SUCCESS STORY

SCCH
Software Competence Center Hagenberg

Programm: COMET – Competence Centers for Excellent Technologies

Förderlinie: COMET-Zentrum K1

Projekttyp:
StraSE
(Strategic Software Engineering)
2019-2022, strategisch

Bildquelle Fotolia: Industriesoftware muss sicher sein

SICHERE UND ROBUSTE INDUSTRIE-SOFTWARE

MIT SOFTWARE ANALYSEN UND SOFTWARE TESTS

Dass man mit der "Bombardierung" mit Daten, die durch einen Zufallsgenerator erzeugt werden, Computerprogramme zum Absturz bringen kann, nutzen Sicherheitsexperten weltweit zum Schutz derselben. Das Software Competence Center Hagenberg verbindet diese Testmethoden für eine höhere Testabdeckung mit der Analyse der Programme. Dazu wird eine sprachunabhängige Analyse-Plattform des SCCH verwendet (eKNOWS), um Informationen aus dem Quellcode auszulesen und die Testmethoden effektiver einsetzen zu können.

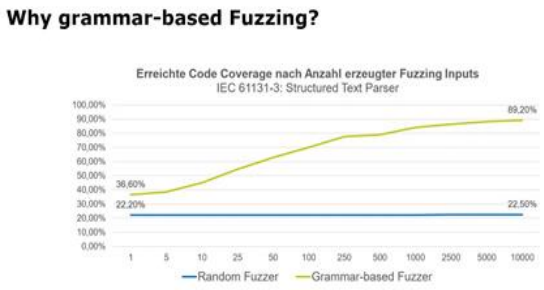
Wirkungen und Effekte

Software wird zunehmend agil entwickelt. Dabei ist die Robustheit gegen Fehler und Angriffe oberstes Ziel, insbesondere bei Softwaresystemen in der Industrie. Daher unterstützen wir die Entwickler dabei, Fehler frühzeitig zu finden und Security in jede Phase des Engineering-Prozesses zu bringen. ‚Fuzzing' oder ‚Fuzzy Testing' gilt als eine der wichtigsten Methoden zur Qualitätssicherung von sicherheitskritischen Programmen. Es wird weltweit von Spezialisten genutzt, um das Auffinden von Sicherheitslücken zu automatisieren. Dabei werden verschiedene Eingabefelder im Programm mit zufälligen, unerwarteten (englisch ‚fuzz') Daten geflutet, um Schwachstellen in der Software aufzudecken. Diese Technik findet Fehler, die sonst übersehen werden. Stürzt das Programm bei bestimmten Daten reproduzierbar ab, wird klar, wo es Daten nicht richtig verarbeiten kann und möglicher-

weise Angriffsfläche für fremden Zugriff bietet. Intelligente Robustheitstests nutzen ein Eingabemodell, um einen höheren Anteil gültiger Eingaben zu generieren und stellen fest, wie sich die Testabdeckung ändert, also welche Teile der Software damit erreicht werden. Sie sind am erfolgreichsten und werden für Syntax- oder Robustheitstests genutzt. Wenn man einen Code analysiert, ist aber nicht auf den ersten Blick erkennbar, welche Daten ein Programm akzeptiert. Für solche Fälle wurde am SCCH eKNOWS (Extracting Knowledge from Software https://www.scch.at/de/eknows) entwickelt. Üblicherweise sind solche Tools nur auf eine Programmiersprache spezialisiert. eKNOWS ist aber eine universelle Plattform mit breiter Sprachunterstützung und eines der wenigen Werkzeuge für Qualitätsanalysen in der Automatisierungsindustrie. Robustheitstests kann man für den Vergleich von Programmen oder Versionen verwenden. Dazu zeichnet man auf, welche Eingabewerte welche Ausgabewerte erzeugen, und das für jede Version oder jene Programme, die man vergleichen will. Dies wird häufig bei der Umstellung alter Produktionssysteme oder Legacy Systems auf moderne IT-Umgebungen angewendet. Für solche Softwaretests verwendet man strukturierte Eingaben. Dafür muss aber für das Testprogramm festgelegt sein, welche Eingaben erlaubt sind (Grammatik). Wenn diese Regeln nicht vorhanden sind, muss man diese erstellen oder durch Analysemethoden herausfinden. Mit der recht jungen Methode des ‚Grammar Minings' geht das SCCH daran, Regeln für gültigen Input aufzustellen.

Universelles Tool für Grammar-based Fuzzing

Um einen höheren Grad an Codeabdeckung zu erreichen, setzt das SCCH auf das kombinierte ‚Grammar-based Fuzzing'. Es wird ein Set an Regeln entwickelt, das den korrekten Input beschreibt und testet, ob das Programm mit diesem Input umgehen kann. Mit absichtlichen Fehlern können spezielle Randfälle gezielt getestet werden, um die Robustheit des Systems festzustellen. Damit kann man dank des sprachunabhängigen ‚Grammar Minings' in der bestehenden Programmierung ein breites Spektrum abdecken, das auch in der Industrie angewendet wird. Erste Tests mit Unternehmenspartnern des SCCH laufen bereits.



Bildquelle SCCH: Auffallend höhere Erfolgsrate mit Grammar-Based-Fuzzing' im Vergleich zu zufälligem 'Fuzzing'

Projektkoordination (Story)
Mag. Martina Höller
Science Communication
Software Competence Center Hagenberg
T +43 50 343 882
martina.hoeller@scch.at

Software Competence Center Hagenberg GmbH
Softwarepark 32a
4232 Hagenberg
T +43 50343
office@scch.at
www.scch.at

Projektpartner

Diese Success Story wurde von der Software Competence Center Hagenberg GmbH und den genannten Projektpartnern zur Veröffentlichung auf der FFG Website freigegeben. Das Software Competence Center Hagenberg wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMK, BMDW, Land Oberösterreich gefördert. Das Programm COMET wird durch die FFG abgewickelt. Weitere Informationen zu COMET: www.ffg.at/comet

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

Österreichische
Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at