What the fuzz!?

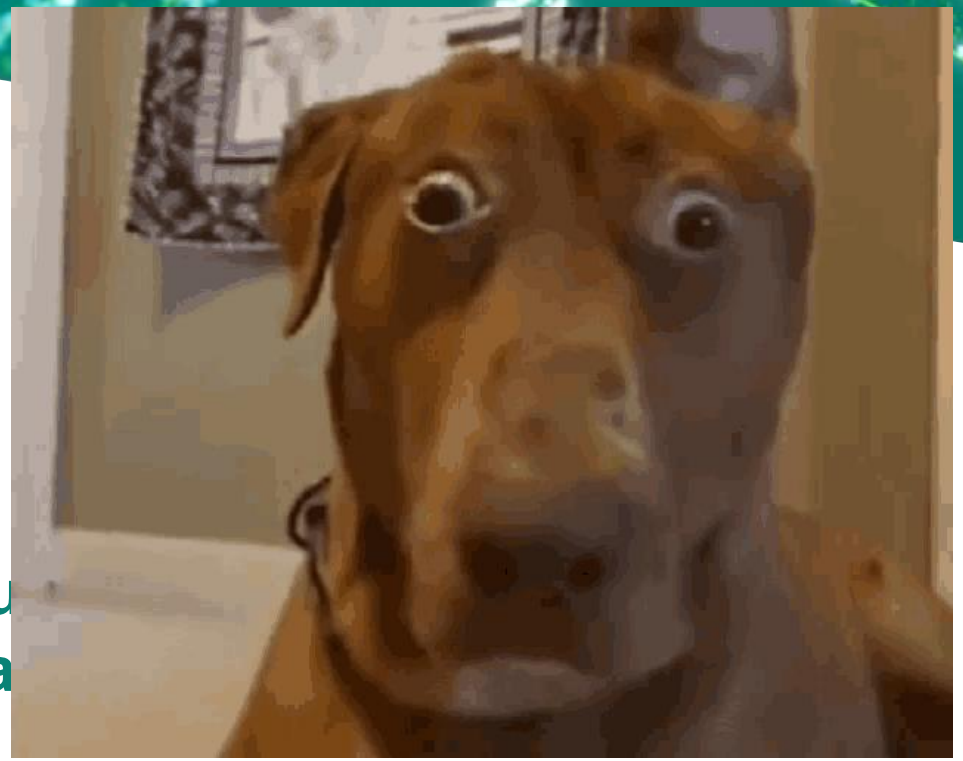
A Journey into Structure-aware Fuzzing on a Rust SUIT-Manifest Parser

Marcel Fink

2026-09-01

What the fuzz!?

A Journey into Structu
Rust SUIT-Manifest Pa



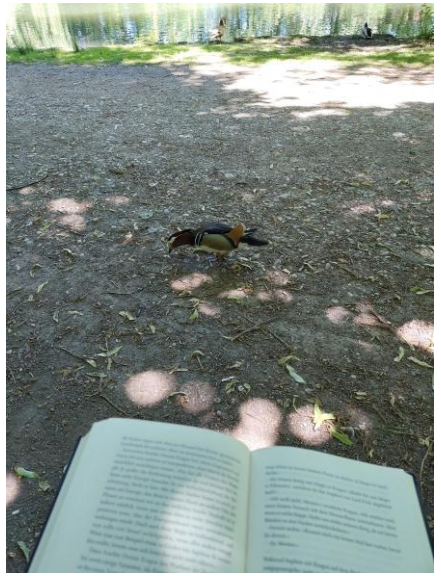
Source: https://media1.tenor.com/m/a4n_xbhGryoAAAAd/o_o-dog.gif

Marcel Fink

2026-09-01

$whoami

- Marcel Fink
- Studying Computer Science at the THA
- Currently working on my bachelor’s thesis at Infineon



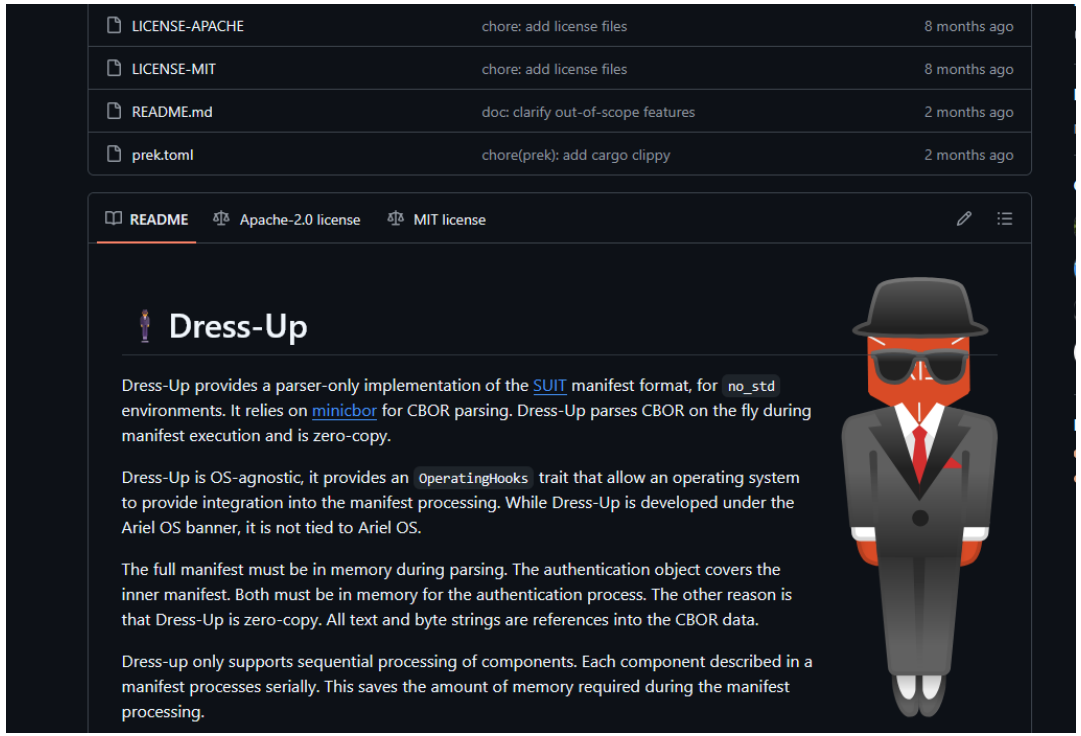
Agenda

- Background
  - What are going to fuzz?
  - What are SUIT-Manifests?
  - What is Fuzzing?
  - Mutation-based (coverage-guided) fuzzing
  - Structure-aware fuzzing
- Target 1: “unaware”
- Target 2: “envlp_wrap”
- Target 3: “manifest_gen”
- Comparison
- What did we learn?

Background

What are we going to fuzz?

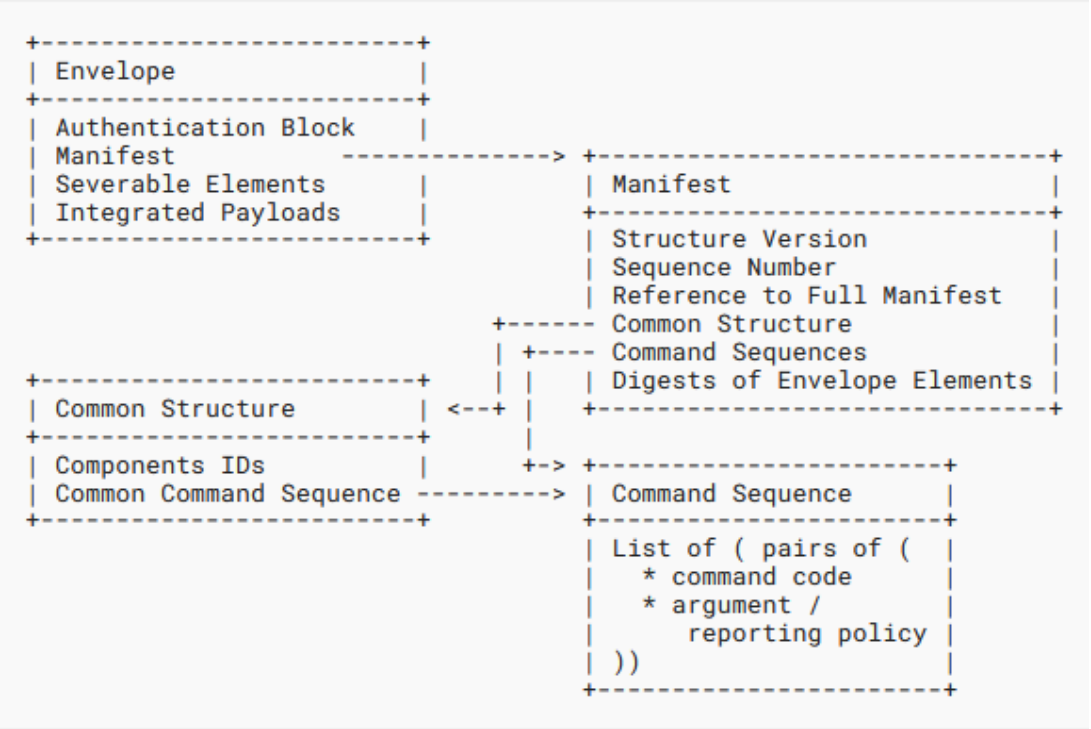
- **Dress-Up**
- Parser for SUIT manifests
- Specifically for “no_std” environments



Source: https://github.com/ariel-os/dress-up

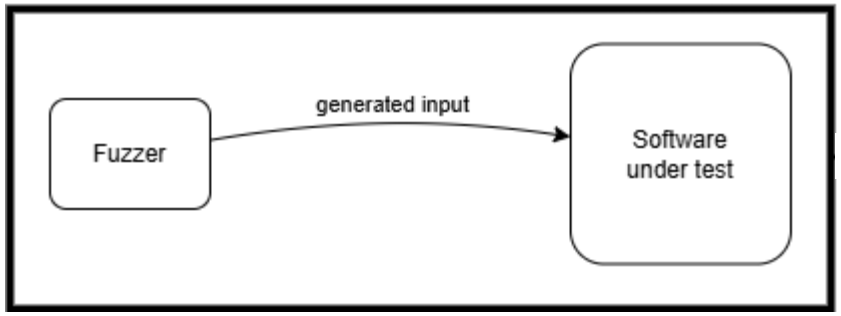
What are SUIT-Manifests?

