An Efficient Greybox Fuzzing Scheme for Linux-based IoT Programs Through Binary Static Analysis

Submitted by grigby1 on Mon, 03/23/2020 - 4:16pm

Title
An Efficient Greybox Fuzzing Scheme for Linux-based IoT Programs Through Binary Static Analysis

Publication Type
Conference Paper

Year of Publication
2019

Authors
Zheng, Yaowen, Song, Zhanwei, Sun, Yuyan, Cheng, Kai, Zhu, Hongsong, Sun, Limin

Conference Name
2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)

Date Published
oct

Keywords
binary static analysis, effective vulnerability discovery technique, embedded security, firmware, fuzzing, Internet of Things, IoT firmware kernel greybox fuzzer, IoT program greybox fuzzing, Linux, Linux-based IoT program, Metrics, program diagnostics, pubcrawl, real-world Linux-based IoT programs, resilience, Resiliency, Router Systems Security, security of data, static binary analysis, vulnerabilities discovery

Abstract
With the rapid growth of Linux-based IoT devices such as network cameras and routers, the security becomes a concern and many attacks utilize vulnerabilities to compromise the devices. It is crucial for researchers to find vulnerabilities in IoT systems before attackers. Fuzzing is an effective vulnerability discovery technique for traditional desktop programs, but could not be directly applied to Linux-based IoT programs due to the special execution environment requirement. In our paper, we propose an efficient greybox fuzzing scheme for Linux-based IoT programs which consist of two phases: binary static analysis and IoT program greybox fuzzing. The binary static analysis is to help generate useful inputs for efficient fuzzing. The IoT program greybox fuzzing is to reinforce the IoT firmware kernel greybox fuzzer to support IoT programs. We implement a prototype system and the evaluation results indicate that our system could automatically find vulnerabilities in real-world Linux-based IoT programs efficiently.

DOI
10.1109/IPCCC47392.2019.8958740

Citation Key zheng_efficient_2019