What’s fuzzing, and how can I find bugs while watching Netflix?

Workshop - 12th of April, Fontys

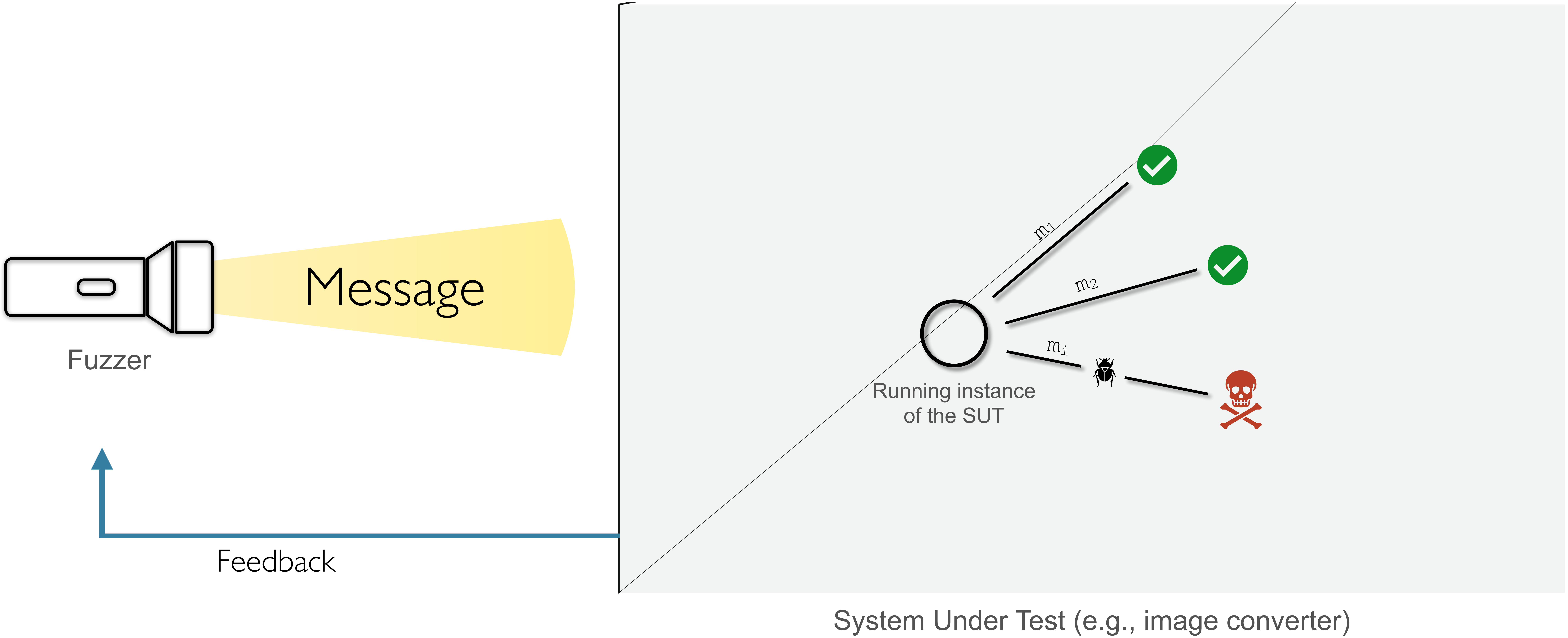
Cristian Daniele, Radboud University - Netherlands

About us

- Third-year PhD at Radboud University, Netherlands
- Doing research in fuzzing (mostly stateful fuzzing)
- Interested in state-model learning

Contact us! :)

What’s fuzzing?