- SUIT = “**S**oftware **U**pdates for **I**nternet of **T**hings”
- Contain metadata for update process
- Encoded in CBOR (**C**oncise **B**inary **O**bject **R**epresentation)

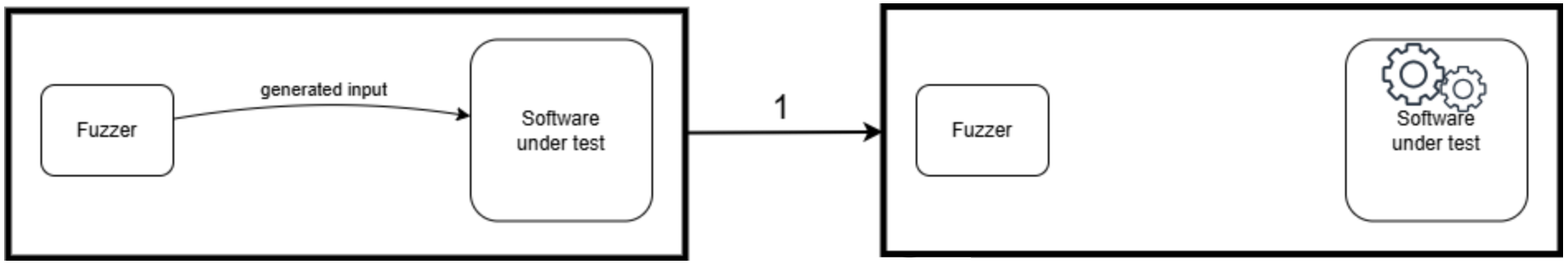


Source: https://www.ietf.org/archive/id/draft-ietf-suit-manifest-37.html

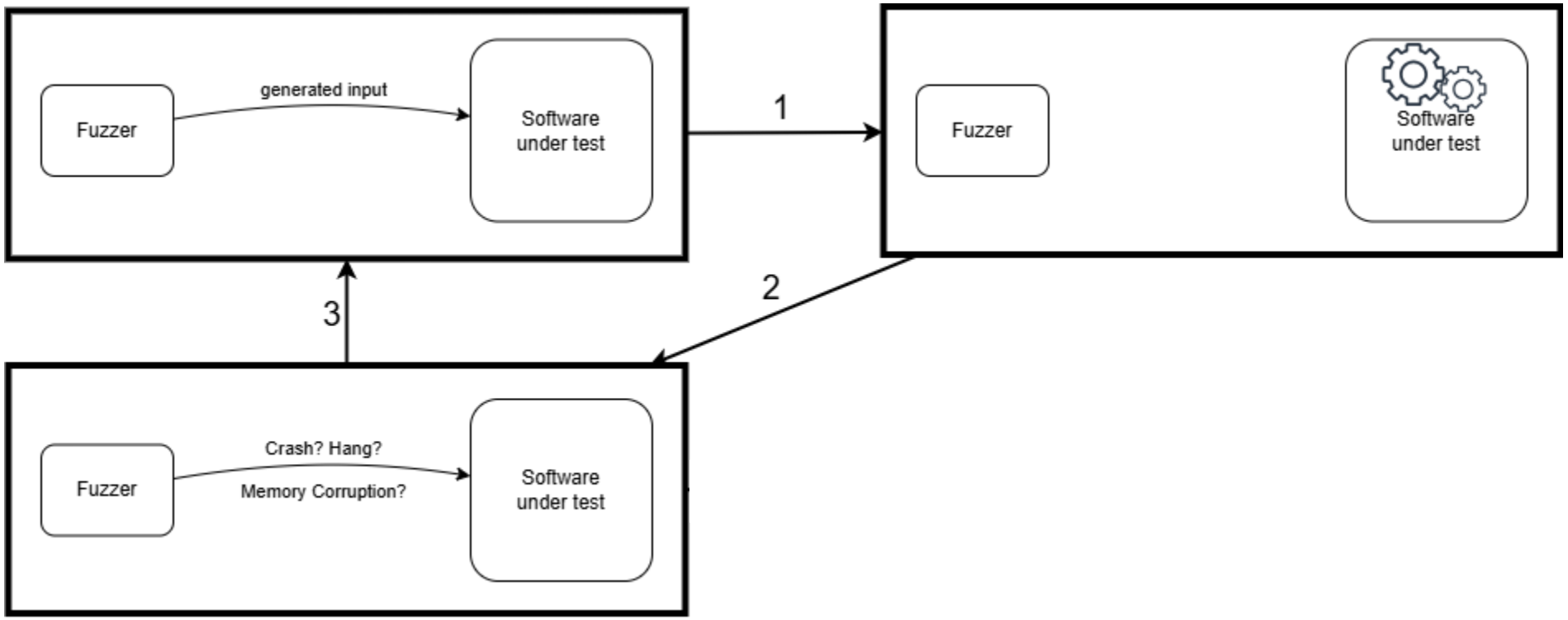
What is fuzzing?



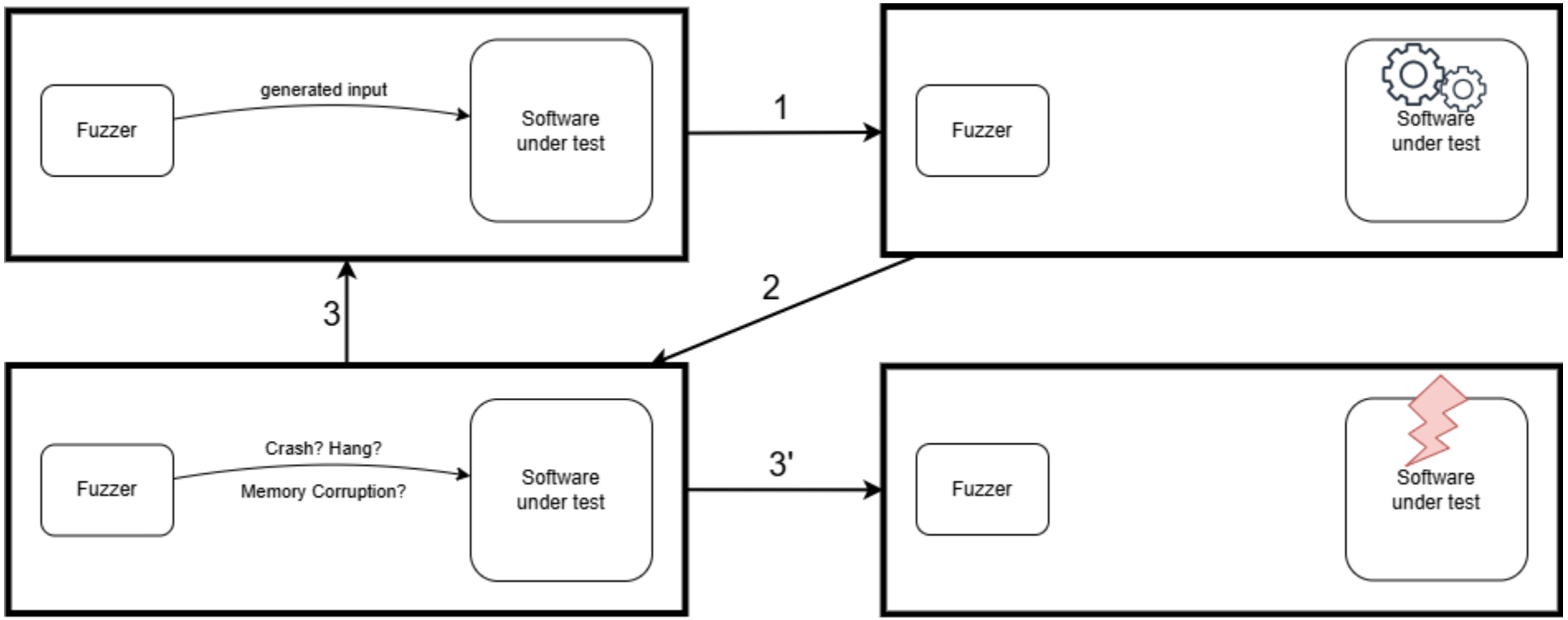
What is fuzzing?



What is fuzzing?



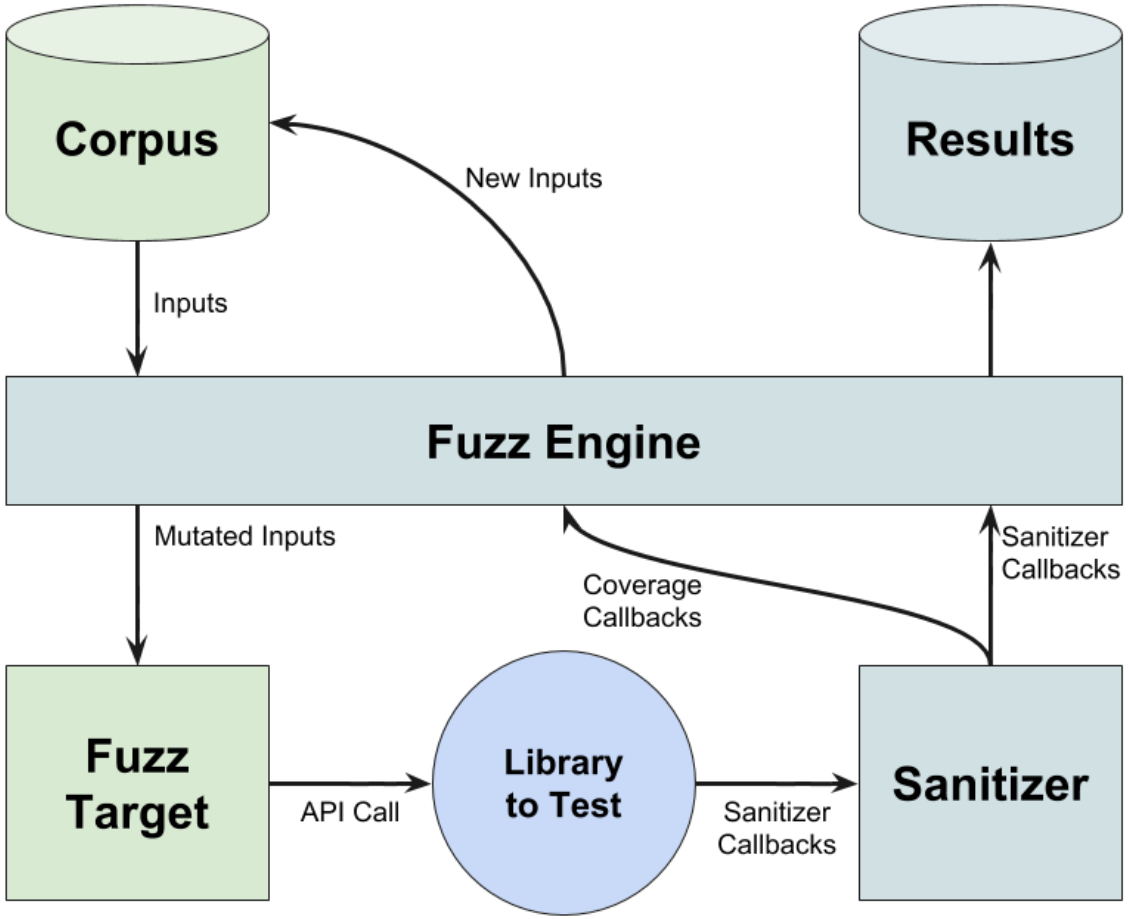
What is fuzzing?



What is fuzzing?

