Khalilov M.
Twitter: @3ntr0py1337
https://github.com/entropy1337

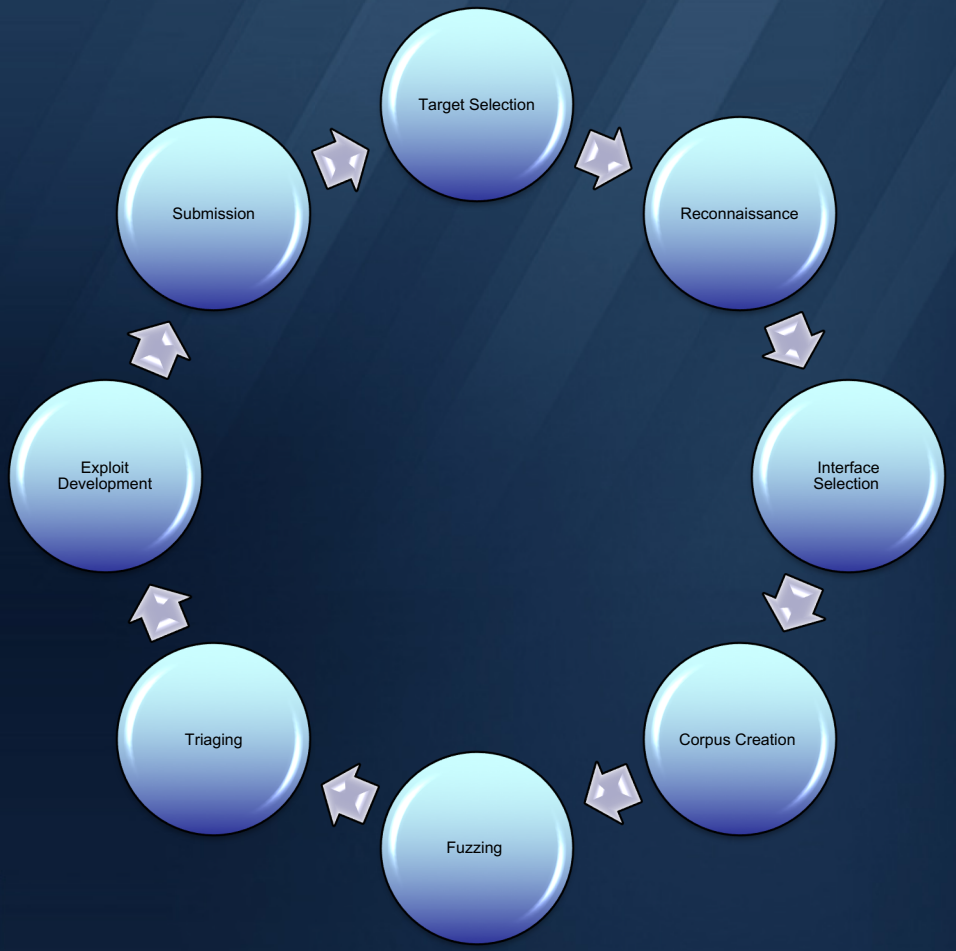
Vulnerability Research

Fuzzing and Triaging with AFL

Agenda

- Life Cycle of Vulnerability RnD
- Why Fuzzing
- Type of Fuzzing
- AFL – Fuzzing thick clients
- Demo

Life Cycle of RnD



Why Fuzzing

Pro:

