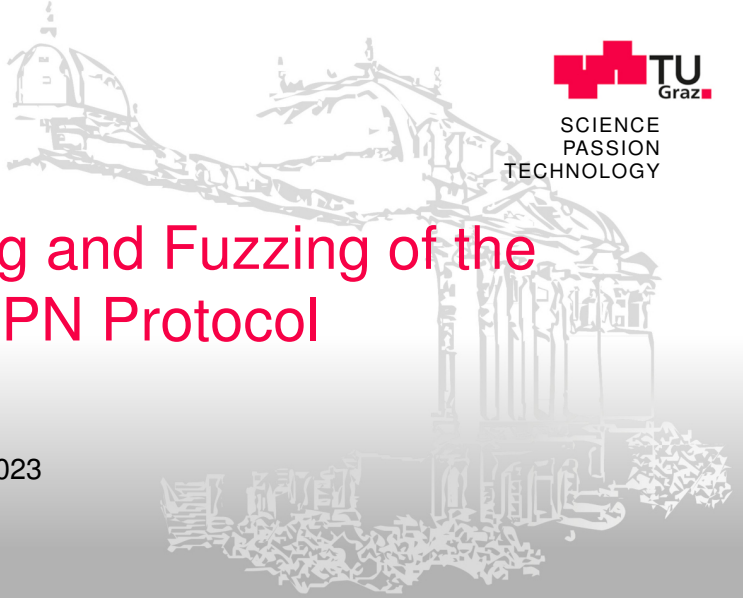


SCIENCE
PASSION
TECHNOLOGY

Model Learning and Fuzzing of the IPsec-IKEv1 VPN Protocol

Benjamin Wunderling

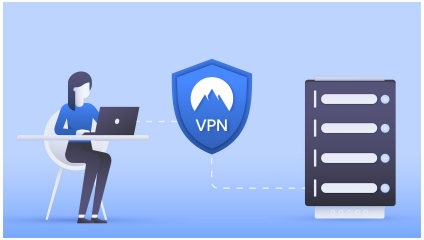
Master's Examination 19.10.2023

› benjamin.wunderling@student.tugraz.at

Outline

Motivation

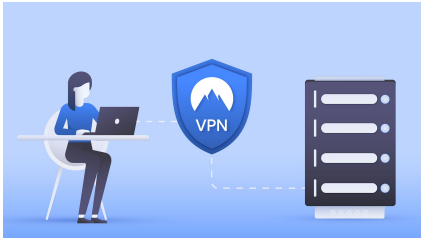
- Increased VPN usage
- IPsec IKEv1 vs IKEv2 (FRITZ!Box)
- Security testing
- Behavioral models
- Black-box systems



https://pixabay.com/photos/personal-data-personal-security-4667362

Motivation

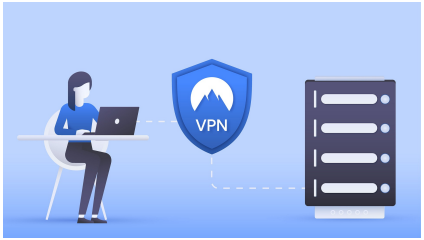
- Increased VPN usage
- IPsec IKEv1 vs IKEv2 (FRITZ!Box)
- Security testing
- Behavioral models
- Black-box systems



https://pixabay.com/photos/personal-data-personal-security-4667362

Motivation

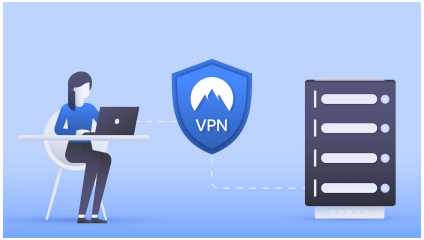
- Increased VPN usage
- IPsec IKEv1 vs IKEv2 (FRITZ!Box)
- Security testing
- Behavioral models
- Black-box systems



https://pixabay.com/photos/personal-data-personal-security-4667362

Motivation

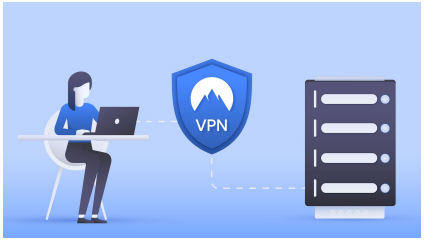
- Increased VPN usage
- IPsec IKEv1 vs IKEv2 (FRITZ!Box)
- Security testing
- Behavioral models
- Black-box systems



https://pixabay.com/photos/personal-data-personal-security-4667362

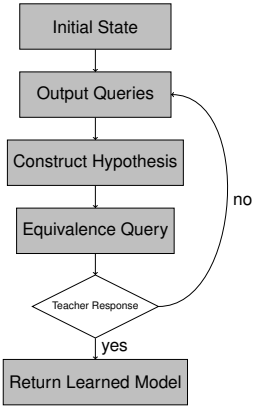
Motivation

- Increased VPN usage
- IPsec IKEv1 vs IKEv2 (FRITZ!Box)
- Security testing
- Behavioral models
- Black-box systems



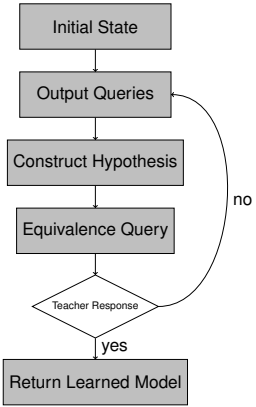
https://pixabay.com/photos/personal-data-personal-security-4667362

Model Learning



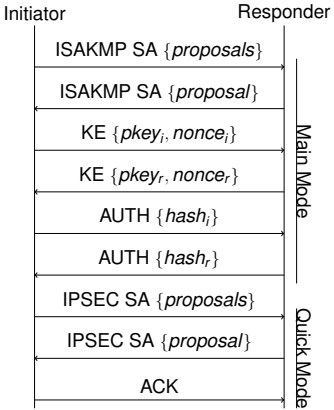
- L^* (Angluin)
- KV (Keans and Vazirani)

Model Learning

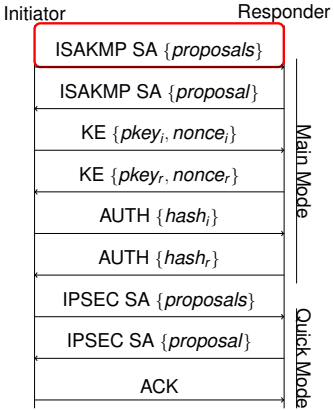


- L^* (Angluin)
- KV (Keans and Vazirani)

