Title:
Empirical Study of Interprocedural Data Flow(IDF) Patterns for Memory Leak Analysis in Linux

Abstract:

Analysis of inter-procedural data flow (IDF) is a commonly encountered challenge for verifying safety and security properties of large software. In order to address this challenge, a pragmatic approach is to identify IDF patterns that are known to occur in practice, and develop algorithms to detect and handle those patterns correctly. We perform an empirical study to gather the IDF patterns in Linux, which is essential to support such a pragmatic approach.

In our study, we first analysed the Linux code to study how reference to dynamically allocated memory in a function flows out of the function. We analysed 838 instances of memory allocation and identified 6 IDF patterns. Second, we mined and analysed 1200 memory leak bug fixes from the Linux git repository. Third, we surveyed the literature for static analysis tools that can detect memory leaks. Based on these studies, we found that the set of IDF patterns associated with the memory leak bug fixes in Linux and those that can be detected by the current static analysis tools is a subset of the 6 IDF patterns we identified.

Keywords
Program Analysis
Inter-procedural Data Flow
Linux