- Very fast iteration
- can be smart and calculated
- Can be fully automated

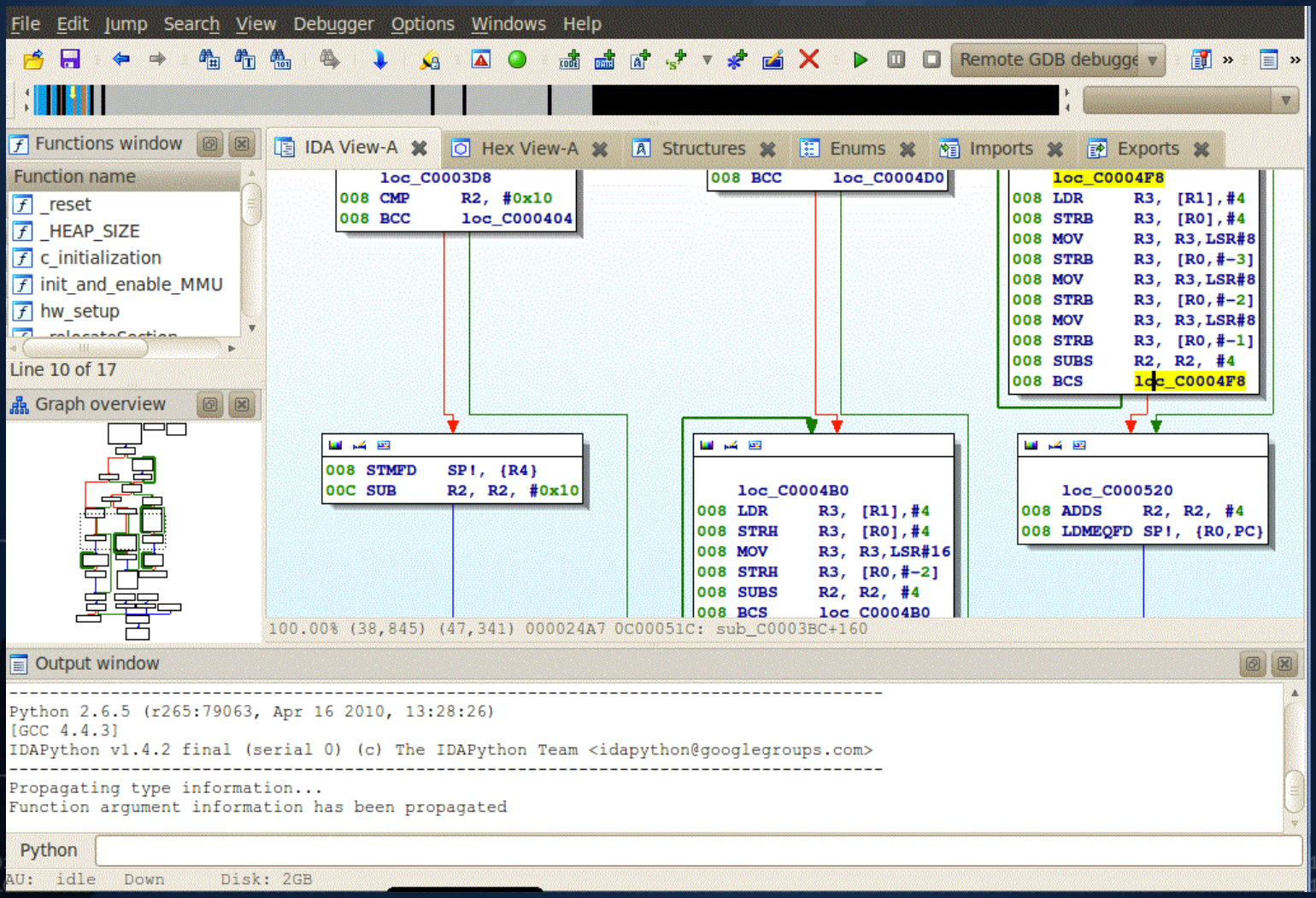
Cons:

- Can miss good bugs
- Can’t find logical bugs

Type of Fuzzing

- Mutation Based / generation based – existing tools to modify the available sample data or feed random content
- Dumb / Smart Fuzzing – Generate input with no structure or provide data which is expected by an application
- White / Grey / Black Box Fuzzing