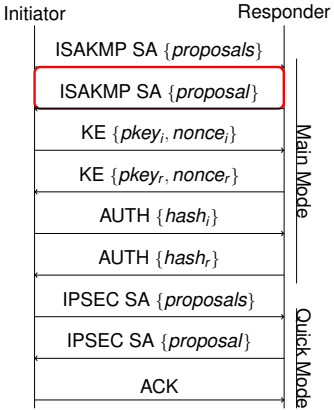
IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

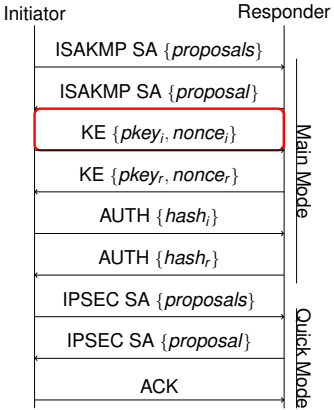
IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

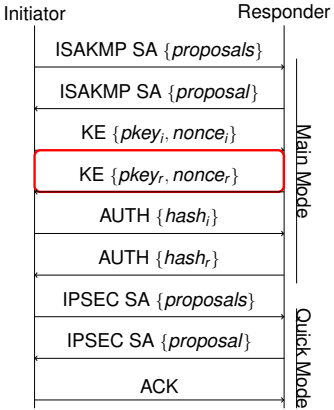
IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

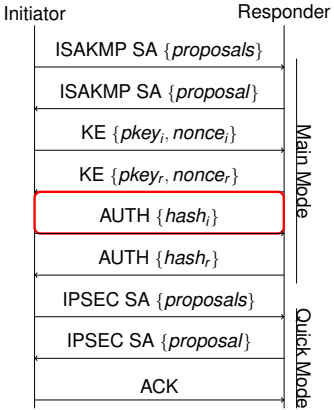
IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

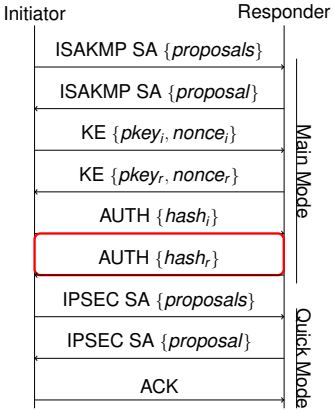
IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

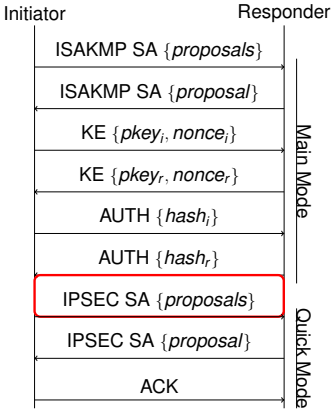
IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

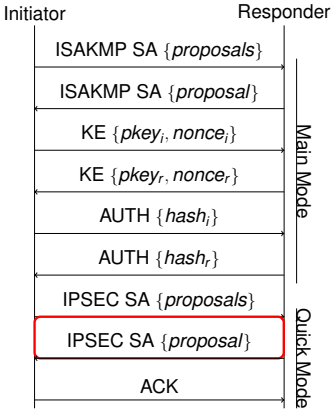
IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

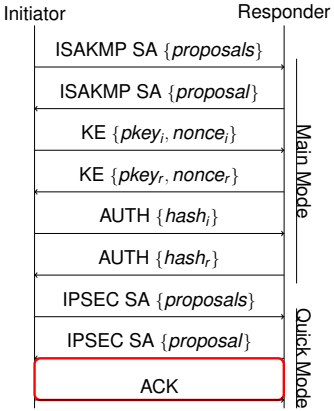
IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

IPsec


Initiator
Responder
ISAKMP SA {proposals}
ISAKMP SA {proposal}
KE {pkey_i, nonce_i}
KE {pkey_r, nonce_r}
AUTH {hash_i}
AUTH {hash_r}
IPSEC SA {proposals}
IPSEC SA {proposal}
ACK
Main Mode
Quick Mode

Environment Setup

- Ubuntu 22.04 LTS VM pairs
- Dedicated virtualized network
- Responder (SUL) / Initiator (learner)
- strongSwan & libreswan SUL

Environment Setup

- Ubuntu 22.04 LTS VM pairs
- Dedicated virtualized network
- Responder (SUL) / Initiator (learner)
- strongSwan & libreswan SUL

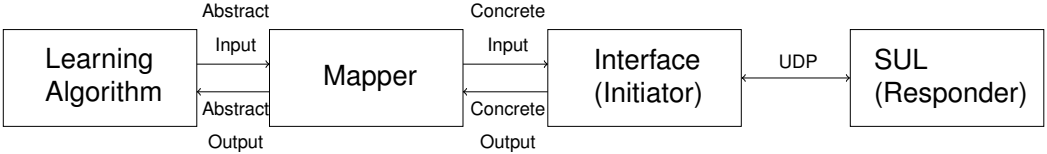
Environment Setup

- Ubuntu 22.04 LTS VM pairs
- Dedicated virtualized network
- Responder (SUL) / Initiator (learner)
- strongSwan & libreswan SUL

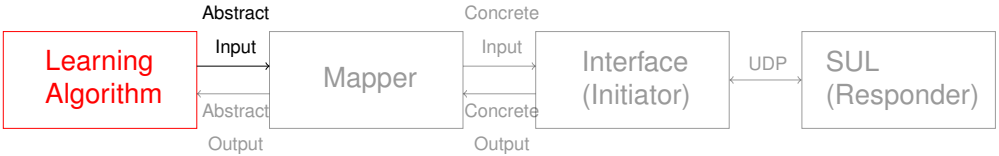
Environment Setup

- Ubuntu 22.04 LTS VM pairs
- Dedicated virtualized network
- Responder (SUL) / Initiator (learner)
- strongSwan & libreswan SUL

Learning Pipeline

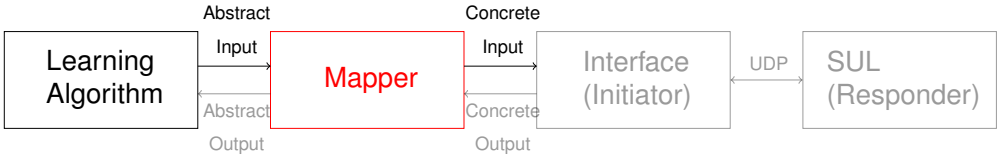


Learning Pipeline



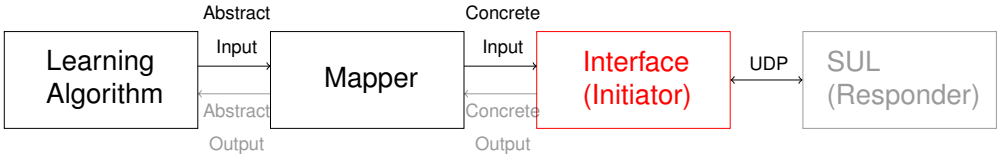
- AALpy
- *KV* / L^*

Learning Pipeline



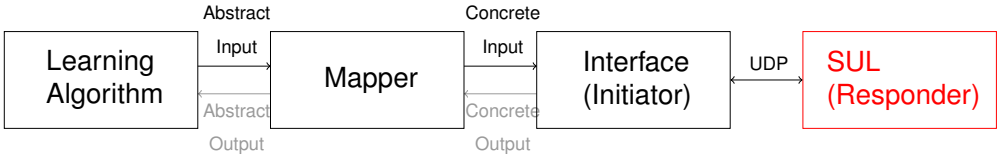
- Scapy
- Key management
- Error and retransmission handling

