Fuzzing Kamailio

Security testing the Kamailio SIP server with fuzzing

Agenda

- About me
- Motivation
- Introduction of fuzzing and afl fuzzer
- Necessary changes to the core and configuration
- Testing setup
- Example SIP messages and results
- Summary and further work

About me

- Henning Westerholt
- With Kamailio project since 2007
- Core developer of the Kamailio project
  - Core, database work and different other modules
  - Administration, code quality, quality assurance
- Senior IT Manager with a broad experience in product IT and internal IT
- Works on different side projects
  - some are payed
  - some are to “give back” to the community

Motivation

- Generally interested in security topics
- Wanted to learn about fuzzing with different tools
- Heard in the past that fuzzing can yield to great results with structured protocols, where brute-force testing is not feasible

Fuzzing

- “Fuzzing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks.”
- “Typically, fuzzers are used to test programs that take structured inputs. This structure is specified, e.g. in a […] protocol and distinguishes valid from invalid input. An effective fuzzer generates semi-valid inputs that are "valid enough" in that they are not directly rejected by the parser, but do create unexpected behaviors deeper in the program and are "invalid enough" to expose corner cases that have not been properly dealt with.

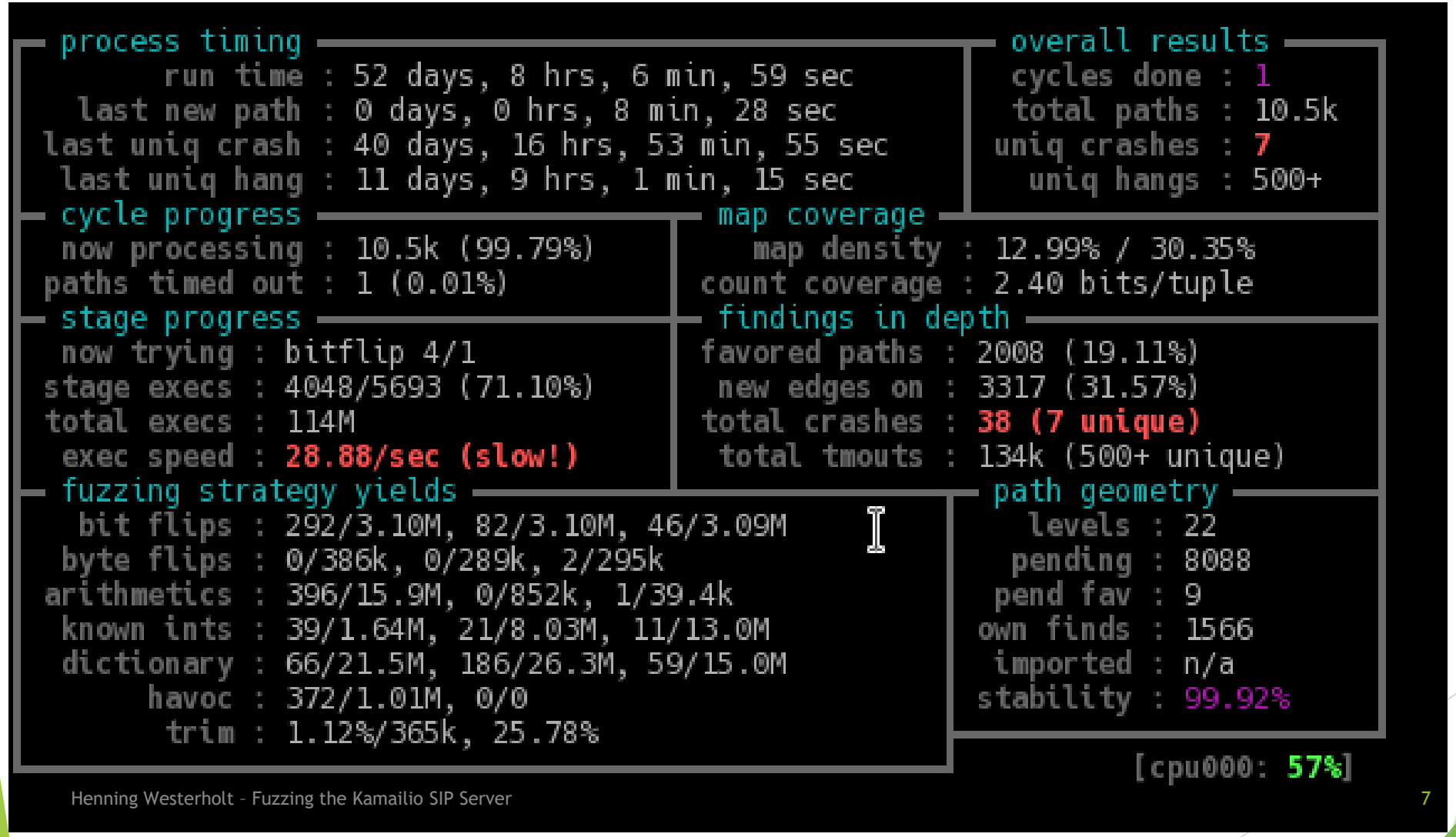
- From https://en.wikipedia.org/wiki/Fuzzing