Dump vs Smart Fuzzing



Dump vs Smart Fuzzing

```
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./faad...done.
(gdb) disassemble main
Dump of assembler code for function main:
   0x00000000004014c0 <+0>:     lea    -0x98(%rsp),%rsp
   0x00000000004014c8 <+8>:     mov    %rdx,(%rsp)
   0x00000000004014cc <+12>:    mov    %rcx,0x8(%rsp)
   0x00000000004014d1 <+17>:    mov    %rax,0x10(%rsp)
   0x00000000004014d6 <+22>:    mov    $0x6cc6,%rcx
   0x00000000004014dd <+29>:    callq  0x41d4e0 <__afl_maybe_log>
   0x00000000004014e2 <+34>:    mov    0x10(%rsp),%rax
   0x00000000004014e7 <+39>:    mov    0x8(%rsp),%rcx
   0x00000000004014ec <+44>:    mov    (%rsp),%rdx
   0x00000000004014f0 <+48>:    lea    0x98(%rsp),%rsp
   0x00000000004014f8 <+56>:    jmpq   0x4115e0 <faad_main>
End of assembler dump.
(gdb) disassemble faad_main
Dump of assembler code for function faad_main:
   0x00000000004115e0 <+0>:     lea    -0x98(%rsp),%rsp
   0x00000000004115e8 <+8>:     mov    %rdx,(%rsp)
   0x00000000004115ec <+12>:    mov    %rcx,0x8(%rsp)
   0x00000000004115f1 <+17>:    mov    %rax,0x10(%rsp)
   0x00000000004115f6 <+22>:    mov    $0xda9d,%rcx
   0x00000000004115fd <+29>:    callq  0x41d4e0 <__afl_maybe_log>
   0x0000000000411602 <+34>:    mov    0x10(%rsp),%rax
   0x0000000000411607 <+39>:    mov    0x8(%rsp),%rcx
   0x000000000041160c <+44>:    mov    (%rsp),%rdx
   0x0000000000411610 <+48>:    lea    0x98(%rsp),%rsp
   0x0000000000411618 <+56>:    push   %r15
   0x000000000041161a <+58>:    push   %r14
   0x000000000041161c <+60>:    xor    %r15d,%r15d
   0x000000000041161f <+63>:    push   %r13
   0x0000000000411621 <+65>:    push   %r12
   0x0000000000411623 <+67>:    mov    %rsi,%r12
   0x0000000000411626 <+70>:    push   %rbp
   0x0000000000411627 <+71>:    push   %rbx
   0x0000000000411628 <+72>:    mov    %edi,%ebx
   0x000000000041162a <+74>:    xor    %r14d,%r14d
   0x000000000041162d <+77>:    xor    %r13d,%r13d
   0x0000000000411630 <+80>:    sub    $0x2e8,%rsp
   0x0000000000411637 <+87>:    mov    %fs:0x28,%rax
   0x0000000000411640 <+96>:    mov    %rax,0x2d8(%rsp)
   0x0000000000411648 <+104>:   xor    %eax,%eax
   0x000000000041164a <+106>:   callq  0x424080 <NeAACDecGetCapabilities>
   0x000000000041164f <+111>:   mov    %rax,0x50(%rsp)
   0x0000000000411654 <+116>:   mov    (%r12),%rax
   0x0000000000411658 <+120>:   lea    0xa0(%rsp),%rbp
   0x0000000000411660 <+128>:   movl   $0x0,0x48(%rsp)
   0x0000000000411668 <+136>:   movl   $0x0,0x8(%rsp)
   0x0000000000411670 <+144>:   movl   $0x0,0x18(%rsp)
   0x0000000000411678 <+152>:   movl   $0x0,(%rsp)
   0x000000000041167f <+159>:   mov    %rax,0x31078a(%rip)        # 0x721e10 <progName>
   0x0000000000411686 <+166>:   movl   $0x0,0x40(%rsp)
   0x000000000041168e <+174>:   movl   $0x1,0x14(%rsp)
   0x0000000000411696 <+182>:   movl   $0x1,0x24(%rsp)
   0x000000000041169e <+190>:   movl   $0x0,0x78(%rsp)
   0x00000000004116a6 <+198>:   movl   $0x0,0x30(%rsp)
   0x00000000004116ae <+206>:   movl   $0x2,0x28(%rsp)
   0x00000000004116b6 <+214>:   movl   $0x0,0x20(%rsp)
   0x00000000004116be <+222>:   movl   $0x0,0x10(%rsp)
   0x00000000004116c6 <+230>:   nopw   %cs:0x0(%rax,%rax,1)
```

```
#include <stdio.h>
int main()
{
   char name[50];
   printf("Enter your name:");
   scanf("%s",&name);
   if(len(name)==0)
   {
            printf("Try again");
   }
   else
   {
            printf("Your name is %s", name);
   }
   return 0;
}
```