Learning Pipeline



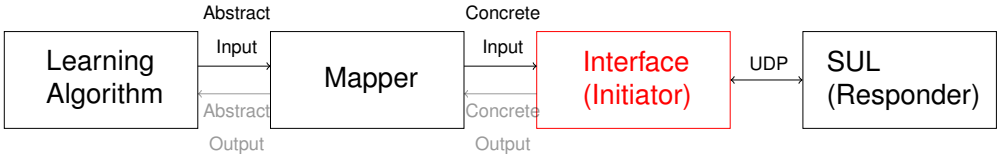
- Simple UDP socket wrapper
- Works with Scapy packets

Learning Pipeline



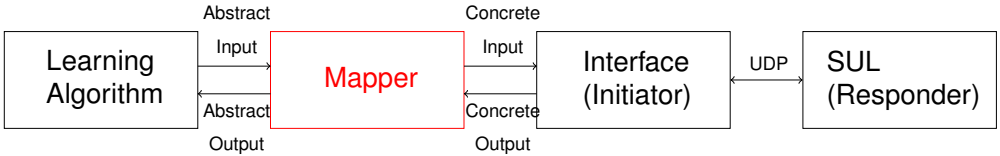
- SUL parses packet

Learning Pipeline



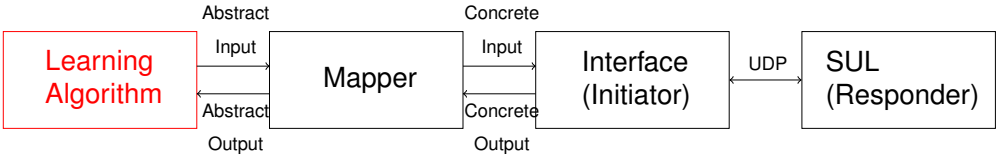
- Unpack response
- Returns Scapy packet

Learning Pipeline



- Parse packet
- Update datastructures

Learning Pipeline



Challenges

- Handling state
- Timing problems
- Retransmissions
- Difficult debugging
- Library error
- Resource limitations

```
[IKE] shared Diffie Hellman secret => 256 bytes @ 0x7fcdc8012410
[IKE]    0: B4 90 E1 03 B5 2C D5 B2 4C 18 80 A9 68 C5 AA 3B  .....,..L...h..;
[IKE]   16: D5 24 27 EB C5 1C 7C 41 94 40 81 D0 B9 25 52 CB  .$'...|A.@...%R.
[IKE]   32: 66 A8 21 B5 3F 6F 7B 39 E7 A6 5A 6B C8 88 0F B2  f.!.?o{9..Zh....
[IKE]   48: B7 7A CB 51 31 4A A1 D9 A7 60 32 0E BE 65 30 42  .z.Q1J...`2..e0B
[IKE]   64: 3F 5B 58 79 13 8D DE 79 C8 57 51 A3 F8 D7 3E 91  ?[Xy...y.WQ...>.
[IKE]   80: 56 9B 67 09 20 BB 3F 3A 9F 87 45 DA CF 25 99 E2  V.g. .?:..E..%..
[IKE]   96: E7 71 70 82 F4 B4 A3 D5 76 91 0C 5C 00 4A 66 17  .qp.....v..\.Jf.
[IKE]  112: 76 C0 24 44 47 68 8B 86 FF 47 74 6B 4A B6 63 61  v.$DGh...GtkJ.ca
[IKE]  128: A7 C6 45 35 1B 1B FF A2 C5 47 43 E2 B1 A4 D7 C8  ..E5.....GC.....
[IKE]  144: E6 52 F4 9C 10 DE 76 11 C2 62 6F 75 3F 87 A7 0D  .R....v..bou?...
[IKE]  160: B2 DB 8B 18 1C C8 FA 26 D7 DD A2 B4 02 12 AB 81  .......&........
[IKE]  176: 9D F9 A3 4D AF AE 5D 41 4E 52 00 3A 11 F2 0C 32  ...M..]ANR.:...2
[IKE]  192: 63 BC 8C 3A 13 C1 CE 9E D6 16 7F 0E 94 4B B9 73  c..:.........K.s
[IKE]  208: DB 17 E1 A5 3D 75 53 3F F6 1E AA 3F B1 12 C4 E7  ....=uS?...?....
[IKE]  224: C9 A5 0E 32 84 E3 AC 59 46 4B 92 66 E5 DD D4 76  ...2...YFK.f...v
[IKE]  240: 63 C8 00 EA CA DE 14 4A 0F 8A 59 F1 9F 91 89 C1  c......J..Y.....
[IKE] SKEYID => 20 bytes @ 0x7fcdc80122d0
[IKE]    0: 09 85 C6 22 57 90 2B CF 1C E2 6C 33 4D 83 14 76  ...."W.+...l3M..v
[IKE]   16: 94 1A F8 07                                      ....
[IKE] SKEYID_d => 20 bytes @ 0x7fcdc8012520
[IKE]    0: 90 56 B1 1C 56 97 0D 48 A9 FF 83 9F 86 09 31 BD  .V..V..H......1.
[IKE]   16: 85 EF C4 D2                                      ....
[IKE] SKEYID_a => 20 bytes @ 0x7fcdc8012670
[IKE]    0: 20 33 5A E0 B5 23 D3 7B 30 66 7C 9B 71 E0 46 A6  (3Z..#.{0f|.q.F.
[IKE]   16: 74 2E F6 ED                                      t...
[IKE] SKEYID_e => 20 bytes @ 0x7fcdc8012690
[IKE]    0: 94 50 C3 62 89 C4 CD D3 D4 4B 44 C1 F5 3D B0 11  .P.b.....KD..=..
[IKE]   16: 26 19 81 41                                      &..A
[IKE] encryption key Ka => 32 bytes @ 0x7fcdc80037a0
[IKE]    0: 13 EB 78 54 A5 F1 1C 41 82 41 27 E8 54 7E 19 98  ..xT...A.A'.T~..
[IKE]   16: E1 BE C3 AF F0 21 7A C2 F8 3D AF B3 36 DB 31 85  .....!z..=..6.1.
[IKE] initial IV => 16 bytes @ 0x7fcdc8012690
[IKE]    0: 62 93 69 45 6A 7A BA 02 B6 2E 0C 07 59 82 61 16  b.iEjz......Y.a.
```