About afl - „american fuzzy lop“

- „afl employs a novel type of compile-time instrumentation and genetic algorithms to automatically discover clean, interesting test cases that trigger new internal states in the targeted binary. This substantially improves the functional coverage for the fuzzed code.”
- So afl “learn” about the program and tries to exploit it “intelligently” – an example follows later
- Impressive number of bugs found in many core infrastructure code
- White box testing approach, comparing to yesterday black box testing talk

- Used version 2.52b from http://lcamtuf.coredump.cx/afl/

Sample output from afl



Necessary changes to the core

- Changes not trivial, but also not excessive complex work
  - Not contributed so far, not suitable right now for a commit
- Process message from file system and not from network
  - Investigated networking approach, but not chosen
  - Connect to stdin socket instead of network socket
  - Hack: use a „magic delimiter“ to signal end of message
- Efficiency improvements
  - Remove any unnecessary forking during start-up
  - Don‘t start RPC, TIMER, TCP master and other processes
  - Other small optimization on the host machine, explained later

Changes to default configuration

- Target compiler for instrumentation: CC="afl-gcc“; CXX="afl-g++“; make;
- Goal to use a stock default configuration without big changes
- Still some changes done:
  - No accounting, no NAT handling
  - Only one process, restrict memory usage
  - No forking mode
- Actual command to run afl:

```
./afl-fuzz -m 200 -t 5000+ -x ../dict_dir/sip.dict -i- -o
../findings_dir/ -- ../../../kamailio/src/kamailio -f
../cfg_dir/kamailio-basic.cfg -L ../../../kamailio/src/modules -Y
../tmp_dir -T -S -n 1 -D -m 16 -M 4
```

Testing setup

- Private (old) workstation
- Kamailio master branch from November, compiled with afl and gcc
- Estimated run-time of four month
- No fancy parallelisation or similar things
- Kernel parameter for run:

```
echo "core" >/proc/sys/kernel/core_pattern
echo "2000" >  /proc/sys/vm/dirty_writeback_centisecs
cd /sys/devices/system/cpu
echo "performance" | tee cpu*/cpufreq/scaling_governor
```

Test corpus

- Four SIP messages
  - One INVITE with invalid content length
  - One INVITE that should result in a „404 not found“
  - One INVITE that should result in a „100 trying“
  - One REGISTER with a new contact
- A SIP dictionary with about 50 entries
  - SIP method names
  - „magic“ strings like z9hG4bKydcnjlpe or IP addresses
  - Other SIP keywords from RFC 3261
- Ok, enough theory – show me some SIP messages!

