Master / Bachelor

Zusammenhang zwischen Code-Qualität und Sicherheitslücken
Correlation between Code Quality and Vulnerability

This thesis can also be supervised and written in English. For the English version of the announcement see below.

Motivation

Aktuelle Forschung hat sich intensiv mit der statischen Designanalyse objektorientierter Programme beschäftigt. Es wurde gezeigt, dass das initiale Design durch kontinuierliche Änderungen erodiert und diese Erosion zu einem erhöhten Aufwand bei Wartung und Erweiterung des jeweiligen Softwareprojekts führt. Solche erodierten oder aber auch initial schlechte Designs sind durch eine hohe Anzahl an Anti-Pattern gekennzeichnet. Anti-Pattern beschreiben formal und funktional korrekte Implementierungen sowie Softwaredesigns, welche jedoch die Wartbarkeit und Erweiterbarkeit beeinträchtigen. Es wird vermutet, dass der erhöhte Aufwand bei der Wartung und Erweiterung eines mit Anti-Pattern durchsetzten Programms eine direkten Einfluss auf die Häufigkeit von Bugs und Sicherheitslücken hat.

Aufgabenstellung/Ziele

In einer vorangegangenen Abschlussarbeit wurde bereits ein Framework zur Analyse der Korrelation zwischen Qualitäts- und einfachen Sicherheitsmetriken entwickelt [Wie17]. Im Rahmen dieser Arbeit soll basierend auf der vorangegangen Abschlussarbeit untersucht werden, ob die vermutete Korrelation zwischen dem Auftreten von Anti-Pattern und der Häufigkeit von Bugs und Sicherheitslücken existiert. Mögliche Teilziele sind hierbei:

- Automatische Erfassung und Kategorisierung der Häufigkeit von Bugs und Sicherheitslücken aus öffentlichen Issue-Trackern.
- Bewertung der Codequalität sowie Häufigkeit von Bugs und Sicherheitslücken für eine große Anzahl von Open-Source-Projekten.
- Auswertung der gesammelten Daten zur Erfassung möglicher Korrelationen.

Motivation

Recent research has dealt intensively with the static design analysis of object-oriented programs. It has been shown that the initial design of software erodes with continuous changes. This erosion results in an increasing effort for maintenance and expansion of the respective software project. Such eroded software designs but also initially bad designs are typically affected by a high number of anti-patterns. Anti-patterns describe formally and functionally correct implementations and software designs which impair maintainability and extensibility of the program. It is believed that the increased effort for maintenance and extension of a program with many anti-patterns directly results in a increasing vulnerability in terms of an increased amount of bugs and safety gaps.

Objectives

A frameowrk for analyzing the corellation between quality and security metrics has been developed in a previous thesis [Wie17]. The goal of this thesis is to investigate if there is a correlation between code quality in terms of present anti-patterns and the amount of bugs and safety gaps. Conceivable sub-goals are:

- Automatic mining of public issue trackers for collecting data about bugs and safety gabs.
- Rating of code quality, amount of bugs and safety gaps for a high amount of open source projects.
- Evaluation of the collected data to detect possible correlations between code quality and vulnerability.

Organisatorisches

Kontakt:
M.Sc. Sven Peldszus (speldszus@uni-koblenz.de)

Literatur

[Wie17] Brigitte Wiebe. Eine empirische Studie über die Korrelation zwischen Sicherheitsschwachstellen und Qualitätseigenschaften von Software-Designs, 2017. `http://nbn-resolving.de/urn:nbn:de:kola-15455`.