Challenges

- Handling state
- Timing problems
- Retransmissions
- Difficult debugging
- Library error
- Resource limitations

```
[IKE] shared Diffie Hellman secret => 256 bytes @ 0x7fcdc8012410
[IKE]    0: B4 90 E1 03 B5 2C D5 B2 4C 18 80 A9 68 C5 AA 3B  .....,..L...h..;
[IKE]   16: D5 24 27 EB C5 1C 7C 41 94 40 81 D0 B9 25 52 CB  .$'...|A.@...%R.
[IKE]   32: 66 A8 21 B5 3F 6F 7B 39 E7 A6 5A 6B C8 88 0F B2  f.!.?o{9..Zh....
[IKE]   48: B7 7A CB 51 31 4A A1 D9 A7 60 32 0E BE 65 30 42  .z.Q1J...`2..e0B
[IKE]   64: 3F 5B 58 79 13 8D DE 79 C8 57 51 A3 F8 D7 3E 91  ?[Xy...y.WQ...>.
[IKE]   80: 56 9B 67 09 20 BB 3F 3A 9F 87 45 DA CF 25 99 E2  V.g. .?:..E..%..
[IKE]   96: E7 71 70 82 F4 B4 A3 D5 76 91 0C 5C 00 4A 66 17  .qp.....v..\.Jf.
[IKE]  112: 76 C0 24 44 47 68 8B 86 FF 47 74 6B 4A B6 63 61  v.$DGh...GtkJ.ca
[IKE]  128: A7 C6 45 35 1B 1B FF A2 C5 47 43 E2 B1 A4 D7 C8  ..E5.....GC.....
[IKE]  144: E6 52 F4 9C 10 DE 76 11 C2 62 6F 75 3F 87 A7 0D  .R....v..bou?...
[IKE]  160: B2 DB 8B 18 1C C8 FA 26 D7 DD A2 B4 02 12 AB 81  .......&........
[IKE]  176: 9D F9 A3 4D AF AE 5D 41 4E 52 00 3A 11 F2 0C 32  ...M..]ANR.:...2
[IKE]  192: 63 BC 8C 3A 13 C1 CE 9E D6 16 7F 0E 94 4B B9 73  c..:.........K.s
[IKE]  208: DB 17 E1 A5 3D 75 53 3F F6 1E AA 3F B1 12 C4 E7  ....=uS?...?....
[IKE]  224: C9 A5 0E 32 84 E3 AC 59 46 4B 92 66 E5 DD D4 76  ...2...YFK.f...v
[IKE]  240: 63 C8 00 EA CA DE 14 4A DF 8A 59 F1 9F 91 89 C1  c......J..Y.....
[IKE] SKEYID => 20 bytes @ 0x7fcdc80122d0
[IKE]    0: 09 85 C6 22 57 90 2B CF 1C E2 6C 33 4D 83 14 76  ...."W.+...l3M..v
[IKE]   16: 94 1A F8 07                                      ....
[IKE] SKEYID_d => 20 bytes @ 0x7fcdc8012520
[IKE]    0: 90 56 B1 1C 56 97 0D 48 A9 FF 83 9F 86 09 31 BD  .V..V..H......1.
[IKE]   16: 85 EF C4 D2                                      ....
[IKE] SKEYID_a => 20 bytes @ 0x7fcdc8012670
[IKE]    0: 28 33 5A E0 B5 23 D3 7B 30 66 7C 9B 71 E0 46 A6  (3Z..#.{0f|.q.F.
[IKE]   16: 74 2E F6 ED                                      t...
[IKE] SKEYID_e => 20 bytes @ 0x7fcdc8012690
[IKE]    0: 94 50 C3 62 89 C4 CD D3 D4 4B 44 C1 F5 3D B0 11  .P.b.....KD..=..
[IKE]   16: 26 19 81 41                                      &..A
[IKE] encryption key Ka => 32 bytes @ 0x7fcdc80037a0
[IKE]    0: 13 EB 78 54 A5 F1 1C 41 82 41 27 E8 54 7E 19 98  ..xT...A.A'.T~..
[IKE]   16: E1 BE C3 AF F0 21 7A C2 F8 3D AF B3 36 DB 31 85  .....!z..=..6.1.
[IKE] initial IV => 16 bytes @ 0x7fcdc8012690
[IKE]    0: 62 93 69 45 6A 7A BA 02 B6 2E 0C 07 59 82 61 16  b.iEjz......Y.a.
```

