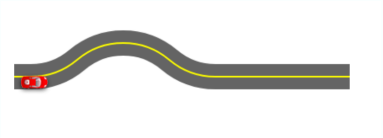
From http://worrydream.com/LadderOfAbstraction/

Fuzzing



From http://worrydream.com/LadderOfAbstraction/

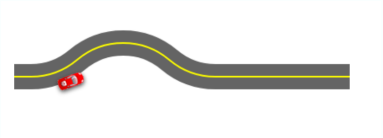
Fuzzing



Debugger (gdb, olly, ...)

From http://worrydream.com/LadderOfAbstraction/

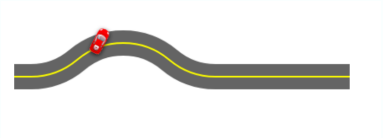
Fuzzing



Debugger (gdb, olly, ...)

From http://worrydream.com/LadderOfAbstraction/

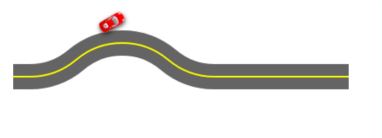
Fuzzing



Debugger (gdb, olly, ...)

From http://worrydream.com/LadderOfAbstraction/

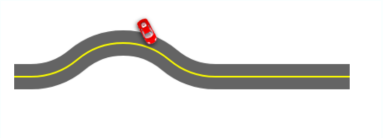
Fuzzing



Debugger (gdb, olly, ...)

From http://worrydream.com/LadderOfAbstraction/

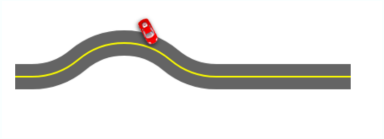
Fuzzing



Debugger (gdb, olly, ...)

From http://worrydream.com/LadderOfAbstraction/

Fuzzing



Debugger (gdb, olly, ...)

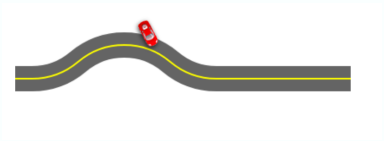
Abstract away Time

Time traveling Debugger

(rr, REVEN, ...)

From http://worrydream.com/LadderOfAbstraction/

Fuzzing



Debugger (gdb, olly, ...)

Abstract away Time

Time traveling Debugger

(rr, REVEN, ...)

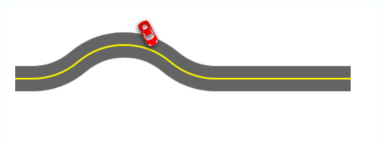
Abstract away Inputs

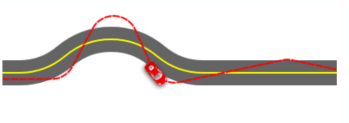
Fuzzing Debugger

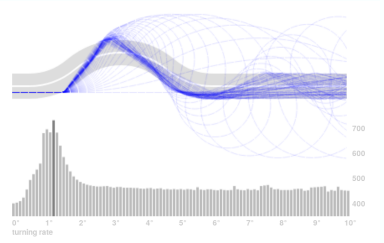
????

From http://worrydream.com/LadderOfAbstraction/

Fuzzing







Debugger (gdb, olly, ...)

Abstract away Time

Time traveling Debugger

(rr, REVEN, ...)

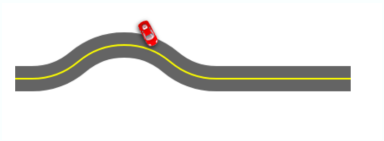
Abstract away Inputs

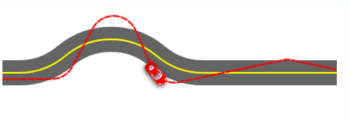
Fuzzing Debugger

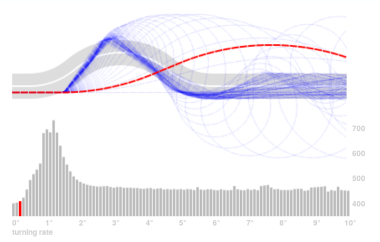
????

From http://worrydream.com/LadderOfAbstraction/

Fuzzing







Debugger (gdb, olly, ...)

Abstract away Time

Time traveling Debugger

(rr, REVEN, ...)

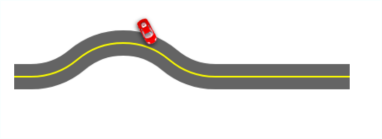
Abstract away Inputs

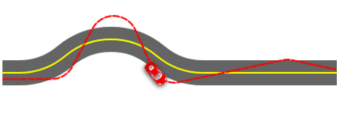
Fuzzing Debugger

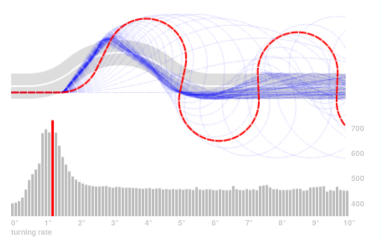
????

From http://worrydream.com/LadderOfAbstraction/

Fuzzing







Debugger (gdb, olly, ...)

Abstract away Time

Time traveling Debugger

(rr, REVEN, ...)

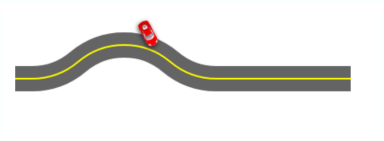
Abstract away Inputs

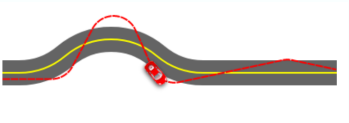
Fuzzing Debugger

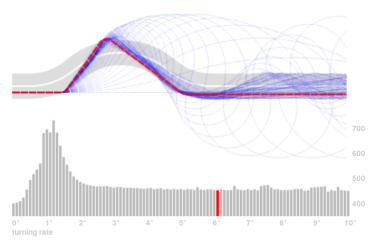
????

From http://worrydream.com/LadderOfAbstraction/

Fuzzing







Debugger (gdb, olly, ...)

Abstract away Time

Time traveling Debugger

(rr, REVEN, ...)

