Politehnica University of Bucharest

Automatic Control and Computers Faculty

Computer Science Department

Fuzz-testing complex protocols

Scientific Student Projects Session - May 2013

Author(s)

Iustina Melinte
iustina_camelia.melinte@cti.pub.ro

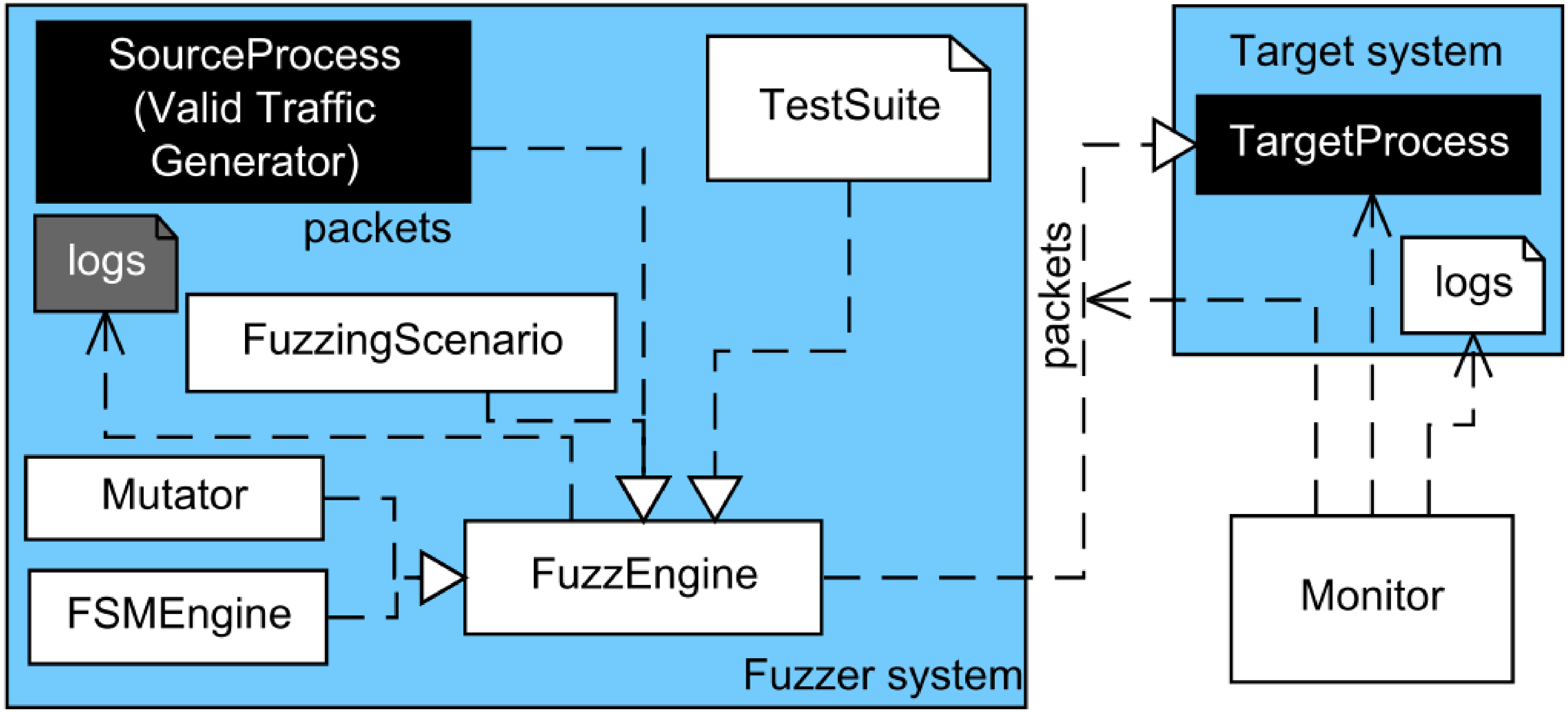
Scientific Advisor

Conf. Dr. Ing. Răzvan Rughiniș

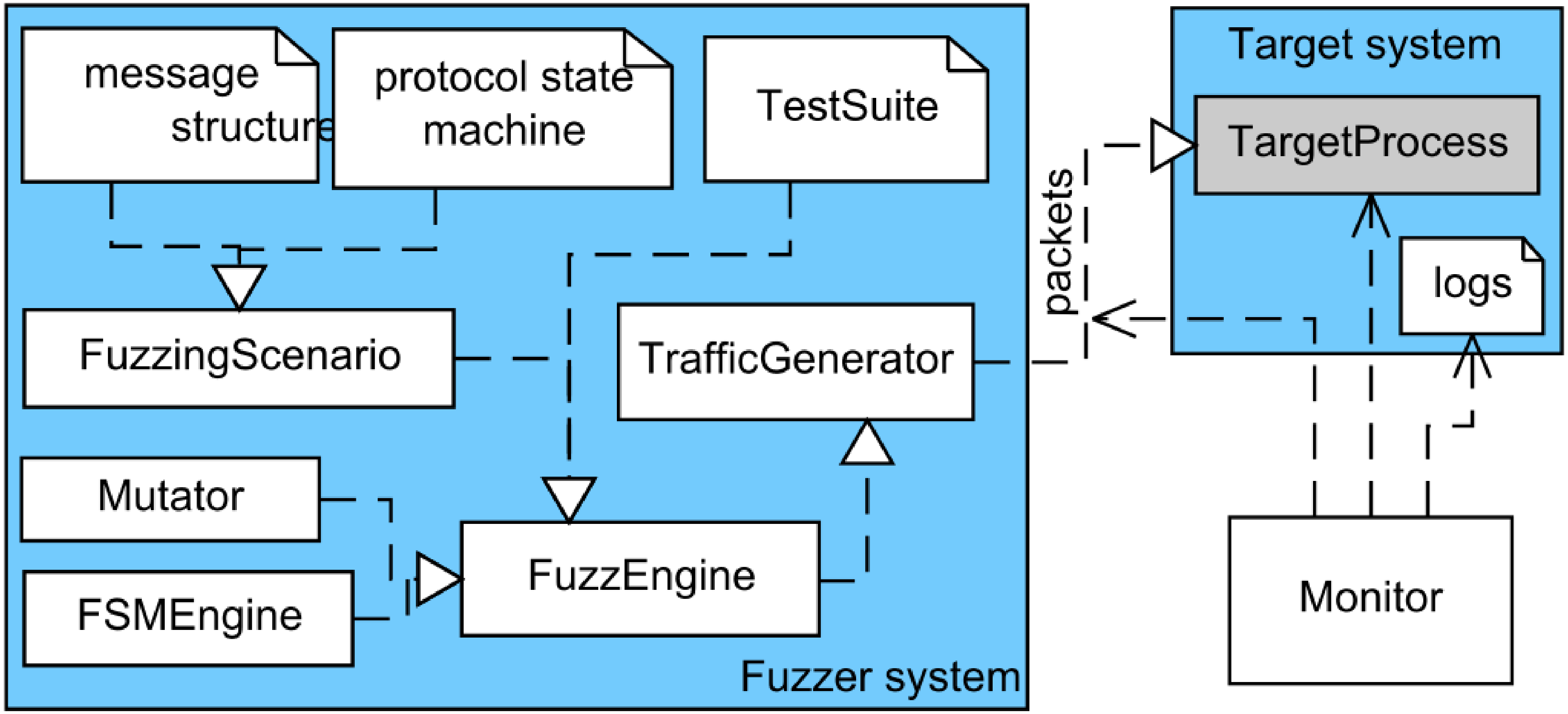
Contents

- Black-box fuzzing
- Grey-box fuzzing
- Protocol model description (IKE case study)
- Features of a good fuzzer
- Fuzzing algorithms and heuristics
- Where we are
- Future ideas

Black-box fuzzing



Grey-box fuzzing



Protocol model description (IKE case study)

Rfc 5996 complexity:

- 4 exchange types (variable structure, optional payloads)
- 16 payload types (variable structure,optional fields)
- more than 40 field types with hundreds of possible valu

.. lots of possible combinations

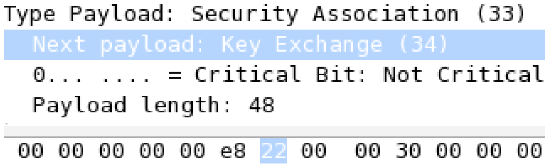
Protocol syntax specification

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                Figure 5:  Generic Payload Header
```

Valid packets

