A Fuzzing-Based Test-Creation Approach for Evaluating Digital TV Receivers via Transport Streams

Fabrício Izumi†, Eddie B. de Lima Filho†, Lucas Cordeiro‡, Orlewilson Maia†,
Rômulo Fabrício†, Bruno Farias‡, and Aguinaldo Silva
†*TPV Technology*, Manaus, Brazil
‡*The University of Manchester*, Manchester, UK
{fabricio.bandeira,eddie.filho,orlewilson.maia,romulo.fabricio,aguinaldo.silva}@tpv-tech.com
{lucas.cordeiro,bruno.farias}@manchester.ac.uk

***Abstract*—Many digital TV (DTV) broadcasters inadvertently misconfigure their devices and transmit wrong information, which may cause incorrect receiver behavior. Moreover, the way those problems are usually introduced in DTV signals presents some randomness, which resembles fuzzing techniques. This scenario is addressed here, which led to a novel receiver robustness evaluation methodology based on non-compliance tests using grammar-based guided fuzzing. Experiments with such a scheme have shown its efficacy and provided opportunities to improve robustness regarding commercial DTV platforms.**

***Index Terms*—Digital TV, Fuzzing, Robustness Testing, Transport Stream, Testing Methodology**

I. Overview

Field problems, i.e., malfunction events in commercial products, usually affect end-user experiences and after-sales costs in digital TV (DTV) environments. A further investigation revealed that several of them were caused by combinations of incorrect information and the way controlling software interacts with it, resembling how fuzz testing is performed.

This perception led to the development of a methodology that creates tests with an approach based on grammar-based guided fuzzing, aiming to identify improvement opportunities concerning robustness [1]. It relies on a structured environment that includes test generation and transmission, device-under-test configuration, and result evaluation.

Figure 1 illustrates the proposed test-generation strategy, where problems and grammar are sent to a fuzzer that generates robustness tests in three groups: field problems, parameters configured in commercial equipment, and critical data with high flexibility. New tests are randomly created with knowledge regarding those three aspects and applicable format specifications, from scratch, which results in error regions.

We have implemented the proposed methodology and carried out experiments with 5 different commercial platforms, whose manufacturers represent 80% of the Brazilian DTV market, finding weaknesses in all of them. The most severe problems seem to be related to the media decoding, which caused a failure rate of 100% in one test platform, and PSI/SI data parts. Our methodology was also compared with an existing popular fuzzing tool named Peach, uncovering more

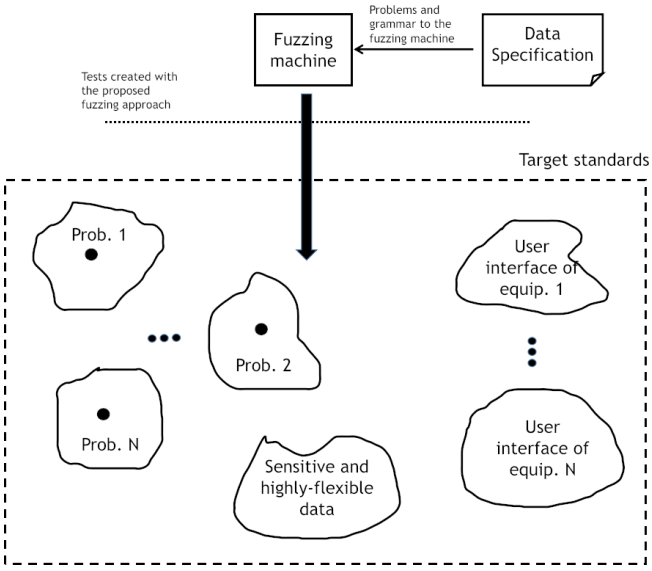

Fig. 1. The proposed strategy for test creation.

fragile parts than the latter. Our experiments also provide a snapshot of commercial platforms sold in Brazil, which can be even more comprehensive due to the software reuse practice.

For future work, other problem groups will be developed, and enhancements to the underlying fuzzer will be provided.

We believe that our paper is suitable for presentation in this journal-first track as it was published in Software Testing, Verification, and Reliability at the end of 2022, tackles test automation and generation using fuzzing, reports completely new research and results in the testing area, and has never been presented or submitted to other journal-first programs.

References

[1] Fabricio Izumi, Eddie B. de Lima Filho, Lucas C. Cordeiro, Orlewilson Maia, Rômulo Fabrício, Bruno Farias, and Aguinaldo Silva, "A fuzzing-based test-creation approach for evaluating digital TV receivers via transport streams," Softw. Test. Verif. Reliab., vol. 33, n. 1, pp. 1–31, Sep. 2022.