Abstract away Inputs

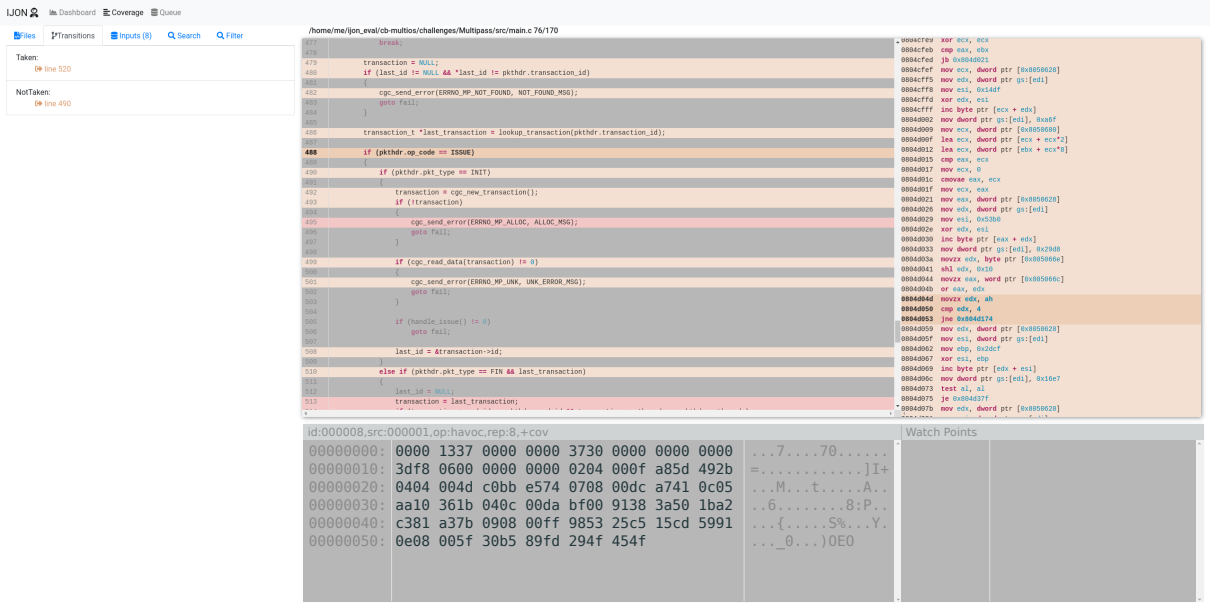
Fuzzing Debugger

????

From http://worrydream.com/LadderOfAbstraction/

A Better Tool...

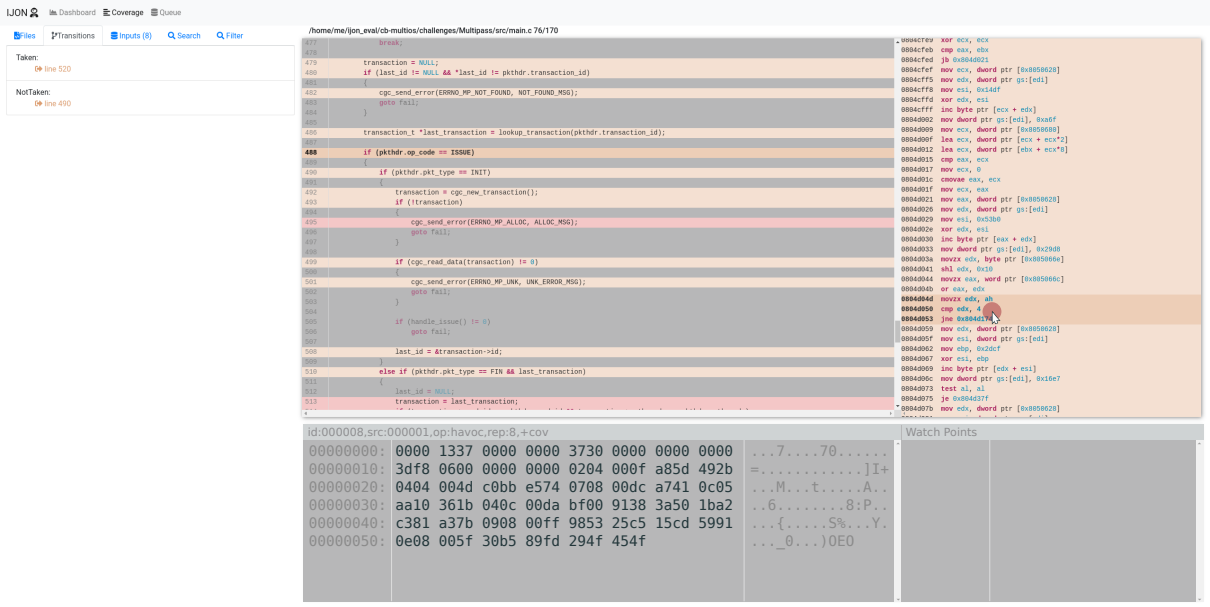
RUHR UNIVERSITÄT BOCHUM RUB



A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB



A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB

IJON Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

Taken:
0↵ line 520

NotTaken:
0↵ 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(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;
```

```
0804cfeb  xor ecx, ecx
0804cfed  cmp eax, ebx
0804cfef  jb 0x804d021
0804cff1  mov ecx, dword ptr [0x8050628]
0804cff5  mov edx, dword ptr gs:[edi]
0804cff8  mov esi, 0x14df
0804cffd  xor edx, esi
0804cfff  inc byte ptr [ecx + edx]
0804d002  mov dword ptr gs:[edi], 0xa6f
0804d009  mov ecx, dword ptr [0x8050688]
0804d00f  lea ecx, dword ptr [ecx + ecx*2]
0804d012  lea ecx, dword ptr [ebx + ecx*8]
0804d015  cmp eax, ecx
0804d017  mov ecx, 0
0804d01c  cmovae eax, ecx
0804d01f  mov ecx, eax
0804d021  mov eax, dword ptr [0x8050628]
0804d026  mov edx, dword ptr gs:[edi]
0804d029  mov esi, 0x53b0
0804d02e  xor edx, esi
0804d030  inc byte ptr [eax + edx]
0804d033  mov dword ptr gs:[edi], 0x29d0
0804d03a  movzx edx, byte ptr [0x805806e]
0804d041  shl edx, 0x10
0804d044  movzx eax, word ptr [0x805806c]
0804d04b  or eax, edx
0804d04d  movzx edx, ah
0804d050  cmp edx, 4
0804d053  jne 0x804d174
0804d059  mov edx, dword p
0804d05f  mov esi, dword p
0804d062  mov ebp, 0x2dcf
0804d067  xor esi, ebp
0804d069  inc byte ptr [edx + esi]
0804d06c  mov dword ptr gs:[edi], 0x10e7
0804d073  test al, al
0804d075  je 0x804d37f
0804d07b  mov edx, dword ptr [0x8050628]
```

Add Watch Point

id:000008,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...)OEO
```

Watch Points

A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB

IJON Dashboard Coverage Queue

Files | Transitions | Inputs (8) | Search | Filter

Taken:
- line 520

NotTaken:
- 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(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;
```

```
0804cfeb  xor ecx, ecx
0804cfed  cmp eax, ebx
0804cfef  jb 0x804d021
0804cff1  mov ecx, dword ptr [0x8050628]
0804cff5  mov edx, dword ptr gs:[edi]
0804cff8  mov esi, 0x14df
0804cffd  xor edx, esi
0804cfff  inc byte ptr [ecx + edx]
0804d002  mov dword ptr gs:[edi], 0xa6f
0804d009  mov ecx, dword ptr [0x8050688]
0804d00f  lea ecx, dword ptr [ecx + ecx*2]
0804d012  lea ecx, dword ptr [ebx + ecx*8]
0804d015  cmp eax, ecx
0804d017  mov ecx, 0
0804d01c  cmovae eax, ecx
0804d01f  mov ecx, eax
0804d021  mov eax, dword ptr [0x8050628]
0804d026  mov edx, dword ptr gs:[edi]
0804d029  mov esi, 0x53b0
0804d02e  xor edx, esi
0804d030  inc byte ptr [eax + edx]
0804d033  mov dword ptr gs:[edi], 0x29d0
0804d03a  movzx edx, byte ptr [0x805806e]
0804d041  shl edx, 0x10
0804d044  movzx eax, word ptr [0x805806c]
0804d04b  or eax, edx
0804d04d  movzx edx, ah
0804d050  cmp edx, 4
0804d053  jne 0x804d174
0804d059  mov edx, dword p
0804d05f  mov esi, dword p
0804d062  mov ebp, 0x2dcf
0804d067  xor esi, ebp
0804d069  inc byte ptr [edx + esi]
0804d06c  mov dword ptr gs:[edi], 0x10e7
0804d073  test ai, ai
0804d075  je 0x804d37f
0804d07b  mov edx, dword ptr [0x8050628]
```

Add Watch Point

id:000008,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...)OEO
```

Watch Points

A Better Tool...