Challenges

- Handling state
- Timing problems
- Retransmissions
- Difficult debugging
- Library error
- Resource limitations

```
[IKE] shared Diffie Hellman secret => 256 bytes @ 0x7fcdc8012410
[IKE]    0: B4 90 E1 03 B5 2C D5 B2 4C 18 80 A9 68 C5 AA 3B  .....,..L...h..;
[IKE]   16: D5 24 27 EB C5 1C 7C 41 94 40 81 D0 B9 25 52 CB  .$'...|A.@...%R.
[IKE]   32: 66 A8 21 B5 3F 6F 7B 39 E7 A6 5A 6B C8 88 0F B2  f.!.?o{9..Zh....
[IKE]   48: B7 7A CB 51 31 4A A1 D9 A7 60 32 0E BE 65 30 42  .z.Q1J...`2..e0B
[IKE]   64: 3F 5B 58 79 13 8D DE 79 C8 57 51 A3 F8 D7 3E 91  ?[Xy...y.WQ...>.
[IKE]   80: 56 9B 67 09 20 BB 3F 3A 9F 87 45 DA CF 25 99 E2  V.g. .?:..E..%..
[IKE]   96: E7 71 70 82 F4 B4 A3 D5 76 91 0C 5C 00 4A 66 17  .qp.....v..\.Jf.
[IKE]  112: 76 C0 24 44 47 68 8B 86 FF 47 74 6B 4A B6 63 61  v.$DGh...GtkJ.ca
[IKE]  128: A7 C6 45 35 1B 1B FF A2 C5 47 43 E2 B1 A4 D7 C8  ..E5.....GC.....
[IKE]  144: E6 52 F4 9C 10 DE 76 11 C2 62 6F 75 3F 87 A7 0D  .R....v..bou?...
[IKE]  160: B2 DB 8B 18 1C C8 FA 26 D7 DD A2 B4 02 12 AB 81  .......&........
[IKE]  176: 9D F9 A3 4D AF AE 5D 41 4E 52 00 3A 11 F2 0C 32  ...M..]ANR.:...2
[IKE]  192: 63 BC 8C 3A 13 C1 CE 9E D6 16 7F 0E 94 48 B9 73  c..:.........H.s
[IKE]  208: DB 17 E1 A5 3D 75 53 3F F6 1E AA 3F B1 12 C4 E7  ....=uS?...?....
[IKE]  224: C9 A5 0E 32 84 E3 AC 59 46 4B 92 66 E5 DD D4 76  ...2...YFK.f...v
[IKE]  240: 63 C8 00 EA CA DE 14 4A 0F 8A 59 F1 9F 91 89 C1  c......J..Y.....
[IKE] SKEYID => 20 bytes @ 0x7fcdc80122d0
[IKE]    0: 09 85 C6 22 57 90 2B CF 1C E2 6C 33 4D 83 14 76  ...."W.+...l3M..v
[IKE]   16: 94 1A F8 07                                      ....
[IKE] SKEYID_d => 20 bytes @ 0x7fcdc8012520
[IKE]    0: 90 56 B1 1C 56 97 0D 48 A9 FF 83 9F 86 09 31 BD  .V..V..H......1.
[IKE]   16: 85 EF C4 D2                                      ....
[IKE] SKEYID_a => 20 bytes @ 0x7fcdc8012670
[IKE]    0: 28 33 5A E0 B5 23 D3 7B 30 66 7C 9B 71 E0 46 A6  (3Z..#.{0f|.q.F.
[IKE]   16: 74 2E F6 ED                                      t...
[IKE] SKEYID_e => 20 bytes @ 0x7fcdc8012690
[IKE]    0: 94 50 C3 62 89 C4 CD D3 D4 4B 44 C1 F5 3D B0 11  .P.b.....KD..=..
[IKE]   16: 26 19 81 41                                      &..A
[IKE] encryption key Ka => 32 bytes @ 0x7fcdc80037a0
[IKE]    0: 13 EB 78 54 A5 F1 1C 41 82 41 27 E8 54 7E 19 98  ..xT...A.A'.T~..
[IKE]   16: E1 BE C3 AF F0 21 7A C2 F8 3D AF B3 36 DB 31 85  .....!z..=..6.1.
[IKE] initial IV => 16 bytes @ 0x7fcdc8012690
[IKE]    0: 62 93 69 45 6A 7A BA 02 B6 2E 0C 07 59 82 61 16  b.iEjz......Y.a.
```

Challenges

- Handling state
- Timing problems
- Retransmissions
- Difficult debugging
- Library error
- Resource limitations

```
[IKE] shared Diffie Hellman secret => 256 bytes @ 0x7fcdc8012410
[IKE]    0: B4 90 E1 03 B5 2C D5 B2 4C 18 80 A9 68 C5 AA 3B  .....,..L...h..;
[IKE]   16: D5 24 27 EB C5 1C 7C 41 94 40 81 D0 B9 25 52 CB  .$'...|A.@...%R.
[IKE]   32: 66 A8 21 B5 3F 6F 7B 39 E7 A6 5A 6B C8 88 0F B2  f.!.?o{9..Zh....
[IKE]   48: B7 7A CB 51 31 4A A1 D9 A7 60 32 0E BE 65 30 42  .z.Q1J...`2..e0B
[IKE]   64: 3F 5B 58 79 13 8D DE 79 C8 57 51 A3 F8 D7 3E 91  ?[Xy...y.WQ...>.
[IKE]   80: 56 9B 67 09 20 BB 3F 3A 9F 87 45 DA CF 25 99 E2  V.g. .?:..E..%..
[IKE]   96: E7 71 70 82 F4 B4 A3 D5 76 91 0C 5C 00 4A 66 17  .qp.....v..\.Jf.
[IKE]  112: 76 C0 24 44 47 68 8B 86 FF 47 74 6B 4A B6 63 61  v.$DGh...GtkJ.ca
[IKE]  128: A7 C6 45 35 1B 1B FF A2 C5 47 43 E2 B1 A4 D7 C8  ..E5.....GC.....
[IKE]  144: E6 52 F4 9C 10 DE 76 11 C2 62 6F 75 3F 87 A7 0D  .R....v..bou?...
[IKE]  160: B2 DB 8B 18 1C C8 FA 26 D7 DD A2 B4 02 12 AB 81  .......&........
[IKE]  176: 9D F9 A3 4D AF AE 5D 41 4E 52 00 3A 11 F2 0C 32  ...M..]ANR.:...2
[IKE]  192: 63 BC 8C 3A 13 C1 CE 9E D6 16 7F 0E 94 4B B9 73  c..:.........K.s
[IKE]  208: DB 17 E1 A5 3D 75 53 3F F6 1E AA 3F B1 12 C4 E7  ....=uS?...?....
[IKE]  224: C9 A5 0E 32 84 E3 AC 59 46 4B 92 66 E5 DD D4 76  ...2...YFK.f...v
[IKE]  240: 63 C8 00 EA CA DE 14 4A DF 8A 59 F1 9F 91 89 C1  c......J..Y.....
[IKE] SKEYID => 20 bytes @ 0x7fcdc80122d0
[IKE]    0: 09 85 C6 22 57 90 2B CF 1C E2 6C 33 4D 83 14 76  ..."W.+...l3M..v
[IKE]   16: 94 1A F8 07                                      ....
[IKE] SKEYID_d => 20 bytes @ 0x7fcdc8012520
[IKE]    0: 90 56 B1 1C 56 97 8D 48 A9 FF 83 9F 86 09 31 BD  .V..V..H......1.
[IKE]   16: 85 EF C4 D2                                      ....
[IKE] SKEYID_a => 20 bytes @ 0x7fcdc8012670
[IKE]    0: 28 33 5A E0 B5 23 D3 7B 30 66 7C 9B 71 E0 46 A6  (3Z..#.{0f|.q.F.
[IKE]   16: 74 2E F6 ED                                      t...
[IKE] SKEYID_e => 20 bytes @ 0x7fcdc8012690
[IKE]    0: 94 50 C3 62 89 C4 CD D3 D4 4B 44 C1 F5 3D B0 11  .P.b.....KD..=..
[IKE]   16: 26 19 81 41                                      &..A
[IKE] encryption key Ka => 32 bytes @ 0x7fcdc80037a0
[IKE]    0: 13 EB 78 54 A5 F1 1C 41 82 41 27 E8 54 7E 19 98  ..xT...A.A'.T~..
[IKE]   16: E1 BE C3 AF F0 21 7A C2 F8 3D AF B3 36 DB 31 85  .....!z..=..6.1.
[IKE] initial IV => 16 bytes @ 0x7fcdc8012690
[IKE]    0: 62 93 69 45 6A 7A BA 02 B6 2E 0C 07 59 82 61 16  b.iEjz......Y.a.
```

