Recycling Test Cases to Detect Security Vulnerabilities

João Antunes and Nuno Neves

Abstract: The design of new protocols and features, e.g., in the context of organizations such as the IETF, produces a flow of novel standards and amendments that lead to ever changing implementations. These implementations can be difficult to test for security vulnerabilities because existing tools often lag behind. In the paper, we propose a new methodology that addresses this issue by recycling test cases from several sources, even if aimed at distinct protocols. It resorts to protocol reverse engineering techniques to build parsers that are capable of extracting the relevant payloads from the test cases, and then applies them to new test cases tailored to the particular features that need to be checked. An evaluation with 10 commercial and open-source testing tools and a large set of FTP vulnerabilities shows that our approach is able to get better or equal vulnerability coverage than the original tools. In a more detailed experiment with two fuzzers, our solution showed an improvement of 19% on vulnerability coverage when compared with the two combined fuzzers, being capable of finding 25 additional vulnerabilities.