Message
Fuzzer
Feedback
m_1
m_2
m_i
Running instance of the SUT
System Under Test (e.g., image converter)

History of fuzzing

1988 - first fuzzer

2013 - AFL

2015 - OSS-Fuzz

General components

Crafter

System Under Test (SUT)

Anomaly Detector

Different categories

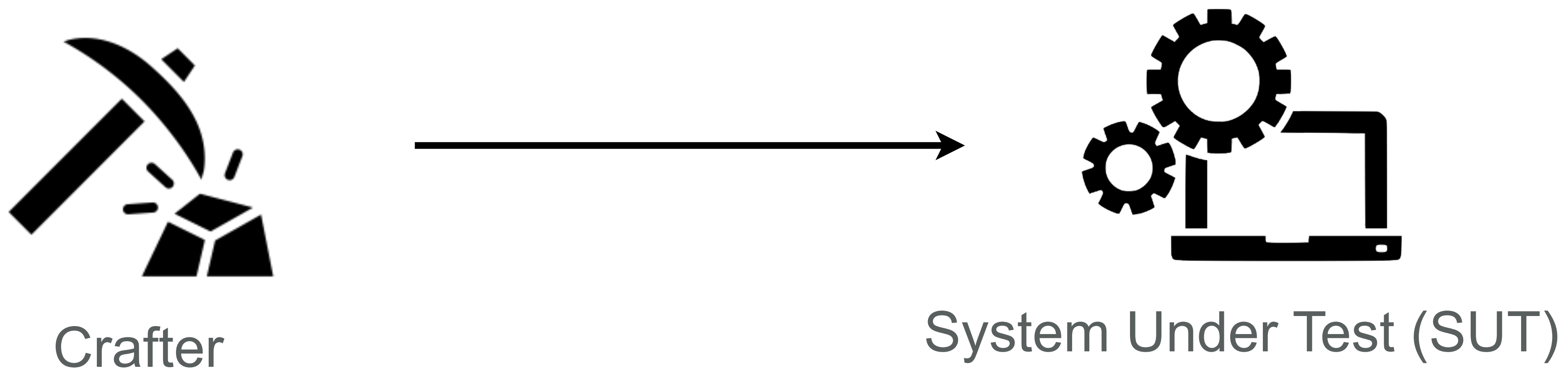
?

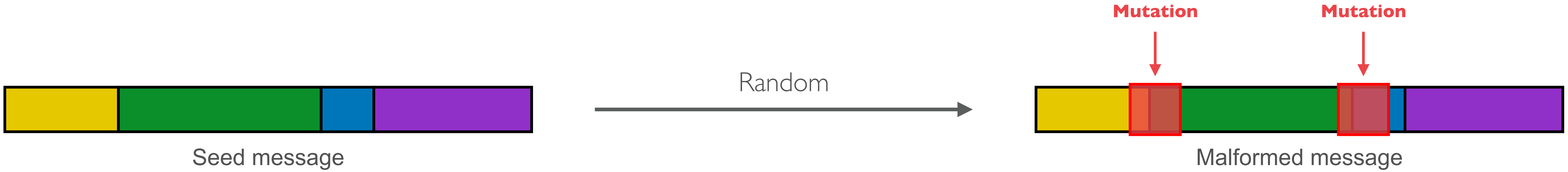
Dumb mutational

Grammar-based

Smart mutational (or evolutionary)