RUHR UNIVERSITÄT BOCHUM RUB

IJON Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

Taken:
0x line 520

NotTaken:
0x 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(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;
```

```
0804cfeb  xor ecx, ecx
0804cfed  cmp eax, ebx
0804cfef  jb 0x804d021
0804cfef  mov ecx, dword ptr [0x8050628]
0804cff5  mov edx, dword ptr gs:[edi]
0804cff8  mov esi, 0x14df
0804cffd  xor edx, esi
0804cfff  inc byte ptr [ecx + edx]
0804d002  mov dword ptr gs:[edi], 0xa6f
0804d009  mov ecx, dword ptr [0x8050688]
0804d00f  lea ecx, dword ptr [ecx + ecx*2]
0804d012  lea ecx, dword ptr [ebx + ecx*8]
0804d015  cmp eax, ecx
0804d017  mov ecx, 0
0804d01c  cmovae eax, ecx
0804d01f  mov ecx, eax
0804d021  mov eax, dword ptr [0x8050628]
0804d026  mov edx, dword ptr gs:[edi]
0804d029  mov esi, 0x53b0
0804d02e  xor edx, esi
0804d030  inc byte ptr [eax + edx]
0804d033  mov dword ptr gs:[edi], 0x29d0
0804d03a  movzx edx, byte ptr [0x805060e]
0804d041  shl edx, 0x10
0804d044  movzx eax, word ptr [0x805066c]
0804d04b  or eax, edx
0804d04d  movzx edx, ah
0804d050  cmp edx, 4
0804d053  jne 0x804d174
0804d059  mov edx, dword p
0804d05f  mov esi, dword p
0804d062  mov ebp, 0x2dcf
0804d067  xor esi, ebp
0804d069  inc byte ptr [edx + esi]
0804d06c  mov dword ptr gs:[edi], 0x10e7
0804d073  test al, al
0804d075  je 0x804d37f
0804d07b  mov edx, dword ptr [0x8050628]
```

Expr
OK

id:000008,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...)OEO
```

Watch Points

A Better Tool...

RUHR UNIVERSITÄT BOCHUM RUB

IJON Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

Taken:
line 520

NotTaken:
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(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;
```

```
0804cfeb  cmp eax, ebx
0804cfed  jb 0x804d021
0804cfef  mov ecx, dword ptr [0x8050628]
0804cff5  mov edx, dword ptr gs:[edi]
0804cff8  mov esi, 0x14df
0804cffd  xor edx, esi
0804cfff  inc byte ptr [ecx + edx]
0804d002  mov dword ptr gs:[edi], 0xa6f
0804d009  mov ecx, dword ptr [0x8050688]
0804d00f  lea ecx, dword ptr [ecx + ecx*2]
0804d012  lea ecx, dword ptr [ebx + ecx*8]
0804d015  cmp eax, ecx
0804d017  mov ecx, 0
0804d01c  cmovae eax, ecx
0804d01f  mov ecx, eax
0804d021  mov eax, dword ptr [0x8050628]
0804d026  mov edx, dword ptr gs:[edi]
0804d029  mov esi, 0x53b0
0804d02e  xor edx, esi
0804d030  inc byte ptr [eax + edx]
0804d033  mov dword ptr gs:[edi], 0x29d0
0804d03a  movzx edx, byte ptr [0x805806e]
0804d041  shl edx, 0x10
0804d044  movzx eax, word ptr [0x805806c]
0804d04b  or eax, edx
0804d04d  movzx edx, ah
0804d050  cmp edx, 4
0804d053  jne 0x804d174
0804d059  mov edx, dword p
0804d05f  mov esi, dword p
0804d062  mov ebp, 0x2dcf
0804d067  xor esi, ebp
0804d069  inc byte ptr [edx + esi]
0804d06c  mov dword ptr gs:[edi], 0x10e7
0804d073  test al, al
0804d075  je 0x804d37f
0804d07b  mov edx, dword ptr [0x8050628]
```

Expr
edx
OK

id:000008,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...)OEO
```

Watch Points

A Better Tool...

RUHR UNIVERSITÄT BOCHUM RUB

IJON Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

/home/me/ijon_eval/cb-multios/challenges/Multipass/src/main.c 76/170

Taken:
0× line 520

NotTaken:
0× 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;
```

```
0804cfeb  cmp eax, ebx
0804cfed  jb 0x804d021
0804cfef  mov ecx, dword ptr [0x8050628]
0804cff5  mov edx, dword ptr gs:[edi]
0804cff8  mov esi, 0x14df
0804cffd  xor edx, esi
0804cfff  inc byte ptr [ecx + edx]
0804d002  mov dword ptr gs:[edi], 0xa6f
0804d009  mov ecx, dword ptr [0x8050688]
0804d00f  lea ecx, dword ptr [ecx + ecx*2]
0804d012  lea ecx, dword ptr [ebx + ecx*8]
0804d015  cmp eax, ecx
0804d017  mov ecx, 0
0804d01c  cmovae eax, ecx
0804d01f  mov ecx, eax
0804d021  mov eax, dword ptr [0x8050628]
0804d026  mov edx, dword ptr gs:[edi]
0804d029  mov esi, 0x53b0
0804d02e  xor edx, esi
0804d030  inc byte ptr [eax + edx]
0804d033  mov dword ptr gs:[edi], 0x29d0
0804d03a  movzx edx, byte ptr [0x805066a]
0804d041  shl edx, 0x10
0804d044  movzx eax, word ptr [0x805066c]
0804d04b  or eax, edx
0804d04d  movzx edx, ah
0804d050  cmp edx, 4
0804d053  jne 0x804d174
0804d059  mov edx, dword p
0804d05f  mov esi, dword p
0804d062  mov ebp, 0x2dcf
0804d067  xor esi, ebp
0804d069  inc byte ptr [edx + esi]
0804d06c  mov dword ptr gs:[edi], 0x10e7
0804d073  test al, al
0804d075  je 0x804d37f
0804d07b  mov edx, dword ptr [0x8050628]
```

Expr
edx
OK

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

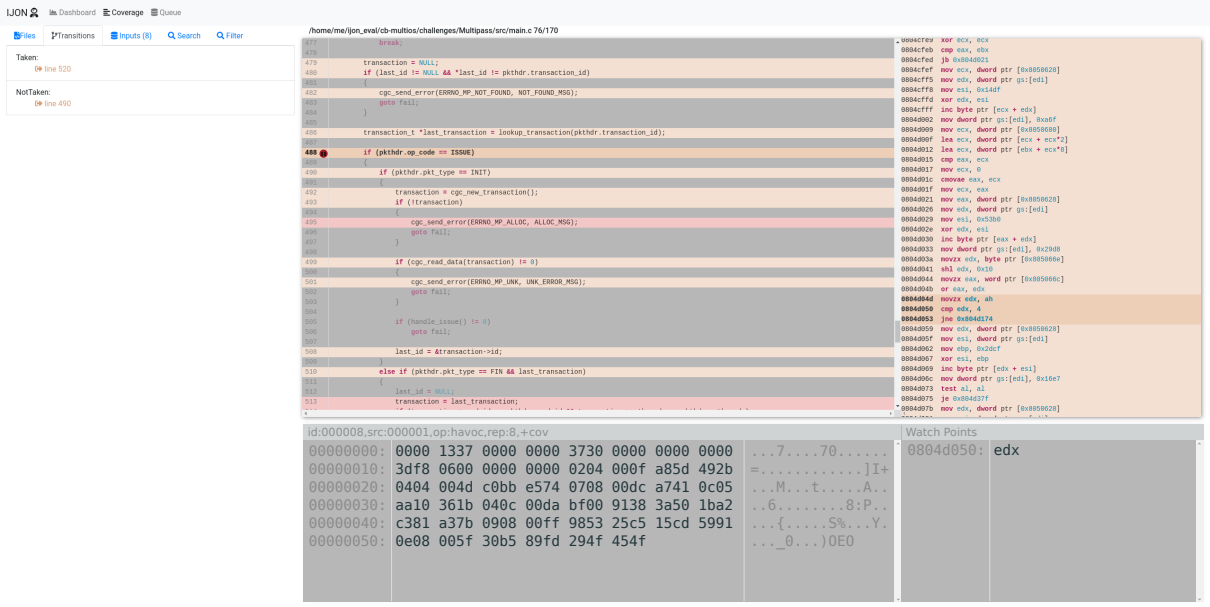
```
00000000: 0000 1337 0000 0000 3730 0000 0000 0000  ...7....70......
00000010: 3df8 0600 0000 0000 0204 000f a85d 492b  =............]I+
00000020: 0404 004d c0bb e574 0708 00dc a741 0c05  ...M...t.....A..
00000030: aa10 361b 040c 00da bf00 9138 3a50 1ba2  ..6........8:P..
00000040: c381 a37b 0908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