Demo – Finding targets

```
[entropy@vmi207130:~/victims/faad2-2.8.0~cvs20150510$ apt-cache search converter ]
bdf2psf - font converter to generate console fonts from BDF source fonts
libasound2-plugins - ALSA library additional plugins
libbabeltrace-ctf-dev - Common Trace Format (CTF) development files
libbabeltrace-ctf1 - Common Trace Format (CTF) library
libbabeltrace-dev - Babeltrace development files
libbabeltrace1 - Babeltrace conversion libraries
libsamplerate0 - Audio sample rate conversion library
libsamplerate0-dev - Development files for audio sample rate conversion
netpbm - Graphics conversion tools between image formats
poppler-utils - PDF utilities (based on Poppler)
qt4-dev-tools - Qt 4 development tools
texlive-extra-utils - TeX Live: TeX auxiliary programs
texlive-font-utils - TeX Live: Graphics and font utilities
texlive-pictures - TeX Live: Graphics, pictures, diagrams
a2ps - GNU a2ps - 'Anything to PostScript' converter and pretty-printer
abcmidi - converter from ABC to MIDI format and back
abw2epub - AbiWord to EPUB format converter
abw2odt - AbiWord to OpenDocument converter
addresses-goodies-for-gnustep - Personal Address Manager for GNUstep (Goodies)
aha - ANSI color to HTML converter
atp - text to PostScript converter with some C syntax highlighting
autotrace - bitmap to vector graphics converter
b5i2iso - BlindWrite image to ISO image file converter
babeltrace - Trace conversion program
bibtexconv - BibTeX Converter
bindechexascii - simple ASCII,binary,decimal and hex converter
biosig-tools - format conversion tools for biomedical data formats
blogofile-converters - blog converter collection for Blogofile
bnfc - Compiler front-end generator based on Labelled BNF
caja-image-converter - Caja extension to mass resize or rotate images
calibre - e-book converter and library management
calibre-bin - e-book converter and library management
caveconverter - Cave survey data format converter
ccd2iso - Converter from CloneCD disc image format to standard ISO
cdi2iso - DiscJuggler image to ISO image file converter
cdr2odg - Corel Draw graphics to to OpenDocument converter
cgiemail - CGI Form-to-Mail converter
cgoban - complete Go board
chordii - Text file (chordpro format) to music sheet converter
cl-babel - A charset encoding/decoding library, not unlike GNU libiconv
codegroup - Convert any file, including binary, into 5 letter code
comix - GTK Comic Book Viewer
converseen - batch image converter and resizer
convert-pgn - chess book format converter
convertall - very flexible unit converter
css2xslfo - XML+CSS2 to XSL-FO converter
csv2latex - command-line CSV to LaTeX file converter
darktable - virtual lighttable and darkroom for photographers
dbtoepub - DocBook XML to .epub converter
dctrl2xml - Debian control data to XML converter
dir2ogg - audio file converter into ogg-vorbis format
docbook-to-man - converter from DocBook SGML into roff man macros
dot2tex - Graphviz to LaTeX converter
dtdinst - XML DTD to XML instance format converter
dvi2ps - TeX DVI-driver for NTT JTeX, MulTeX and ASCII pTeX
ebook2epub - other E-Book formats to EPUB converter
ebook2odt - E-Book formats to OpenDocument converter
eep24c - read and write serial I2C eeprom devices
elyxer - standalone LyX to HTML converter
```

