Title: Automatically Diagnosing and Repairing Error Handling Bugs in C
Authors: Yuchi Tian, Baishakhi Ray
Review written by: Doti SandhyaRani

Motivation:

To develop secure and reliable software, correct error handling mechanism is required. However, low-level languages like C do not have any native error handling primitives. Developers are required to write the code to handle the exceptions, which is usually repetitive and complex and leads to error handling bugs. These bugs results in security and reliability faults. The normal testing techniques could not able to identify these bugs, as many of the errors do not appear during regular executions. Hence, researchers developed a tool ***ErrDoc,*** which detects and fixes the error handling bugs.

Proposed Solution:

The paper proposed a tool ***ErrDoc*** that can detect, categorize all classes of error handling bugs, and automatically fixes them. They also proposed an algorithm called ***patch generation algorithm*** ,that generates patches for fixing different types of bugs. Due to the large number of error handling bugs, researchers decided to detect them automatically. To understand more clearly the nature of the bugs, researchers conducted a comprehensive study of real world error handling bugs and their fixes. They mentioned that error handling bugs are due to Incorrect/Missing Error Checks, Incorrect/Missing Error Propagation, Incorrect/Missing Error Outputs and Incorrect/Missing Resource Release. Based on the study conducted, they designed, implemented and evaluated ***ErrDoc*** that automatically detects, diagnoses and fixes error handling bugs. ErrDoc first identifies all the error paths. If a function call fails and returns an error, then that error needs to be handled properly along the error path, otherwise ErrDoc reports a bug. ErrDoc uses a static analysis techniques to examine whether the failing function call is handled or not. ErrDoc also indicates that on releasing all the allocated resources, program can fail.

Evaluation:

The evaluation was done on five open-source projects in which ErrDoc can detect handling bugs with high accuracy of 100% to 84% precision and around 95% recall. To give developers more information about the main causes of the bugs , ErrDoc categorizes these bugs with 83% to 96% precision and above 90% recall. The patch generation algorithm not only fixes the bugs but also combine them in to the existing error handling code. Overall, bug fixing phase generates acceptable patches with 72% to 84% precision.

Analysis:

Good Point: In this paper, the tool ErrDoc not only detects error handling bugs but also automatically fixes them , which reduces the overhead for the developers and makes the system more secure and reliable.

Bad Point: The evaluation of the tool ***ErrDoc*** is done only on five open-source projects, in which their results are not generalized. The evaluation could have done considering different types of datasets across all the projects.

Potential Project: This project can be extended to examine the most common error handling bugs and can also extend to inspect error handling performance for other programming languages.

Questions:

1) How efficiently ***ErrDoc*** detects error handling bugs for large real world programs ?

2) Does ***ErrDoc*** in turn finds any other new errors internally when identifying and fixing the existing error handling bugs?