Watch Points

A Better Tool...

RUHR UNIVERSITÄT BOCHUM

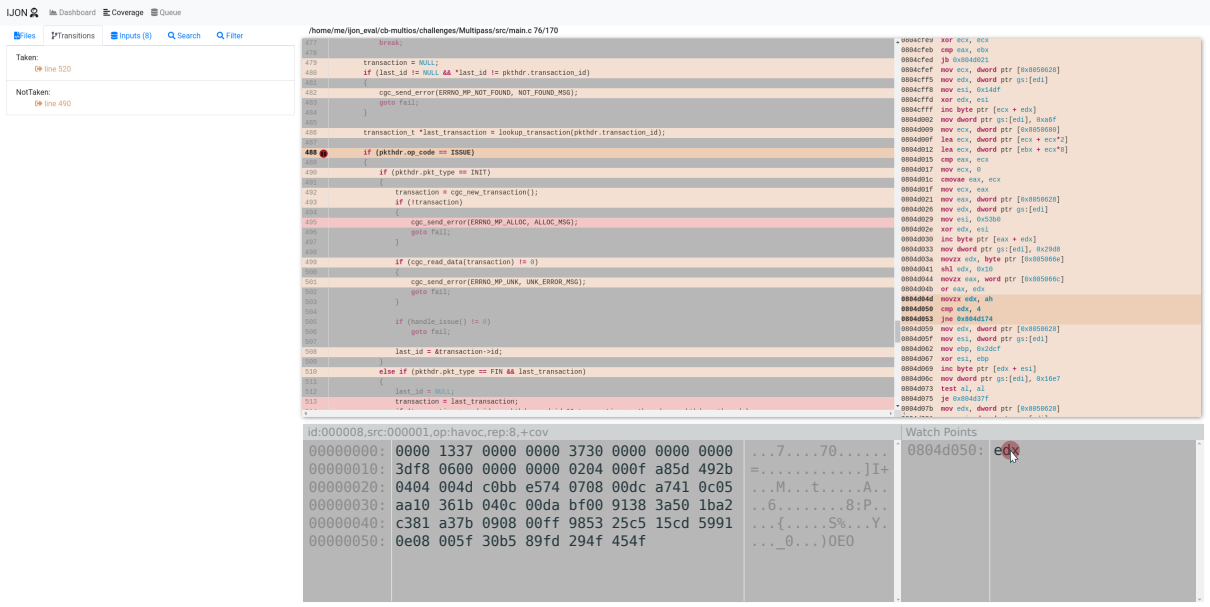
RUB



A Better Tool...

RUHR UNIVERSITÄT BOCHUM

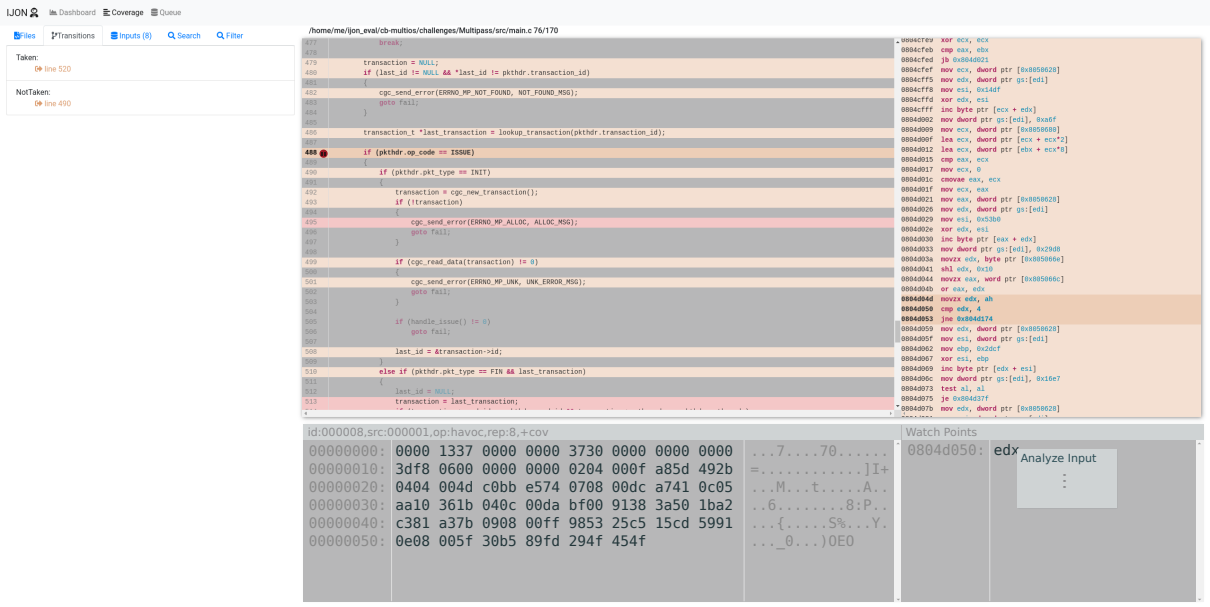
RUB



A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB



A Better Tool...