Instrumenting Target

```
[entropy@vmi207130:~/victims/faac-1.29.9.2$ ls
aclocal.m4  ChangeLog  compile       config.h.in  configure     COPYING  docs      include  install-sh  ltmain.sh    Makefile.in  NEWS    TODO
AUTHORS     common     config.guess  config.sub   configure.ac  depcomp  frontend  INSTALL  libfaac     Makefile.am  missing      README
entropy@vmi207130:~/victims/faac-1.29.9.2$ CC=afl-gcc CXX=afl-g++ ./configure --disable-shared
```

```
config.status: creating Makefile
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing libtool commands
[entropy@vmi207130:~/victims/faad2-2.8.8$ make
make  all-recursive
make[1]: Entering directory '/home/entropy/victims/faad2-2.8.8'
Making all in libfaad
make[2]: Entering directory '/home/entropy/victims/faad2-2.8.8/libfaad'
/bin/bash ../libtool  --tag=CC   --mode=compile afl-gcc -DHAVE_CONFIG_H -I. -I..  -iquote ../include  -fvisibility=hidden -g -O2 -MT libfaad_la-bits.lo -MD -MP -MF .deps/libfaad_la-bits.Tpo -c -o libfaad_
la-bits.lo `test -f 'bits.c' || echo './'`bits.c
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-bits.lo -MD -MP -MF .deps/libfaad_la-bits.Tpo -c bits.c  -fPIC -DPIC -o .libs/libfaad_la-bi
ts.o
afl-cc 2.52b by <lcamtuf@google.com>
afl-as 2.52b by <lcamtuf@google.com>
[+] Instrumented 161 locations (64-bit, non-hardened mode, ratio 100%).
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-bits.lo -MD -MP -MF .deps/libfaad_la-bits.Tpo -c bits.c -o libfaad_la-bits.o >/dev/null 2>&
1
mv -f .deps/libfaad_la-bits.Tpo .deps/libfaad_la-bits.Plo
/bin/bash ../libtool  --tag=CC   --mode=compile afl-gcc -DHAVE_CONFIG_H -I. -I..  -iquote ../include  -fvisibility=hidden -g -O2 -MT libfaad_la-cfft.lo -MD -MP -MF .deps/libfaad_la-cfft.Tpo -c -o libfaad_
la-cfft.lo `test -f 'cfft.c' || echo './'`cfft.c
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-cfft.lo -MD -MP -MF .deps/libfaad_la-cfft.Tpo -c cfft.c  -fPIC -DPIC -o .libs/libfaad_la-cf
ft.o
afl-cc 2.52b by <lcamtuf@google.com>
cfft.c:63:13: warning: inline function 'cfftf1' declared but never defined
 INLINE void cfftf1(uint16_t n, complex_t *c, complex_t *ch,
             ^
afl-as 2.52b by <lcamtuf@google.com>
[+] Instrumented 309 locations (64-bit, non-hardened mode, ratio 100%).
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-cfft.lo -MD -MP -MF .deps/libfaad_la-cfft.Tpo -c cfft.c -o libfaad_la-cfft.o >/dev/null 2>&
1
mv -f .deps/libfaad_la-cfft.Tpo .deps/libfaad_la-cfft.Plo
/bin/bash ../libtool  --tag=CC   --mode=compile afl-gcc -DHAVE_CONFIG_H -I. -I..  -iquote ../include  -fvisibility=hidden -g -O2 -MT libfaad_la-decoder.lo -MD -MP -MF .deps/libfaad_la-decoder.Tpo -c -o li
bfaad_la-decoder.lo `test -f 'decoder.c' || echo './'`decoder.c
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-decoder.lo -MD -MP -MF .deps/libfaad_la-decoder.Tpo -c decoder.c  -fPIC -DPIC -o .libs/libf
aad_la-decoder.o
afl-cc 2.52b by <lcamtuf@google.com>
afl-as 2.52b by <lcamtuf@google.com>
[+] Instrumented 460 locations (64-bit, non-hardened mode, ratio 100%).
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-decoder.lo -MD -MP -MF .deps/libfaad_la-decoder.Tpo -c decoder.c -o libfaad_la-decoder.o >/
dev/null 2>&1
mv -f .deps/libfaad_la-decoder.Tpo .deps/libfaad_la-decoder.Plo
/bin/bash ../libtool  --tag=CC   --mode=compile afl-gcc -DHAVE_CONFIG_H -I. -I..  -iquote ../include  -fvisibility=hidden -g -O2 -MT libfaad_la-drc.lo -MD -MP -MF .deps/libfaad_la-drc.Tpo -c -o libfaad_la
-drc.lo `test -f 'drc.c' || echo './'`drc.c
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-drc.lo -MD -MP -MF .deps/libfaad_la-drc.Tpo -c drc.c  -fPIC -DPIC -o .libs/libfaad_la-drc.o
afl-cc 2.52b by <lcamtuf@google.com>
afl-as 2.52b by <lcamtuf@google.com>
[+] Instrumented 29 locations (64-bit, non-hardened mode, ratio 100%).
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-drc.lo -MD -MP -MF .deps/libfaad_la-drc.Tpo -c drc.c -o libfaad_la-drc.o >/dev/null 2>&1
mv -f .deps/libfaad_la-drc.Tpo .deps/libfaad_la-drc.Plo
/bin/bash ../libtool  --tag=CC   --mode=compile afl-gcc -DHAVE_CONFIG_H -I. -I..  -iquote ../include  -fvisibility=hidden -g -O2 -MT libfaad_la-drm_dec.lo -MD -MP -MF .deps/libfaad_la-drm_dec.Tpo -c -o li
bfaad_la-drm_dec.lo `test -f 'drm_dec.c' || echo './'`drm_dec.c
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-drm_dec.lo -MD -MP -MF .deps/libfaad_la-drm_dec.Tpo -c drm_dec.c  -fPIC -DPIC -o .libs/libf
aad_la-drm_dec.o
afl-cc 2.52b by <lcamtuf@google.com>
afl-as 2.52b by <lcamtuf@google.com>
[!] WARNING: No instrumentation targets found.
libtool: compile:  afl-gcc -DHAVE_CONFIG_H -I. -I.. -iquote ../include -fvisibility=hidden -g -O2 -MT libfaad_la-drm_dec.lo -MD -MP -MF .deps/libfaad_la-drm_dec.Tpo -c drm_dec.c -o libfaad_la-drm_dec.o >/
dev/null 2>&1
mv -f .deps/libfaad_la-drm_dec.Tpo .deps/libfaad_la-drm_dec.Plo
/bin/bash ../libtool  --tag=CC   --mode=compile afl-gcc -DHAVE_CONFIG_H -I. -I..  -iquote ../include  -fvisibility=hidden -g -O2 -MT libfaad_la-error.lo -MD -MP -MF .deps/libfaad_la-error.Tpo -c -o libfaa
d_la-error.lo `test -f 'error.c' || echo './'`error.c
```