Source: https://i.imgflip.com/4igxyl.png

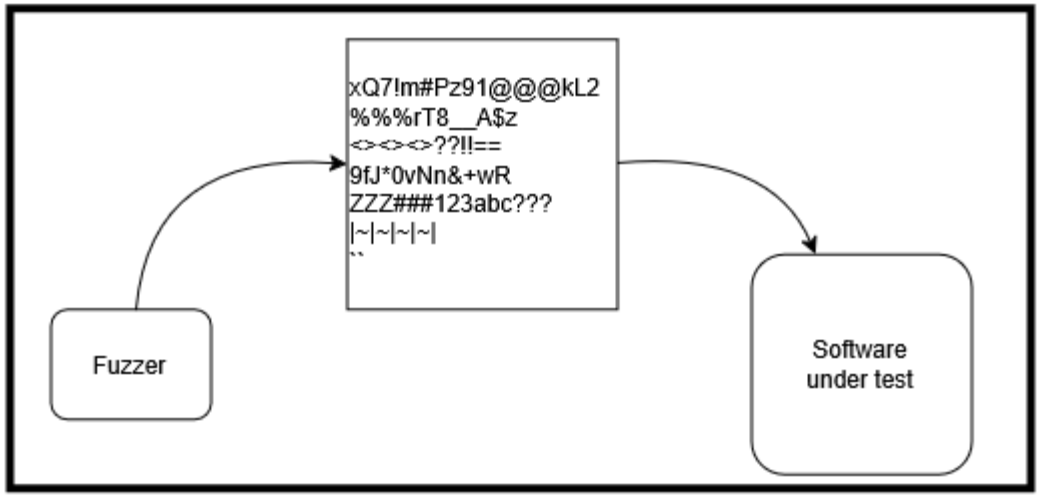
Mutation-based (coverage-guided) fuzzing



Source: https://fuchsia.dev/static/fuchsia-src/images/fuzzing/coverage-guided.png

Problem

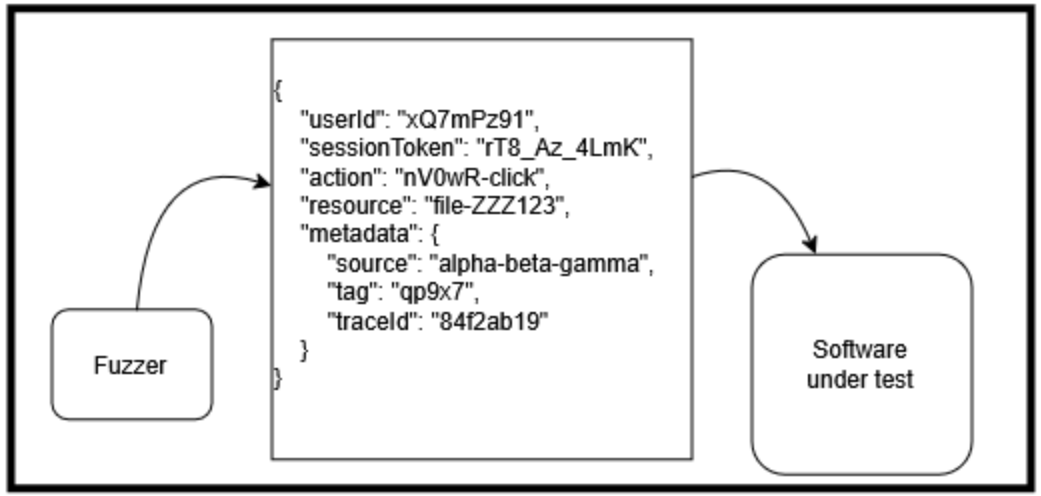
- Highly structured input needed (e.g. JSON, PDF, SUIT manifests, …)
- “random” input gets rejected early
- **Result:** shallow code coverage



Source: https://images.meme-arsenal.com/616e18835b0052475c03c544f04c358a.jpg

Solution

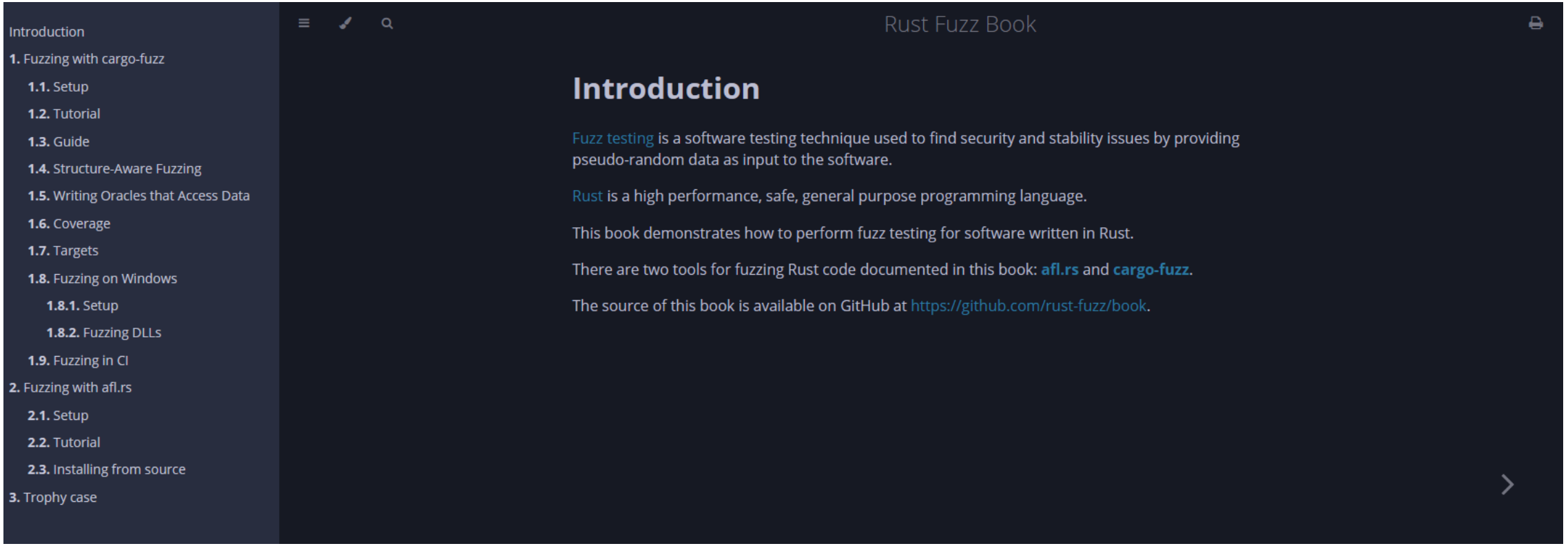
- **Structure-awareness**
- Input follows structure / syntax
- Doesn’t get rejected by structure-checks
- **Result:** deeper code coverage



Source: https://images.meme-arsenal.com/616e18835b0052475c03c544f04c358a.jpg

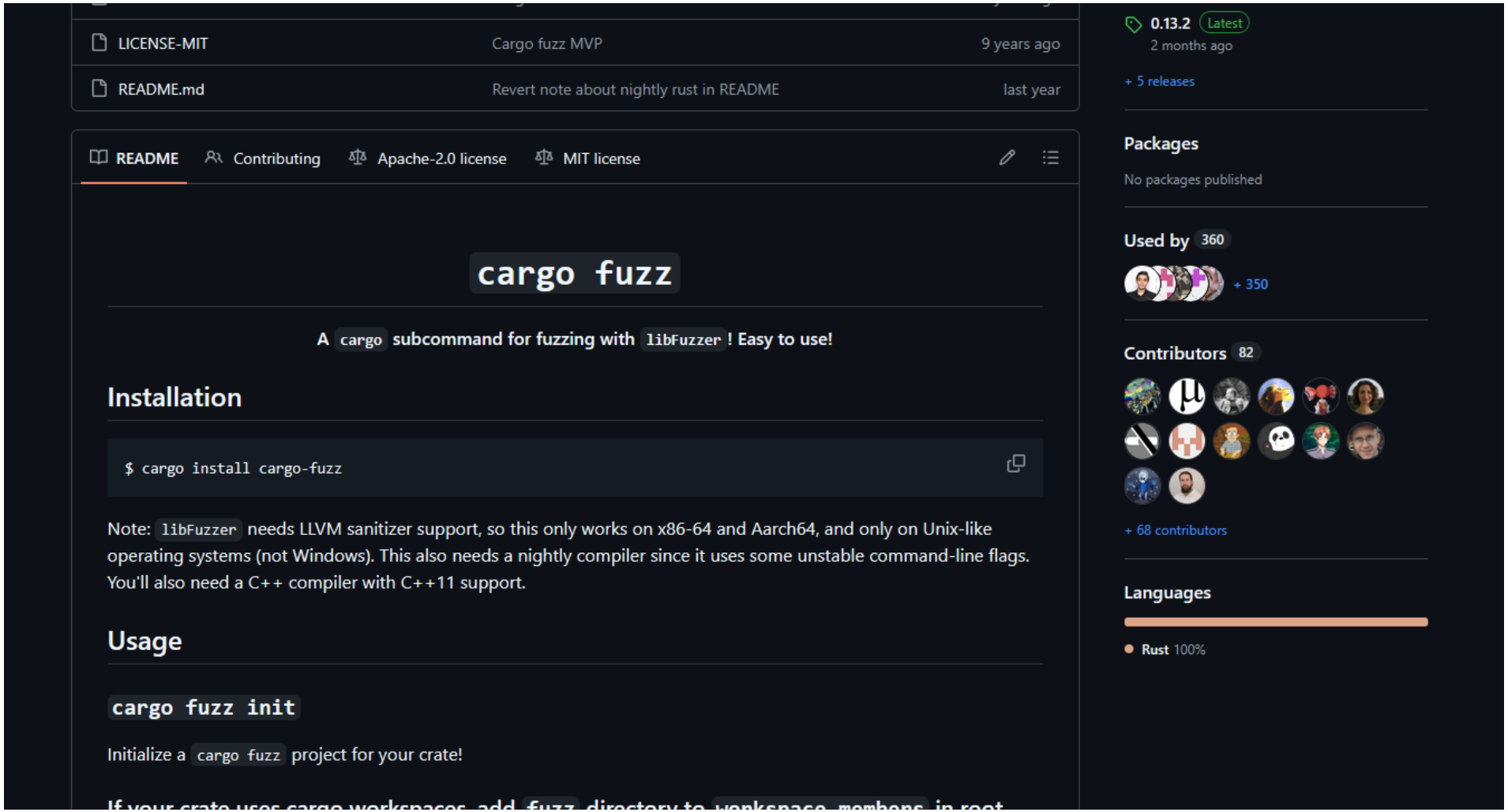
Background: ✅

Rust Fuzz Book



https://rust-fuzz.github.io/book/

Cargo Fuzz



https://github.com/rust-fuzz/cargo-fuzz

Target 1: “unaware”