RUHR UNIVERSITÄT BOCHUM RUB

IJON Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

Taken:
- line 520

NotTaken:
- 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(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;
```

```
0804cfeb  xor ecx, ecx
0804cfed  cmp eax, ebx
0804cfef  jb 0x804d021
0804cfef  mov ecx, dword ptr [0x8050628]
0804cff5  mov edx, dword ptr gs:[edi]
0804cff8  mov esi, 0x14df
0804cffd  xor edx, esi
0804cfff  inc byte ptr [ecx + edx]
0804d002  mov dword ptr gs:[edi], 0xa6f
0804d009  mov ecx, dword ptr [0x8050688]
0804d00f  lea ecx, dword ptr [ecx + ecx*2]
0804d012  lea ecx, dword ptr [ebx + ecx*8]
0804d015  cmp eax, ecx
0804d017  mov ecx, 0
0804d01c  cmovae eax, ecx
0804d01f  mov ecx, eax
0804d021  mov eax, dword ptr [0x8050628]
0804d026  mov edx, dword ptr gs:[edi]
0804d029  mov esi, 0x53b0
0804d02e  xor edx, esi
0804d030  inc byte ptr [eax + edx]
0804d033  mov dword ptr gs:[edi], 0x29d0
0804d03a  movzx edx, byte ptr [0x805806e]
0804d041  shl edx, 0x10
0804d044  movzx eax, word ptr [0x805806c]
0804d04b  or eax, edx
0804d04d  movzx edx, ah
0804d050  cmp edx, 4
0804d053  jne 0x804d174
0804d059  mov edx, dword ptr [0x8050628]
0804d05f  mov esi, dword ptr gs:[edi]
0804d062  mov ebp, 0x2dcf
0804d067  xor esi, ebp
0804d069  inc byte ptr [edx + esi]
0804d06c  mov dword ptr gs:[edi], 0x10e7
0804d073  test ai, ai
0804d075  je 0x804d37f
0804d07b  mov edx, dword ptr [0x8050628]
```

id:000008,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...)OEO
```

Watch Points

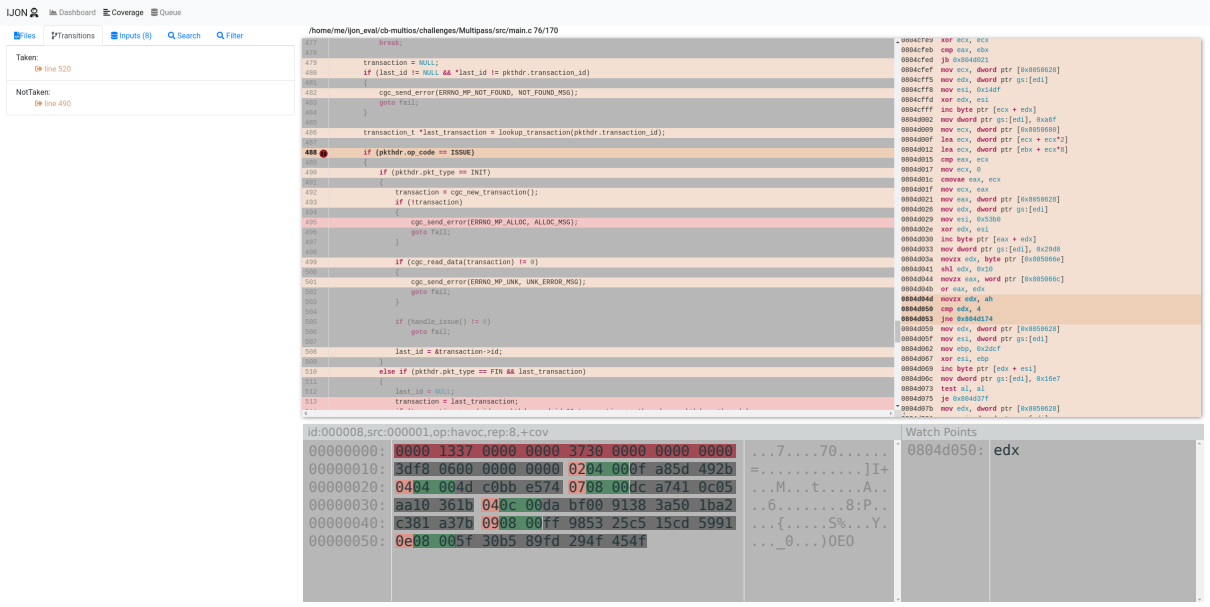
0804d050: edx

Analyze Input

A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB



A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB

A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB

A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB

A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB

IJON Dashboard Coverage Queue

Files Transitions Inputs (8) Search Filter

Taken:
0x line 520

NotTaken:
0x 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(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;
```

```
0804cfeb  cmp eax, ebx
0804cfed  jb 0x804d021
0804cfef  mov ecx, dword ptr [0x8050628]
0804cff5  mov edx, dword ptr gs:[edi]
0804cff8  mov esi, 0x14df
0804cffd  xor edx, esi
0804cfff  inc byte ptr [ecx + edx]
0804d002  mov dword ptr gs:[edi], 0xa6f
0804d009  mov ecx, dword ptr [0x8050688]
0804d00f  lea ecx, dword ptr [ecx + ecx*2]
0804d012  lea ecx, dword ptr [ebx + ecx*8]
0804d015  cmp eax, ecx
0804d017  mov ecx, 0
0804d01c  cmovae eax, ecx
0804d01f  mov ecx, eax
0804d021  mov eax, dword ptr [0x8050628]
0804d026  mov edx, dword ptr gs:[edi]
0804d029  mov esi, 0x53b0
0804d02e  xor edx, esi
0804d030  inc byte ptr [eax + edx]
0804d033  mov dword ptr gs:[edi], 0x29d0
0804d03a  movzx edx, byte ptr [0x805806e]
0804d041  shl edx, 0x10
0804d044  movzx eax, word ptr [0x805806c]
0804d04b  or eax, edx
0804d04d  movzx edx, ah
0804d050  cmp edx, 4
0804d053  jne 0x804d174
0804d059  mov edx, dword ptr [0x8050628]
0804d05f  mov esi, dword ptr gs:[edi]
0804d062  mov ebp, 0x2dcf
0804d067  xor esi, ebp
0804d069  inc byte ptr [edx + esi]
0804d06c  mov dword ptr gs:[edi], 0x10e7
0804d073  test ai, ai
0804d075  je 0x804d2f7
0804d07b  mov edx, dword ptr [0x8050628]
```

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

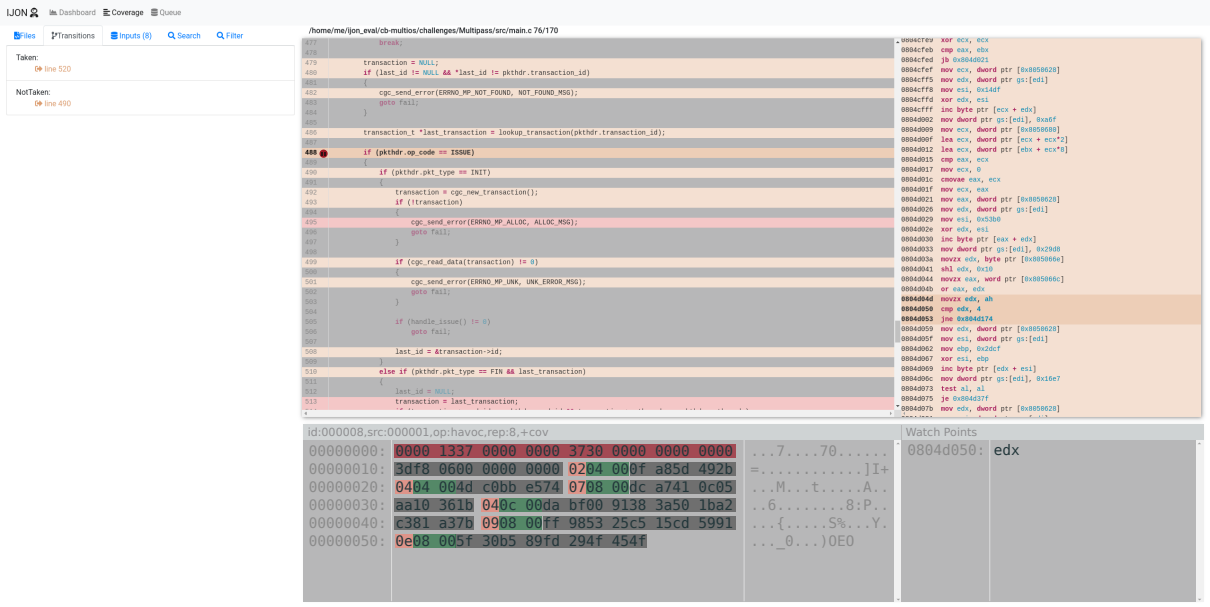
```
00000000: 0000 1337 0000 0000 ...
00000010: 3df8 0600 0000 00[illegible] 000f a[illegible]
00000020: 0404 004d c0bb [illegible] 0708 00dc a741 0c05  ...M...t.....A..
00000030: aa10 361b 040c [illegible] bf00 9138 3a50 1ba2  ..6.......8:P..
00000040: c381 a37b 0908 00ff 9853 25c5 15cd 5991  ...{.....S%...Y.
00000050: 0e08 005f 30b5 89fd 294f 454f            ..._0...)OEO
```

affects the number how often the BP was hit

A Better Tool...

RUHR UNIVERSITÄT BOCHUM

RUB



A Better Tool...

RUHR UNIVERSITÄT BOCHUM RUB

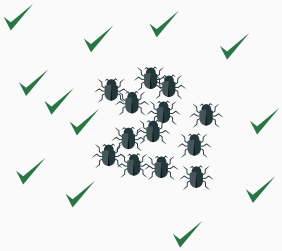
A Better Tool...

RUHR UNIVERSITÄT BOCHUM RUB

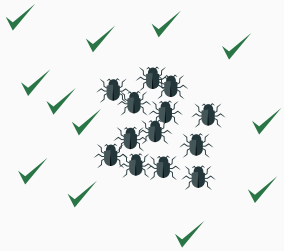
```
[lcamtuf@raccoon afl]$ ./afl-analyze -e -i testcases/images/png/not_kitty.png ~/readpng
afl-analyze 2.00b by <lcamtuf@google.com>

