AUF EINEN BLICK

LEISTUNGEN

Im Bereich des Fuzz Testing unterstützt Fraunhofer FOKUS durch verschiedene Leistungen die Entwicklung sicherer Softwareprodukte, u. a. durch:

- die Analyse produktspezifischer Schnittstellen, Protokolle und Dienste sowie die Entwicklung maßgeschneiderter Fuzzing-Heuristiken,
- die Vorbereitung und Durchführung von Sicherheits- und Robustheits-Tests von Softwareprodukten mit Data und Behavioral Fuzzing
- die Unterstützung bei der Einführung von Fuzz Testing in bestehende Testprozesse,
- die Integration von Fuzzino in bestehende Testwerkzeuge,
- eine Security-Risikoanalyse als Grundlage für einen effizienten, risikobasierten Security-Testprozess.

Fuzzino-Basisversion auf GitHub:
https://github.com/fraunhoferfokus/Fuzzino/

FUZZINO

KONTAKT

Dipl.-Inform. Martin Schneider
Geschäftsbereich SQC
Tel. +49 (0)30 3463-7383
Fax +49 (0)30 3463-99 7383
martin.schneider@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de

iku | 1711 (Fotos: Olexandr Taranukhin/shutterstock, Nikada/iStock)

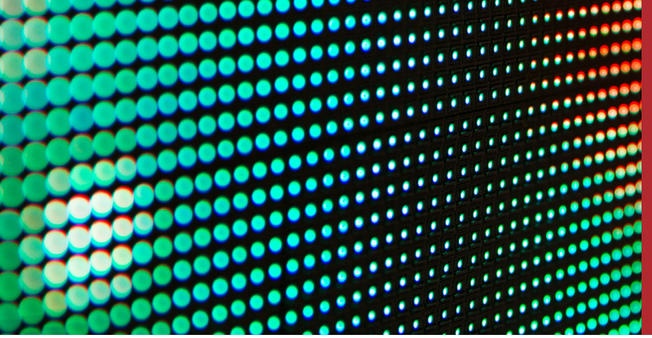
Fraunhofer
FOKUS

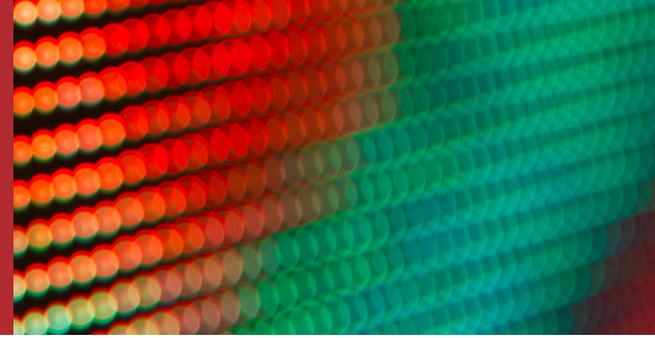
FRAUNHOFER-INSTITUT FÜR
OFFENE KOMMUNIKATIONSSYSTEME FOKUS

SECURITY TESTING MIT FUZZING

HERAUSFORDERUNG

Die zunehmende Vernetzung von Geräten sowie die steigende Komplexität von Systemen stellen Entwickler und Hersteller sicherer Softwareprodukte vor die Herausforderung, dass Sicherheitslücken immer schwieriger zu identifizieren sind. Sicherheitslücken entstehen häufig während der Implementierungsphase. Sie sind potenzielle Ziele von Angreifern und können daher weitreichende Folgen haben. Insbesondere Schwachstellen in ausgelieferten Produkten können lange Zeit unbemerkt ausgenutzt werden. Deren Beseitigung sowie mögliche Schadenersatzforderungen ziehen oft hohe Kosten nach sich und haben einen negativen Einfluss auf die Reputation eines Produkts oder einer Organisation. Prominente Beispiele sind zum Beispiel der Heartbleed-Bug, der die Verschlüsselung eines Großteils des Internets gefährdete, sowie der Bundeshack, bei dem über eine fehlerhafte eLearning-Plattform letztlich das Außenministerium des Bundes angegriffen wurde.