Target 1: “unaware”

```rust
#![no_main]

use libfuzzer_sys::fuzz_target;

use dress_up::SuitManifest;

fuzz_target!(|data: &[u8]| {

    let suit = SuitManifest::from_bytes(&data);

    if let Ok(envelope) = suit.envelope() {
        let _ = envelope.manifest();
    }
});
```

```
#12617  NEW    cov: 285 ft: 521 corp: 124/1075b lim: 29 exec/s: 0 rss: 40Mb L: 18/28 MS: 2 ChangeBit-InsertRepeatedBytes-
#12618  REDUCE cov: 285 ft: 528 corp: 125/1104b lim: 29 exec/s: 0 rss: 40Mb L: 29/29 MS: 1 CopyPart-
#12644  REDUCE cov: 285 ft: 528 corp: 125/1101b lim: 29 exec/s: 0 rss: 40Mb L: 15/29 MS: 1 EraseBytes-
#12662  REDUCE cov: 285 ft: 528 corp: 125/1096b lim: 29 exec/s: 0 rss: 40Mb L: 23/29 MS: 3 CrossOver-InsertByte-EraseBytes-
#12681  NEW    cov: 285 ft: 531 corp: 126/1125b lim: 29 exec/s: 0 rss: 40Mb L: 29/29 MS: 4 InsertRepeatedBytes-ChangeBit-Era
#12775  NEW    cov: 292 ft: 539 corp: 127/1149b lim: 29 exec/s: 0 rss: 40Mb L: 24/29 MS: 4 InsertByte-ChangeBinInt-PersAutoD
#12863  NEW    cov: 292 ft: 542 corp: 128/1168b lim: 29 exec/s: 0 rss: 41Mb L: 19/29 MS: 3 CopyPart-EraseBytes-ChangeBinInt-
#12938  NEW    cov: 292 ft: 543 corp: 129/1186b lim: 29 exec/s: 0 rss: 41Mb L: 18/29 MS: 5 InsertByte-InsertByte-ChangeBinIn
#12941  REDUCE cov: 292 ft: 543 corp: 129/1183b lim: 29 exec/s: 0 rss: 41Mb L: 10/29 MS: 3 ChangeBinInt-ShuffleBytes-EraseBy
#12943  NEW    cov: 292 ft: 544 corp: 130/1201b lim: 29 exec/s: 0 rss: 41Mb L: 18/29 MS: 2 ChangeBinInt-CopyPart-
#12999  NEW    cov: 295 ft: 547 corp: 131/1207b lim: 29 exec/s: 0 rss: 41Mb L: 6/29 MS: 1 EraseBytes-
#13036  NEW    cov: 298 ft: 550 corp: 132/1211b lim: 29 exec/s: 0 rss: 41Mb L: 4/29 MS: 2 ChangeBinInt-EraseBytes-
#13055  REDUCE cov: 298 ft: 550 corp: 132/1210b lim: 29 exec/s: 0 rss: 41Mb L: 14/29 MS: 4 ShuffleBytes-CrossOver-PersAutoDi
#13112  NEW    cov: 303 ft: 555 corp: 133/1236b lim: 29 exec/s: 0 rss: 41Mb L: 26/29 MS: 2 CrossOver-InsertRepeatedBytes-
#13118  REDUCE cov: 303 ft: 555 corp: 133/1234b lim: 29 exec/s: 0 rss: 41Mb L: 14/29 MS: 1 EraseBytes-
#13161  NEW    cov: 304 ft: 556 corp: 134/1245b lim: 29 exec/s: 0 rss: 41Mb L: 11/29 MS: 3 PersAutoDict-CMP-EraseBytes- DE:
#13192  REDUCE cov: 304 ft: 556 corp: 134/1244b lim: 29 exec/s: 0 rss: 41Mb L: 15/29 MS: 1 EraseBytes-
#13213  REDUCE cov: 304 ft: 556 corp: 134/1243b lim: 29 exec/s: 0 rss: 41Mb L: 18/29 MS: 1 EraseBytes-
#13237  REDUCE cov: 304 ft: 556 corp: 134/1242b lim: 29 exec/s: 0 rss: 41Mb L: 9/29 MS: 4 InsertByte-ChangeBit-EraseBytes-Co
#13269  REDUCE cov: 304 ft: 556 corp: 134/1241b lim: 29 exec/s: 0 rss: 41Mb L: 20/29 MS: 2 ChangeByte-EraseBytes-
#13290  NEW    cov: 304 ft: 557 corp: 135/1270b lim: 29 exec/s: 0 rss: 41Mb L: 29/29 MS: 1 ShuffleBytes-
#13297  REDUCE cov: 307 ft: 560 corp: 136/1292b lim: 29 exec/s: 0 rss: 41Mb L: 22/29 MS: 2 CMP-ChangeBit- DE: "\000\000\000\
#13430  NEW    cov: 307 ft: 561 corp: 137/1316b lim: 29 exec/s: 0 rss: 41Mb L: 24/29 MS: 3 CopyPart-CrossOver-CopyPart-
#13436  REDUCE cov: 307 ft: 561 corp: 137/1312b lim: 29 exec/s: 0 rss: 41Mb L: 22/29 MS: 1 EraseBytes-
#13538  REDUCE cov: 307 ft: 562 corp: 138/1335b lim: 29 exec/s: 0 rss: 41Mb L: 23/29 MS: 2 InsertByte-ChangeBinInt-
#13601  REDUCE cov: 307 ft: 562 corp: 138/1334b lim: 29 exec/s: 0 rss: 41Mb L: 22/29 MS: 3 ShuffleBytes-ChangeByte-EraseByte
#13622  NEW    cov: 307 ft: 563 corp: 139/1346b lim: 29 exec/s: 0 rss: 41Mb L: 12/29 MS: 1 CrossOver-
#13643  REDUCE cov: 307 ft: 563 corp: 139/1342b lim: 29 exec/s: 0 rss: 41Mb L: 17/29 MS: 1 CrossOver-
```

Target 1: “unaware”

```
#![no_main]

use libfuzzer_s

use dress_up::S

fuzz_target!(|d

    let suit =

    if let Ok(e
        let _ =
    }
});
```

```
er/FuzzerLoop.cpp:910:21
    #30 0x596270ebd80b in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long))
rDriver.cpp:923:10
    #31 0x596270ecee2d in main /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/libfuzzer-sy
    #32 0x7e47aa629d8f  (/lib/x86_64-linux-gnu/libc.so.6+0x29d8f) (BuildId: 22ca0a83a4004122e30a69b597be96e2
    #33 0x7e47aa629e3f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x29e3f) (BuildId: 22ca0a83a400
    #34 0x596270ddda04 in _start (/home/mfink/BA/dress-up/fuzz/target/x86_64-unknown-linux-gnu/release/unaw

SUMMARY: libFuzzer: timeout
────────────────────────────────────────────────────────────────────────────────

Failing input:

        fuzz/artifacts/unaware/timeout-9620fe4bd0a0a7f8e02b384bd704be94c491d45b

Output of `std::fmt::Debug`:

        [216, 107, 191, 216]

Reproduce with:

        cargo fuzz run unaware fuzz/artifacts/unaware/timeout-9620fe4bd0a0a7f8e02b384bd704be94c491d45b

Minimize test case with:

        cargo fuzz tmin unaware fuzz/artifacts/unaware/timeout-9620fe4bd0a0a7f8e02b384bd704be94c491d45b

────────────────────────────────────────────────────────────────────────────────

Error: Fuzz target exited with exit status: 70
```

```
2 ChangeBit-InsertRepeatedBytes-
1 CopyPart-
1 EraseBytes-
3 CrossOver-InsertByte-EraseBytes-
4 InsertRepeatedBytes-ChangeBit-Era
4 InsertByte-ChangeBinInt-PersAutoD
3 CopyPart-EraseBytes-ChangeBinInt-
5 InsertByte-InsertByte-ChangeBinIn
3 ChangeBinInt-ShuffleBytes-EraseBy
2 ChangeBinInt-CopyPart-
 EraseBytes-
 ChangeBinInt-EraseBytes-
4 ShuffleBytes-CrossOver-PersAutoDi
2 CrossOver-InsertRepeatedBytes-
1 EraseBytes-
3 PersAutoDict-CMP-EraseBytes- DE:
1 EraseBytes-
1 EraseBytes-
 InsertByte-ChangeBit-EraseBytes-Co
2 ChangeByte-EraseBytes-
1 ShuffleBytes-
2 CMP-ChangeBit- DE: "\000\000\000\
3 CopyPart-CrossOver-CopyPart-
1 EraseBytes-
2 InsertByte-ChangeBinInt-
3 ShuffleBytes-ChangeByte-EraseByte
1 CrossOver-
1 CrossOver-
```

Target 1: “unaware”

```
#![no_main]

use libfuzzer_s

use dress_up::S

fuzz_target!(|d

    let suit =

    if let Ok(e
        let _ =
    }
});
```

```
er/FuzzerLoop.cpp:910:21
    #30 0x596270ebd80b in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long))
rDriver.cpp:923:10
    #31 0x596270ecee2d in main /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/libfuzzer-sy
    #32 0x7e47aa629d8f  (/lib/x86_64-linux-gnu/libc.so.6+0x29d8f) (BuildId: 22ca0a83a4004122e30a69b597be96e2
    #33 0x7e47aa629e3f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x29e3f) (BuildId: 22ca0a83a400
    #34 0x596270ddda04 in _start (/home/mfink/BA/dress-up/fuzz/target/x86_64-unknown-linux-gnu/release/unaw

SUMMARY: libFuzzer: timeout

────────────────────────────────────────────────────────────────────────────────

Failing input:

        fuzz/artifacts/unaware/timeout-9620fe4bd0a0a7f8e02b384bd704be94c491d45b

Output of `std::fmt::Debug`:

        [216, 107, 191, 216]

Reproduce with:

        cargo fuzz run unaware fuzz/artifacts/unaware/timeout-9620fe4bd0a0a7f8e02b384bd704be94c491d45b

Minimize test case with:

        cargo fuzz tmin unaware fuzz/artifacts/unaware/timeout-9620fe4bd0a0a7f8e02b384bd704be94c491d45b

────────────────────────────────────────────────────────────────────────────────

Error: Fuzz target exited with exit status: 70
```

```
2 ChangeBit-InsertRepeatedBytes-
1 CopyPart-
1 EraseBytes-
3 CrossOver-InsertByte-EraseBytes-
4 InsertRepeatedBytes-ChangeBit-Era
4 InsertByte-ChangeBinInt-PersAutoD
3 CopyPart-EraseBytes-ChangeBinInt-
5 InsertByte-InsertByte-ChangeBinIn
3 ChangeBinInt-ShuffleBytes-EraseBy
2 ChangeBinInt-CopyPart-
 EraseBytes-
 ChangeBinInt-EraseBytes-
4 ShuffleBytes-CrossOver-PersAutoDi
2 CrossOver-InsertRepeatedBytes-
1 EraseBytes-
3 PersAutoDict-CMP-EraseBytes- DE:
1 EraseBytes-
1 EraseBytes-
 InsertByte-ChangeBit-EraseBytes-Co
2 ChangeByte-EraseBytes-
1 ShuffleBytes-
2 CMP-ChangeBit- DE: "\000\000\000\
3 CopyPart-CrossOver-CopyPart-
1 EraseBytes-
2 InsertByte-ChangeBinInt-
3 ShuffleBytes-ChangeByte-EraseByte
1 CrossOver-
1 CrossOver-
```

What caused the timeout?

