

Evaluation von Modernen Fuzzing Ansätzen und Frameworks

Eine Literaturübersicht

Sebastian Peschke**

sebastian.peschke@hof-university.de

Institut für Informationssysteme Hof

Hof, Bayern, Germany

ABSTRACT

A clear and well-documented \LaTeX document is presented as an article formatted for publication by ACM in a conference proceedings or journal publication. Based on the “acmart” document class, this article presents and explains many of the common variations, as well as many of the formatting elements an author may use in the preparation of the documentation of their work.

KEYWORDS

Fuzzing, Testing, Automation, Security, Machine Learning, Reverse Engineering, Network Security, Binary Analysis, Vulnerability Detection, Exploit Generation, Program Analysis, Program Optimization

ACM Reference Format:

Sebastian Peschke. 2024. Evaluation von Modernen Fuzzing Ansätzen und Frameworks: Eine Literaturübersicht. *J. ACM* 37, 4, Article 420 (January 2024), ?? pages. <https://doi.org/10.1145/36420>

1 EINFÜHRUNG

2 HINTERGRUND

2.1 Fuzzing Herangehensweisen

2.1.1 *Black Box Fuzzing.*

2.1.2 *White Box Fuzzing.*

2.1.3 *Grey Box Fuzzing.*

2.2 Sparten des Fuzzing

2.2.1 *IoT Fuzzing.*

2.2.2 *Firmware Fuzzing.*

2.2.3 *Binary Fuzzing.*

2.2.4 *Netzwerkprotokoll Fuzzing.*

2.2.5 *Betriebssystem Fuzzing.*

*

Author’s address: Sebastian Peschke, sebastian.peschke@hof-university.de, Institut für Informationssysteme Hof, Hof, Bayern, Germany.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.

0004-5411/2024/1-ART420 \$15.00

<https://doi.org/10.1145/36420>

3 UNTERSCHIEDUNG VON FUZZING-ANSÄTZEN

3.1 Input Generation

3.2 Intelligenz des Fuzzers

3.3 Explorationsstrategien

4 RECHERCHE

evtl doch Diskussion?

5 KONKLUSION