id_000003,orig_register

A valid SIP message from SIPp

```
REGISTER sip:192.168.1.1 SIP/2.0
Via: SIP/2.0/UDP 172.17.13.240:5061;rport;branch=z9hG4bKydcnjlpe
Max-Forwards: 70
To: <sip:user@127.0.0.1>
From: <sip:user@127.0.0.1>;tag=dyggg
Call-ID: ccgdnpeqtepegxu@172.17.13.240
CSeq: 479 REGISTER
Contact: <sip:user@172.17.13.240:5061>;expires=3600
Allow:
INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO
User-Agent: SIPp/Linux
Content-Length: 1
```

id_001441,src_000003,op_flip4,pos_14,+cov

```
REGISTER sip:1A2.168.1.1 SIP/2.0
Via: SIP/2.0/UDP 172.17.13.240:5061;rport;branch=z9hG4bKydcnjlpe
Max-Forwards: 70
To: <sip:user@127.0.0.1>
From: <sip:user@127.0.0.1>;tag=dyggg
Call-ID: ccgdnpeqtepegxu@172.17.13.240
CSeq: 479 REGISTER
Contact: <sip:user@172.17.13.240:5061>;expires=3600
Allow:
INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO
User-Agent: SIPp/Linux
Content-Length: 1
```

id_003535,src_001441,op_arith8,pos_22,val_+12

```
REGISTER sip:1A2.168.1:1 SIP/2.0
Via: SIP/2.0/UDP 172.17.13.240:5061;rport;branch=z9hG4bKydcnjlpe
Max-Forwards: 70
To: <sip:user@127.0.0.1>
From: <sip:user@127.0.0.1>;tag=dyggg
Call-ID: ccgdnpeqtepegxu@172.17.13.240
CSeq: 479 REGISTER
Contact: <sip:user@172.17.13.240:5061>;expires=3600
Allow:
INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO
User-Agent: SIPp/Linux
Content-Length: 1
```

id_004778,src_003535,op_flip1,pos_23,+cov

```
REGISTER sip:1A2.168.1:0 SIP/2.0
Via: SIP/2.0/UDP 172.17.13.240:5061;rport;branch=z9hG4bKydcnjlpe
Max-Forwards: 70
To: <sip:user@127.0.0.1>
From: <sip:user@127.0.0.1>;tag=dyggg
Call-ID: ccgdnpeqtepegxu@172.17.13.240
CSeq: 479 REGISTER
Contact: <sip:user@172.17.13.240:5061>;expires=3600
Allow:
INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO
User-Agent: SIPp/Linux
Content-Length: 1
```

id_005518,src_004778,op_ext_AO,pos_13,+cov

Found different cfg processing for localhost REGISTER!

```
REGISTER sip:127.0.0.1:0 SIP/2.0
Via: SIP/2.0/UDP 172.17.13.240:5061;rport;branch=z9hG4bKydcnjlpe
Max-Forwards: 70
To: <sip:user@127.0.0.1>
From: <sip:user@127.0.0.1>;tag=dyggg
Call-ID: ccgdnpeqtepegxu@172.17.13.240
CSeq: 479 REGISTER
Contact: <sip:user@172.17.13.240:5061>;expires=3600
Allow:
INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO
User-Agent: SIPp/Linux
Content-Length: 1
```

id_006317,src_005518,op_havoc,rep_8,+cov

Testing permutiations of the transaction cookie

```
REGISTER sip:127.0.0.1:0 SIP/2.0
Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcnjlpe
Max-Forwards: 70
To: <sip:user@127.0.0.1>
From: <sip:user127.0.0.1>;tag=dyggg
Call-ID: ccgdnpeqtepeg€u@172.17.13.240
CSeq: 479 REGISTER
Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO
User-Agent:???p/Linux
Content-Length: 1
```

id_010335,src_006317,op_havoc,rep_2,+cov

After a long time the havoc permutation find a new path

```
REGISTER
sip:127uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0
SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcîjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010398,src_010335,op_havoc,rep_4