Challenges

- Handling state
- Timing problems
- Retransmissions
- Difficult debugging
- Library error
- Resource limitations

```
[IKE] shared Diffie Hellman secret => 256 bytes @ 0x7fcdc8012410
[IKE]    0: B4 90 E1 03 B5 2C D5 B2 4C 18 80 A9 68 C5 AA 3B  .....,..L...h..;
[IKE]   16: D5 24 27 EB C5 1C 7C 41 94 40 81 D0 B9 25 52 CB  .$'...|A.@...%R.
[IKE]   32: 66 A8 21 B5 3F 6F 7B 39 E7 A6 5A 6B C8 88 0F B2  f.!.?o{9..Zh....
[IKE]   48: B7 7A CB 51 31 4A A1 D9 A7 60 32 0E BE 65 30 42  .z.Q1J...`2..e0B
[IKE]   64: 3F 5B 58 79 13 8D DE 79 C8 57 51 A3 F8 D7 3E 91  ?[Xy...y.WQ...>.
[IKE]   80: 56 9B 67 09 20 BB 3F 3A 9F 87 45 DA CF 25 99 E2  V.g. .?:..E..%..
[IKE]   96: E7 71 70 82 F4 B4 A3 D5 76 91 0C 5C 00 4A 66 17  .qp.....v..\.Jf.
[IKE]  112: 76 C0 24 44 47 68 8B 86 FF 47 74 6B 4A B6 63 61  v.$DGh...GtkJ.ca
[IKE]  128: A7 C6 45 35 1B 1B FF A2 C5 47 43 E2 B1 A4 D7 C8  ..E5.....GC.....
[IKE]  144: E6 52 F4 9C 10 DE 76 11 C2 62 6F 75 3F 87 A7 0D  .R....v..bou?...
[IKE]  160: B2 DB 8B 18 1C C8 FA 26 D7 DD A2 B4 02 12 AB 81  .......&........
[IKE]  176: 9D F9 A3 4D AF AE 5D 41 4E 52 00 3A 11 F2 0C 32  ...M..]ANR.:...2
[IKE]  192: 63 BC 8C 3A 13 C1 CE 9E D6 16 7F 0E 94 4B B9 73  c..:.........K.s
[IKE]  208: DB 17 E1 A5 3D 75 53 3F F6 1E AA 3F B1 12 C4 E7  ....=uS?...?....
[IKE]  224: C9 A5 0E 32 84 E3 AC 59 46 4B 92 66 E5 DD D4 76  ...2...YFK.f...v
[IKE]  240: 63 C8 00 EA CA DE 14 4A DF 8A 59 F1 9F 91 89 C1  c......J..Y.....
[IKE] SKEYID => 20 bytes @ 0x7fcdc80122d0
[IKE]    0: 09 85 C6 22 57 90 2B CF 1C E2 6C 33 4D 83 14 76  ..."W.+...l3M..v
[IKE]   16: 94 1A F8 07                                      ....
[IKE] SKEYID_d => 20 bytes @ 0x7fcdc8012520
[IKE]    0: 90 56 B1 1C 56 97 8D 48 A9 FF 83 9F 86 09 31 BD  .V..V..H......1.
[IKE]   16: 85 EF C4 D2                                      ....
[IKE] SKEYID_a => 20 bytes @ 0x7fcdc8012670
[IKE]    0: 28 33 5A E0 B5 23 D3 7B 30 66 7C 9B 71 E0 46 A6  (3Z..#.{0f|.q.F.
[IKE]   16: 74 2E F6 ED                                      t...
[IKE] SKEYID_e => 20 bytes @ 0x7fcdc8012690
[IKE]    0: 94 50 C3 62 89 C4 CD D3 D4 4B 44 C1 F5 3D B0 11  .P.b.....KD..=..
[IKE]   16: 26 19 81 41                                      &..A
[IKE] encryption key Ka => 32 bytes @ 0x7fcdc80037a0
[IKE]    0: 13 EB 78 54 A5 F1 1C 41 82 41 27 E8 54 7E 19 98  ..xT...A.A'.T~..
[IKE]   16: E1 BE C3 AF F0 21 7A C2 F8 3D AF B3 36 DB 31 85  .....!z..=..6.1.
[IKE] initial IV => 16 bytes @ 0x7fcdc8012690
[IKE]    0: 62 93 69 45 6A 7A BA 02 B6 2E 0C 07 59 82 61 16  b.iEjz......Y.a.
```

Challenges

- Handling state
- Timing problems
- Retransmissions
- Difficult debugging
- Library error
- Resource limitations

```
[IKE] shared Diffie Hellman secret => 256 bytes @ 0x7fcdc8012410
[IKE]    0: B4 90 E1 03 B5 2C D5 B2 4C 18 80 A9 68 C5 AA 3B  .....,..L...h..;
[IKE]   16: D5 24 27 EB C5 1C 7C 41 94 40 81 D0 B9 25 52 CB  .$'...|A.@...%R.
[IKE]   32: 66 A8 21 B5 3F 6F 7B 39 E7 A6 5A 6B C8 88 0F B2  f.!.?o{9..Zk....
[IKE]   48: B7 7A CB 51 31 4A A1 D9 A7 60 32 0E BE 65 30 42  .z.Q1J...`2..e0B
[IKE]   64: 3F 5B 58 79 13 8D DE 79 C8 57 51 A3 F8 D7 3E 91  ?[Xy...y.WQ...>.
[IKE]   80: 56 9B 67 09 20 BB 3F 3A 9F 87 45 DA CF 25 99 E2  V.g. .?:..E..%..
[IKE]   96: E7 71 70 82 F4 B4 A3 D5 76 91 0C 5C 00 4A 66 17  .qp.....v..\.Jf.
[IKE]  112: 76 C0 24 44 47 68 88 86 FF 47 74 6B 4A B6 63 61  v.$DGh...GtkJ.ca
[IKE]  128: A7 C6 45 35 1B 1B FF A2 C5 47 43 E2 B1 A4 D7 C8  ..E5.....GC.....
[IKE]  144: E6 52 F4 9C 10 DE 76 11 C2 62 6F 75 3F 87 A7 0D  .R....v..bou?...
[IKE]  160: B2 DB 8B 18 1C C8 FA 26 D7 DD A2 B4 02 12 AB 81  .......&........
[IKE]  176: 9D F9 A3 4D AF AE 5D 41 4E 52 00 3A 11 F2 0C 32  ...M..]ANR.:...2
[IKE]  192: 63 BC 8C 3A 13 C1 CE 9E D6 16 7F 0E 94 48 B9 73  c..:.........H.s
[IKE]  208: DB 17 E1 A5 3D 75 53 3F F6 1E AA 3F B1 12 C4 E7  ....=uS?...?....
[IKE]  224: C9 A5 0E 32 84 E3 AC 59 46 4B 92 66 E5 DD D4 76  ...2...YFK.f...v
[IKE]  240: 63 C8 00 EA CA DE 14 4A 0F 8A 59 F1 9F 91 89 C1  c......J..Y.....
[IKE] SKEYID => 20 bytes @ 0x7fcdc80122d0
[IKE]    0: 09 85 C6 22 57 90 2B CF 1C E2 6C 33 4D 83 14 76  ..."W.+...l3M..v
[IKE]   16: 94 1A F8 07                                      ....
[IKE] SKEYID_d => 20 bytes @ 0x7fcdc8012520
[IKE]    0: 90 56 B1 1C 56 97 8D 48 A9 FF 83 9F 86 09 31 BD  .V..V..H......1.
[IKE]   16: 85 EF C4 D2                                      ....
[IKE] SKEYID_a => 20 bytes @ 0x7fcdc8012670
[IKE]    0: 28 33 5A E0 B5 23 D3 7B 30 66 7C 9B 71 E0 46 A6  (3Z..#.{0f|.q.F.
[IKE]   16: 74 2E F6 ED                                      t...
[IKE] SKEYID_e => 20 bytes @ 0x7fcdc8012690
[IKE]    0: 94 50 C3 62 89 C4 CD D3 D4 4B 44 C1 F5 3D B0 11  .P.b.....KD..=..
[IKE]   16: 26 19 81 41                                      &..A
[IKE] encryption key Ka => 32 bytes @ 0x7fcdc80037a0
[IKE]    0: 13 EB 78 54 A5 F1 1C 41 82 41 27 E8 54 7E 19 98  ..xT...A.A'.T~..
[IKE]   16: E1 BE C3 AF F0 21 7A C2 F8 3D AF B3 36 DB 31 85  .....!z..=..6.1.
[IKE] initial IV => 16 bytes @ 0x7fcdc8012690
[IKE]    0: 62 93 69 45 6A 7A BA 02 B6 2E 0C 07 59 82 61 16  b.iEjz......Y.a.
```

