SUCCESS STORY

SCCH
Software Competence Center Hagenberg

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET-Centre K1

Type of project:
StraSE
(Strategic Software Engineering)
2019-2022, strategic

Source Fotolia: Industrial software must be reliable

SECURE AND ROBUST INDUSTRIAL SOFTWARE

WITH SOFTWARE ANALYSIS AND SOFTWARE TESTING

The fact that computer programs can be crashed by "bombing" them with data generated by a random generator is used by security experts worldwide to protect them. The Software Competence Center Hagenberg combines these test methods for higher test coverage with the analysis of the programs. For this purpose, a language-independent analysis platform of SCCH is used (eKNOWS) to read information from the source code and to use the test methods more effectively.

Impact and effect

Software is increasingly being developed in an agile manner. Robustness against errors and attacks is the top priority, especially for software systems in industry. Therefore, we support developers in finding errors early on and bringing security into every phase of the engineering process. 'Fuzzing' or 'Fuzzy Testing' is considered one of the most important methods for quality assurance of security-critical programs. It is used by specialists worldwide to automate the detection of security vulnerabilities. It involves flooding various input fields in the program with random, unexpected (English 'fuzz') data to uncover vulnerabilities in the software. This technique finds errors that would otherwise be overlooked. If the program crashes reproducibly on certain data, it becomes clear where it cannot process data properly and may provide attack surfaces for outside access. Intelligent robustness tests use an input model to generate a higher percentage of valid inputs and determine how the test coverage changes, i.e., which parts of the software it reaches. They are most successful and are used for syntax or robustness testing. However, when analyzing a code, it is not obvious at first glance which data a program accepts. For such cases eKNOWS

Federal Ministry
Republic of Austria
Climate Action, Environment, Energy, Mobility, Innovation and Technology

Federal Ministry
Republic of Austria
Digital and Economic Affairs

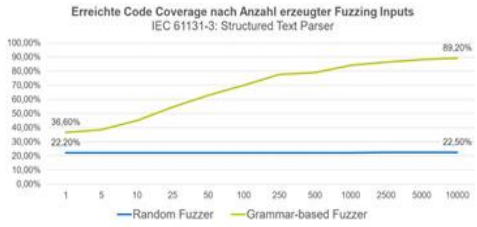
Version 01/2020

(Extracting Knowledge from Software https://www.scch.at/de/eknows) was developed at SCCH. Usually such tools are specialized for only one programming language, but eKNOWS is a universal platform with broad language support and one of the few tools for quality analysis in the automation industry. Robustness tests can be used to compare programs or versions. This is done by recording which input values produce which output values, for each version or those programs that you want to compare. This is often used when converting old production systems or legacy systems to modern IT environments. For such software tests one uses structured inputs. For this, however, it must be defined for the test program which inputs are permitted (grammar). If these rules do not exist, one must create these or find out by analysis methods. With the rather young method of 'grammar mining', SCCH sets out to establish rules for valid input.

Universal tool for grammar-based fuzzing

To achieve a higher degree of code coverage, SCCH relies on combined 'grammar-based fuzzing'. A set of rules is developed that describes the correct input and tests whether the program can handle this input. Intentional errors can be used to specifically test special edge cases to determine the robustness of the system. Thus, thanks to language-independent 'grammar mining' in existing programming, it is possible to cover a broad spectrum that is also used in industry. Initial tests with SCCH's corporate partners are already underway.

Why grammar-based Fuzzing?



Source SCCH: Strikingly higher success rate with 'Grammar-Based-Fuzzing' compared to random 'Fuzzing'

Project coordination (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

Project partner

This success story was provided by the Software Competence Center Hagenberg and by the mentioned project partners for the purpose of being published on the FFG website. Software Competence Center Hagenberg is a COMET Centre within the COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, Upper Austria. The COMET Programme is managed by FFG. Further information on COMET: www.ffg.at/comet