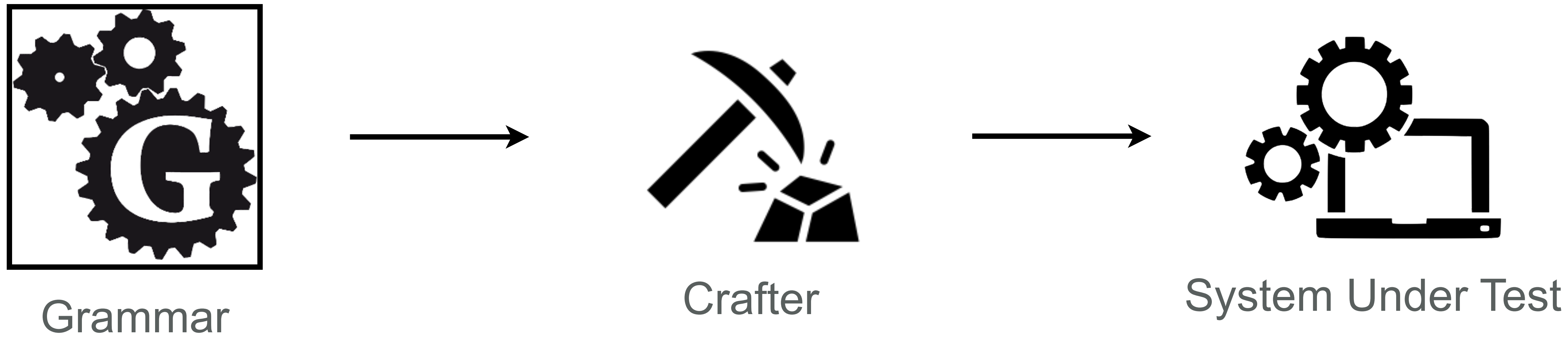
Dumb mutational

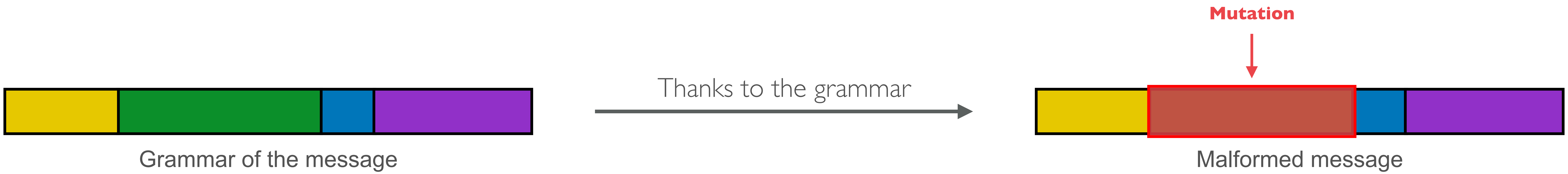




Experiment with zzuf

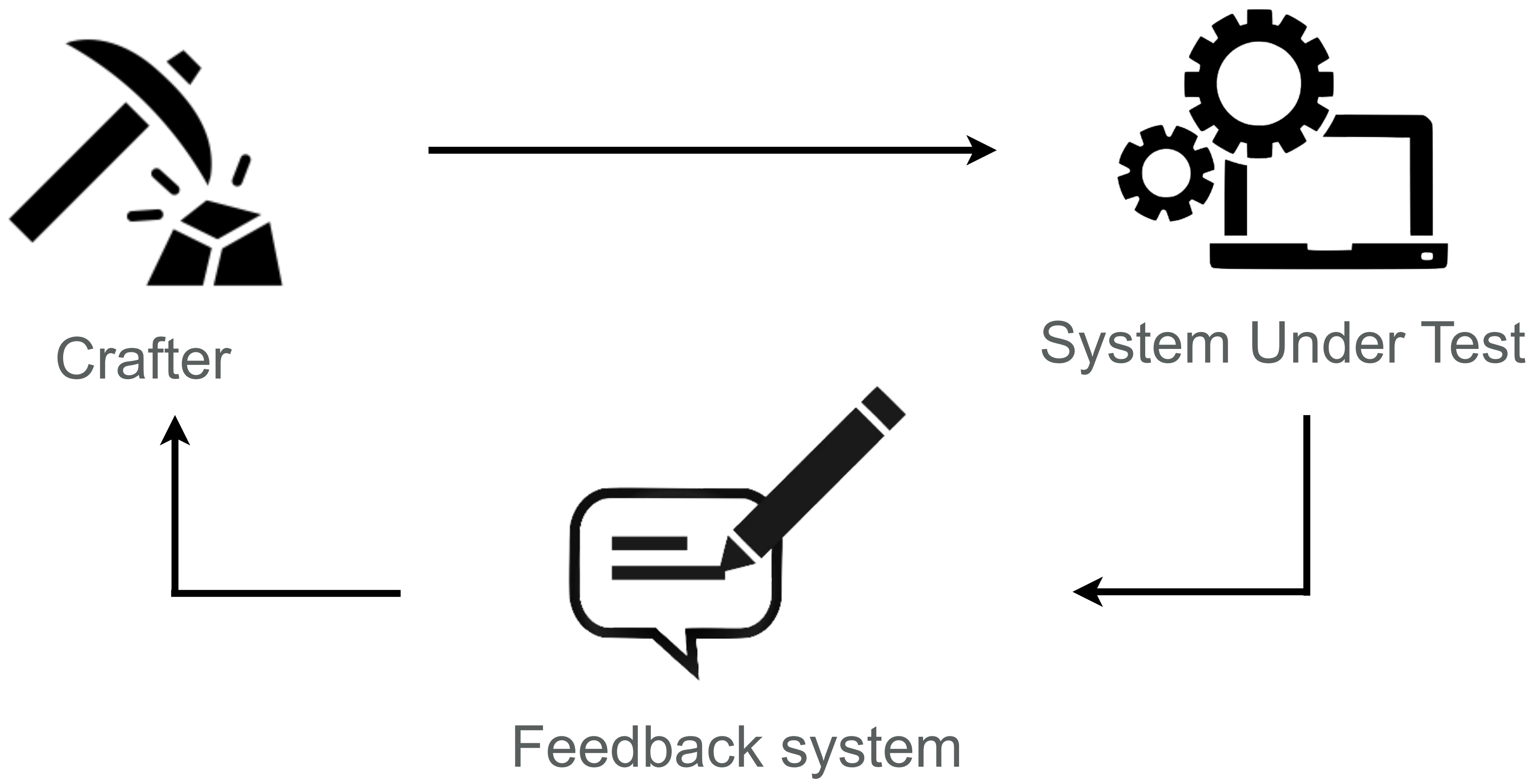
Grammar-based

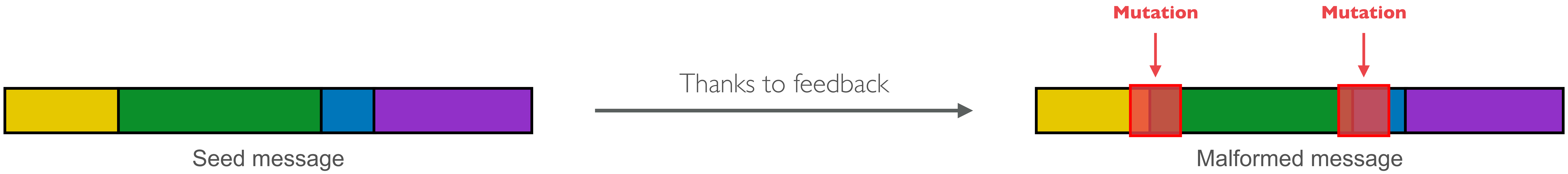




Experiment with BooFuzz

Evolutionary

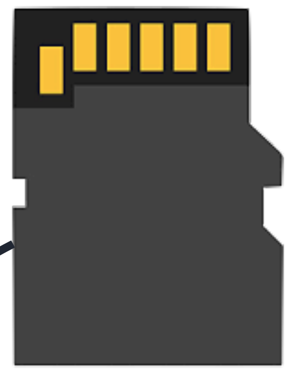




Experiment with AFL++

LUNCH

An overview about sanitisers

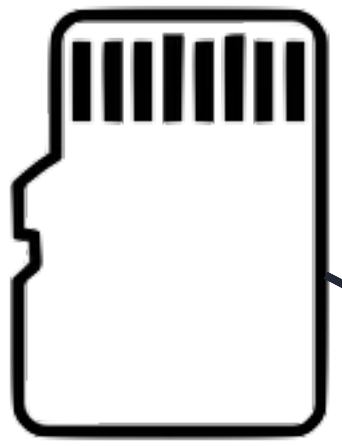


AddressSanitizer (ASan)

- Buffer overflow
- Use-after-free
- Memory corruption bugs
- …

Undefined BehaviorSanitizer (UBSan)

- Divisions by zero
- Accessing uninitialised variables
- …



MemorySanitizer (MSan)

- Uninitialised memory

ThreadSanitizer

- Critical races
- Synchronisation issues
- …