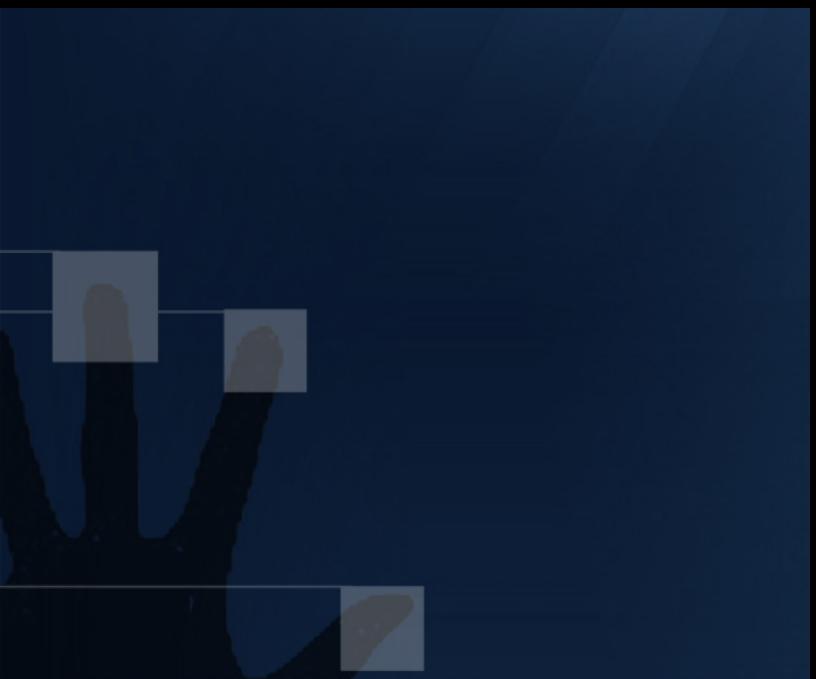
Corpus Minimization

```
[entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ afl-cmin -i input/ -o corpus-min/ ./faac -b 96 @@ -o sample.mp4
corpus minimization tool for afl-fuzz by <lcamtuf@google.com>

[*] Testing the target binary...
[+] OK, 2261 tuples recorded.
[*] Obtaining traces for input files in 'input/'...
    Processing file 1/1...
[*] Sorting trace sets (this may take a while)...
[+] Found 261 unique tuples across 1 files.
[*] Finding best candidates for each tuple...
    Processing file 1/1...
[*] Sorting candidate list (be patient)...
[*] Processing candidates and writing output files...
    Processing tuple 261/261...
[!] WARNING: All test cases had the same traces, check syntax!
[+] Narrowed down to 1 files, saved in 'corpus-min/'.

entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$
```