- Input in Hex: **D8 6B BF D8**
- Issue was only one byte: BF
- CBOR: BF = map with indefinite length

```
Failing input:

        fuzz/artifacts/unaware/timeout-9620fe4bd0

Output of `std::fmt::Debug`:

        [216, 107, 191, 216]

Reproduce with:

        cargo fuzz run unaware fuzz/artifacts/una

Minimize test case with:
```

An example of an indefinite-length map (that happens to have two key/value pairs) might be:

```
0xbf6346756ef563416d7421ff
BF          -- Start indefinite-length map
   63       -- First key, UTF-8 string length 3
      46756e --   "Fun"
   F5       -- First value, true
   63       -- Second key, UTF-8 string length 3
      416d74 --   "Amt"
   21       -- Second value, -2
   FF       -- "break"
```

Source: https://www.rfc-editor.org/rfc/rfc8949.html

Target 1: “unaware”

fix: catch incorrect indefinite maps for the manifest

```
let mut decoder = self.decoder.clone();
let version = decoder
    .map_iter::<i16, Token>()?
    .find_map(|item| match item {
        Ok((key, value)) if key == crate::consts::Manifest::EncodingVersion.into() => {
            Some(value)
let len = decoder.map()?.ok_or(Error::UnexpectedIndefiniteLength {
    position: decoder.position(),
})?;
for _ in 0..len {
    let key = decoder.i16()?;
    if key == crate::consts::Manifest::EncodingVersion.into() {
        let version = decoder.u8()?;
        if version == crate::consts::SUIT_SUPPORTED_VERSION {
            return Ok(version);
        } else {
            return Err(Error::UnsupportedManifestVersion);
```

fix: end iterator on errors in item

```
298 298     impl<'a, S: AuthState> Envelope<'a, S> {
299 299         fn get_object(&self, search_key: SuitEnvelope) -> Result<Option<&'a ByteSlice>, Error> {
300 300             let mut decoder = self.decoder.clone();
301     -           Ok(decoder
    301 +           decoder
302 302                 .map_iter::<i16, &ByteSlice>()?
303 303                 .find_map(|item| match item {
304     -               Ok((key, item)) if key == search_key.into() => Some(item),
    304 +               Ok((key, item)) if key == search_key.into() => Some(Ok(item)),
    305 +               Err(e) => Some(Err(e.into())),
305 306                 _ => None,
306     -           }))
    307 +           })
    308 +           .transpose()
307 309         }
308 310
309 311         fn get_object_wrapped(&self, search_key: SuitEnvelope) -> Result<Option<&'a ByteSlice>, Error> {
```

Target 1: “unaware”

```
fix: catch incorrect indefinite maps for the manifest
```

```
let mut decoder = self.decoder.clone();
let version = decoder
    .map_iter::<i16, Token>()?
    .find_map(|item| match item {
        Ok((key, value)) if key == crate::consts::Manifest::EncodingVersion.into
            Some(value)
let len = decoder.map()?.ok_or(Error::UnexpectedIndefiniteLength {
    position: decoder.position(),
})?;
for _ in 0..len {
    let key = decoder.i16()?;
    if key == crate::consts::Manifest::EncodingVersion.into() {
        let version = decoder.u8()?;
        if version == crate::consts::SUIT_SUPPORTED_VERSION {
            return Ok(version);
        } else {
            return Err(Error::UnsupportedManifestVersion);
```

```
fix: end iterator on errors in item
```

```
298 298  impl<'a, S: AuthState> Envelope<'a, S> {
299 299      fn get_object(&self, search_key: SuitEnvelope) -> Result<Option<&'a ByteSlice>, Error> {
300 300          let mut decoder = self.decoder.clone();
301      -       Ok(decoder
                                                    p_iter::<i16, &ByteSlice>()?
                                                    nd_map(|item| match item {
                                                    Ok((key, item)) if key == search_key.into() => Some(item),
                                                    Ok((key, item)) if key == search_key.into() => Some(Ok(item)),
                                                    Err(e) => Some(Err(e.into())),
                                                    _ => None,
                                                    anspose()
                                                    ct_wrapped(&self, search_key: SuitEnvelope) -> Result<Option<&'a ByteSlice>, Error> {
```

Source: https://media.tenor.com/ks12xrf_3rgAAAAM/nice-michael-rosen.gif

Target 1: “unaware”

Filename	Regions	Missed Regions	Cover
auth.rs	67	37	44.78%
cbor.rs	16	0	100.00%
command.rs	709	709	0.00%
component.rs	118	118	0.00%
consts.rs	87	87	0.00%
digest.rs	170	165	2.94%
error.rs	101	91	9.90%
lib.rs	133	34	74.44%
manifest.rs	406	406	0.00%
manifeststate.rs	227	227	0.00%
operatinghooks.rs	24	24	0.00%
report.rs	25	25	0.00%
TOTAL	2083	1923	7.68%

Target 1: “unaware”

```rust
// test functions on unauthenticated manifest
if let Ok(envelope) = suit.envelope() {
    if let Ok(manifest) = envelope.manifest() {
        let _ = manifest.version();
        let _ = manifest.sequence_number();
    }
}

// test functions on authenticated manifest
if let Ok(suit) = suit.authenticate(|cose, payload| {···
}) {
    if let Ok(envelope) = suit.envelope() {
        if let Ok(manifest) = envelope.manifest() {
            let _ = manifest.has_payload_fetch();
            let _ = manifest.has_payload_installation();
            let _ = manifest.has_image_validation();
            let _ = manifest.has_image_loading();
            let _ = manifest.has_invoke();

            let _ = match fun_select % 6 {
                0 => manifest.execute_payload_fetch(&hooks),
                1 => manifest.execute_payload_installation(&hooks),
                2 => manifest.execute_image_validation(&hooks),
                3 => manifest.execute_image_loading(&hooks),
                4 => manifest.execute_invoke(&hooks),
                5 => manifest.execute_full(&hooks),
                _ => unreachable!(),
            };
        }
    }
```

Filename	Regions	Missed Regions	Cover
auth.rs	67	12	82.09%
cbor.rs	16	0	100.00%
command.rs	709	709	0.00%
component.rs	118	118	0.00%
consts.rs	87	87	0.00%
digest.rs	170	68	60.00%
error.rs	103	90	12.62%
lib.rs	133	11	91.73%
manifest.rs	406	343	15.52%
manifeststate.rs	227	227	0.00%
operatinghooks.rs	24	24	0.00%
report.rs	25	25	0.00%
TOTAL	2085	1714	17.79%

Source: https://www.thebiglebow.ski/stills/13-with-text.jpg

Where is my coverage?

```
48  1   pub(crate) fn authenticate<F>(&self, authenticate: F) -> Result<(), Error>
49  1   where
50  1       F: Fn(&[u8], &[u8]) -> Result<bool, Error>,
51      {
52  1       let mut decoder = self.decoder.clone();
53  1       for _ in 0..self.num_auth {
54  1           let auth_block = decoder.bytes()?;
55  0           let res = authenticate(auth_block, self.digest)?;
56  0           if res {
57  0               return Ok(());
58  0           }
59      }
60  0   Err(Error::AuthenticationFailure)
61  1   }
```

```
let suit = SuitManifest::from_bytes(&input);

if let Ok(suit) = suit.authenticate(|cose, payload| {
    let mut verify = CoseMessage::new_sign();
    verify.bytes = cose.to_vec();
    verify
        .init_decoder(Some(payload.to_vec()))
        .map_err(|_| Error::AuthenticationFailure)?;
    verify.key(&key).map_err(|_| Error::AuthenticationFailure)?;
    verify
        .decode(None, None)
        .map_err(|_| Error::AuthenticationFailure)?;
    Ok(true)
}) {
    if let Ok(envelope) = suit.envelope() {
        if let Ok(manifest) = envelope.manifest() {
```

Where is my coverage?

```
48  1   pub(crate) fn authenticate<F>(&self, authenticate: F) -> Result<(), Error>
49  1   where
50  1       F: Fn(&[u8], &[u8]) -> Result<bool, Error>,
51      {
52  1       let mut decoder = self.decoder.clone();
53  1       for _ in 0..self.num_auth {
54  1           let auth_block = decoder.bytes()?;
55  0           let res = authenticate(auth_block, self.digest)?;
56  0           if res {
57  0               return Ok(());
58  0           }
59      }
60  0   Err(Error::AuthenticationFailure)
61  1   }
```

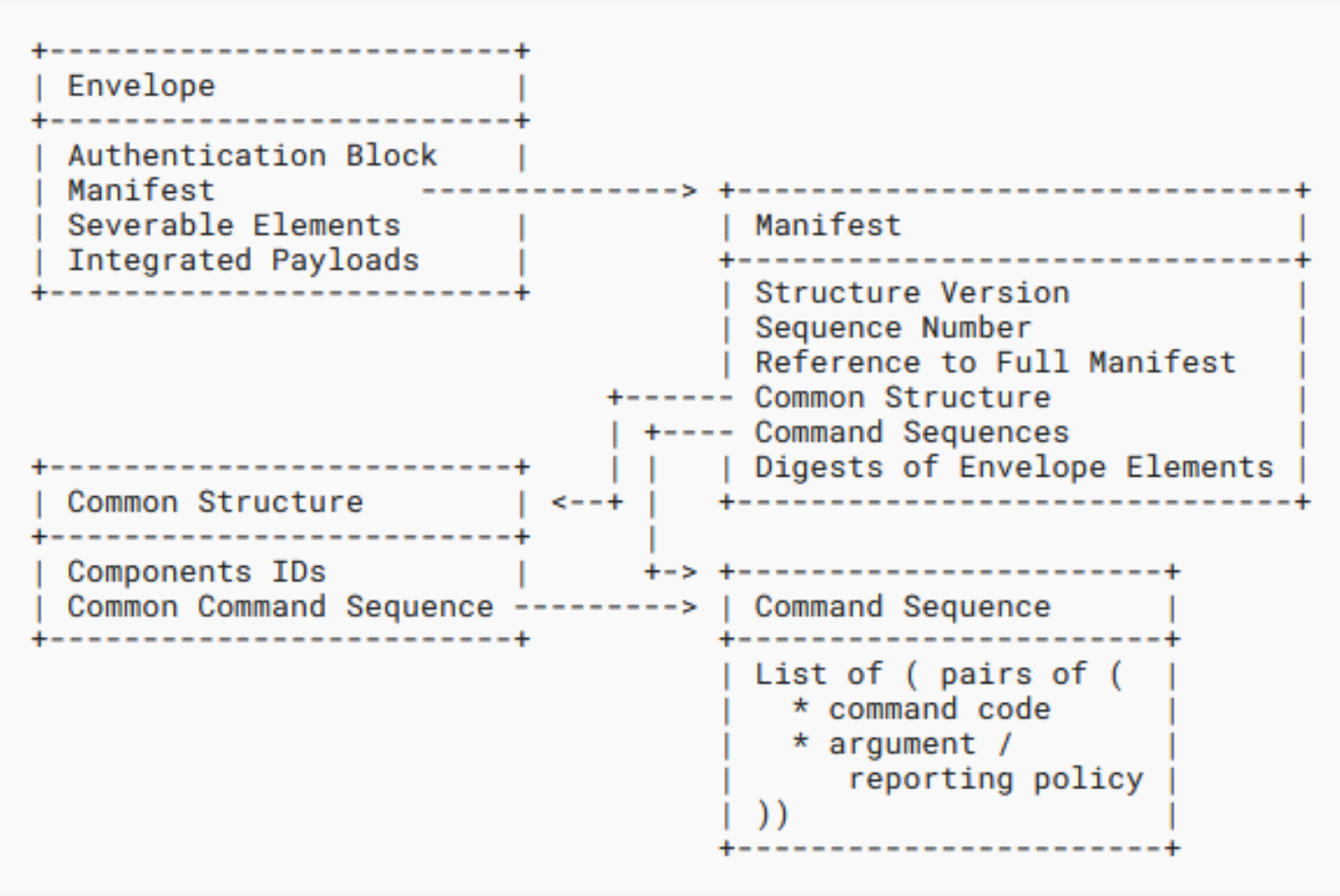
```
let suit = SuitManifest::from_bytes(&input);

if let Ok(suit) = suit.authenticate(|_cose, _payload| {
    // let mut verify = CoseMessage::new_sign();
    // verify.bytes = cose.to_vec();
    // verify
    //     .init_decoder(Some(payload.to_vec()))
    //     .map_err(|_| Error::AuthenticationFailure)?;
    // verify.key(&key).map_err(|_| Error::AuthenticationFailure)?;
    // verify
    //     .decode(None, None)
    //     .map_err(|_| Error::AuthenticationFailure)?;
    Ok(true)
}) {
    if let Ok(envelope) = suit.envelope() {
        if let Ok(manifest) = envelope.manifest() {
```

Where is my coverage?