```
REGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu127uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010441,src_010398,op_havoc,rep_4

Random permutations with the request URI

```
REGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;;;;;;;;;;;;;
;;;;;;;;;;Z;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010472,src_010441,op_ext_AO,pos_82,+cov

```
REGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172
.17.13.240:5061;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010485,src_010472,op_arith8,pos_110,val_+18,+cov

```
REGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172
.17.13.240:5061;M;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010506,src_010485,op_flip1,pos_111,+cov

```
REGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172.17.13.240:5061;M?
;;;;;;;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010529,src_010506,op_arith8,pos_87,val_+2

```
REGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172.17.13.240:5061;MA
;;;;;;;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010552,src_010529,op_arith8,pos_88,val_+9,+cov

```
REGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172.17.13.240:5061;MA
D;;;;;;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010570,src_010552,op_flip1,pos_0

```
ÒEGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172.17.13.240:5061;MA
D;;;;;;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010594,src_010570,op_arith8,pos_89,val_+9

```
ÒEGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172.17.13.240:5061;MA
DD;;;;;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010604,src_010594,op_arith8,pos_90,val_+23,+cov

We found that the parser recognise „maddr“!

```
ÒEGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172.17.13.240:5061;MA
DDR;;;;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010615,src_010604,op_flip1,pos_91,+cov

```
ÒEGISTER
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172.17.13.240:5061;MA
DDR?;;;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

id_010627,src_010615,op_ext_UO,pos_0

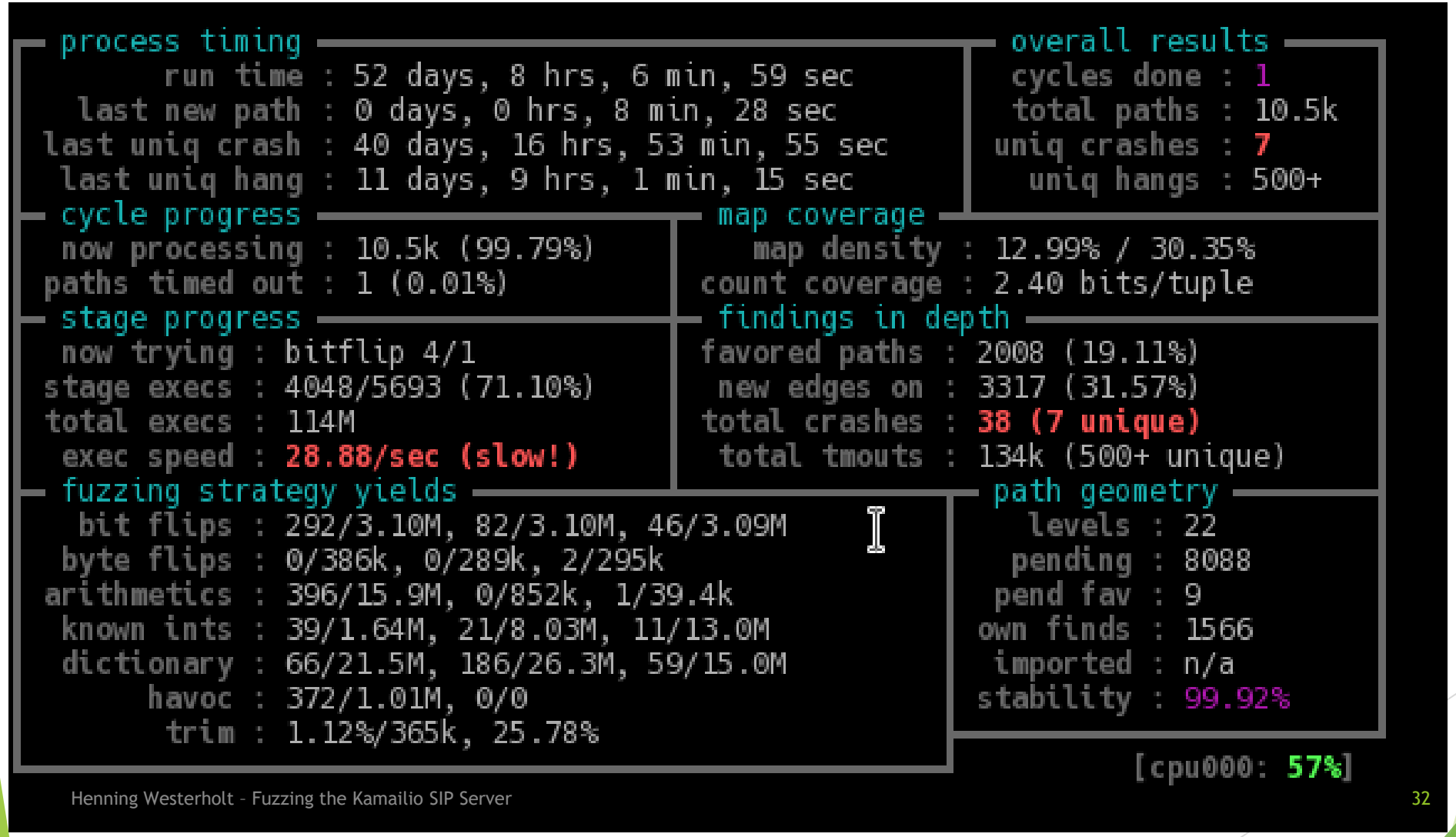
We found a new supported SIP message type by the cfg!

```
 OPTIONS
sip:uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu;sip:user@172.17.13.240:5061;MA
DDR?;;;;;;;;;;;;uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu=27uuuuuuuuuuuuuuuuuuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuuuuHuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu??èuuuuuuuuu
uuuuuuuuuuuuuuuuuuuuuuu.0.0.1:0 SIP/2.0

Via: SIP/2.0/UDP 172.17.13.240:5061;ÿport;branch=9hG4bKydcjlpe

Max-Forwards: 70

To: <sip:user@127.0.0.1>

From: <sip:user127.0.0.1>;tag=dyggg

Call-ID: ccgdnpeqtepeg€u@172.17.13.240

CSeq: 479 REGISTER

Contact: <sip:user@172.17.13.440:5061>,BYE,CANCEL,OPT
Accept:CK,REFER,NOTIFY,SUBSCRIBE,INFO

User-Agent:???p/Linux

Content-Length: 1
```