Interface Selection

```
[entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ ./faac -b 96 input/file_example_WAV_1MG.wav -o test.mpg
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Initial quantization quality: 75
Average bitrate: 48 kbps/channel
Bandwidth: 3437 Hz
PNS level: 4
Object type: Low Complexity(MPEG-2) + IS + PNS
Container format: Transport Stream (ADTS)
Encoding input/file_example_WAV_1MG.wav to test.mpg
   frame          | bitrate | elapsed/estim | play/CPU | ETA
  263/263   (100%)|    95.3 |     0.2/0.2   |  165.02x | 0.0
entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$
```

```
entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ afl-fuzz -i input/ -o output/ ./faac -b 96 @@ -o sampleout.mp4
```



american fuzzy lop 2.52b (faac)

process timing		overall results	
run time	0 days, 0 hrs, 7 min, 39 sec	cycles done	0
last new path	0 days, 0 hrs, 0 min, 56 sec	total paths	106
last uniq crash	0 days, 0 hrs, 2 min, 27 sec	uniq crashes	14
last uniq hang	0 days, 0 hrs, 5 min, 22 sec	uniq hangs	14
cycle progress		**map coverage**	
now processing	67 (63.21%)	map density	0.42% / 1.04%
paths timed out	0 (0.00%)	count coverage	1.42 bits/tuple
stage progress		**findings in depth**	
now trying	arith 32/8	favored paths	50 (47.17%)
stage execs	442/1645 (26.87%)	new edges on	66 (62.26%)
total execs	406k	total crashes	2361 (14 unique)
exec speed	1343/sec	total tmouts	10.9k (19 unique)
fuzzing strategy yields		**path geometry**	
bit flips	33/12.2k, 8/12.1k, 3/12.0k	levels	3
byte flips	0/1520, 1/1480, 0/1400	pending	67
arithmetics	5/84.8k, 4/42.1k, 0/17.5k	pend fav	13
known ints	4/7033, 13/31.8k, 5/54.8k	own finds	105
dictionary	0/0, 0/0, 0/5399	imported	n/a
havoc	43/120k, 0/0	stability	100.00%
trim	99.18%/430, 0.00%		

[cpu000: 47%]

Crash Identification

```
entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ ls output/crashes/
id:000000,sig:08,src:000000,op:flip1,pos:22          id:000005,sig:08,src:000000,op:havoc,rep:4          id:000010,sig:08,src:000030,op:int16,pos:24,val:+0
id:000001,sig:08,src:000000,op:int16,pos:24,val:+0   id:000006,sig:08,src:000009,op:flip1,pos:22         id:000011,sig:08,src:000031,op:int16,pos:24,val:+0
id:000002,sig:08,src:000000,op:int32,pos:22,val:+16  id:000007,sig:08,src:000012,op:int16,pos:24,val:+0  id:000012,sig:08,src:000033,op:int16,pos:24,val:+0
id:000003,sig:08,src:000000,op:int32,pos:22,val:+32  id:000008,sig:08,src:000014,op:int16,pos:24,val:+0  id:000013,sig:08,src:000037,op:int16,pos:24,val:+0
id:000004,sig:08,src:000000,op:havoc,rep:2           id:000009,sig:08,src:000015,op:int16,pos:24,val:+0  README.txt
entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ ./faac -b 96 output/crashes/id\:000012\,sig\:08\,src\:000033\,op\:int16\,pos\:24\,val\:+0 -o sampleout.mp4
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Remapping input channels: Center=3, LFE=4
Floating point exception
entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$
```

```
README.txt: No such file or directory
Couldn't open input file README.txt
entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ for i in $(ls output/crashes/); do ./faac -b 96 output/crashes/$i -o sampleout.mp4; done
entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ for i in $(ls output/crashes/); do ./faac -b 96 output/crashes/$i -o sampleout.mp4; done
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Remapping input channels: Center=3, LFE=4
Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Remapping input channels: Center=3, LFE=4
Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Remapping input channels: Center=3, LFE=4
Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Remapping input channels: Center=3, LFE=4
Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Remapping input channels: Center=3, LFE=4
Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Floating point exception
Freeware Advanced Audio Coder
FAAC 1.29.9.2

Remapping input channels: Center=3, LFE=4
Floating point exception
```

