Project References

Project Acronym	XIVT		
Project Title	eXcellence In Variant Testing		
Project Number	17039		
Project Start Date	November 1, 2018	Project Duration	36 months
Project Manager	Gunnar Widforss, Bombardier Transportation, Sweden		
Website	https://www.xivt.org/		

Document References

Work package	WP3: Testing of Configurable Products		
Deliverable	D3.4: Tool for fault and attack injection in variant and configurable systems – initial version		
Deliverable type	Software (SW)		
Dissemination level	Public	Date & Version	Oct 31 st, 2020 V1.0
Mapped tasks	T3.4 Fuzzing and security testing in configurable systems		

Executive Summary

This deliverable includes the initial version of the tools that are developed and extended in the XIVT project in the scope of WP3 for testing the security of variant and configurable systems.

Access Information

XIVT project has its repository on Gitlab at: https://gitlab.com/xivt

The following D3.4 tools are accessible at https://gitlab.com/xivt/itea with username: ITEA3XIVT & password: 20222018XIVT

DeltaFuzzer Tool (FCUL)

DeltaFuzzer is a grey-box fuzzer based on AFL that is able to detect several classes of vulnerabilities, which might appear in software programmed in C/C++. It is a fuzzer that implements a *Targeted Fuzzer Approach,* allowing the tool to focus the testing on pre-identified parts of the code (e.g., lines that change between two variants) and reuse knowledge acquired in previous testing campaigns.

DeltaFuzzer generates a testcase (through various mutation strategies of existing testcases) for running it in the software under test (SUT) and collects various runtime metrics. Next, it uses the metrics to determine if the testcase is capable of uncovering new execution paths towards the targets, saving it in the affirmative case, and reusing it to generate other testcases. If the program suffers a failure, such as a crash or a hang, the testcase is saved as it is capable of uncovering a SUT bug.

DeltaFuzzer is under development as part of the solution to XIVT use cases that run C/C++ programs in theirs variant and configurable systems. DeltaFuzzer will help teams detect software security faults and vulnerabilities in their programs in order to improve their security and turn them more reliable. Currently, the tool implements the minimal functionality to perform targeted fuzzing, but it still requires further evaluation and testing to remove potential remaining bugs. For the next release, we intend to revise the current testcase scheduling policy of the fuzzer and enhance the data flow analysis capabilities.

Webpage: N/A

Source or Binary Link: https://gitlab.com/xivt/itea/deltafuzzer

Instruction manual for the tool: (same as above)

Type: Closed Source

Additional Info: N/A