[+] 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)...

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

[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

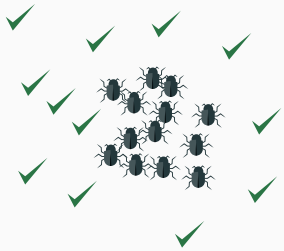


Root Cause Analysis



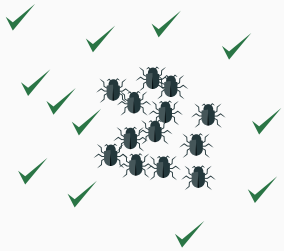
```
val.type != MRB_TT_EXCEPTION
```

Root Cause Analysis



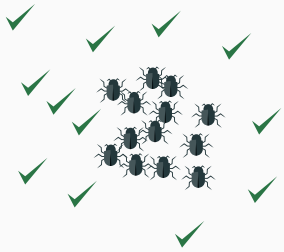
```
val.type != MRB_TT_EXCEPTION
val.type < 123
```

Root Cause Analysis

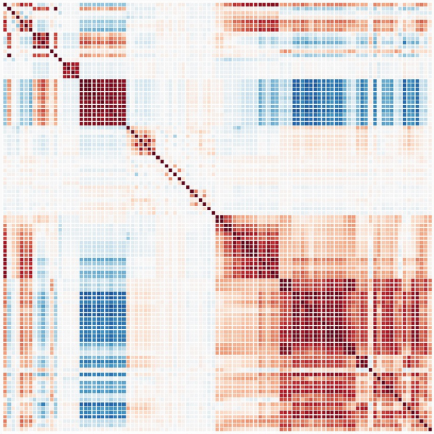


```
val.type != MRB_TT_EXCEPTION
val.type < 123
       ⋮
```

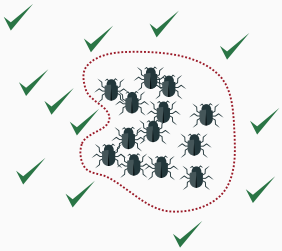
Root Cause Analysis

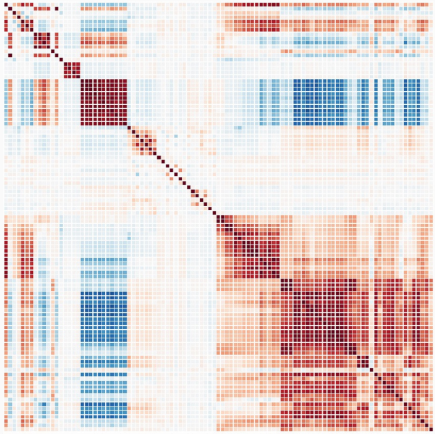


```
val.type != MRB_TT_EXCEPTION
val.type < 123
```



Root Cause Analysis





```
val.type != MRB_TT_EXCEPTION
val.type < 123
```

⋮

Heap Feng Shui

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

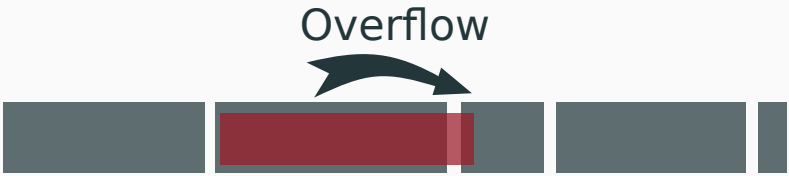
Heap Feng Shui

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

Heap Feng Shui

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

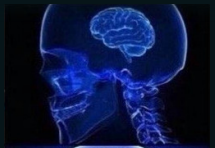
Heap Feng Shui



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

Key Takeaways:

printf

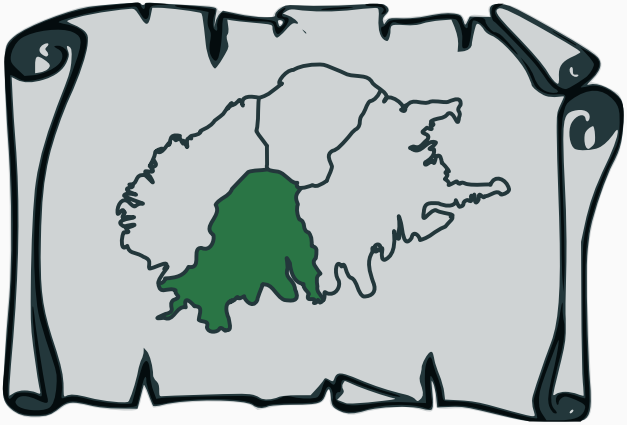


Debugger

Time Traveling Debugger

Fuzzer + Debugger

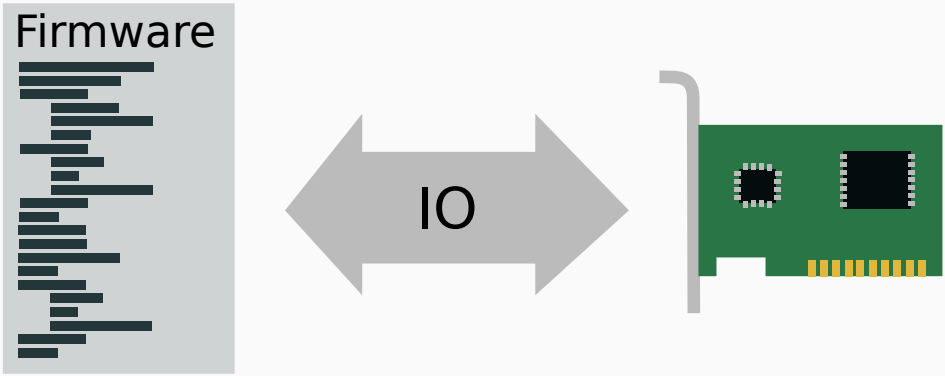
Unfuzzable Code



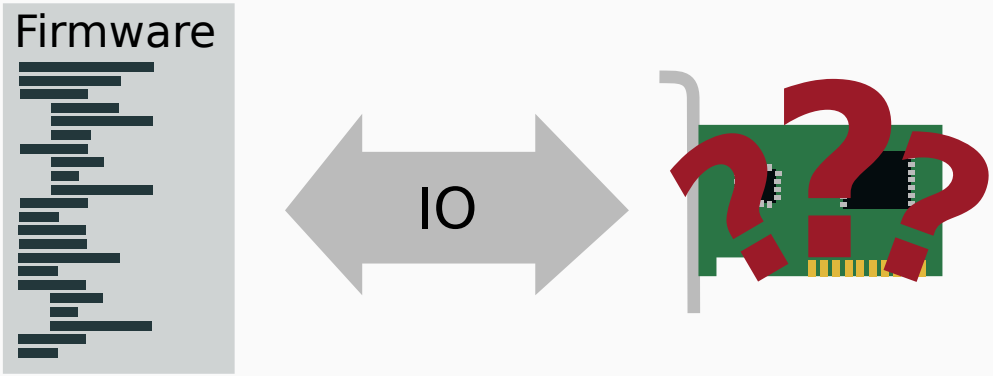
Code that doesn't run?

Code that doesn't run?

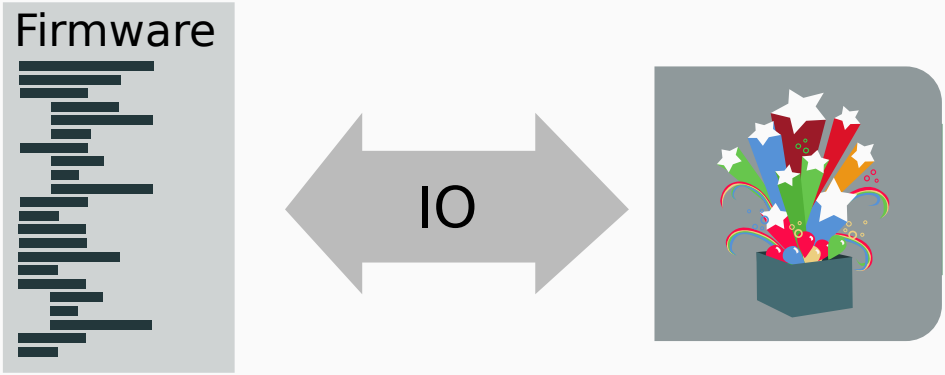
Code that doesn't run?



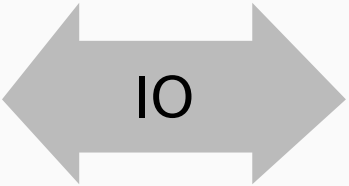
Code that doesn't run?



Code that doesn't run?



Code that doesn't run?

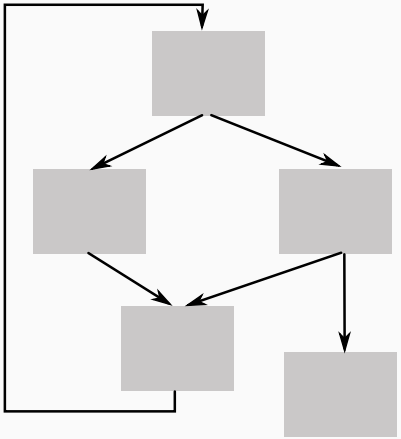


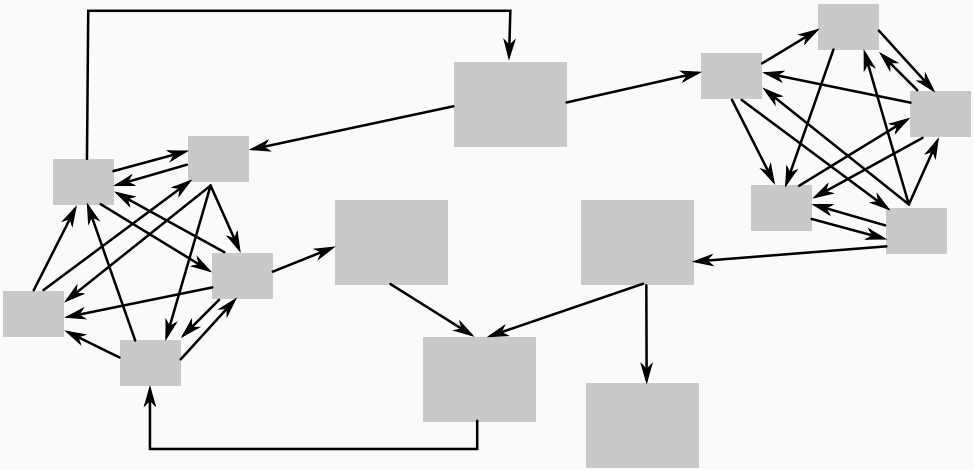
P^{2}IM [1]
HALucinator [2]

[1] https://arxiv.org/pdf/1909.06472.pdf
[2] https://nebelwelt.net/publications/files/20SEC2.pdf

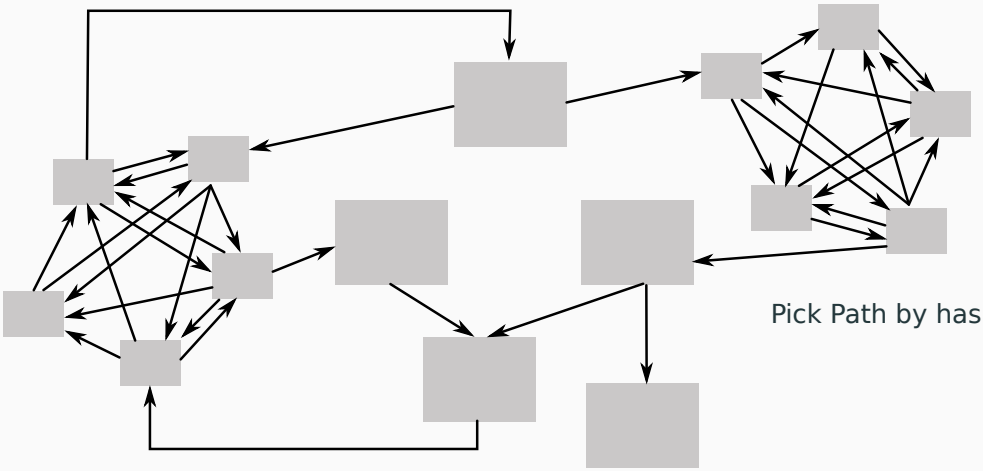
Key Takeaways:

AntiFuzz



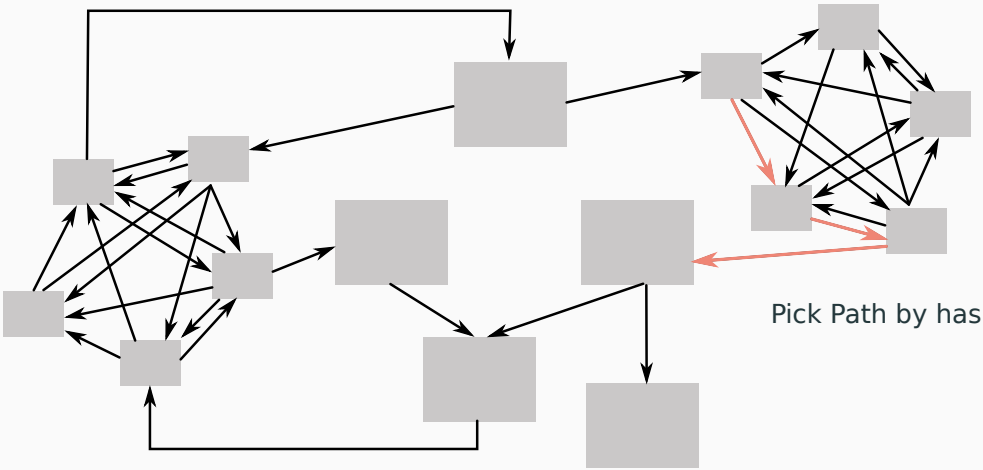


AntiFuzz



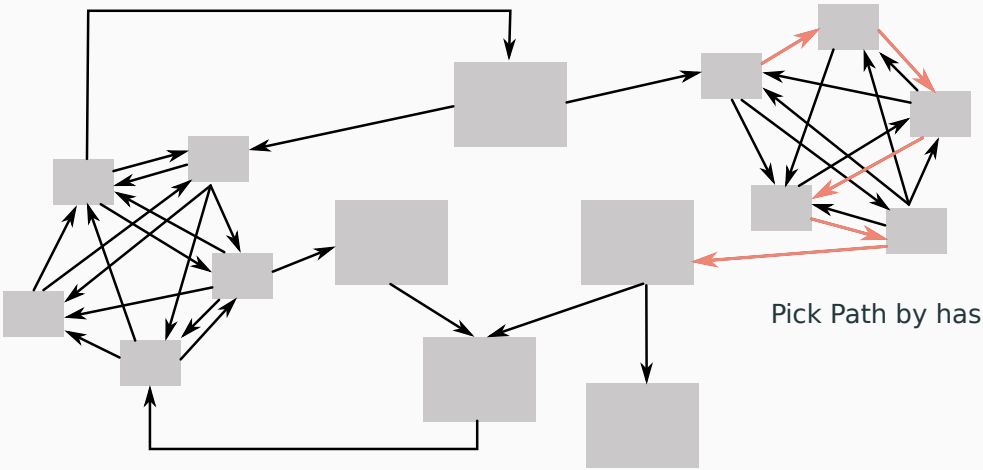
Pick Path by hash(input)

AntiFuzz



Pick Path by hash(input)

AntiFuzz



Pick Path by hash(input)


SLOW
DOWN!


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


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


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

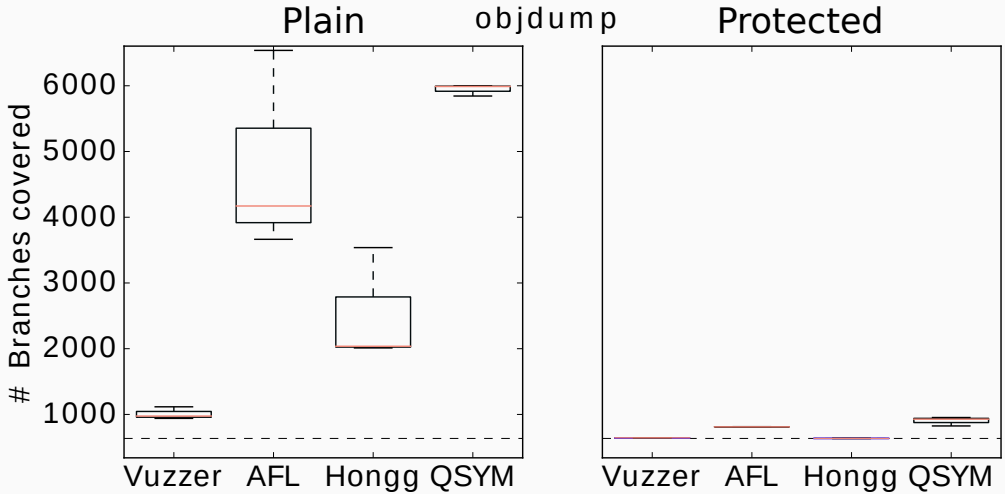
Signal Handler!

Symbolic Execution? Taint Tracking?

Symbolic Execution? Taint Tracking?

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

objdump


objdump
Plain
Protected
Branches covered
6000
5000
4000
3000
2000
1000
Vuzzer
AFL
Hongg
QSYM
Vuzzer
AFL
Hongg
QSYM

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"

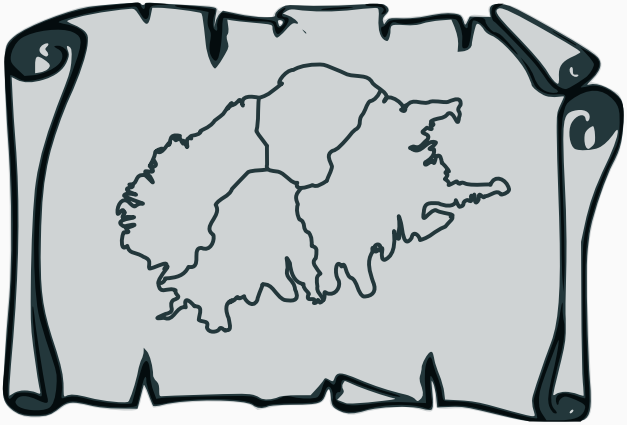
1 4

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


Let's Build Better Tools

github.com/RUB-SysSec/kAFL

github.com/RUB-SysSec/nautilus

github.com/RUB-SysSec/grimoire

github.com/RUB-SysSec/antifuzz

github.com/eqv/fuzz_ui

@is_eqv
github.com/eqv
cornelius.aschermann@rub.de

@ms_s3c
github.com/schumilo
sergej.schumilo@rub.de

Special Thanks to:
Ali Abbasi, Tim Blazytko, Robert Gawlik, Emre Güler, Thorsten Holz, Moritz Schlögel, Daniel Teuchert, Simone Wörner, and all the others that made this research possible.