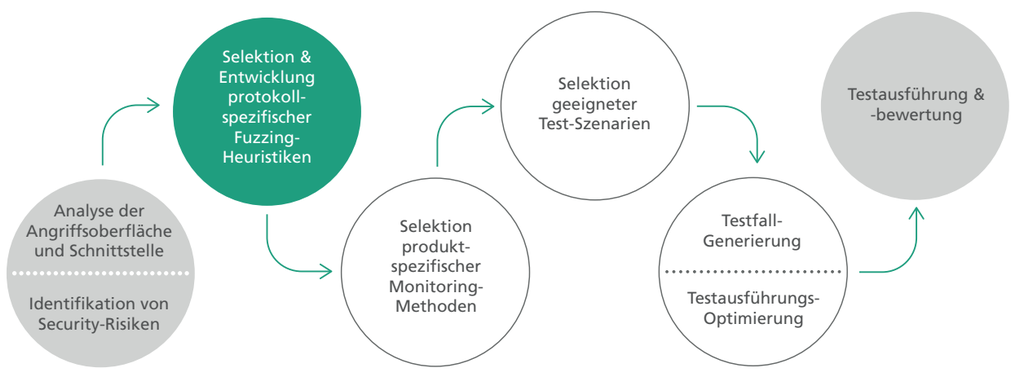


FUZZ TESTING

Security Testing ist in einer vernetzten Welt zu einem Grundbaustein bei der Entwicklung von sicheren Systemen geworden. Dabei hat sich Fuzz Testing (auch Fuzzing) als effektive Technik bewährt, um unbekannte Sicherheitslücken (0-Day-Vulnerabilities) aufzudecken. Fuzzing ist eine Testtechnik, bei dem die Schnittstellen des zu testenden Systems mit ungültigen und unerwarteten Eingaben konfrontiert werden, um so deren Robustheit zu testen.

Zufallsbasiertes Fuzzing ist die einfachste Form, um Sicherheitslücken aufzudecken. Auf Grund der Komplexität des Eingaberaums bietet es jedoch nicht die notwendige Effizienz, um ein System hinreichend zu testen. Smart Fuzzing hingegen nutzt Modelle von Schnittstellen, Protokollen und Diensten, um semi-valide Eingabedaten zu generieren. Damit verringert sich die Anzahl der Testfälle substanziell, wodurch komplexe Fehler schneller aufgedeckt werden.
Ein komplementärer Ansatz ist das von Fraunhofer FOKUS entwickelte Behavioral Fuzzing. Diesem liegt die Idee zu Grunde, dass beispielsweise Sicherheitsmechanismen nicht nur durch die Akzeptanz ungültiger Eingaben umgangen werden können, sondern auch durch die Verarbeitung ungültiger Nachrichten. Im Gegensatz zum traditionellen Fuzz Testing, das sich auf die Generierung ungültiger Eingabedaten fokussiert, werden durch Behavioral Fuzzing ungültige und unerwartete Aufrufe generiert. Dadurch können Fehler aufgedeckt werden, die mit traditionellem Fuzzing nicht identifizierbar sind. So wurden mit Hilfe des Behavioral Fuzzing zum Beispiel Schwachstellen im weit verbreiteten Apache Webserver aufgedeckt.

Abbildung: Fuzzing von der Analyse bis zur Testausführung



FUZZINO

Mit Fuzzino bietet Fraunhofer FOKUS eine Bibliothek an, die Testdaten für Fuzz Testing generiert. Dadurch können bereits im Einsatz befindliche Testwerkzeuge um Fuzzing nahtlos erweitert werden, ohne eine neue Werkzeuglandschaft integrieren zu müssen.
Fuzzino unterstützt das Fuzzing vieler verschiedener Datentypen, die auf Zeichenketten, Zahlen, regulären Ausdrücken und Grammatiken basieren, sowie komplexe Datenstrukturen. Dabei implementiert Fuzzino die Fuzzing-Heuristiken etablierter Open Source-Fuzzing-Tools und stellt darüber hinaus auch ganz neue Heuristiken zur Verfügung, die in verschiedenen Fallstudien erfolgreich evaluiert wurden. Zusätzlich stellt Fuzzino umfangreiche Informationen zu den generierten Fuzz-Testdaten bereit, die eine tiefergehende Untersuchung potenzieller Schwachstellen ermöglichen. Fuzzino ist plattform- und werkzeugübergreifend einsetzbar und bietet sowohl eine API als auch ein XML-basiertes Datenaustauschformat an.

Eine Basisversion von Fuzzino ist auf GitHub verfügbar.

INTEGRATION UND FALLSTUDIEN

Fuzzino wurde von verschiedenen Herstellern in deren Testwerkzeuge integriert. Dazu zählen *do.Atoms*, ein Werkzeug zum modellbasiertem Testen von Dornier Consulting, sowie *TTworkbench*, eine TTCN-3-basierte Testautomatisierungslösung von Spirent.
In diversen Fallstudien unterschiedlichster Domänen wurden die von Fraunhofer FOKUS entwickelten Fuzzing-Lösungen bereits erfolgreich eingesetzt, u. a.:

- im Bereich eHealth für Tests von HL7/IHE PIX und PDQ (kommerziell und Open Source),
- im Bereich Intelligent Transport Systems nach dem ETSI G5-Stack
- Implementierung eines OpenID/OAuth-Authentifizierungsservices
- für den Test eines Bluetooth-Moduls im Automotive-Umfeld,
- für den Test einer Geldbearbeitungsmaschine.