Automated Detection, Localization and Removal of Information Exposure Errors

M.Sc. thesis problem statement

Goal of the master thesis is to develop a quick fix generation tool for information exposure bugs. Based on the available information exposure checker which detects bugs in the open source Juliet test cases: CWE-526, CWE-534 and CWE-535 a new quick fix tool for the removal of these bugs should be developed. The bug location and the bug fix location can can be different (code lines) in a buggy program. Thus, the student will develop a bug quick fix localization algorithm based on software bug fix localization techniques which helps to determine the code location where the quick fix should be inserted. Based on the bug location the developed algorithm should indicate where the quick fix should be inserted in the program.

We can consider a valid bug fix the removal of the confidential parameter inside a function call to a system trust boundary. In case there are other solutions these have to be addressed as well. After the quick fix location was determined and the format of the quick fix was chosen than the quick fix will be inserted in the program with the help of the Eclipse CDT/LTK API.

The validity of the fix should be checked by re-running the information flow checker. In case the checker detects no bug than the quick fix will be considered valid.

Requirements

Good Java skills, Eclipse CDT/LTK, Secure information flow propagation knowledge is an advantage

Contact

M.Sc. Paul Muntean,
E-Mail: paul@sec.in.tum.de,
Tel.: (089) 289-18566,
Tender date: March 18, 2015,
Beginning: 01.04.2015