```
if s_block_start("gen_hdr_sa"):
    s_byte("ke",format="binary",name="gen_hdr_sa_np")
    s_bits(0b00000000,8,name="gen_hdr_sa_reserved")
    t_size(payl_name, length=2, endian=">", name="gen_hdr_sa_len")
    s_block_end("gen_hdr_sa")
```

Mutator,
FSMEngine



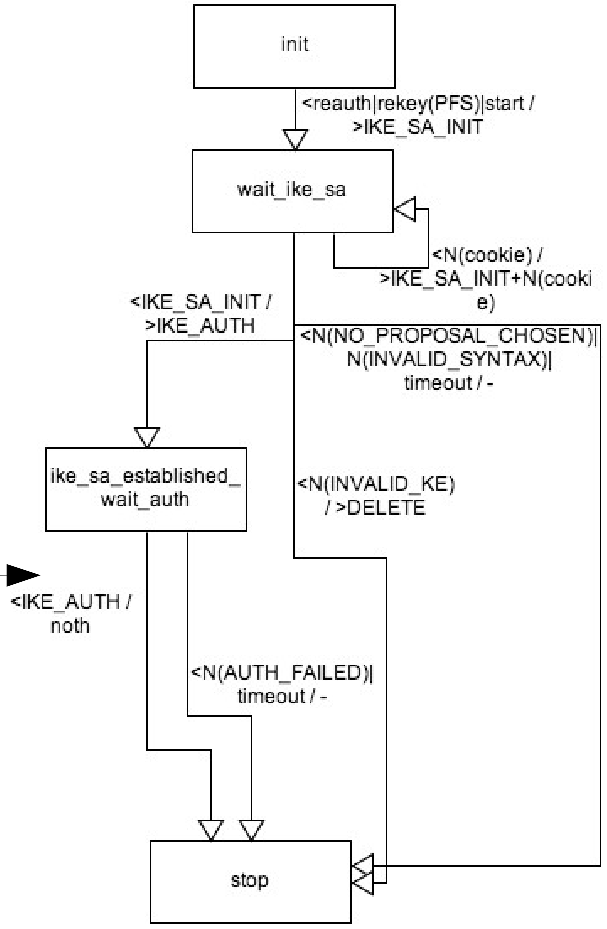
```
Type Payload: Security Association (33)
  Next payload: Key Exchange (34)
  0... .... = Critical Bit: Not Critical
  Payload length: 48

 00 00 00 00 00 e8 22 00  00 30 00 00 00
```

Evil packets

TARGET

Protocol state machine

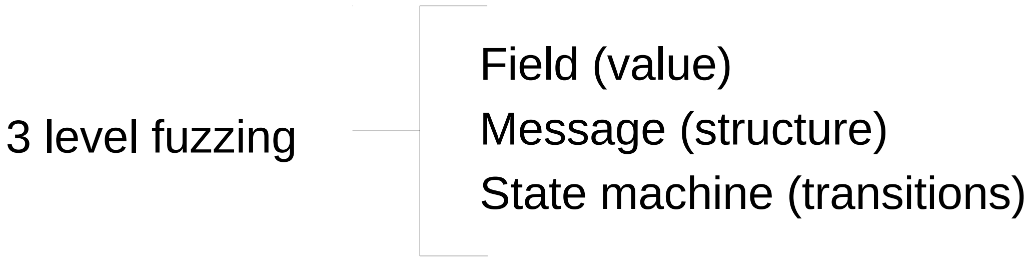


Features of a good fuzzer

Criteria:

- Modularity and portability
- Protocol model description
- Fuzzing algorithms and heuristics
- Target monitoring
- Results reporting
- Utilities and helpers

Fuzzing algorithms and heuristics



3 level fuzzing

Field (value)
Message (structure)
State machine (transitions)

Methods:

- boundary values (for integer type fields)
- format strings, directory traversal, SQL injection
- fuzz lists: specific values (eg. valid types taken from the rfc, but used inappropriately)
- repeat/delete/insert unexpected fields/payloads/messages
- scramble message payloads

The test suite

- .. a list: [(item,method,arguments,description),(..),..]

... where we are

- grey-box,model-driven fuzzing
- established a flexible architecture, based on our+others experience
  - u.. hacker friendly.
- support for complex network protocols
- only IKEv2, initiator role

Future ideas

- try other protocols, see patterns
- IKEv2
  - test the client side..client implementation
  - support for state machine fuzzing,
  - move on to other nodes in the state graph, ESP

.. last slide

... the reality

”...(bla bla bla)... deriving the shared secret from a password is not secure. ..(bla bla bla)... it is anticipated that people will do it anyway.” - rfc 5996 (IKEv2)

>:)

?

Questions