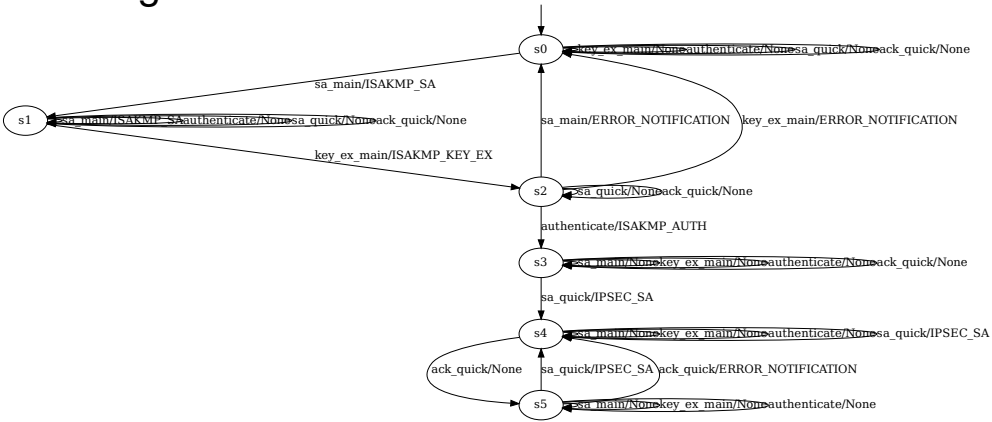
Model Overview

- StrongSwan Base
- StrongSwan Fuzzing Reference
- libreswan Base
- libreswan Fuzzing Reference

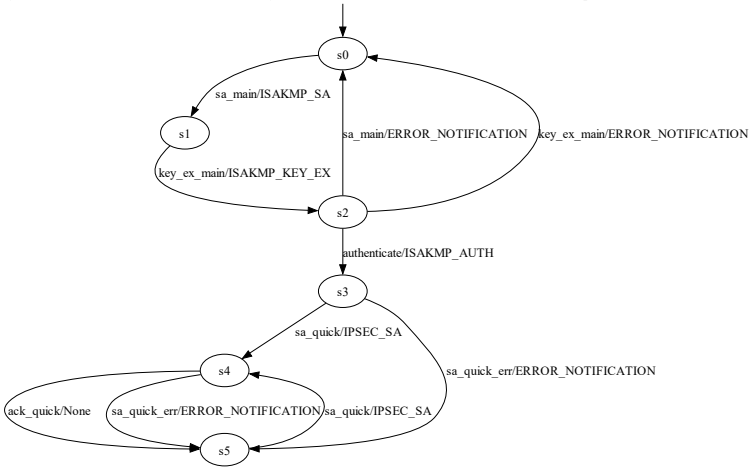
Model Overview

- StrongSwan Base
- StrongSwan Fuzzing Reference
- libreswan Base
- libreswan Fuzzing Reference

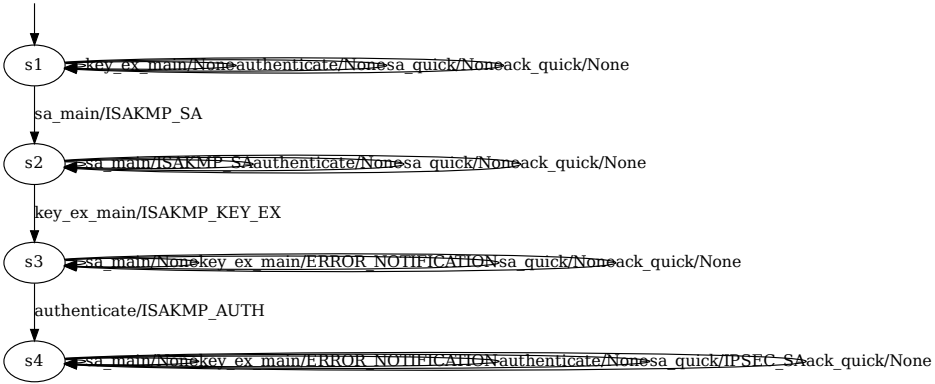
StrongSwan Base



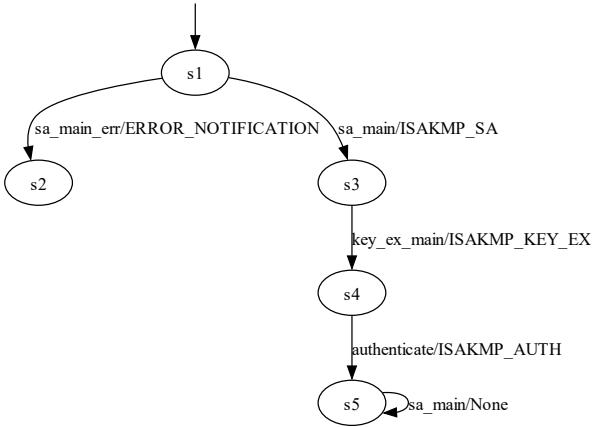
StrongSwan Fuzzing Reference (Simplified)



libreswan Base



libreswan Fuzzing Reference (Simplified)