Triaging

```
  -f --functions         Show function names
  -C --demangle[=style]  Demangle function names
  -h --help              Display this information
  -v --version           Display the program's version

addr2line: supported targets: elf64-x86-64 elf32-i386 elf32-iamcu elf32-x86-64 a.out-i386-linux pei-i386 pei-x86-64 elf64-l1om elf64-k1om elf64-little elf64-big elf32-little elf32-big pe-x86-64 pe-bigobj-
x86-64 pe-i386 plugin srec symbolsrec verilog tekhex binary ihex
Report bugs to <http://www.sourceware.org/bugzilla/>
[entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ gdb faac                                                                                                                                          ]
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 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-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"...
Reading symbols from faac...done.
[(gdb) run -b 96 output/crashes/                                                                                                                                                                       ]
README.txt                              id:000004,sig:08,src:000000,op:havoc,rep:2          id:000009,sig:08,src:000015,op:int16,pos:24,val:+0
id:000000,sig:08,src:000000,op:flip1,pos:22         id:000005,sig:08,src:000000,op:havoc,rep:4          id:000010,sig:08,src:000030,op:int16,pos:24,val:+0
id:000001,sig:08,src:000000,op:int16,pos:24,val:+0  id:000006,sig:08,src:000009,op:flip1,pos:22         id:000011,sig:08,src:000031,op:int16,pos:24,val:+0
id:000002,sig:08,src:000000,op:int32,pos:22,val:+16 id:000007,sig:08,src:000012,op:int16,pos:24,val:+0  id:000012,sig:08,src:000033,op:int16,pos:24,val:+0
id:000003,sig:08,src:000000,op:int32,pos:22,val:+32 id:000008,sig:08,src:000014,op:int16,pos:24,val:+0  id:000013,sig:08,src:000037,op:int16,pos:24,val:+0
[(gdb) run -b 96 output/crashes/id:000004,sig:08,src:000000,op:havoc,rep:2                                                                                                                             ]
Starting program: /home/entropy/victims/faac-1.29.9.2/frontend/faac -b 96 output/crashes/id:000004,sig:08,src:000000,op:havoc,rep:2
Freeware Advanced Audio Coder
FAAC 1.29.9.2


Program received signal SIGFPE, Arithmetic exception.
wav_open_read (name=name@entry=0x7fffffffe7b7 "output/crashes/id:000004,sig:08,src:000000,op:havoc,rep:2", rawinput=rawinput@entry=0) at input.c:257
257         sndf->samples = riffsub.len / (sndf->samplebytes * sndf->channels);
[(gdb) disassemble 0x7fffffffe7b7                                                                                                                                                                      ]
No function contains specified address.
[(gdb) q                                                                                                                                                                                               ]
A debugging session is active.

        Inferior 1 [process 3941] will be killed.

[Quit anyway? (y or n) y                                                                                                                                                                               ]
[entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ addr2line -a 0x7fffffffe7b7 -e ./faac -b 96 output/crashes/id\:000001\,sig\:08\,src\:000000\,op\:int16\,pos\:24\,val\:+0                          ]
addr2line: ./faac: Invalid bfd target
[entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ addr2line 7fffffffe7b7 -e ./faac -b 96 output/crashes/id\:000001\,sig\:08\,src\:000000\,op\:int16\,pos\:24\,val\:+0                            ]
addr2line: ./faac: Invalid bfd target
[entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ addr2line -a 0x7fffffffe7b7 -e ./faac output/crashes/id\:000001\,sig\:08\,src\:000000\,op\:int16\,pos\:24\,val\:+0                              ]
0x00007fffffffe7b7
??:0
0x0000000000000000
??:0
[entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ addr2line -a 0x7fffffffe7b7 -e ./faac                                                                                                             ]
0x00007fffffffe7b7
??:0
[entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$ addr2line -a 0x7fffffffe7b7 -e ./faac -b elf64-x86-64                                                                                             ]
0x00007fffffffe7b7
??:0
entropy@vmi207130:~/victims/faac-1.29.9.2/frontend$
```

References

- https://github.com/ThalesIgnite/afl-training
- http://lcamtuf.coredump.cx/afl/
- https://fuzzing-project.org/tutorial3.html

Zero Day Research - More

- Windows Thick Clients
- CLI / GUI based application
- Thin Clients
- Libraries
- Interpreted Programming Languages
- Web Browsers
- Kernel IOCTL