

Technische Berichte des Hasso-Plattner-Instituts für
Softwaresystemtechnik an der Universität Potsdam

Lena Feinbube | Daniel Richter | Sebastian Gerstenberg |
Patrick Siegler | Angelo Haller | Andreas Polze

Software-Fehlerinjektion

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.dnb.de/> abrufbar.

Universitätsverlag Potsdam 2016

<http://verlag.ub.uni-potsdam.de/>

Am Neuen Palais 10, 14469 Potsdam

Tel.: +49 (0)331 977 2533 / Fax: 2292

E-Mail: verlag@uni-potsdam.de

Die Schriftenreihe **Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam** wird herausgegeben von den Professoren des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam.

ISSN (print) 1613-5652

ISSN (online) 2191-1665

Das Manuskript ist urheberrechtlich geschützt.

Druck: docupoint GmbH Magdeburg

ISBN 978-3-86956-386-2

Zugleich online veröffentlicht auf dem Publikationsserver der Universität Potsdam:

URN <urn:nbn:de:kobv:517-opus4-97435>

<http://nbn-resolving.de/urn:nbn:de:kobv:517-opus4-97435>

Inhaltsverzeichnis

1	Experimentelle Beurteilung der Verlässlichkeit von Software durch Fehlerinjektion	1
1.1	Software-Fehlerinjektion	2
1.2	Ziel des Berichts	6
2	Fehlerinjektion auf Betriebssystemebene	7
2.1	Historischer Überblick	8
2.2	Zielorte für Fehlerinjektion	9
2.3	Fehlerinjektion durch Stresstests	9
3	Fehlerinjektion in Systemaufrufen	11
3.1	Systemaufruf-Fuzzing am Beispiel von Trinity	12
3.2	Weitere Fuzzing-Werkzeuge für Fehlerinjektion in Systemaufrufen .	14
3.3	Diskussion	15
4	Fehlerinjektion an Bibliotheksschnittstellen	17
4.1	Fehlermodelle für Schnittstellen	17
4.2	Fehlerinjektionsansätze	18
4.3	Diskussion	22
5	Fehlerinjektion in verwaltete Sprachen mit Laufzeitumgebungen	23
5.1	Fehlermodelle	23
5.2	Implementierungsansätze	24
5.3	Diskussion	33
6	Fehlerinjektion in Grafikbeschleuniger	35
6.1	Fehlermodelle und Fehlertoleranzmechanismen für Grafikkarten .	35
6.2	Fehlerinjektion auf Grafikkarten am Beispiel von GPU-Qin	36
6.3	Diskussion	39
7	Zusammenfassung	41