Filename	Regions	Missed Regions	Cover
auth.rs	67	12	82.09%
cbor.rs	16	0	100.00%
command.rs	709	709	0.00%
component.rs	118	118	0.00%
consts.rs	87	87	0.00%
digest.rs	170	68	60.00%
error.rs	103	90	12.62%
lib.rs	133	11	91.73%
manifest.rs	406	343	15.52%
manifeststate.rs	227	227	0.00%
operatinghooks.rs	24	24	0.00%
report.rs	25	25	0.00%
TOTAL	2085	1714	17.79%

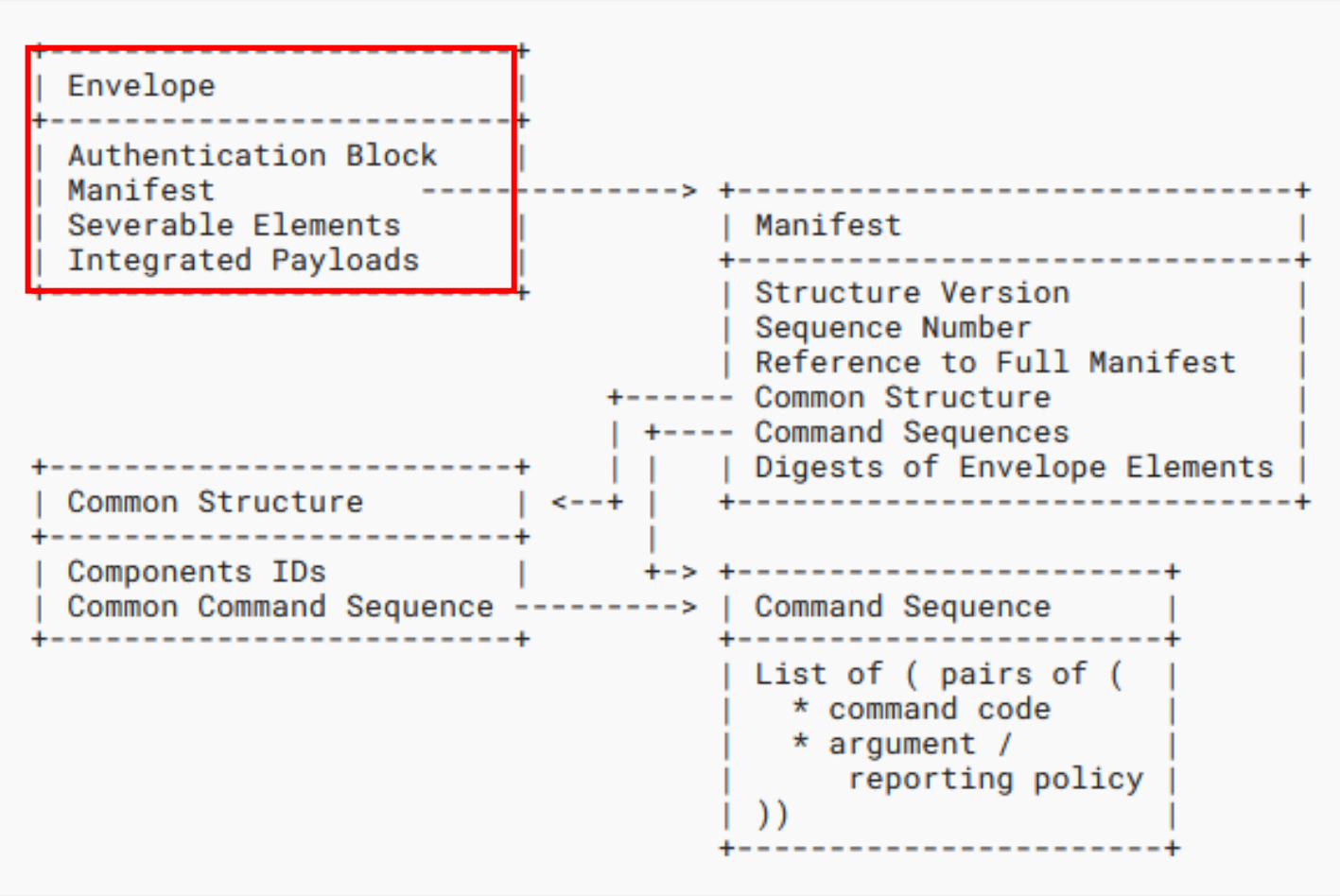
Would have been too easy!

Where is my coverage?



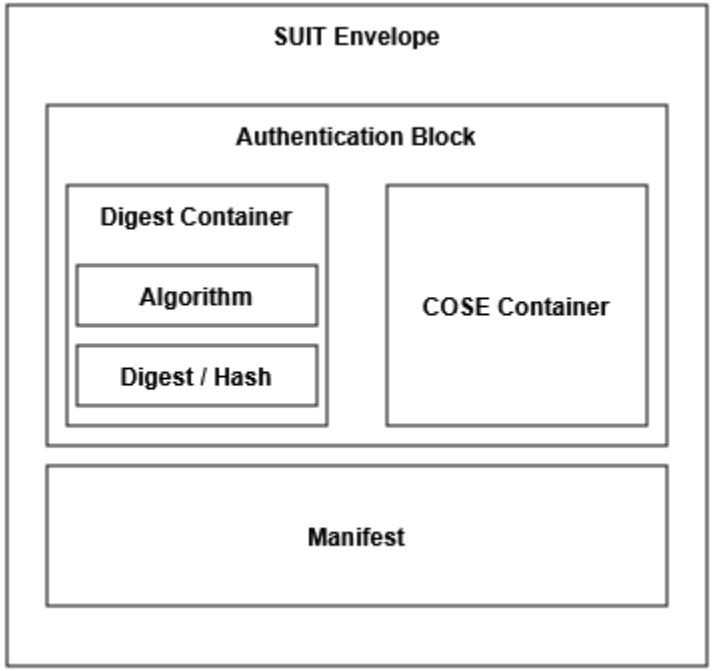
Source: https://www.ietf.org/archive/id/draft-ietf-suit-manifest-37.html

Where is my coverage?

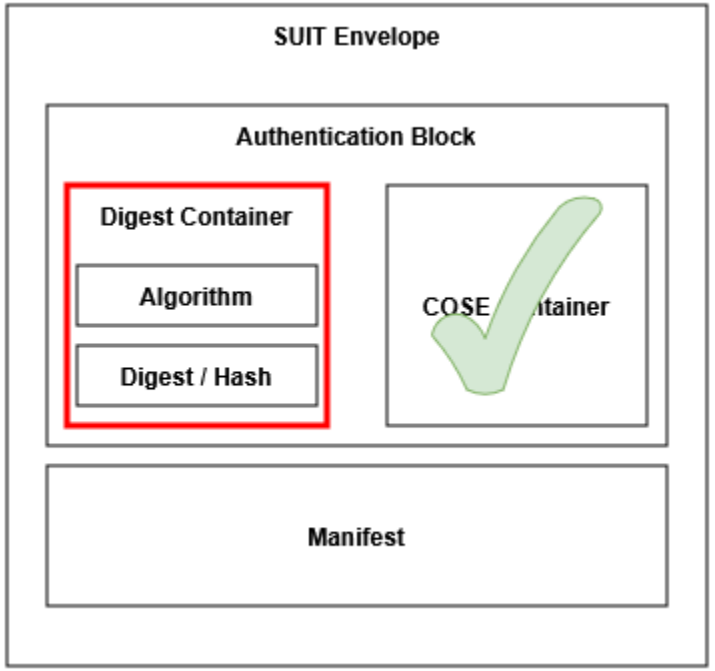


Source: https://www.ietf.org/archive/id/draft-ietf-suit-manifest-37.html

Where is my coverage?



Where is my coverage?



Target 2: “envlp_wrap”

Target 2: “envlp_wrap”

- Take generated bytes
- Treat them as “inner manifest”
- Build valid Envelope around
- Use that as input

```rust
// repair auth-constraint by wrapping inner manifest
// in valid SUIT envelope with valid auth block
let input = build_envelope(data, hash_alg);

let suit = SuitManifest::from_bytes(&input);

// circumvent COSE authentication by just returning true
if let Ok(suit) = suit.authenticate(|_cose, _payload| Ok(true)) {
    if let Ok(envelope) = suit.envelope() {
        if let Ok(manifest) = envelope.manifest() {
            let _ = manifest.has_payload_fetch();
```

```rust
pub fn build_envelope(manifest: &[u8], alg: HashAlg) -> Vec<u8> {
    let auth_block: Vec<u8> = gen_auth(manifest, alg);

    // --- envelope header ---
    let mut envlp: Vec<u8> = vec![];
    envlp.extend(iter: suit::MANIFEST_TAG); // Tag for SUIT Manifest
    envlp.push(cbor::map(2)); // map with 2 entries

    // --- auth block header ---
    envlp.push(labels::envelope_elements::AUTHENTICATION_WRAPPER); // envelop key
    "Authentication"
    envlp.extend(iter: cbor_bstr_header(auth_block.len())); // auth block length

    // --- auth block ---
    envlp.extend_from_slice(&auth_block);

    // --- manifest header ---
    envlp.push(labels::envelope_elements::MANIFEST); // envelop key "Manifest"
    envlp.extend(iter: cbor_bstr_header(manifest.len())); // manifest length
```

Target 2: “envlp_wrap”