Fuzzing Overview

- Software testing technique
- Random / unexpected input
- Categorization:
  - Data generation
  - Access to SUT information

Fuzzing Overview

- Software testing technique
- Random / unexpected input
- Categorization:
  - Data generation
  - Access to SUT information

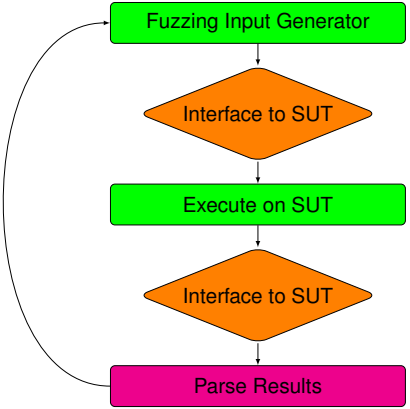
Fuzzing Overview

- Software testing technique
- Random / unexpected input
- Categorization:
  - Data generation
  - Access to SUT information

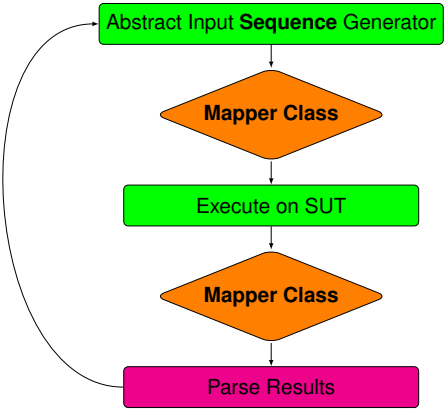
Fuzzing Overview

- Software testing technique
- Random / unexpected input
- Categorization:
  - Data generation
  - Access to SUT information

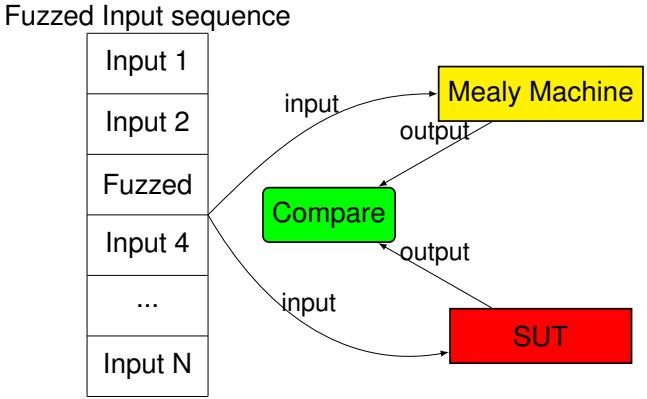
Fuzzing Setup - Generic



Fuzzing Setup - Our Approach

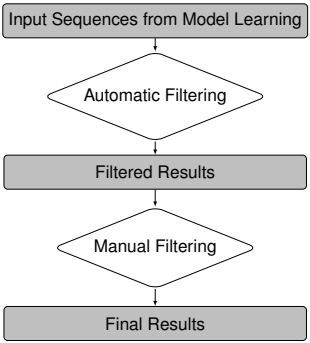


Detecting new behavior



Input Sequence Generation - Filtering

- Reuse input sequences from model learning
- Automatic Filtering
- Manual Filtering



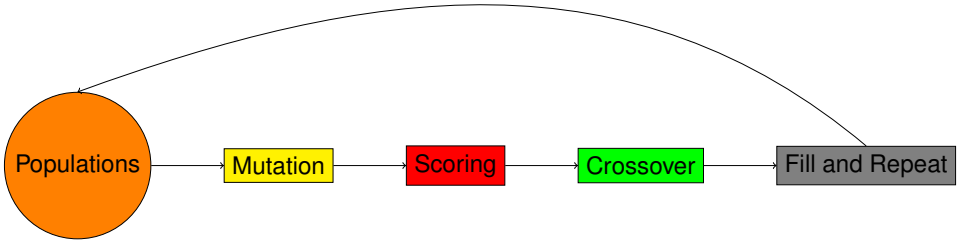
Input Sequence Generation - Search

- Single input sequence
- Search-based
- Fitness function

$$f_{\text{seq}} = \sum_{0}^{n-1} \frac{b_{\text{new}}}{n} \frac{s_{\text{visited}}}{s_{\text{total}}} \quad (1)$$

Input Sequence Generation - Genetic

- Pool of populations
- Mutation operations



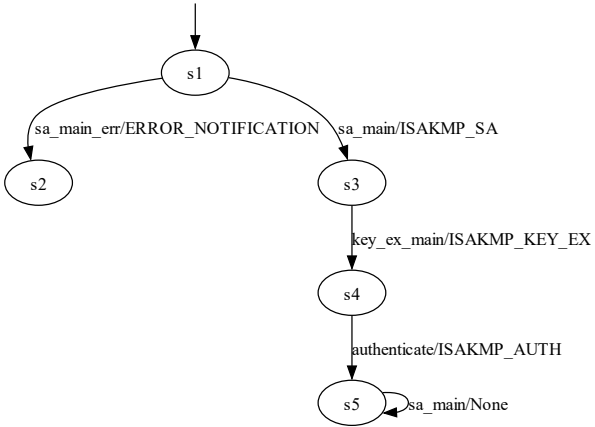
Finding - ISAKMP Length

```
Fuzzing ISAKMP length field with: b'\ xff \x00\x00\x00'
Input  sequence: ['sa_main_fuzz', 'key_ex_main', 'authenticate',    ...]

$sa_main_fuzz
$key_ex_main


 **********
Expected: ERROR_NOTIFICATION | Received: ISAKMP_SA
Expected: None | Received: ISAKMP_KEY_EX
 **********
```

Finding - libreswan Deadlock



Finding - StrongSwan Authentication

Fuzzing SA Transform with: [..., (’Authentication’, ’FUZZED_VALUE’), ...]

Run: [..., ’sa_main_fuzz’, ...]

$sa_main_fuzz

****
Expected: ERROR_NOTIFICATION | Received: ISAKMP_SA
****

Conclusion

- Learned models of popular IPsec implementations
- Fuzzing revealed several deviations from specifications
- Future work:
  - Mapper class improvements
  - Additional input-sequence / fuzz-data generation methods
  - Fuzz with more resources

Conclusion

- Learned models of popular IPsec implementations
- Fuzzing revealed several deviations from specifications
- Future work:
  - Mapper class improvements
  - Additional input-sequence / fuzz-data generation methods
  - Fuzz with more resources