Results

- All found issues are nicely summarized from afl
- Big picture
  - Kamailio is really stable, over 310 million completed tests!
  - error rate smaller than 1 in 44 millions messages
  - 7 major crashes found (all one identical cause)
- Statistics
  - a complete test exhaustive cycle finished
  - „level 22“ finding depths reached
  - Over 10.700 code path tested
  - Over 500 individual hangs found – failure to respond with a proper error message

Output from afl - again



Crashes

- One crash found in the core message parser!
- Stable and immediate crash with just one UDP message
- Occurs with different modules (sanity, registrar..) and on different versions
- Disclosure:
  - No details published today
  - will be later be available after the next releases
- How to protect
  - Fix for this issue available in master branch and maintened stable branches
  - Will be included in the next minor releases as usual

Summary and further work

- Summary
  - Fuzzing with afl is effective, it can find really rare and critical bugs
  - Setup is nothing for a „script kiddie“, but doable for a motivated hacker
  - Further work in this area important to protect our all critical infrastructure

- Further (possible) work
  - Let afl run continuously on a dedicated machine (spare machines are available)
  - Import code and test suite into the Kamailio git repository
  - Extend afl setup to cover more modules or also RPC interfaces
  - Anybody interested in support (sponsor) this work, please contact me!

Thank you for your attention

- Contact:
  - Henning Westerholt
  - hw@kamailio.org
  - https://www.linkedin.com/in/henning-westerholt/
  - https://www.xing.com/profile/Henning_Westerholt