- Take generated by
- Treat them as “inn
- Build valid Envelo
- Use that as input

```
ALARM: working on the last Unit for 5 seconds
       and the timeout value is 5 (use -timeout=N to change)
==712523== ERROR: libFuzzer: timeout after 5 seconds
    #0 0x5612a33edf91 in __sanitizer_print_stack_trace /rustc/llvm/src/llvm-project/compiler-rt/lib/asan/asan_stack.cpp:87:3
    #1 0x5612a3492453 in fuzzer::PrintStackTrace() /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/libfuzze
    #2 0x5612a346be8b in fuzzer::Fuzzer::AlarmCallback() /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/li
    #3 0x5612a346bee2 in fuzzer::Fuzzer::StaticAlarmCallback() /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b5
    #4 0x5612a347395a in fuzzer::AlarmHandler(int, siginfo_t*, void*) /home/mfink/.cargo/registry/src/index.crates.io-1949cf
    #5 0x72a642e4251f  (/lib/x86_64-linux-gnu/libc.so.6+0x4251f) (BuildId: 22ca0a83a4004122e30a69b597be96e134068616)
    #6 0x5612a3366aa6 in SetShadow /rustc/llvm/src/llvm-project/compiler-rt/lib/asan/asan_fake_stack.cpp:35:17
    #7 0x5612a3366aa6 in OnMalloc /rustc/llvm/src/llvm-project/compiler-rt/lib/asan/asan_fake_stack.cpp:280:3
    #8 0x5612a3366aa6 in __asan_stack_malloc_3 /rustc/llvm/src/llvm-project/compiler-rt/lib/asan/asan_fake_stack.cpp:323:1
    #9 0x5612a342d8f1 in <minicbor::decode::decoder::ArrayIter<dress_up::component::Component> as core::iter::traits::iterat
minicbor-2.2.1/src/decode/decoder.rs
    #10 0x5612a342fdd0 in <dress_up::component::ComponentIter as core::iter::traits::iterator::Iterator>::next /home/mfink/B
    #11 0x5612a341969b in next<dress_up::component::ComponentIter> /home/mfink/.rustup/toolchains/nightly-2026-04-20-x86_64-
:27
    #12 0x5612a341969b in <dress_up::manifest::Manifest<dress_up::Authenticated>>::execute_section_with_common::<suit_fuzz_a
    #13 0x5612a341ee17 in execute_invoke<suit_fuzz_auth_stra1::OsHooks> /home/mfink/BA/dress-up/src/manifest.rs:238:14
    #14 0x5612a341ee17 in suit_fuzz_auth_stra1::_::__libfuzzer_sys_run /home/mfink/BA/dress-up/fuzz/fuzz_targets/suit_fuzz_a
    #15 0x5612a3422a83 in rust_fuzzer_test_input /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/libfuzzer-
    #16 0x5612a3466c14 in {closure#0} /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/libfuzzer-sys-0.4.12/
    #17 0x5612a3466c14 in std::panicking::catch_unwind::do_call::<libfuzzer_sys::test_input_wrap::{closure#0}, i32> /home/mf
st/library/std/src/panicking.rs:581:40
    #18 0x5612a3467c8b in __rust_try libfuzzer_sys.40b1348255557a02-cgu.0
    #19 0x5612a34661dd in catch_unwind<i32, libfuzzer_sys::test_input_wrap::{closure_env#0}> /home/mfink/.rustup/toolchains/
cking.rs:544:19
    #20 0x5612a34661dd in catch_unwind<libfuzzer_sys::test_input_wrap::{closure_env#0}, i32> /home/mfink/.rustup/toolchains/
c.rs:359:14
    #21 0x5612a34661dd in LLVMFuzzerTestOneInput /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/libfuzzer-
    #22 0x5612a346c1a7 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) /home/mfink/.cargo/registry/s
:15
    #23 0x5612a3475e1b in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /home/mfink/.cargo/registry/src/ir
    #24 0x5612a347e53e in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned long)) /home/mfink/.car
rDriver.cpp:871:19
    #25 0x5612a348fefd in main /home/mfink/.cargo/registry/src/index.crates.io-1949cf8c6b5b557f/libfuzzer-sys-0.4.12/libfuzz
    #26 0x72a642e29d8f  (/lib/x86_64-linux-gnu/libc.so.6+0x29d8f) (BuildId: 22ca0a83a4004122e30a69b597be96e134068616)
    #27 0x72a642e29e3f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x29e3f) (BuildId: 22ca0a83a4004122e30a69b597be
    #28 0x5612a3358d54 in _start (/home/mfink/BA/dress-up/fuzz/target/x86_64-unknown-linux-gnu/release/suit_fuzz_auth_stra1+

SUMMARY: libFuzzer: timeout

Error: Fuzz target exited with exit status: 70
```

```
nifest

rning true
ayload| Ok(true)) {

t() {
();
```

```
Vec<u8> {

UIT Manifest

_WRAPPER); // envelop key

)); // auth block length

envelop key "Manifest"
; // manifest length
```

What caused this timeout?

```
    for (idx: usize, component: Result<Component<'_>, Error>) in ComponentIter::new(&mut component_decoder)
     Result…
        .map_err(|e: Error| e.add_offset(common.component_offset))? ComponentIter<'_, '_>
        .enumerate()
    {
        if let Ok(component: Component<'_>) = component {
            let idx: u32 = idx.try_into().map_err(|_| Error::UnexpectedCbor {
                position: self.decoder.position(),
            })?;
            let component_info: ComponentInfo<'_> = ComponentInfo::new(component, index: idx);

            let state: ManifestState<'_> = common.shared_sequence().execute(
                start_state.clone(),
                &component_info,
                os_hooks,
            )?;
            command_section.execute(state, &component_info, os_hooks)?;
        }
    }
    Ok(())
} fn execute_section_with_common
```

What caused this timeout?

```
fix: return error from ComponentIter to prevent infinite loop on malformed manifest (#17)
```

```
181  -              if let Ok(component) = component {
182  -                  let idx = idx.try_into().map_err(|_| Error::UnexpectedCbor {
183  -                      position: self.decoder.position(),
184  -                  })?;
185  -                  let component_info = ComponentInfo::new(component, idx);
186  -
187  -                  let state = common.shared_sequence().execute(
188  -                      start_state.clone(),
189  -                      &component_info,
190  -                      os_hooks,
191  -                  )?;
192  -                  command_section.execute(state, &component_info, os_hooks)?;
193  -              }
     181  +              let component = component.map_err(|e| e.add_offset(common.component_offset))?;
     182  +
     183  +              let idx = idx.try_into().map_err(|_| Error::UnexpectedCbor {
     184  +                  position: self.decoder.position(),
     185  +              })?;
     186  +              let component_info = ComponentInfo::new(component, idx);
     187  +
     188  +              let state =
     189  +                  common
     190  +                      .shared_sequence()
     191  +                      .execute(start_state.clone(), &component_info, os_hooks)?;
     192  +              command_section.execute(state, &component_info, os_hooks)?;
```

Target 2: “envlp_wrap”

Filename	Regions	Missed Regions	Cover
auth.rs	67	11	83.58%
cbor.rs	16	0	100.00%
command.rs	709	657	7.33%
component.rs	118	95	19.49%
consts.rs	87	87	0.00%
digest.rs	170	109	35.88%
error.rs	103	86	16.50%
lib.rs	133	29	78.20%
manifest.rs	406	100	75.37%
manifeststate.rs	227	227	0.00%
operatinghooks.rs	24	24	0.00%
report.rs	25	25	0.00%
TOTAL	2085	1450	30.46%

Target 2: “envlp_wrap”

Filename	Regions	Missed Regions	Cover
auth.rs	67	11	83.58%
cbor.rs	16	0	100.00%
command.rs	709	657	7.33%
component.rs	118	95	19.49%
consts.rs	87	87	0.00%
digest.rs	170	109	35.88%
error.rs	103	86	16.50%
lib.rs	133	29	78.20%
manifest.rs	406	100	75.37%
manifeststate.rs	227	227	0.00%
operatinghooks.rs	24	24	0.00%
report.rs	25	25	0.00%
TOTAL	2085	1450	30.46%

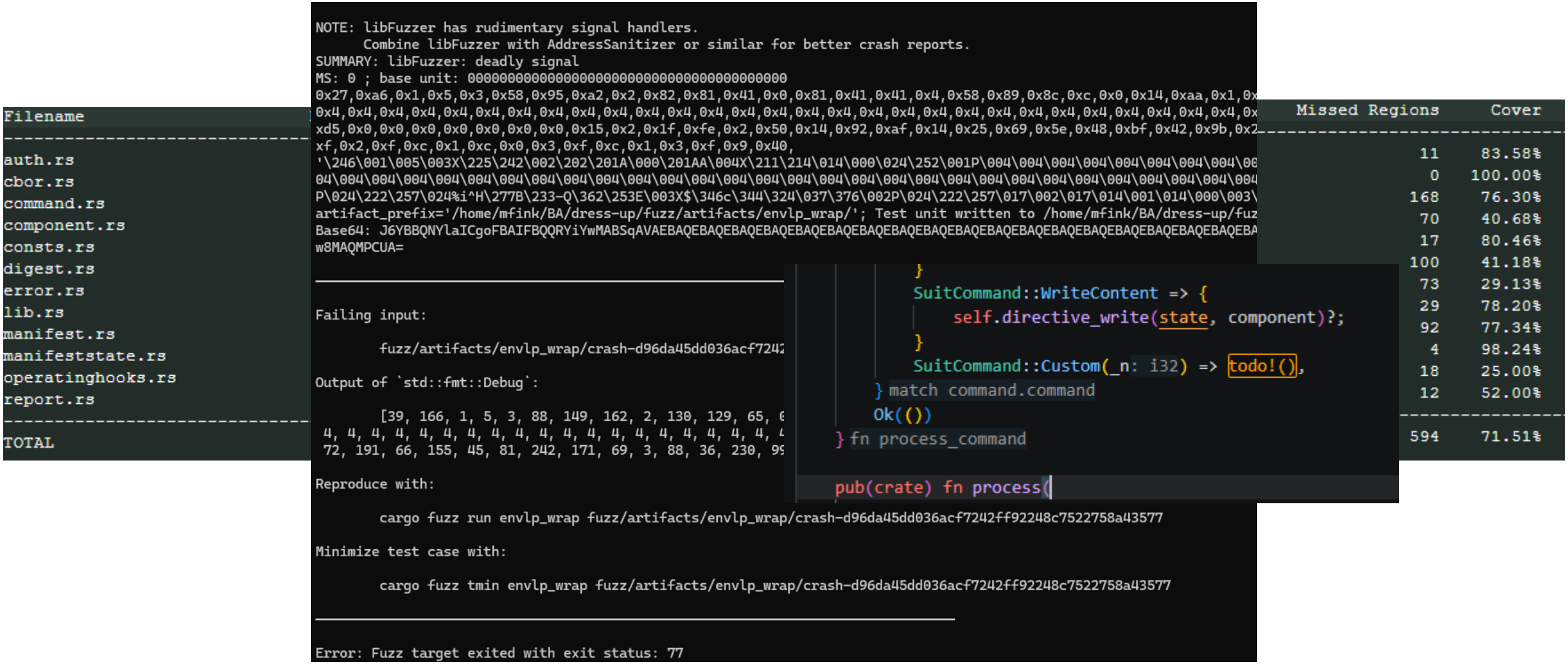
Filename	Regions	Missed Regions	Cover
auth.rs	67	11	83.58%
cbor.rs	16	0	100.00%
command.rs	709	168	76.30%
component.rs	118	70	40.68%
consts.rs	87	17	80.46%
digest.rs	170	100	41.18%
error.rs	103	73	29.13%
lib.rs	133	29	78.20%
manifest.rs	406	92	77.34%
manifeststate.rs	227	4	98.24%
operatinghooks.rs	24	18	25.00%
report.rs	25	12	52.00%
TOTAL	2085	594	71.51%

Target 2: “envlp_wrap”

```
NOTE: libFuzzer has rudimentary signal handlers.
      Combine libFuzzer with AddressSanitizer or similar for better crash reports.
SUMMARY: libFuzzer: deadly signal
MS: 0 ; base unit: 0000000000000000000000000000000000000000
0x27,0xa6,0x1,0x5,0x3,0x58,0x95,0xa2,0x2,0x82,0x81,0x41,0x0,0x81,0x41,0x41,0x4,0x58,0x89,0x8c,0xc,0x0,0x14,0xaa,0x1,0x
0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x
xd5,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x15,0x2,0x1f,0xfe,0x2,0x50,0x14,0x92,0xaf,0x14,0x25,0x69,0x5e,0x48,0xbf,0x42,0x9b,0x2
xf,0x2,0xf,0xc,0x1,0xc,0x0,0x3,0xf,0xc,0x1,0x3,0xf,0x9,0x40,
'\246\001\005\003X\225\242\002\202\201A\000\201AA\004X\211\214\014\000\024\252\001P\004\004\004\004\004\004\004\004\00
04\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004
P\024\222\257\024%i^H\277B\233-Q\362\253E\003X$\346c\344\324\037\376\002P\024\222\257\017\002\017\014\001\014\000\003\
artifact_prefix='/home/mfink/BA/dress-up/fuzz/artifacts/envlp_wrap/'; Test unit written to /home/mfink/BA/dress-up/fuz
Base64: J6YBBQNYlaICgoFBAIFBQQRYiYwMABSqAVAEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBA
w8MAQMPCUA=

────────────────────────────────────────────────────────────────────

Failing input:

        fuzz/artifacts/envlp_wrap/crash-d96da45dd036acf7242ff92248c7522758a43577

Output of `std::fmt::Debug`:

        [39, 166, 1, 5, 3, 88, 149, 162, 2, 130, 129, 65, 0, 129, 65, 65, 4, 88, 137, 140, 12, 0, 20, 170, 1, 80, 4, 4
 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 250, 1
 72, 191, 66, 155, 45, 81, 242, 171, 69, 3, 88, 36, 230, 99, 228, 212, 31, 254, 2, 80, 20, 146, 175, 15, 2, 15, 12, 1,

Reproduce with:

        cargo fuzz run envlp_wrap fuzz/artifacts/envlp_wrap/crash-d96da45dd036acf7242ff92248c7522758a43577

Minimize test case with:

        cargo fuzz tmin envlp_wrap fuzz/artifacts/envlp_wrap/crash-d96da45dd036acf7242ff92248c7522758a43577

────────────────────────────────────────────────────────────────────

Error: Fuzz target exited with exit status: 77
```

Filename	Missed Regions	Cover
auth.rs	11	83.58%
cbor.rs	0	100.00%
command.rs	168	76.30%
component.rs	70	40.68%
consts.rs	17	80.46%
digest.rs	100	41.18%
error.rs	73	29.13%
lib.rs	29	78.20%
manifest.rs	92	77.34%
manifeststate.rs	4	98.24%
operatinghooks.rs	18	25.00%
report.rs	12	52.00%
TOTAL	594	71.51%

Target 2: “envlp_wrap”



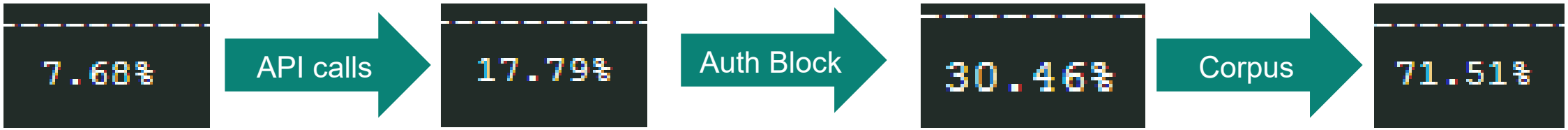
```
Filename
--------------------------------
auth.rs
cbor.rs
command.rs
component.rs
consts.rs
digest.rs
error.rs
lib.rs
manifest.rs
manifeststate.rs
operatinghooks.rs
report.rs
--------------------------------
TOTAL
```

```
NOTE: libFuzzer has rudimentary signal handlers.
      Combine libFuzzer with AddressSanitizer or similar for better crash reports.
SUMMARY: libFuzzer: deadly signal
MS: 0 ; base unit: 0000000000000000000000000000000000000000
0x27,0xa6,0x1,0x5,0x3,0x58,0x95,0xa2,0x2,0x82,0x81,0x41,0x0,0x81,0x41,0x41,0x4,0x58,0x89,0x8c,0xc,0x0,0x14,0xaa,0x1,0x
0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x4,0x
xd5,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x0,0x15,0x2,0x1f,0xfe,0x2,0x50,0x14,0x92,0xaf,0x14,0x25,0x69,0x5e,0x48,0xbf,0x42,0x9b,0x2
xf,0x2,0xf,0xc,0x1,0xc,0x0,0x3,0xf,0xc,0x1,0x3,0xf,0x9,0x40,
'\246\001\005\003X\225\242\002\202\201A\000\201AA\004X\211\214\014\000\024\252\001P\004\004\004\004\004\004\004\004\00
04\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004\004
P\024\222\257\024%i^H\277B\233-Q\362\253E\003X$\346c\344\324\037\376\002P\024\222\257\017\002\017\014\001\014\000\003\
artifact_prefix='/home/mfink/BA/dress-up/fuzz/artifacts/envlp_wrap/'; Test unit written to /home/mfink/BA/dress-up/fuz
Base64: J6YBBQNYlaICgoFBAIFBQQRYiYwMABSqAVAEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBA
w8MAQMPCUA=

Failing input:

        fuzz/artifacts/envlp_wrap/crash-d96da45dd036acf7242

Output of `std::fmt::Debug`:

        [39, 166, 1, 5, 3, 88, 149, 162, 2, 130, 129, 65, 0
 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4,
 72, 191, 66, 155, 45, 81, 242, 171, 69, 3, 88, 36, 230, 99

Reproduce with:

        cargo fuzz run envlp_wrap fuzz/artifacts/envlp_wrap/crash-d96da45dd036acf7242ff92248c7522758a43577

Minimize test case with:

        cargo fuzz tmin envlp_wrap fuzz/artifacts/envlp_wrap/crash-d96da45dd036acf7242ff92248c7522758a43577

Error: Fuzz target exited with exit status: 77
```

```
                }
                SuitCommand::WriteContent => {
                    self.directive_write(state, component)?;
                }
                SuitCommand::Custom(_n: i32) => todo!(),
            } match command.command
            Ok(())
        } fn process_command

    pub(crate) fn process(
```

Missed Regions	Cover
11	83.58%
0	100.00%
168	76.30%
70	40.68%
17	80.46%
100	41.18%
73	29.13%
29	78.20%
92	77.34%
4	98.24%
18	25.00%
12	52.00%
594	71.51%

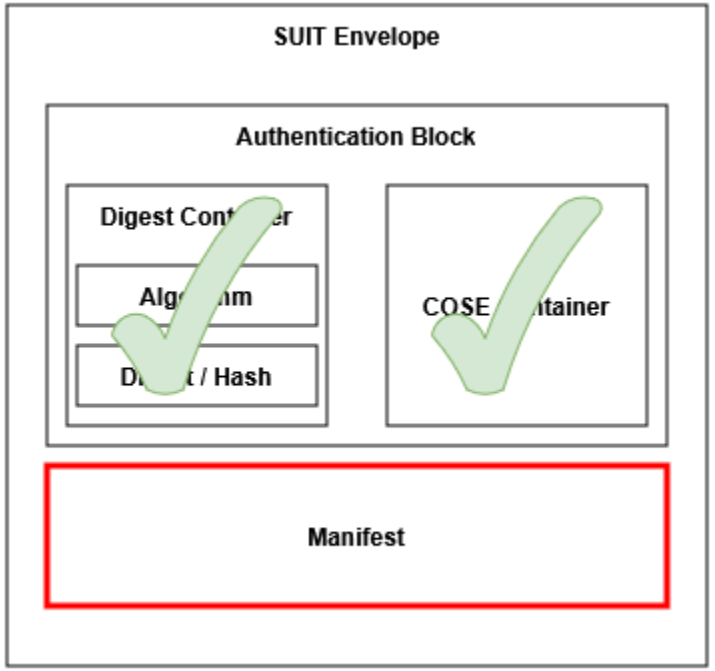
Recap



Source: https://a.pinatafarm.com/1920x950/fce2488035/kylo-ren-more.jpg

Target 3: “manifest_gen”

Target 3: “manifest_gen”



Target 3: “manifest_gen”

- **Idea:** create “skeleton” of a valid manifest
- Fill fields with fuzzer-generated input
- Build envelope around
- Use this as input

```rust
let vendor_id: &[u8] = &data[4..20];
let class_id: &[u8] = &data[20..36];
let img_hash: &[u8] = &data[36..68];
let img_size: [u8; 2] = [data[68], data[69]];

// create common data block
let common_data: Vec<u8> = build_common_data(comp_ident, vendor_id, class_id, img_hash, &img_size);

// create command sequences
let com_seq_val: Vec<u8> = build_command_seq(label: labels::manifest_elements::IMAGE_VALIDATION);
let com_seq_inv: Vec<u8> = build_command_seq(label: labels::manifest_elements::IMAGE_INVOCATION);

// build manifest structure
let mut manifest: Vec<u8> = vec![];
manifest.push(consts::cbor::map(5)); // map containing all of the manifest

// --- suit-manifest-version ---
manifest.push(labels::manifest_elements::ENCODING_VERSION);
manifest.push(version);

// --- suit-manifest-sequence-number ---
manifest.push(labels::manifest_elements::SEQUENCE_NUMBER);
```

Filename	Regions	Missed Regions	Cover
auth.rs	67	11	83.58%
cbor.rs	16	1	93.75%
command.rs	709	493	30.47%
component.rs	118	93	21.19%
consts.rs	87	60	31.03%
digest.rs	170	109	35.88%
error.rs	103	86	16.50%
lib.rs	133	29	78.20%
manifest.rs	406	115	71.67%
manifeststate.rs	227	125	44.93%
operatinghooks.rs	24	24	0.00%
report.rs	25	14	44.00%
TOTAL	2085	1160	44.36%

Target 3: “manifest_gen”

- **Next step:** make manifest generation more dynamic

- Dynamic Elements
- Random bytes as payload
- Dynamic command sequence
- Dynamic common data block

- Decisions based on input bytes

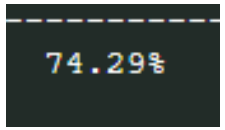
- **Still not finished**

Filename	Regions	Missed Regions	Cover
auth.rs	67	11	83.58%
cbor.rs	16	0	100.00%
command.rs	709	270	61.92%
component.rs	118	70	40.68%
consts.rs	87	17	80.46%
digest.rs	170	100	41.18%
error.rs	103	73	29.13%
lib.rs	133	29	78.20%
manifest.rs	406	92	77.34%
manifeststate.rs	227	4	98.24%
operatinghooks.rs	24	18	25.00%
report.rs	25	12	52.00%
TOTAL	2085	696	66.62%

Comparison

Target	Total LoC	Coverage (11h)	Bugs found
unaware	55	17.79%	1
envlp_wrap	444	70.79%	1
manifest_gen	903	66.38%	0

Coverage of all targets combined:



What did we learn?

What did we learn?

- Provide a corpus for your fuzzer
- Different levels oft structure-awareness make sense
- More structure-awareness = more complexity
- **Here:** partial structure-awareness had best trade-off


Infineon